CAHIERS DE LA SÉCURITÉ

n°6

La criminalité numérique

Mafias, pédophilie, fraudes, sectes, rumeurs, jihad, propagande, terrorisme, cyberdéfense, normes...

Également dans ce numéro :

La chaîne hiérarchique du ministère public

Le compte-rendu des XV^e Journées européennes des représentants de l'État

INHES
INSTITUT NATIONAL DES HAUTES ETUDES DE SECURITE

octobre-décembre 2008

CAHIERS DE LA SÉCURITÉ
n°6

La criminalité numérique

INHES
INSTITUT NATIONAL DES HAUTES ETUDES DE SECURITE

octobre - décembre 2008

CAHIERS DE LA SÉCURITÉ

INSTITUT NATIONAL DES HAUTES ETUDES DE SECURITE

Directeur de la publication : Pierre MONZANI

Publicité et communication : Corinne FAYOLLE – corinne.fayolle@interieur.gouv.fr

Conception graphique et fabrication : Daniel VIZET, Laetitia BÉGOT

Ventes et abonnements : La documentation Française – 29-31, quai Voltaire – 75344 Paris Cedex 07 – Tél. : 01 40 15 70 00 – Télex : 204 826 DOCFRAN Paris

Par correspondance – La documentation française, 124, rue Henri-Barbusse, 93308 Aubervilliers Cedex – www.ladocumentationfrancaise.fr

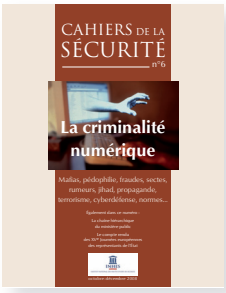
Tarifs : Prix de vente au numéro : 18,90 € – Abonnement France (4 numéros) : 60,50 € – Abonnement Europe (4 numéros) : 63 €
Abonnement DOM-TOM-CTOM : 66,10 € (HT, avion éco) – Abonnement hors Europe (HT, avion éco) : 69,20 €

Conditions de publication : Les Cahiers de la sécurité publient des articles, des comptes rendus de colloques ou de séminaires et des notes bibliographiques relatifs aux différents aspects nationaux et comparés de la sécurité et de ses acteurs. Les offres de contribution sont à proposer à la rédaction pour évaluation. Les manuscrits soumis ne sont pas retournés à leurs auteurs. Toute correspondance est à adresser à l'INHES à la rédaction de la revue. Tél. : 01 55 84 53 74 – Fax : 01 55 84 54 26 – cs.inhes@interieur.gouv.fr

www.cahiersdelasecurite.fr — www.inhes.interieur.gouv.fr

Cahiers de la sécurité

CAHIERS DE LA SÉCURITÉ



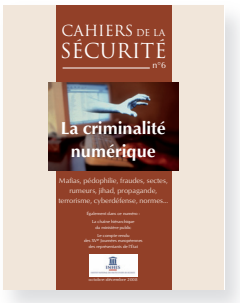
SOMMAIRE

n°6
octobre-décembre 2008

INHES
INSTITUT NATIONAL
DES HAUTES ETUDES
DE SECURITE

"Les Borromées"
3 avenue du Stade de France
93218 Saint-Denis-La-Plaine cedex
Tél. 01.55.84.53.00
Fax. 01.55.84.54.26
www.inhes.interieur.gouv.fr

CAHIERS DE LA SÉCURITÉ



SOMMAIRE

n°6
octobre-décembre 2008

Économie/Gestion de crise

Vie des organisations

Notes de lecture

Événements

INHES
INSTITUT NATIONAL DES HAUTES ETUDES DE SECURITE

"Les Borromées"
3 avenue du Stade de France
93218 Saint-Denis-La-Plaine cedex
Tél. 01.55.84.53.00
Fax. 01.55.84.54.26
www.inhes.interieur.gouv.fr

Poursuivant ses investigations sur les nouveaux champs de la sécurité, notre revue vous propose un voyage à travers les paysages, que l'on pourrait croire fantaisistes, mais qui sont bien actuels, de la criminalité numérique.

Une décennie plus tôt, ce numéro aurait été œuvre de science-fiction, c'est aujourd'hui une recherche éminemment contemporaine.

La cybercriminalité inscrit dans la troisième dimension virtuelle les invariants du crime et du vice. Les motivations malveillantes sont inchangées – abuser de la naïveté, déstabiliser les démocraties, exploiter les êtres humains et notamment les plus faibles... – mais elles trouvent une ampleur nouvelle qui aggrave les dangers du terrorisme, de la délinquance financière ou de la pédophilie.

Cette nouvelle dimension du crime souligne cruellement nos vulnérabilités, tant individuelles que collectives, et l'urgence d'une réponse adaptée des pouvoirs publics, tant nationaux qu'européens. C'est tout le sens de la politique de modernisation de nos forces de sécurité qui est au cœur de l'action de Michèle Alliot-Marie, c'est toute l'ambition de l'évolution rapide et prometteuse de notre administration voulue par le président de la République.

Comme toujours, cette volonté politique, que traduit la prochaine LOPPSI – loi d'orientation et de programmation de la performance pour la sécurité intérieure – doit s'accompagner d'une mobilisation civique et culturelle pour que nos concitoyens, qui profitent légitimement des progrès technologiques, soient armés pratiquement, juridiquement et moralement contre leurs inévitables dérives.

Dans ce cyber-territoire sans frontière, c'est encore et toujours le citoyen éclairé qui est le plus efficace serviteur du droit et de l'honnêteté. C'est, nos lecteurs le savent, l'ambition humaniste qui nous guide.

Pierre MONZANI

Cybercriminalité : un univers sans territoire

Ce numéro consacré à la cybercriminalité nous propose plusieurs réflexions. Nous l'avons conçu sans parti pris. Son ultime but, comme pour chaque numéro des cahiers de la sécurité intérieure, est de susciter la réflexion et le débat. Bien sûr, nous n'avons pas tout abordé, nous avons parfois évoqué rapidement un sujet, et, au contraire, avons proposé à d'autres reprises plusieurs points de vue. Le lecteur découvrira ici des aperçus forts divers.

Nous sommes vulnérables rappelle le sénateur Roger Romani. Des pays ont déjà été victimes d'attaques, une réflexion sur le dispositif national s'impose. Face à un État vulnérable et à des citoyens menacés, Frédéric Malon évoque les enfants victimes de la cyberpédopornographie, une menace qu'il faut traiter avec des moyens divers et qui doivent s'adapter aux évolutions sociétales.

Noël Pons présente Internet comme une cour des miracles où règnent combines et corruption que charlatans et sectes sauront utiliser à leur fin selon Henri-Pierre Debord. Lieu de chasse privilégié où des passants peu prudents croiseront ceux dont le désarroi surpasse l'envie de quête, Internet est aussi un lieu de rumeurs et de désinformation que décrit Franck Bulinge. Walter Akmouche et Henri Hemery abordent spécifiquement la propagande jihadiste démontrant qu'Internet devient une arme redoutable. Laurence Ifrah présente un panorama des nouvelles menaces criminelles numériques que complétera Michel Riguidel, remettant en question quelques dogmes en sécurité numérique.

En matière de surveillance, Jean-Marc Zuccolini évoque la supervision du trafic internet à destination du CEA. Didier Duval présente la plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements « PHAROS », au sein de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), dont le renforcement fait partie du plan présenté par Madame Alliot-Marie, ministre de l'Intérieur, de l'Outre-mer et des Collectivités territoriales. Christian Aghroum insiste sur la nécessaire coopération européenne. Il souligne l'importance de la création, en 2004, de l'agence européenne chargée de la sécurité des réseaux et de l'information. Il rappelle le plan ambitieux présenté par Madame Michèle Alliot-Marie, faisant largement écho aux préconisations des rapports Lasbordes et Romani que Serge Perrine passe en revue.

Stanilas de Maupeou souligne que les attaques informatiques sont classées dans le Livre blanc sur la Défense et la Sécurité nationale parmi les menaces les plus élevées sur notre société. La création d'une agence de la sécurité des systèmes d'information, rattachée au futur Secrétariat général de la Défense et de la Sécurité nationale - SGDSN – a été décidée afin de mieux répondre à ces enjeux. Gageons donc que cette agence travaillera activement avec les structures européennes et les pays émergents. Se pose aussi l'adaptation de notre droit et des outils juridiques. Yves Charpenel soutient que la complexité et la spécificité du droit pénal de l'Internet passé au filtre de la chambre criminelle n'ont pas fragilisé l'édifice mis en place sous l'ombre de la Cour européenne des droits de l'homme pour prévenir les dérives du cybermonde. Notre droit offre encore à l'institution judiciaire pénale les moyens d'une riposte grâce à un arsenal juridique qu'évoque aussi Daniel Martin. La cybercriminalité peut toucher les infrastructures vitales de la nation (transports, énergie...) comme l'a souligné le sénateur Romani.

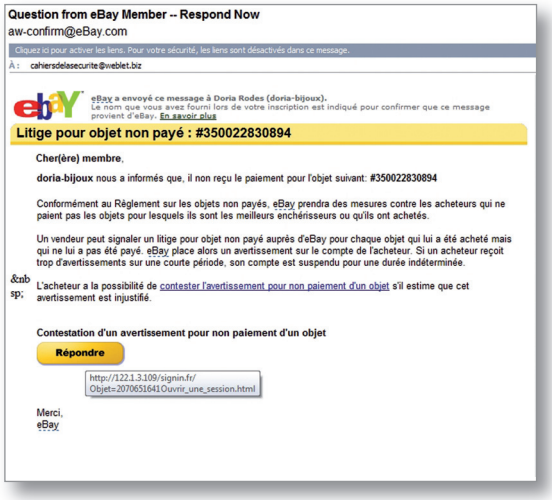
Dans un tout autre registre, Walter Schön se propose de mettre en perspective pour les systèmes dits « critiques » les problématiques de résistance à la cybercriminalité, et de faculté à éviter des comportements catastrophiques dont l'origine peut être technique, environnementale voire humaine. Ainsi, la conception des systèmes doit être globale. C'est ce que nous mentionnons dans le chapitre consacré à la normalisation. Cette dernière est prépondérante et devient le bras armé de toutes les technologies. Dans ce cyber-paysage la dimension humaine est omniprésente, selon le témoignage de Daniel Martin. Il présente les motivations et le profil des cybercriminels et de leurs victimes, ce que Myriam Quéméner complète à travers sa typologie des cyberfraudes dans le domaine financier.

Après ces quelques mots de présentation, je vous laisse donc le soin de découvrir la réflexion souvent passionnée de nos auteurs. Mais permettez-moi de conclure sur une question soulevée par Michel Riguidel, évoquant dans son article la perte de souveraineté. Il n'y a pas, paraît-il, d'État sans territoire. Que devient ainsi la notion de territoire géographique et donc d'État dans ce monde de la virtualité ? Curieusement, ce cyber-espace recrée ses propres « règles », ses propres féodalités, de sorte que l'on a peine à imaginer à terme les formes de pouvoirs dans ce monde virtuel. Viendront-ils à remettre en cause la notion d'État. Quel sens donner à la citoyenneté sur le Net ? Comment bâtir des règles dans un univers sans territoire ?

Jean Marc PICARD

Le Web et les organisations mafieuses : *mythes et réalités*

Patrice HERNU


Question from eBay Member -- Respond Now
aw-confirm@eBay.com
Cliquez ici pour activer les liens. Pour votre sécurité, les liens sont désactivés dans ce message.
A: cahiersdelasecurite@weblet.biz
eBay a envoyé ce message à Doria Rodes (doria-bijoux).
Le nom que vous avez fourni lors de votre inscription est indiqué pour confirmer que ce message provient d'eBay. En savoir plus
Litige pour objet non payé : #350022830894
Cher(ère) membre,
doria-bijoux nous a informés que, il non reçu le paiement pour l'objet suivant: #350022830894
Conformément au Règlement sur les objets non payés, eBay prendra des mesures contre les acheteurs qui ne paient pas les objets pour lesquels ils sont les meilleurs enchérisseurs ou qu'ils ont achetés.
Un vendeur peut signaler un litige pour objet non payé auprès d'eBay pour chaque objet qui lui a été acheté mais qui ne lui a pas été payé. eBay place alors un avertissement sur le compte de l'acheteur. Si un acheteur reçoit trop d'avertissements sur une courte période, son compte est suspendu pour une durée indéterminée.
  L'acheteur a la possibilité de contester l'avertissement pour non paiement d'un objet s'il estime que cet avertissement est injustifié.
Contestation d'un avertissement pour non paiement d'un objet
Répondre
http://122.1.3.109/signin.fr/Objet=2070651641Ouvrir_une_session.html
Merci,
eBay

Avant que les cybercriminels ne mettent en danger la sécurité de l'État et des entreprises, ceux qui pénétraient les systèmes d'exploitation des premiers ordinateurs étaient simplement des passionnés, supplantés désormais par des réseaux organisés, aux conduites aussi criminelles que celles des mafias. Paradoxalement, alors que les systèmes étaient vulnérables, ils n'étaient attaqués qu'en surface. Maintenant que la sécurité est renforcée, que les lignes de codes se sont sophistiquées, ils sont rendus plus fragiles par l'effet combiné de la complexification et de la vulgarisation des pratiques qui n'échappent donc plus à la criminalité ordinaire et nécessitent une réaction de l'État et de la société.

The Web and the Mafia: Myths and Realities

Before cybercriminals started to exploit the net, the first hackers who threatened state security were those who engaged in the activity for excitement and fame. They have now been replaced by organized crime and mafias. Paradoxically, in the past when systems were most vulnerable, they were only attacked on the surface. Now that their security has been reinforced and defenses are more sophisticated, they have become more fragile under the combined effects of the increased complexity of the instruments used for attacks and their general public diffusion. We have gone beyond the menace of common criminality and entered an era that requires better responses in order protect the state and society.

Patrice Hernu

Économiste de formation, il est diplômé de l'École nationale de la statistique et de l'administration économique (ENSAE). Il est titulaire d'un doctorat d'économie appliquée, d'un doctorat de mathématiques appliquées à la gestion des entreprises et d'un diplôme d'expert fiscal (ENI). Il commence sa carrière à l'Institut national de la statistique et des études économiques (INSEE) en tant qu'administrateur, puis devient sous-directeur du service d'études statistiques et des systèmes d'informations (Sesi) au ministère de la Santé. Depuis 2001, il est conseiller scientifique du ministère de l'Écologie et du Développement durable. Il est également, depuis 2007, conseiller du directeur de l'Inhes.

Snobisme et effet de mode s'étaient conjugués pour inciter à vanter les prouesses de tel ou tel pirate sur la toile : le plus souvent, les mérites de ces nouveaux David du cyberespace sont imaginaires. Le fait est que les supposés Goliath des temps modernes, les grandes entreprises comme les organisations gouvernementales ou non gouvernementales et les bureaucraties dont la culture de sécurité reste le plus souvent obsolète, sont des colosses aux pieds d'argile. Les murailles et les remparts ne tiennent que dans la mesure où la communauté qui les habite se défend de donner les clefs des portes dérobées aux robins des bois, par inadvertance, intérêt, bêtise, perversité ou oisiveté. Tout cela est plus affaire de culture et d'éducation que de hauteur des barricades érigées. Une société libre, comme le prétend être celle du réseau global, ne peut être une société de barrières, de quarantaines et de trousseaux de clefs de protection numérique démultipliés à l'envi.

Oui mais... la criminalité et la délinquance sur l'Internet se développent au rythme de ses interconnexions. Et, les petits génies obscurs en quête d'une célébrité dans la communauté de ceux qui « sont dans le coup de la société moderne » ont laissé la place à de vrais cybercriminels, puis à des organisations de type mafieux, quand leur naïveté généreuse ne les a pas conduits à être totalement instrumentalisés par ces mafias d'un nouveau genre.

Le ministère de l'Intérieur, à l'initiative de la ministre Michèle Alliot-Marie, a intégré le constat, parfois alarmant, de cette évolution et prend les dispositions nécessaires pour tenter, à notre échelle, d'endiguer le phénomène. Évidemment, pour ne pas laisser l'imagination criminelle distancer ceux dont la mission est de nous protéger, tandis que la bataille se joue sur un terrain qui précisément échappe aux contours de l'État traditionnel, il faut se donner les moyens de lutter « à armes égales ». C'est la volonté affichée par la ministre en présentant en février 2008 son plan de lutte contre la cybercriminalité (*cf.* son plan en encadré)

Le temps des pionniers de légende

Quand le temps est venu de raconter l'époque des pionniers, la légende est déjà en marche et le péché originel se mélange tant au plaisir qu'à la grandeur d'âme. Dans une civilisation où l'on cherche à construire en toute chose l'idéal du bien et du mal, ce mélange est de bon aloi. La société de l'Internet n'y échappe pas. Puis, vient le temps où il faut mettre à bas les idées reçues. Le *Far West* n'était pas si grandiose et les hommes pas si différents... Le spam, ce fléau qui consiste à inonder un destinataire de courriels qu'il n'a pas sollicités parce que son adresse a été récupérée par un moyen licite ou illicite, aurait pu fêter ses trente ans en mai dernier. « Spam », ne veut rien dire ou presque [1]! En ce mois de mai 1978, un cadre de la société DEC adresse 400 ou 600 [2] messages sur le réseau Arpanet [3] pour vanter les mérites de nouveaux produits. La réaction fut vive en paroles dès cette première et tout le problème et les risques étaient déjà posés par le major Raymond Czahor, responsable de l'Arpanet. Mais, l'impuissance de l'individu réel face à la société des séries virtuelles apparaît aussitôt. Ce sont les Monthy Python qui comprennent immédiatement le parti pris comique et la réalité de la situation. Ils reprennent, en fait, le sketch de Fernand Raynaud sur la société obsessionnelle de consommation et ses « deux croissants ». Mais, tout s'est inversé et c'est désormais l'offreur qui va créer l'obsession sérielle avant que maintenant, au bout de la chaîne, chacun s'imagine être source. Tandis qu'un couple tente de prendre un petit-déjeuner à la manière de Raynaud, la patronne ne propose en réponse que des plats à base de « spam, spam, spam, spam ». C'est la répétition qui guette la défaillance du gogo, qui guette cet instant où une porte va s'ouvrir et où va s'engouffrer votre ami ou votre ennemi... La mécanique du spam actuel et de tous les zombies qui le servent est née. Elle est encore loin d'être criminelle [4]!

....

(1) En fait, le terme est apparu en 1937 pour désigner du Jambon épicé en boîte (SPiced hAM) et, de ce fait, c'est une marque créée et déposée par Hormel Foods cette année-là ! Ce « pâté » a été largement utilisé par l'intendance des forces armées US pour la nourriture des soldats. Le copyright date de 1944. Il s'agit de la première émergence publique du mot pour désigner un objet repoussant dont on aimerait bien ne pas être le destinataire.

(2) On ne sait déjà plus très bien !

(3) Un réseau professionnel précurseur de l'Internet qui n'aurait dû être utilisé que pour diffuser des informations officielles du gouvernement américain.

(4) Nous n'abordons pas dans cet article certaines activités criminelles exercées via Internet, comme les réseaux pédophiles ou le « squam » (activité apparentée au spam où des émetteurs cherchent à extorquer de l'argent en faisant vibrer les bons sentiments). Dans cette activité, Internet ne sert qu'à accélérer la communication, et les spams ne font que reprendre des techniques vieilles comme le monde auxquelles le courrier postal suffisait auparavant. Nous nous intéressons aux activités criminelles pouvant donner lieu à constitution ou pérennisation d'organisations à orientation mafieuse.

Certes, tout avait déjà été imaginé dans des œuvres de fiction [5] qui ont formaté notre imaginaire et conduit les hackers [6] en herbe à reproduire une forme d'idéal transgressif ou à simuler ces exploits. Les faux exploits jalonnent l'histoire des hackers. Ainsi, le casse virtuel du siècle qu'a failli réussir un jeune russe en 1994. Après avoir fait virer près de onze millions de dollars sur différents comptes à partir de la Citibank, il se révèle incapable de réaliser le mouvement des fonds extorqués ; ses complices sont arrêtés comme lui-même, dans un second temps, à Londres, où il tentait de récupérer une part des fonds. En fait, il avait dû acheter pour 100 $ une « Back Door » du système et avait, comme bien des princes des hackers, voulu s'offrir un peu de gloire éphémère avec l'appât du gain qui n'est rien sans un peu de reconnaissance... La morale est sauve ! Après trois années de prison, bien qu'il ait été un des plus célèbres des génies obscurs, il n'est plus dans la légende vivante. Les vrais surdoués ne l'ont pas fait savoir et sont soit du côté de la vertu affichée – ils dirigent des entreprises de pointe – soit du côté du crime, et l'histoire réelle montre qu'il n'est en réalité pas utile d'être surdoué !

L'histoire véritable de l'industrie du virus est donc une autre histoire. Le premier virus connu, capable d'infecter un ordinateur personnel date de 1982. Destiné à l'Apple II, il se contente d'écrire un poème sur l'écran. Autorépliquant, donc authentiquement viral, il donne des idées, d'abord aux universitaires qui vont immédiatement théoriser le principe et fournir un mode d'emploi à tous les apprentis. En 1986, deux Pakistanais, amateurs sans savoir-faire supérieur à celui de milliers de jeunes informaticiens en herbe, appliquent le manuel et créent le premier virus à succès pour l'IBM PC, « Brain », lequel sera copié, recopié et adapté. Le virus se contentait d'afficher la publicité pour le magasin que tenaient les frères Alvid à Lahore au Pakistan. Mais, faute d'obstacle, le virus fait le tour du monde et provoque une panique. Alors que le monde n'a connu que deux virus principaux, le mythe du cataclysme numérique emporte tout. La presse titre : « Débranchez vos ordinateurs pour éviter la fin du monde ! »

John McAfee imagine alors le profit qu'il peut tirer de cette panique et fait créer [7] le premier antivirus. Dans la foulée, apparaît Norton Antivirus [8]. Cette agitation suscite l'engouement d'autres gamins qui veulent déjouer non pas les machines - jeu d'enfant à cette époque - mais les antivirus ! De plus, ces virus se transmettaient par les disquettes et non par les réseaux, de sorte que leur réputation, celle qui persiste, tout comme les antivirus, a bel et bien précédé la réalité de leur apparition.

Les virus - au sens commun actuel - sont donc en réalité relativement récents. Ils ont été pensés, imaginés et, fait surprenant, combattus avant qu'ils ne se présentent comme des menaces réelles. En 1988, un étudiant en informatique lâche un virus autorépliquant sur l'Internet universitaire. Gros dégâts. Nouveaux progrès des antivirus qui se déportent du secteur d'amorçage des disques [9] vers les fichiers qui exécutent des programmes. Cela donne l'idée, en 1991, à un étudiant de Jérusalem de mettre au point un virus qui dort avec le fichier et le supprime s'il est exécuté un « vendredi 13 » !

Le côté magique de la date n'est pas innocent. Mais, si les antivirus et la menace virale échauffent les esprits dans les universités, spécialement américaines avec un arrière-plan de théorie du complot, le bon peuple tarde à réagir et se contente de fermer le PC les vendredi 13. Assez curieusement, apparaît alors le fameux virus Michelangelo. Oui, Michel-Ange ! Aucun rapport ? Si. Sa date de naissance est en 1992, comme chaque année, le 6 mars. Mais, en 1992, c'est une semaine avant un fameux « vendredi 13 ». Et ce virus est censé effacer les cent premiers secteurs du disque dur et le rendre ainsi inutilisable si le fichier infecté s'exécute le... 6 mars sans être protégé par le fameux antivirus McAfee. Ne tirons aucune conclusion hâtive, mais John McAfee passe en boucle à la télévision pour annoncer que, faute d'antivirus, jusqu'à cinq millions de machine pourraient être infectées. En fait, ni McAfee ni Norton ne purent montrer à la presse le moindre PC infecté par le virus le 6 mars, sauf celui qu'ils avaient infecté eux-mêmes avec une souche dont personne n'eut l'outrecuidance de leur demander où ils l'avaient trouvée.

Bref, nous voilà en 1995, et dès que Windows tombe en panne, « c'est la faute au virus ». Il faut comprendre

....

(5) Le principe du virus informatique serait apparu dans un roman de John Brunner, *Sur l'onde de Choc* (1975). Il évoque les mécanismes grâce auxquels des programmes seraient capables de passer d'un ordinateur à l'autre sans repérage possible. En fait, il a généralisé le principe d'un premier « ver », le « ver Creeper », capable de se répandre sur un réseau, apparu en 1971.

(6) « Hacker » signifie en anglais *bricoleur, bidouilleur* ; il désigne aujourd'hui le détenteur d'une maîtrise technique et vaguement magique lui permettant de détourner ou de contourner un processus numérique pour accéder à des informations ou pour les modifier. Comme la programmation sur Internet se fait par couches successives (couches métiers, couches soft, couches langages, couches d'interface avec le hardware, etc.), il y a donc autant de type et de niveau de « Hacker » qu'il y a de niveaux de programmation et d'objet informatique.

(7) Par Dave Chambers, un jeune de 19 ans, passionné certes...

(8) Écrit par le même Dave Chambers débauché par Peter Norton.

(9) Dit secteur de « boot ». « Donner un coup de pied » pour faire démarrer.

que le virus n'a d'intérêt que s'il sert une activité mafieuse, criminelle ou commerciale - situations très différentes - et que, tant que cet intérêt n'est pas objectivé, il reste, pour l'essentiel, un mythe, réel, éventuellement destructeur, mais qui n'a pas les caractéristiques cataclysmiques qui lui sont prêtées. Or, ces premiers virus ne servent en réalité à rien qu'à faire du bruit, c'est-à-dire à faire parler d'eux-mêmes ou de leur supposé auteur.

Avec l'apparition du Pentium qui interdit de lui-même l'opérabilité de certains virus, les grands éditeurs veulent se dégager de ce secteur... qui n'a plus très bonne réputation. Les virus, ce serait fini ! Mais, en fait, c'est à cet instant que commence la vraie histoire des virus, celle que la légende avait prédite, mais que ni les éditeurs ni les universitaires en mal de notoriété n'avaient réalisée.

Apparaît, en effet, en Bulgarie, le premier virus capable de générer son propre cryptage, et se présentant avec une signature auto-flexible, donc non repérable par les antivirus antérieurs. Il n'a certes d'autre but que d'assurer la promotion des paroles et citations d'Iron Maiden [10]. Cela allait entraîner une nouvelle mutation de ce secteur, d'autant que d'après l'aveu même de David Perry [11], avec la version d'essai de Windows 95, Microsoft avait livré elle-même aux éditeurs d'antivirus le premier virus de macro au monde [12]. De fait, de 1995 à 1999, les entreprises sont visées par ces virus de macro, notamment par ceux qui vont arriver via le réseau et le truchement d'Outlook.

De 1995 à 1999, c'est la naissance et la mort des virus traditionnels. Les hackers n'étaient que de gentils garçons. Ceux qui ont écrit ces virus continuent de travailler, les plus doués pour de grandes maisons. Les hackers se réunissent en congrès et sont passés - pas toujours - du bon côté de la force. Les autres, ceux de la « dark side » se sont mis au service d'organisations mafieuses menées par des criminels. Car, faire un virus n'est plus un art. C'est devenu une industrie. Une question de patience. C'est à la portée de tout informaticien. Un virus a son prix proportionné non pas aux dégâts qu'il peut engendrer, mais aux bénéfices qu'il peut générer pour ceux qui les utilisent. La première attaque Web massive n'a eu lieu que l'année dernière par l'intermédiaire d'un malware acheté à la mafia russe.

Dans notre histoire, nous avions la réalité, les grandes épopées antiques puis la légende, le mythe. En matière de virus, nous avons eu la légende, le mythe, nous entrons maintenant, et maintenant seulement, dans la réalité. Elle nous vient du monde virtuel. Pénétrons sa réalité, celle de la cybercriminalité.

La cybercriminalité, une réalité à combattre

Les bidouilleurs voulaient s'amuser, se faire une publicité à bon compte. Quelques-uns, plus pervers, voulaient détruire votre disque dur, vos données... Mais, c'était l'exception, sauf si ce type de virus était intentionnellement envoyé dans le cadre d'une attaque personnelle. Faites le compte : détruire des données ne fait que la fortune des éditeurs d'antivirus. À moins qu'il ne faille faire mal quelque part pour que chacun songe à se protéger de menaces qui ne nous concerneraient que modérément sinon : le pillage de nos données et non leur destruction, la surveillance de nos relations, la collecte des adresses de nos amis, etc.

Bref, tout comme la biodiversité et le processus de sélection naturelle conduisent à élaborer une société où la lutte aboutit à instaurer des processus d'équilibre, la diversité des virus - il pourrait en naître des milliers chaque jour - conduit à un processus de sélection où le problème n'est plus de les produire, mais de les mettre en état de servir des finalités.

Pour ce qui concerne les finalités criminelles, il faut donc distinguer le cyber-terrorisme dont le but peut être de détruire ponctuellement et la cybercriminalité avide des profits réalisables par le commerce illicite ou l'extorsion d'identité. Mais l'une et l'autre, dans cette nouvelle ère qui a commencé il y a environ deux ou trois ans, ont tout intérêt à ce que l'Internet, « ça marche ». Les criminels n'ont pas intérêt à détruire ni importuner, mais plutôt à « endormir », ce qui explique la fabuleuse et extrême sophistication de l'activité frauduleuse sur l'Internet depuis les années 2000. Qui aurait intérêt à faire tomber en panne nos micros ? Même une attaque terroriste d'État ou non

....

(10) Iron Maiden est un groupe formé en 1975 au Royaume-Uni par le bassiste Steve Harris et son ami d'enfance Dave Murray. Ils furent les pionniers de ce qui fut appelé la NWOBHM (*New Wave Of British Heavy Metal*). Dans une filiation à message du style Punk, il évolue dans une mythologie baroque et virtuelle qui va de la Bible aux grandes figures de l'histoire.

(11) David Perry était un salarié de Norton dans les années 1990. Il est aujourd'hui directeur global pour l'éducation chez l'éditeur d'antivirus Trend Micro. Certains éléments de cet article sont attestés par une interview qu'il a accordée à SVM (*Sciences & Vie Magazine*) sur l'histoire de la sécurité informatique.

(12) « Word Concept Macrovirus », en clair le mode d'emploi pour fabriquer un virus s'infiltrant par le logiciel Word. Écrit par un « salarié inconnu », un bon soldat à moins que ce ne soit par le patron lui-même, il affichait sans détruire : « Cela prouve que je suis ce que je dis ». Il ne restait plus aux éditeurs qu'à attendre pour dire à leur tour : « Je panse, donc je suis » !

gouvernementale a intérêt à se tapir, à se préparer, puis à frapper d'un coup comme pour le 11 septembre. C'est le regain de confiance qui constitue une menace tandis que les risques, en fait, se multiplient.

Les escrocs opèrent sur un champ qui, apparemment, semble échapper au contrôle des États traditionnels. La Chine vient de nous montrer qu'en fait les moyens de contrôle existent et sont même négociables avec les grands pourvoyeurs (officiels) de contenu. Il demeure que la grande majorité des affaires traitées par les services *ad hoc* [13] présentent des ramifications extérieures au territoire national. Les instigateurs se retranchent derrière la multiplication des relais intermédiaires et l'évidente mauvaise volonté de certains États à engager une coopération judiciaire efficace.

La cybercriminalité professionnelle a « malheureusement » étouffé la production traditionnelle des programmes malicieux. Certaines équipes se sont spécialisées dans la production des outils. D'autres assemblent ces outils pour les mettre au service d'autres équipes qui les achètent et les confient enfin aux cyber-hommes de main, lesquels vont gérer l'infrastructure mafieuse mise en place. Architectes, techniciens, ingénieurs, donneurs d'ordre, parrains et complices mafieux constituent un réseau global où chacun ignore l'autre maillon, comme dans les organisations mafieuses traditionnelles, mais ici, sans que cela ne résulte forcément d'une volonté organisatrice, mais de la seule inertie organisationnelle de l'internet. D'où le danger et la démultiplication du modèle depuis que la volonté criminelle fait corps avec l'organisation du réseau.

Une cellule produit le virus, une autre l'armera comme cheval de Troie capable de pénétrer un système local, une autre encore concevra l'architecture du système en assignant des tâches différenciées à ces Troyens. Prenons le cas du « phishing » [14] au stade industriel (Russie, Chine, Inde). Il nécessite certes des intrusions parfois violentes dans certaines machines locales pour les transformer en « zombies » intégrés dans un réseau afin de les utiliser pour relayer les envois de spams et l'hameçonnage final qui caractérise le phishing [15]. Cela permet d'étendre de manière virale la surface du réseau, de masquer les vrais opérateurs et de l'utiliser comme moyen de transmission. Mais, l'intérêt des opérateurs est de se faire aussi discret que possible pour pouvoir utiliser votre machine efficacement. De la même façon, quand le réseau passe à l'attaque en envoyant des liens comportant des hameçons, l'efficacité commande que les machines attaquées fonctionnent aussi bien que possible.

Aussi bien, n'est-il pas curieux que les virus destructeurs aient disparu au rythme auquel les vrais réseaux mafieux se sont eux-mêmes développés ? Question éminemment gênante. Elle explique que la France, notamment, ait décidé de se doter d'une véritable politique offensive en la matière (*cf.* encadré), car un corps qui ne sait plus, par le mal qu'il ressent, qu'il est attaqué, est d'autant plus vulnérable. Un Internet de ouate est évidemment un Internet de tous les dangers surtout avec la démocratisation et le manque d'éducation des usagers sur la forme des menaces.

À l'origine, c'est le virus « Storm Worm » diffusé par voie d'e-mail qui a investi jusqu'à quelques millions [16] de systèmes informatiques. Le Storm botnet a été identifié vers Janvier 2007 [17]. Le Storm botnet a été utilisé dans diverses activités criminelles. Ses contrôleurs, et les créateurs du Storm Worm, n'ont pas encore été identifiés [18].

••••

(13) Police et gendarmerie.

(14) Le phishing recouvre l'ensemble des techniques qui consiste à se faire passer pour un tiers de confiance (site, message, etc.) de manière à obtenir de vous des informations qu'il est possible de rentabiliser financièrement (vol de coordonnées bancaires par exemple). Voir plus loin.

(15) Votre micro-ordinateur est-il intégré sans que vous le sachiez dans un réseau, un « BotNet », de machines zombies ? Un outil gratuit à ce jour vous permet assez aisément de le vérifier : RUBooted. Vous pouvez le télécharger sur www.trendsecure.com. Sans danger ! Ce programme, après détection, est capable d'éliminer la plupart des logiciels malveillants (actuels) qui tournent sur votre machine pour le compte d'un réseau tiers. À l'origine, un botnet est un ensemble de robots IRC qui sont reliés entre eux.

(16) Les estimations varient de 1 à 50 millions de machines. Certains réseaux de la mafia russe auraient cumulé jusqu'à plus de 300 000 machines sous un seul contrôleur global.

(17) Le Storm worm représentait alors 8 % des logiciels malveillants sur les ordinateurs Microsoft Windows. Il ne constitue qu'une des menaces très actives en 2007.

(18) Comme bien des virus actuels, le virus Storm semble malgré tout d'origine russe. Il a sans doute été imaginé par la cybermafia considérée encore récemment comme la plus importante : le RBN ou « Russian Business Network » (petite réserve, car tous les spams viraux que j'ai personnellement reçus depuis un trimestre proviennent d'Inde et, particulièrement, d'un centre qu'il est aisé d'identifier sur *GoogleEarth*. Mais ils utilisent des outils d'origine russe). Le RBN a créé une suite logicielle, le MPack vendu à 1 000 $ aux impétrants qui veulent vendre leurs services aux criminels. Inutile de préciser que ces outils mettent leurs utilisateurs eux-mêmes sous un double contrôle. Ils sont en perpétuelle évolution. Un des derniers venus assure, par exemple, le cryptage de votre disque dur avec une clef inviolable de 1 024 bits. Pour récupérer les données, il faut payer, très cher, la clef et le logiciel de décryptage qui l'accompagne.

Ce virus a été particulièrement étudié. De manière plus inquiétante, il a fait preuve de comportements défensifs [19]. Le botnet a surtout attaqué des cibles spécifiques et notamment certains chercheurs qui tentaient de l'enrayer. Les opérateurs du botnet central ont de ce fait commencé à décentraliser leurs opérations, pour se protéger. Mais, du coup, les spécialistes pensent qu'ils ont vendu des portions du Storm botnet à d'autres opérateurs, et, notamment, à des réseaux mafieux chinois et/ou indiens. Le Storm botnet, traqué désormais par les antivirus nouvelle formule, est, sous cette forme, certes en déclin, mais plusieurs experts en sécurité considèrent que le botnet, dans son principe constitutif, demeure une menace majeure. Pour le FBI (États-Unis), le botnet est un risque majeur d'augmentation des fraudes bancaires, d'usurpation d'identité et de toute une kyrielle d'autres cybercrimes.

Des spécialistes font un autre calcul. À supposer que quatre millions de connexions ADSL standard puissent être instrumentalisées simultanément pour mener une attaque contre la sécurité globale d'un pays, cela représente un volume de bandes passantes plutôt inquiétant. De telles ressources, réparties autour du monde avec une présence significative dans de nombreux pays, signifient que ces réseaux pourraient mener des attaques réparties contre des hébergeurs internet ciblés et, partant, paralyser les données critiques d'un pays pendant un laps de temps suffisant pour distraire l'attention des pouvoirs publics, et laisser mener par d'autres des attaques d'un nouveau genre. Ainsi, seraient réunies les caractéristiques usuelles de la convergence entre terrorisme, mafia et luttes politico-ethno-environnementales qui se retrouvent dans la plupart des conflits extra-étatiques modernes. Ce danger ne peut être ignoré et, dans ce domaine comme dans d'autres, il apparaît que la notion même de sécurité globale appelle une convergence en miroir entre le souci de la sécurité intérieure qui s'intéresse surtout à la cyber criminalité et celui de la défense qui affronte la menace cyber-terroriste.

Au bout de la chaîne des robots mafieux, le phishing et ses dérivés

Les machines zombies, les virus qui instrumentalisent vos micro-ordinateurs pour pirater les adresses de vos connaissances, vérifier si vous avez des relations avec tel ou tel organisme où l'usurpation de votre identité pourrait être source de profit, dresser votre profil pour mieux vous séduire ensuite, tout cela ne fait que créer une opportunité de revenus, est illégal, mais n'est pas encore constitutif du crime (au sens pénal) perpétré par une organisation mafieuse, même si ces réseaux d'opportunité n'existent aujourd'hui à ce niveau que parce que des organisations mafieuses vont les utiliser. Les contrôleurs de ces réseaux d'opportunité, botnets, fichiers d'adresse comportant des millions d'adresses qualifiées [20] ou générateurs de sites simulés vont vendre tout ou partie des outils et systèmes à des réseaux mafieux.

Il y a dix ans, un employé peu scrupuleux vendait pour « dix fois rien » la clef d'une backdoor d'une grande entreprise, le fichier qualifié de ses clients ou le mot de passe administrateur du site à un hacker prétendu de génie. Les vrais hackings furent rares ! Le plus souvent, une once de délinquance servait de base au hacker dont l'activité était certes elle-même délictueuse. Aujourd'hui, le modèle est industriel, et les outils sont, de ce fait, rarement durablement secrets ! Il y a donc de la concurrence dans l'offre des malwares, et les tarifs d'achat par les réseaux mafieux sont hors de proportion avec les bénéfices qu'ils peuvent en tirer, s'ils les utilisent malicieusement.

Au bout de la chaîne, tout se termine donc par la visite sur un site ou l'envoi d'un e-mail où l'usager va être sollicité pour cliquer sur un lien ou une autorisation d'exécution d'un programme qui va se charger du braquage, du piratage des données quand ce n'est pas l'usager lui-même qui les livrera en pensant de bonne foi se trouver ailleurs que là où il est en fait. Plus besoin de virus tordus qui entrent par une porte dérobée pour exécuter une tâche complexe sur votre machine et renvoyer par le réseau,

....

(19) Sous l'action de ses contrôleurs. Si ces virus s'auto-répliquent, ils ne savent pas encore se défendre. Mais gageons que cela viendra. Il est désormais aisé d'imaginer par quels processus.

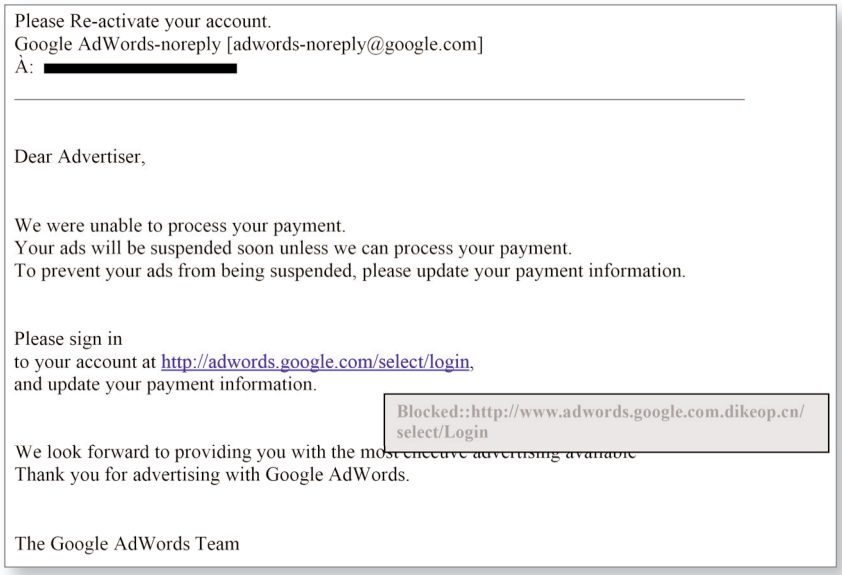
(20) Une adresse n'a vraiment d'intérêt que si elle est qualifiée par rapport à des usages criminels. « Qualifiée » signifie que lui sont attachées des informations pertinentes sur votre profil financier, sexuel, relationnel ou professionnel. Il existe de nombreuses entreprises qui expédient vos e-mails à des milliers de personnes, voire, en France, à deux ou trois millions de destinataires. Elles ont quasiment pignon sur rue et se présentent même comme des agents du respect de la Loi numérique. Envoyer un message publicitaire, légal ou illégal, sur un fichier non qualifié de deux millions d'adresse est à la portée du premier venu. La plupart de ce qu'il faut bien qualifier de spams (le spam commence dès qu'il y a usage d'un robot et ne se limite pas à un seul envoi à une adresse donnée) vont dans la boîte à courrier indésirable. Les programmes mis à disposition par les éditeurs (Microsoft pour Outlook, Thunderbird ou les outils de Firefox) sont relativement efficaces. Mais les grands fauves savent les contourner et leur harcèlement finit parfois par tromper les internautes.

dans votre dos, les informations au commanditaire du fric-frac. C'est l'internaute qui donne l'autorisation et qui ouvre la porte aux cambrioleurs.

La technique est apparemment simple au point que de plus en plus d'amateurs s'y frottent. Ils trouveront sans peine sur Internet un kit [21] leur permettant de jouer aux apprentis mafieux [22]. Quel intérêt pour les laboratoires qui distribuent à prix modique ces générateurs de spam-phishing ? D'abord, cela finance leurs innovations. Ensuite, cela sert de banc d'essai. Enfin, et surtout, cela jette le trouble sur la toile et renforce l'efficacité des vrais « spam-phishers ». En effet, les spams amateurs sont souvent imparfaits. Ils émanent d'une multitude d'individus isolés ne disposant que de quelques adresses IP d'émission, voire d'une seule, aisément repérables et que les salles de veille se préoccupent de suivre pour les fermer. Ces individus opèrent sur des serveurs mutualisés ; il est souvent impossible de fermer totalement ces derniers même si l'exploitant a fait preuve d'une trop grande tolérance. Le fameux « blacklistage » est parfois relativement inefficace, bien que nécessaire, et ne gêne le plus souvent que des contrevenants involontaires. Les vrais mafieux mettent au point des techniques beaucoup plus sophistiquées aptes à tromper réellement. La prolifération de phishings de basse qualité, aisément reconnaissables, contribue à faire passer les meilleurs. D'autant que la multiplication des barrières antivirus, anti-spam, anti-chevaux de Troie, anti-Botnet, anti-toute menace [23], conduit l'usager soit à déléguer à la machine le soin d'autoriser ou de refuser l'exécution des programmes importés (activeX et autres exécutables), soit à cliquer soi-même en série [24], et donc, à autoriser tel lien ou programme proposé par un hameçon qui aura les meilleures apparences... À ce stade, cela relève rarement de la prouesse numérique, mais plutôt du savoir-faire dans l'art de l'illusion.

Au plus haut niveau, les techniques peuvent être combinées et la prouesse technique jointe à l'artifice. Ainsi, certains réseaux ont réussi à insérer des pages de hameçonnage au sein même du site [25] que ces pages sont censées imiter. Concernant eBay et PayPal par exemple, l'imitation est « presque » parfaite. Tout est fait pour cacher l'identité réelle du domaine à l'œuvre. Si vous cliquez sur les liens, vous êtes automatiquement redirigé vers un exécutable qui, selon le rôle et l'intérêt que vous présentez, vous proposera soit un site à l'image du hameçon, soit d'installer un programme qui tournera sur votre machine à d'autres fins.

Avec un peu d'expérience, il n'est certes pas possible de se laisser prendre. Les noms de domaine sont déguisés, même si le pied de message comporte des liens tout à fait réguliers. Ainsi sur le spam-phishing (figure 1) imitant


Please Re-activate your account.
Google AdWords-noreply [adwords-noreply@google.com]
À: [redacted]

Dear Advertiser,

We were unable to process your payment.
Your ads will be suspended soon unless we can process your payment.
To prevent your ads from being suspended, please update your payment information.

Please sign in
to your account at http://adwords.google.com/select/login,
and update your payment information.

Blocked::http://www.adwords.google.com.dikeop.cn/select/Login

We look forward to providing you with the most effective advertising available
Thank you for advertising with Google AdWords.

The Google AdWords Team

Figure 1 - Un spam - phishing visant à introduire des pages phishing de second rang dans des sites normalement hors de tout soupçon.

....

(21) Ce kit « Rock Phish », du hameçonnage en béton, permet de créer de fausses pages ou de faux messages, ou aspire les vraies pages censées tromper l'internaute.

(22) Là encore, il serait bien illusoire de les appeler des hackers !

(23) Ce qui relève de la publicité mensongère. Les protections sont le plus souvent efficaces, mais elles ne peuvent prétendre combattre toutes les menaces potentielles.

(24) Trop d'informations nuisent à l'information (Syndrome dit de l'Air Bus). Trop de messages préventifs contribuent à fatiguer et à endormir l'usager, ce que précisément recherchent ces spammeurs de haute voltige (« spear phishing » ou hameçonnage de pointe).

(25) Des cas récents (2007, 2008) sont souvent cités et concernent même des sites publics (Grande-Bretagne, Italie notamment).

un message de Google AdWords, si le lien semble tout à fait correct vers adworks.google.com, en fait il conduit vers adwords. google.com.dikeop.cn ou adwords.google.com. coail.cn ! Le site est donc celui de coail.cn et non celui de Google. Mais, quand la souris passe rapidement sur le lien, l'œil croit reconnaître l'identité de Google et vous risquez de ne pas percevoir la supercherie. Un tour sur un des multiples sites capables d'extraire les informations des registres internationaux (*registrars*) permet de constater que ce domaine est enregistré [26] par un certain « hrthh-tfhrthv » (!) On peut lire de plus que cette personne est passée par l'intermédiaire d'un serveur de domaine chinois et qu'il a fait enregistrer pour son compte 320 autres domaines. Inutile de préciser que les outils (non publics ou payants) du même type permettent de tracer sans difficulté ces 320 comptes [27]. Ce domaine a été créé le jour même où nous avons nous-mêmes reçu le spam. Bien des leçons pourraient être tirées de ce simple exemple pris au hasard des messages d'une adresse ordinaire. Il relativise les efforts qui peuvent être entrepris à l'échelle nationale sans coopération internationale. Il est clair que la traque de ces vrais cybercriminels atteindrait vite ses objectifs si les États imposaient le respect des règles. D'un côté, le réseau est mondial, mais de l'autre, le monde est un nid de repères où règne le non-droit, sans qu'il y ait besoin d'aller chercher ici quelque pavillon de complaisance dans de petits États qui, au contraire, semblent plutôt jouer le jeu.

Aussi, les moyens mis en œuvre, pour ces raisons, atteignent la moyenne et la petite délinquance plutôt que les nouvelles mafias, dont les relations avec certaines des « nouvelles » puissances mériteraient d'être étudiées de plus près. Courons-nous un risque en écrivant cela ? Le site des *Cahiers de la sécurité* a lui-même été attaqué par un virus exploitant les failles du système de base de données SQL. C'était mal fait et ce fut vite repéré et sans conséquence. Mais, il est clair qu'il y a deux batailles.

Les responsables de ces attaques restent pour la plupart du temps impunis. Quelques-uns se sont fait prendre, souvent du fait de l'inexpérience d'un ou de deux complices opérant sur des réseaux à petite échelle. À l'échelle qui nous intéresse ici, celle de la criminalité organisée, il faut reconnaître que les prises sont maigres et ne concernent pas l'étage supérieur des organisations mafieuses. D'où d'ailleurs la difficulté à décrire dans le détail la réalité de leur fonctionnement. Beaucoup de lignes sont écrites et peu correspondent à la réalité.

Mais les États sont contraints de s'intéresser à la sécurité des réseaux, car elle devient un enjeu important. Des États ont ainsi accusé la Chine d'avoir attaqué des sites stratégiques. Le hacking est devenu une industrie de série pour les mafias, il est en passe de devenir un instrument discret, sophistiqué et de pointe pour la guerre économique et celle du renseignement. L'Estonie, attaquée de toute part, a dû isoler ses réseaux pendant deux jours et demander l'intervention de l'OTAN pour la protéger des attaques supposées de la Russie. La situation actuelle de la Géorgie a été influencée par ce type de conflit. Deux sortes d'attaque peuvent être menées, celle qui consiste à intercepter des informations et celle qui vise à créer un chaos subit. Aussi, la guerre conventionnelle tendra à se doubler de plus en plus d'une guerre numérique. Sur ce point encore, les catastrophes naturelles, dont les crises sont gérées par les autorités de la sécurité civile, convergent vers les situations que peut créer une guérilla numérique. Si l'on excepte les couches les plus critiques des applications militaires (dont le coût – relatif- est de ce fait sans cesse croissant), les systèmes informatiques utilisés par les infrastructures critiques [28] sont fondés sur les couches les plus répandues des systèmes de communication numérique. Parce qu'ils sont clairement plus efficaces et moins onéreux que des systèmes propriétaires que seuls peuvent – ou doivent [29]- s'offrir quelques industries de pointe, comme les industries militaires ou nucléaires. Une large diffusion crée la menace. Ainsi, les logiciels dits libres ou minoritaires (comme Apple) n'ont acquis la réputation d'être plus « sécurisés » que parce qu'ils sont moins soumis aux attaques. Ils présentent d'autres types de danger.

En fait, tous les États (sauf peut-être la France, la Suisse et la Suède ?) attaquent leurs partenaires pour renforcer leurs positions et celles de leurs entreprises. Certes, certains pays comme la Chine ne cachent rien de la réalité de ce

••••

(26) Recherche réalisée le 31 août 2008 sur le moteur d'extraction du site http://whois.domaintools.com/ alors que le message a été reçu une semaine auparavant, le 24 août, par des milliers sinon des millions de personne... Cela donne une idée du mur auquel les polices se heurtent dans leur combat contre ces mafias alors que l'envoi d'une centaine d'e-mails individuels sur un serveur d'un des plus grands pourvoyeurs d'adresses mail vous « blackliste » temporairement mais immédiatement...

(27) En utilisant un autre outil à la disposition de tous, il apparaît que le serveur de ces domaines est localisé à... Stuttgart. Autre particularité de ce message : il est envoyé depuis l'adresse usurpée du destinataire qui n'aura donc pas la possibilité de la déclarer comme indésirable.

(28) Réseaux d'approvisionnement et de traitement des eaux, systèmes de détection des incendies, les centrales, les systèmes de gestion des transports et de la circulation, les barrages... et même les réseaux de pilotage des crises.

(29) En 2003, un « ver » a paralysé le réseau de surveillance d'une centrale nucléaire américaine (l'obligation de résultat plus que de moyens peut, dans ce domaine, comporter des conséquences inattendues).

combat si bien qu'une culture du hacking a gagné les milieux mafieux qui accompagnent leur formidable décollage économique. Un phénomène semblable s'est produit en Russie où les services de renseignement recrutent les meilleurs ingénieurs informatiques qui sortent des écoles. Mais, le « sale boulot » est confié aux prestataires sans vouloir voir qu'ils sont également au service des mafias. Si les mafias sont poursuivies, les prestataires de service sont relativement épargnés. Tous ces milieux sont liés. Et la question se pose, lancinante, de savoir s'il est possible de lutter contre les menaces émergentes qui nous concernent sans, quelque part, pactiser avec le diable. C'est le pari légitime qui sous-tend le plan français (*cf.* encadré). Mais, alors, il faudra y mettre les moyens car ces cybercriminels n'ont rien de la bande à Bonnot.

2008 : un plan officiel contre la cybercriminalité

Ce plan a été présenté en février 2008. En fait, le pivot de la lutte contre la cybercriminalité en France se situe à l'OCLCTIC, l'Office central de lutte contre la criminalité liée aux techniques de l'information et de la communication. Dépendant de la direction centrale de la Police judiciaire (DCPJ), l'OCLCTIC est l'interlocuteur privilégié du gouvernement et représente la France lors des réunions étrangères. Il a été créé en mai 2000 et s'est largement appuyé sur les méthodes virales en vigueur dans les années 1995-99. Il compte une cinquantaine de personnes regroupées en trois sections principales. La première rassemble des enquêteurs habilités à faire un travail de police sur tout le territoire et à l'étranger. La deuxième est une section technique (veille, formation). La dernière gère la plate-forme de signalement.

Comme le reconnaît lui-même Christian Aghroum [30], chef de l'OCLCTIC, la cyber-délinquance a beaucoup évolué. Nous sommes sortis de l'ère des pionniers. L'Internet ressemble finalement à la société. D'un côté du triangle, les voleurs à la tire utilisent le réseau et les recettes virales (ou non virales) qu'il est aisé de trouver sur Internet pour extorquer de l'argent aux usagers les plus crédules. D'un autre côté, des pirates organisés attaquent des sites, des processus où transitent des données sensibles afin de voler identifiants, données monnayables ou secrets de fabrication. Sur le troisième pilier, innovation et « hackage » se donnent la main sans relation directe avec la délinquance, celle allant de la délinquance simple au grand banditisme criminel et à l'instrumentalisation par des organisations mafieuses nouvelles ou reconverties, voire par des organisations terroristes.

La qualification criminelle de ces délinquants relève de niveaux très différents. Les détecter puis les poursuivre constituent des métiers différents. De fait, les 500 enquêteurs dont disposent la police et la gendarmerie à ces fins, sont répartis dans différents services. Le dispositif a dû difficilement suivre le rythme de l'évolution et de la diversification de la délinquance. La ministre de l'Intérieur a donc légitimement voulu adapter l'effort de l'État par une remise à plat du dispositif en programmant le doublement des effectifs des enquêteurs spécialisés d'une part, et en renforçant le rôle pivot de l'OCLCTIC d'autre part. L'office se concentrerait sur la délinquance qui demande une coopération internationale renforcée, assurerait une veille technologique, et partant, constituerait le référent expert des nouvelles technologies utilisées à des fins délinquantes et assurerait les formations des enquêteurs spécialisées.

D'autres mesures sont proposées par ce plan pour accompagner cette évolution :

- la création d'un cursus spécialisé au sein de la Police nationale ;
- l'extension de la plateforme de signalement des communications xénophiles et pédophiles à toutes les formes d'escroquerie et de terrorisme en ligne ;
- la mise à disposition des policiers d'outils de captation de données à distance ;
- la création d'un site de référence pour les internautes [31] ;
- l'obligation de conserver les données de connexion utiles à l'identification des créations de contenu ;

(30) Se reporter à l'article de Christian Aghroum dans ce numéro.
(31) Pour l'heure, le site est à cette adresse : http://www.interieur.gouv.fr/sections/contact/police/questions-cybercriminalite

- la création d'un délit d'usurpation d'identité sur internet (jusqu'à un an d'emprisonnement et 15 000 euros d'amende) ;

- l'utilisation des compétences des « hackers » condamnés pour les utiliser au service de la collectivité, en créant une nouvelle peine alternative (type de sanction existant déjà à l'étranger et d'efficacité relative tant les compétences de ces hackers relèvent parfois du mythe).

En fait, cette volonté amorce un effort pour prendre en compte progressivement la différenciation qui s'est opérée. Entre la blague potache qui consiste à usurper l'e-mail d'un ami sur MSN, la délinquance de proximité (diffuser des photos volées par exemple) et organiser un réseau de robots rabattant des données escroquées et monnayables sur une grande échelle, il y a une différence dans le niveau du délit et la qualification criminelle. Le problème est que, contrairement à l'idée reçue, les outils sont souvent les mêmes et pis, les outils de l'Internet permettent ces escroqueries mineures ou majeures sans aucun recours à des malwares [32] ; il est à la portée de tout utilisateur d'envoyer un e-mail en empruntant l'identité d'un tiers...

Nous voilà revenus à la case départ de la délinquance ordinaire. Faut-il mettre sous surveillance tous les tournevis au motif qu'ils peuvent servir à crocheter une porte... Il est possible de demander aux opérateurs comme aux hébergeurs de conserver toutes les données susceptibles d'identifier [33] les poseurs [34] de contenu en ligne. Cela ne nous conduira pas vers la société de « big brother » contrairement à ce qui est souvent avancé. En revanche, cela risque de conforter les risques et de déporter les menaces. S'il s'agit de la petite délinquance, il est envisageable de demander aux hébergeurs de réaliser un minimum de « flicage ». Ce n'est en réalité ni plus ni moins que du ressort de l'éthique. Mais, cela ne règle pas la question des organisations criminelles mafieuses car, le plus souvent, ils contrôlent leurs hébergeurs centraux dans des États qui, souvent, les tolèrent. Encore une fois, ce n'est pas une question d'outil. Usurper l'identité d'un e-mail pour faire une blague et créer un robot qui utilise la même technique reproduite des millions de fois pour escroquer ne peut relever de la même approche. De la civilité ordinaire et de ses manquements à l'attentat criminel à l'ordre public, il y a une marge que les décrets prévus par le plan Alliot-Marie vont devoir apprécier. En clair, la cybercriminalité ne peut être traitée isolément des questions qui relèvent de la sécurité globale, civile, certes, mais aussi économique (question de l'intelligence économique et/ou territoriale), mais aussi militaire.

Patrice HERNU

DOSSIER

....

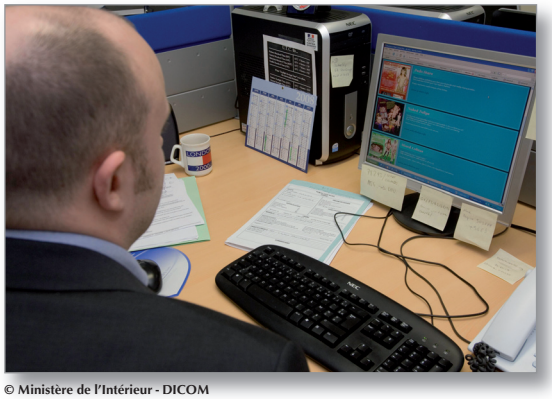
(32) Softwares (logiciels) malicieux.

(33) Adresse IP, mot de passe, identifiant, machine utilisée, etc.

(34) « Créateurs » est un bien grand mot pour ce qui effectivement transite par ces canaux !

Quelles ripostes contre la pédopornographie par Internet ?

Frédéric MALON



© Ministère de l'Intérieur - DICOM

Le présent article vise à mieux faire comprendre ce qu'est le phénomène criminel de la cyberpédopornographie : qui sont ses acteurs ? Quelles formes d'organisations existent ? Quels sont les moyens juridiques pour lutter contre ? Sous quels angles d'attaque peut-on combattre ce phénomène criminel ? L'étude de ces différents points fait apparaître qu'une coopération internationale exemplaire est indispensable pour parvenir aux sources du problème.

Dealing with Child Pornography on the Internet

How is the criminal activity of child pornography to be understood? Who is involved? What kinds of organisations exist? What are the legal means available to combat it? How can it be combated? In answering these questions there emerges the need for indispensable international cooperation in order to get to the source of the problem.

Frédéric Malon

Commissaire divisionnaire, chef de l'Office central pour la répression des violences aux personnes à la direction centrale de la Police judiciaire. Titulaire d'une maîtrise en droit. A exercé successivement à la sûreté urbaine de Rouen (1992-1995), dans les divisions criminelles des services régionaux de police judiciaire de Rouen (1959-1997), Toulouse (1997-2004) et Versailles (2004-2006).

En matière de la lutte contre la cybercriminalité, la problématique des mineurs victimes d'abus sexuels a fait l'objet d'une attention croissante au cours de ces dernières années, de sorte qu'elle se trouve aujourd'hui au cœur des préoccupations d'un nombre de plus en plus important de pays, dont la France fait partie. Quatre-vingt-cinq pays restent néanmoins, à ce jour, dépourvus de législation spécifique.

Parmi ses différentes attributions, l'Office central pour la répression des violences aux personnes (OCRVP) de la direction centrale de la Police judiciaire (DCPJ) a été chargé, dans son décret de création en date du 6 mai 2006, de la lutte contre la pédopornographie et les abus sexuels au préjudice des mineurs. Un groupe d'enquêteurs est spécialisé dans ce domaine, et mène de nombreuses enquêtes qui aboutissent quasiment chaque semaine à l'interpellation de cyberpédophiles. L'OCRVP participe également à de nombreuses réunions à caractère stratégique, tant au plan national qu'au niveau international, visant à améliorer l'efficacité de la lutte contre cette forme de criminalité. Ces réunions sont l'occasion d'échanger, d'évoquer des retours d'expérience, de partager les bonnes pratiques, d'harmoniser les législations, de présenter des outils nouveaux d'aide à l'enquête, de mettre en œuvre des actions communes, préventives ou répressives, etc. La coopération internationale est, en effet, indispensable pour aboutir à des résultats significatifs en ce domaine, en raison de la nature même du réseau Internet.

Le droit français, quant à lui, a dû prendre en compte l'émergence de l'utilisation d'Internet, notamment en matière de lutte contre la pédopornographie. Il ne faut pas oublier que derrière chaque image de pédopornographie, il y a au moins un mineur victime d'abus sexuels et au moins un auteur de ces abus. Des infractions spécifiques ont été ainsi ajoutées au Code pénal.

Avant d'aborder les différents angles d'attaque utilisés pour lutter contre la pédopornographie sur Internet, il convient au préalable de présenter ce qu'est ce phénomène criminel, et d'évoquer les éléments essentiels du dispositif législatif français existant.

La cyberpédopornographie

À l'instar du trafic de drogue, la pédopornographie sur Internet est un phénomène criminel qui dépasse, par définition, les frontières puisqu'il a recours au réseau Internet. Elle implique, d'un côté, une forme de criminalité de comportement active, mettant en cause ceux que l'on peut qualifier de « producteurs », c'est-à-dire ceux qui filment ou photographient des mineurs victimes d'abus sexuels, puis diffusent ces images sur le Net, et, de l'autre côté, une forme de criminalité passive, avec les « consommateurs », c'est-à-dire ceux qui derrière leur ordinateur, visionnent ces images, les téléchargent, les rediffusent. Dans cette dernière catégorie, toutes les couches sociales sont représentées : cadres, ouvriers, employés... Il suffit de posséder un ordinateur. Il est à noter, d'ailleurs, que parmi les métiers les plus concernés, on trouve les informaticiens. Leurs connaissances professionnelles font qu'ils sont souvent les plus difficiles à incriminer, mais aussi les plus intéressants pour les enquêteurs.

La part du crime organisé (au sens mafieux) dans la pédopornographie sur Internet est assurément importante au vu du nombre sans cesse croissant d'images circulant sur la toile (évalué à au moins trois millions). Elle se rapporte aux criminels qui organisent le viol ou la prostitution de mineurs et intègrent ensuite les vidéos ou photographies sur le Net en vue d'en tirer des bénéfices. Elle présente également moins de risques pour ceux-ci d'être identifiés, interpellés et poursuivis que le trafic de drogue par exemple.

C'est ainsi que très peu d'organisations de ce type ayant été démantelées (USA, Russie), les spécialistes en ce domaine s'accordent à dire qu'elles sont implantées, pour l'essentiel, en Asie, dans les ex-pays du bloc de l'Est et aux États-Unis. L'existence de nombreux enfants, facilement accessibles dans certains pays, est également de nature à attirer ces organisations criminelles. L'affaire « koala » (baptisée comme telle car initiée en Australie), médiatisée en fin d'année 2007, avait permis d'identifier les membres d'un réseau international de malfaiteurs dont les principaux étaient domiciliés en Italie, Ukraine, Russie, Roumanie et Belgique. C'est grâce à une coopération policière et judiciaire exemplaire que cette affaire avait pu aboutir avec succès. Si, à ce jour, l'existence de ce type d'organisation criminelle n'a pas été démontrée en France, on ne peut exclure, à la lumière de « koala », qu'il en existe néanmoins quelques-unes dont au moins une partie se trouve sur notre territoire national.

Parfois certains « consommateurs » sont aussi des « producteurs ». Une partie des affaires concernant les « consommateurs » débouche en effet, quelquefois, sur la révélation de faits plus graves de viols ou autres agressions sexuelles. En pratique, en France, en l'absence d'étude ou de statistique précise, on évalue cette partie à 10 % des cas en moyenne. Une étude américaine sur la période 1990-2006 a, pour sa part, établi qu'un tiers des personnes qui regardent des images de pornographie enfantine a eu

des contacts sexuels avec des enfants. À l'inverse, selon une étude canadienne de 1998, 53 % des agresseurs sexuels pédophiles visionnaient auparavant des photos pédopornographiques. Avec la démocratisation d'Internet, il faut considérer que ce chiffre a certainement évolué.

Pour revenir à la France, on observe que ces affaires incidentes se situent, pour l'essentiel, dans un contexte familial ou relationnel proche (baby-sitter, enseignant, éducateur sportif, curé, etc.), et non dans un milieu criminel organisé. C'est ce type d'affaires qui est à l'origine de la seconde catégorie d'images de pornographie enfantine que l'on trouve sur le Net. Il n'est pas rare de constater, en effet, que des pères de famille, qui abusent de leurs enfants, photographient ou filment leurs actes et les diffusent ensuite sur la toile.

À côté de la pédopornographie sur Internet, il convient de mentionner, pour mémoire, qu'il existe un autre type de comportements qui s'est développé sur la toile et se rapporte au terme anglais de « grooming ». Il a été défini par le droit français comme étant le fait pour un majeur de faire des propositions sexuelles à un mineur de 15 ans ou à une personne se présentant comme telle, par le biais d'Internet. L'infraction est constituée quand bien même ces propositions n'ont pas été suivies d'effet. Les peines sont aggravées si un contact physique s'est ensuivi et une relation sexuelle a eu lieu.

Le dispositif législatif

Les infractions spécifiques à la cyberpédopornographie

Applicables aux « producteurs », « consommateurs » et aux intermédiaires, ces infractions sont fixées à l'article 227-23 du Code pénal (instauré par la loi du 17 juin 1998 et complété par des lois de 2002, 2004 et 2007), qui réprime ainsi :

- l'enregistrement ou la transmission d'images ou de représentations à caractère pornographique d'un mineur, en vue de leur diffusion (cinq ans d'emprisonnement et 75 000 euros d'amende) ;

- l'offre, la diffusion, l'importation ou l'exportation de ce type d'images ou de représentations (cinq ans d'emprisonnement et 75 000 euros d'amende) ;
- ces peines sont aggravées lorsqu'est utilisé un réseau de communications électroniques tel qu'Internet (sept ans d'emprisonnement et 100 000 euros d'amende) ;
- la consultation habituelle de ce type d'images ou représentations par un service de communication au public en ligne tel qu'Internet ou leur détention (deux ans d'emprisonnement et 30 000 euros d'amende).

- lorsque ces infractions sont commises en bande organisée, les peines sont portées à dix ans d'emprisonnement et 500 000 euros d'amende.

La notion d'image ou de représentation permet de réprimer non seulement les photographies, mais aussi tous dessins ou images virtuelles à caractère pédopornographique. Le texte précise qu'il suffit que les images soient celles d'une personne dont l'aspect physique est celui d'un mineur, sauf s'il est établi qu'elle a plus de 18 ans. En pratique toutefois, compte tenu des incertitudes quant à la détermination de l'âge de certaines victimes adolescentes, et des instructions des magistrats, seules les images ou représentations d'enfants prépubères sont prises en compte dans les enquêtes. Il en va évidemment différemment si la victime est identifiée et que les abus sexuels ont eu lieu alors qu'elle était mineure.

Les infractions aggravées en matière de pédophilie avec recours à Internet

Un certain nombre d'infractions sont aggravées lorsqu'un réseau de télécommunications, tel qu'Internet, est utilisé pour les commettre et/ou lorsqu'elles sont commises à l'égard d'un mineur.

- Les articles 222-23 et 222-24 du Code pénal aggravent la répression du viol, non seulement lorsqu'il est commis à l'égard d'un mineur de 15 ans, mais aussi lorsque la victime a été mise en contact avec l'auteur des faits grâce à l'utilisation d'un réseau de télécommunications (vingt ans de réclusion criminelle).

- L'article 222-29 du Code pénal aggrave également la répression des agressions sexuelles lorsqu'elles sont commises à l'égard d'un mineur de 15 ans (sept ans d'emprisonnement et 100 000 euros d'amende). Par ailleurs, les agressions sexuelles sont punies des mêmes peines lorsque la victime a été mise en contact avec l'auteur des faits grâce à l'utilisation d'un réseau de télécommunications (article 222-28 du C.P.).

- Les articles 225-7 et 225-7-1 du Code pénal aggravent la répression du proxénétisme, non seulement lorsqu'il est commis à l'égard d'un mineur ou d'un mineur de

15 ans, mais aussi lorsqu'il est commis grâce à l'utilisation d'un réseau de télécommunications (dix ans d'emprisonnement et 1 500 000 euros d'amende).

- L'article 225-12-2 du Code pénal aggrave la répression du recours à la prostitution de mineurs lorsque la victime a été mise en contact avec l'auteur des faits grâce à l'utilisation d'un réseau de télécommunications (cinq ans d'emprisonnement et 75 000 euros d'amende).

En outre, l'article 227-28-3 du Code pénal réprime l'incitation à la commission de ces actes pédopornographiques. Cette infraction autonome suppose que ces actes n'aient été ni commis ni tentés. Les sanctions sont trois ans d'emprisonnement et 45 000 euros d'amende lorsqu'il s'agit d'un délit et sept ans d'emprisonnement et 100 000 euros d'amende lorsqu'il s'agit d'un crime.

Les angles d'attaque de la cyber-pédopornographie

Les auteurs

Lorsqu'un internaute se connecte sur un site pédopornographique, il laisse une trace informatique. C'est le même principe que pour le téléphone. Avec Internet, son numéro de téléphone, c'est son adresse IP (Internet Protocol). Les services de police peuvent donc avoir accès, dans le cadre de leurs enquêtes et dans certaines limites de temps, à ces traces de connexion et ainsi identifier un ordinateur qui s'est connecté à un site pédopornographique. Il reste ensuite à identifier l'utilisateur de cet ordinateur.

L'enseignement tiré par les Britanniques, à la suite de plusieurs affaires, est qu'il ne faut pas négliger au cours des enquêtes le rôle des femmes. Les femmes pédophiles ou cyberpédophiles existent, et sont plus nombreuses qu'on ne peut le croire. Elles agissent parfois sur leurs propres enfants, activement ou passivement, mais parfois avec leur mari ou concubin. Peu de femmes pédophiles ont été recensées en France, la plus célèbre étant l'épouse de Michel Fourniret, mais sans qu'elle ait eu recours à Internet.

L'enquête d'identification doit prendre en compte également la possibilité que l'auteur ait utilisé un ordinateur à l'insu de son propriétaire, en recourant au système WiFi.

Une fois l'auteur identifié, une procédure sur la base de l'article 227-23 du Code pénal est diligentée. L'objectif est d'aller plus loin et de vérifier s'il n'a pas été également auteur d'abus sexuels sur mineurs. Un travail d'environnement est alors nécessaire afin d'identifier les contacts qu'il a pu nouer avec des enfants, que ce soit les siens ou non, et de vérifier, notamment au travers d'auditions effectuées par des personnels spécialement formés, que ceux-ci n'ont pas été victimes. Une perquisition approfondie est indispensable, non seulement de tous les supports informatiques en sa possession, mais également de l'ensemble de son domicile. Une culotte de fillette au domicile d'un célibataire serait un indice intéressant. Dans une affaire récente, la perquisition chez un internaute s'étant simplement connecté sur un site pédopornographique avait amené la découverte, dans sa cave, de plusieurs vidéos révélant ses intenses activités de touriste sexuel en Asie du sud-est.

Ces auteurs doivent tous être signalisés : prise de photographies, d'empreintes digitales, prélèvements génétiques. Ils peuvent être ainsi identifiés plus rapidement dans d'autres affaires déjà commises ou qu'ils commettraient ultérieurement. Cette signalisation peut également participer de la prévention en dissuadant certains de passer de leur ordinateur à l'acte sexuel avec un mineur.

Il est également important que ces délinquants soient intégrés au fichier judiciaire des auteurs d'infractions sexuelles et/ou violentes (FIJAIS). Il revient à la justice d'y veiller. Cette inscription est obligatoire pour les infractions dont la peine est supérieure à cinq ans d'emprisonnement (diffusion, importation via Internet, etc.), mais elle n'est que facultative lorsque la peine est inférieure ou égale à cinq ans (consultation habituelle).

Enfin, la confiscation judiciaire du matériel informatique, souvent dernier cri, est aussi une sanction efficace.

Les enquêtes peuvent débuter de plusieurs manières :

- Par le démantèlement d'un site diffusant de la pédopornographie. Il suffit de travailler sur la liste des internautes qui s'y sont connectés. La plupart des sites étant hébergés à l'étranger, ces informations parviennent à la France dans le cadre des canaux de coopération internationale que sont Interpol et Europol. L'OCRVP est alors le point d'entrée unique de ces informations provenant de l'étranger. Son travail consiste à identifier les internautes français s'étant connectés sur les sites ainsi démantelés. Selon leur nombre, il traite lui-même les dossiers ou les retransmet à un parquet territorialement compétent qui saisira le service d'enquête de son choix. À l'inverse, on peut citer l'affaire d'envergure internationale baptisée « d'Artagnan », initiée en 2005 par la France, au cours de laquelle 842 connexions Internet

illicites avaient été repérées à partir d'un site illicite. Elle avait débouché sur l'identification de 528 internautes en France, et 559 de nationalité étrangère répartis dans 42 pays différents.

- Par une dénonciation par un autre internaute : elles sont relativement fréquentes, notamment à partir du site Internet www.internet-mineurs.gouv.fr, hébergé à l'Office central de lutte contre les infractions liées aux technologies de l'information et de la communication (OCLCTIC), au sein de la plate-forme de signalement des contenus illicites de l'Internet.

- Par l'identification incidente au cours d'une enquête, d'autres internautes en relation avec une première personne identifiée.

- À partir d'un travail de veille sur Internet : en France, par exemple, la gendarmerie dispose d'une unité spécialisée installée à Rosny sous Bois, qui effectue la surveillance des réseaux pair-à-pair (*peer to peer*). Il est ainsi possible d'identifier des internautes attirés par les images pédophiles.

- Par la « cyberpatrouille » : allant plus loin que la veille sur Internet, la cyberpatrouille est une forme d'infiltration de la toile. Cette technique d'enquête a été introduite en droit français par la loi du 5 mars 2007 relative à la prévention de la délinquance. Elle n'est pas encore entrée en vigueur, un arrêté interministériel, qui devrait être pris très prochainement, étant nécessaire. La cyberpatrouille consiste très schématiquement, pour un policier ou un gendarme, à surfer sur la toile en vue de détecter des internautes pédophiles. Pour ce faire, il peut utiliser un pseudo, puis échanger ou détenir des images à caractère pédopornographique en toute légalité. Comme pour l'infiltration classique, l'agent ne doit cependant pas user de provocation à la commission de l'infraction.

Cette technique peut être utile notamment pour débusquer les internautes pédophiles qui entrent en contact avec des mineurs en se faisant, eux aussi, passer pour des mineurs, afin de leur fixer un rendez-vous ou de les pousser à commettre des actes à connotation sexuelle, par exemple devant une webcam. Elle peut servir également à infiltrer des réseaux pédophiles organisés. En tant que technique d'enquête d'exception, elle est prévue pour n'être employée que par les services spécialisés centraux et territoriaux. Par ailleurs, la spécificité du réseau Internet exige une centralisation et une coordination optimales. Le Service interministériel d'assistance technique (SIAT), déjà désigné pour être l'institution nationale unique pour les opérations d'infiltration liées à la criminalité organisée, sera chargé de gérer les pseudos utilisés par les enquêteurs afin d'éviter, par exemple, qu'un policier de l'OCRVP entre en contact sans le savoir avec un gendarme de la section de recherches de Marseille. Ses contacts avec ses homologues étrangers lui permettront également de s'assurer d'une bonne coordination au niveau international.

Les sites

L'OCLCTIC a pour mission de centraliser les sites identifiés au cours d'une enquête. La très grande majorité des sites de pédopornographie étant hébergés à l'étranger (USA, Russie, Panama, Corée du sud, Turquie, etc.). Le rôle de l'Office consiste à informer officiellement le pays d'origine du site, à charge, pour ce dernier, de prendre les mesures *ad hoc*, pour d'abord le faire cesser et ensuite identifier les personnes qui se cachent derrière afin d'engager des poursuites contre elles.

En pratique, il est, en revanche, extrêmement difficile de connaître les suites données aux transmissions de signalement. Cela a ainsi été une heureuse surprise d'apprendre, fin 2007, que la Russie avait mis fin à une des principales plates-formes d'hébergement de sites pédopornographiques qui rassemblait près de 40 % des sites mondiaux (*Russian Business Network*). Il apparaît aujourd'hui, toutefois, que la plupart de ces sites ont trouvé, par la suite, d'autres pays d'hébergement.

Compte tenu de la durée de vie parfois très courte de certains sites, la réactivité est de mise. Il en va ainsi lorsque de temps en temps, un site français est découvert. L'information est en principe transmise à l'OCRVP qui la traite en priorité. Ces rares sites français ainsi démantelés n'ont révélé aucune organisation criminelle, mais simplement des pédophiles isolés qui mettaient en ligne les photos ou films qu'ils avaient pris de leurs abus.

L'action en matière de lutte contre la cybercriminalité peut être également préventive. Un projet de blocage des accès aux sites de pédopornographie est en effet d'actualité. Ce projet avait été discuté initialement dans un groupe de travail d'Europol auquel l'OCRVP était partie prenante. À l'instar de la Norvège, qui avait instauré un tel filtrage en 2004, plusieurs pays européens ont adopté (Suède, Danemark, Finlande, Pays-Bas, Royaume-Uni, Italie, Suisse) ou sont en cours d'adoption du même système (Espagne, Belgique, Irlande). La France est quelque peu à la traîne, mais s'attache actuellement à rattraper son retard.

Le projet a été repris à son compte par le ministère de l'Intérieur, de l'Outre-mer et des Collectivités territoriales dans son plan de lutte contre le cybercrime, et intéresse de

près d'autres ministères. Il vise à empêcher les internautes de se connecter aux sites de pédopornographie répertoriés (*blacklistés*) par les services de police. De l'autre côté, il tend à réduire les bénéfices que tirent les organisations criminelles de la production et de la diffusion de telles images. À titre d'exemple, 30 000 tentatives de connexion sont bloquées chaque jour au Royaume-Uni, 5,5 millions par an en Norvège pour 4,5 millions d'habitants. À défaut d'accord amiable avec les fournisseurs d'accès à Internet, points de passage obligés pour la mise en place du filtrage, une réforme législative s'avère nécessaire. Les premiers travaux ont été engagés en vue d'aboutir au plus vite.

Les images

Derrière chaque image de pédopornographie, il y a au moins un mineur victime d'abus sexuels et au moins un auteur de ces abus. Il est estimé qu'au moins trois millions d'images circulent aujourd'hui sur Internet, et leur nombre est sans cesse croissant. On constate également de plus en plus de vidéos. Une fois sur la toile, les images ne peuvent quasiment jamais être enlevées. Tout au moins, on ne peut jamais être sûr de les enlever définitivement. En effet, quand bien même on remonte à leur source, une fois diffusées, ces images peuvent ensuite être téléchargées et rediffusées par d'autres internautes sans qu'il soit possible d'en être sûr ou de l'empêcher. L'intérêt de travailler sur les images est donc de parvenir à identifier les victimes et les auteurs.

L'exemple extrême des enquêtes menées à partir des images est celui de l'appel au public pour identifier l'auteur. C'est le cas des affaires « VICO » et « IDENT », pour lesquelles Interpol a effectué une médiatisation mondiale en diffusant la photographie de l'auteur des abus sexuels sur mineurs. Dans les deux cas, l'auteur a pu être identifié très rapidement. Cette technique doit rester exceptionnelle et n'être utilisée qu'en dernier recours. Elle n'a pas été sans poser certains problèmes, notamment d'ordre juridique. Pour l'affaire « VICO » par exemple, l'OCRVP, point de contact central d'Interpol, n'avait jamais reçu officiellement les photographies incriminantes établissant les infractions commises. Toutes les vérifications entreprises en France dans cette affaire l'avaient été dans un cadre juridique plutôt bancal, à telle enseigne que certains parquets avaient refusé que des perquisitions soient menées chez les suspects. Les retours d'expérience de ces deux affaires ont, semble-t-il, permis à Interpol de tirer les enseignements nécessaires pour éviter ce genre de difficultés à l'avenir.

Depuis 2001, Interpol possède une base d'images pédopornographiques, située à son siège à Lyon. Elle comprend environ 600 000 images. Elle constitue un outil de coopération internationale de premier plan pour l'identification de victimes et d'auteurs. Cette base est alimentée par 26 pays. À ce jour, plus de 640 victimes, dont les images circulent sur Internet, ont été identifiées de par le monde, dont 43 en France, la plupart par l'OCRVP. Interpol projette d'ici à 2009, d'accorder l'accès direct à son fichier aux pays qui l'alimentent. Cette mesure est de nature à donner à l'OCRVP un atout opérationnel supplémentaire, lui permettant de vérifier, en temps réel, la présence dans la base, des photographies saisies au cours d'une perquisition, et donc de travailler, le cas échéant, sur celles qui n'y sont pas enregistrées, afin de tenter d'identifier les victimes et leurs agresseurs qui pourraient se trouver en France. L'intérêt est d'autant plus grand que ces photographies auraient toutes les chances d'être récentes, et donc que les victimes aient gardé leur apparence. Il arrive parfois de découvrir des photos datant de plus de vingt ans, ce qui, outre des problèmes éventuels de prescription, engendre forcément d'importantes difficultés pour identifier les victimes.

La plupart des victimes identifiées en France l'ont été à partir de photographies découvertes en perquisition, dont l'examen a révélé un lien relationnel (familial ou environnemental) avec l'utilisateur de l'ordinateur. Ce dernier s'avérait ainsi être le producteur des images saisies. Quand bien même la très grande majorité des photographies découvertes ne sont pas d'origine française, il est nécessaire de développer le travail d'identification des victimes par l'analyse approfondie des images pour lesquelles le mis en cause n'est pas le producteur et qui sont susceptibles de provenir de France.

La France possède également sa base d'images pédopornographiques baptisée CNAIP (Centre national d'analyse des images pédopornographiques). Composée, en principe, de gendarmes et de policiers détachés de l'OCRVP, cette structure est installée à Rosny-sous-Bois, dans les locaux de la gendarmerie. La base comprend à peu près le même nombre d'images que celle d'Interpol. Elle est chargée entre autres d'alimenter les services d'enquête qui auront recours à la cyberpatrouille en leur fournissant des images de pornographie enfantine.

Les flux financiers

Cet angle d'attaque n'a pas encore été appliqué en France. Il vise à remonter la chaîne des flux financiers générés par la pédopornographie pour identifier les bénéficiaires, vraisemblablement des organisations criminelles très structurées. Les spécialistes américains estiment à 21 milliards de dollars les bénéfices générés dans le monde entier par ce type de commerce en 2006.

Cet aspect financier fait l'objet d'un projet en cours de développement au sein du groupe de travail d'Europol dont fait partie l'OCRVP. Pour l'instant, il en est au stade des études et réflexions. L'expérience américaine démontre la nécessité pour la police de nouer des liens étroits avec les organismes de paiement en ligne et les banques, détenteurs d'informations susceptibles de permettre de tracer les flux financiers générés par la cyberpédopornographie.

Deux difficultés majeures ont été observées :

- les flux financiers peuvent se déplacer à travers les frontières et atterrir dans la banque d'un paradis fiscal ;

- la circulation des flux financiers est très rapide.

Dans les deux cas, la coopération internationale judiciaire et policière actuelle est impuissante pour remonter à l'identification des bénéficiaires finaux. Elle doit impérativement être améliorée et toutes les possibilités étudiées. En fonction de l'évolution et des études qui seront menées, il pourra s'avérer nécessaire, en France, d'impliquer dans cette lutte des services financiers très spécialisés tels que l'Office central pour la répression de la grande délinquance financière (OCRGDF).

Conclusion

Avec le développement d'Internet, on observe une augmentation très nette du nombre des affaires. Les moyens de lutte contre la cyberpédopornographie doivent donc s'adapter en conséquence. Les moyens informatiques doivent suivre de près les évolutions technologiques et davantage de personnels devront être spécialement formés.

Actuellement, la France obtient de bons résultats. Mais elle peut et doit faire mieux. Il lui reste notamment à développer son action sur les images saisies et à parvenir à mieux remonter jusqu'aux organisations criminelles qui produisent la cyberpédopornographie en les atteignant là où cela fait mal, c'est-à-dire au portefeuille.

Il faut également poursuivre les efforts en termes de coopération internationale. C'est la seule solution pour parvenir à démanteler des organisations criminelles qui engrangent des bénéfices juteux par l'exploitation sexuelle de mineurs. Une grande majorité de pays a dépassé le stade de la prise de conscience du phénomène criminel qu'est la cyberpédopornographie. Et même si de nombreux pays sont encore en retrait, les législations s'adaptent progressivement, en se durcissant, et la coopération internationale s'améliore en conséquence.

Frédéric MALON

Internet, fraudes et corruptions

Noël PONS

© Gettyimages

Internet a ouvert le monde à la criminalité. Camouflée derrière le paravent de la liberté sans contrôle, elle peut aisément développer des escroqueries, créer un marché efficace pour la contrefaçon et corrompre le sport grâce aux paris manipulés.

Internet, fraud and Corruption

The internet has been opened up to the world of crime. Camouflaged behind the shield of freedom without controls, criminals have easily developed their scams, created an effective market for counterfeiting and corrupted sports with manipulated gaming

Noël Pons

Il est conseiller au Service central de prévention de la corruption (SCPC), auditeur interne certifié (CIA), inspecteur des Impôts. Il a publié plusieurs ouvrages dont, en 2006, *Cols blancs et mains sales-Economie criminelle, mode d'emploi* aux éditions Odile Jacob ; en 2004, il a coécrit avec François Vidaux, *Audit et fraudes*, paru aux éditions IFACI. Il est aussi l'auteur de plusieurs articles relatifs aux fraudes, à la corruption et au blanchiment, en particulier dans la rubrique « fraudes » de *La revue française de l'audit interne*.

Le grand banditisme a saisi l'opportunité de l'économie virtuelle offerte par l'Internet. Ce dernier a créé des débouchés nouveaux, inespérés, difficilement contrôlables, ainsi qu'une assise fiable pour les montages anciens. La criminalité a trouvé là un univers à sa mesure pour implanter et donner un essor nouveau à ses manipulations. C'est, pour elle, une nouvelle conquête de l'Ouest !

Avec Internet, on entre de plain-pied dans la mondialisation : tout peut être exécuté, depuis n'importe où, par n'importe qui. Certains sites permettent même un camouflage quasi parfait car ils ne gardent pas les données de leurs utilisateurs ; d'autres se refusent à répondre à tout droit de communication en jouant à « saute-paradis » fiscaux. Même si des poursuites sont diligentées par des structures d'État, elles mettent nécessairement du temps à atteindre leur but, l'essentiel est alors sauvé : les fonds ont disparu depuis longtemps

L'intérêt criminel pour Internet a existé dès l'origine. La première grande escroquerie connue aurait été le fait de mafiosi new-yorkais. En effet, ces derniers ont créé des sites pornographiques accessibles en payant une modique cotisation par carte de crédit. En revanche, une fois les codes des cartes récupérés, des milliers de prélèvements illégaux ont été effectués sur ces cartes, les personnes escroquées hésitant à porter plainte car, à l'époque, surfer sur de tels sites était honteux. Nous en sommes bien loin maintenant.

L'absence d'établissement stable, physiquement identifiable rend la commission d'infractions plus facile. Utiliser des sociétés écrans, de fausses identités, de fausses qualités est chose aisée, surtout sur la toile. La saisie des actifs est difficile, voire impossible en cas de condamnation, ce qui pérennise le montage frauduleux. De plus, dans le cas où une investigation serait couronnée de succès après la collaboration maximale des divers pays engagés, le nombre d'opérations frauduleuses qui ne peuvent être sanctionnées rend la peine peu dissuasive. Comme pour le blanchiment ou le trafic de drogues, la criminalité « embourbe » les contrôles. L'effet masse dont il joue rend la sanction acceptable, voire lui permet de lancer des leurres.

Internet et les manipulations

Les montages les plus développés sont constitués par des montages anciens adaptés au support. Il s'agit essentiellement :

- Opérations classiques telles que des extorsions de fonds contre des sociétés. La méthode est celle du « déni de service » : les sociétés qui ne payent pas voient leurs serveurs bloqués par la multiplication de requêtes, et ne peuvent plus travailler. Les cibles sont diverses : les casinos internet et les sociétés de paris mais aussi des sociétés commerciales plus classiques.
- Des blocages des comptes clients ou fournisseurs par des encodages frauduleux. Une rémunération est demandée pour débloquer les comptes.
- De l'utilisation de contrefaçons de jeux dans des sites nouvellement créés et liquidés dans la journée permettant de récupérer les mises sans payer les paris.
- Des opérations de « Phishing » et leur corollaire le « cukoo smurfing » (coucou), qui est une stratégie d'utilisation des comptes personnels de particuliers pour transférer des fonds.

Pour bien montrer l'implication criminelle de cette manipulation, dans l'un des cas identifiés, il s'agissait de transférer des fonds obtenus par la revente de drogue et par des escroqueries bancaires vers un pays de l'Est. Les fonds étaient regroupés dans une banque de l'hémisphère sud, éclatés entre une multitude de comptes particuliers, ils atteignaient ainsi le pays de destination. Une fois sur place, des étudiants locaux, chichement rémunérés, se servaient d'une entreprise de transfert de fonds pour les transmettre à leurs bénéficiaires. Donc, le blanchiment d'un montage relativement simple mettait en place trois méthodologies complexes différentes.

- Les données qui peuvent aussi être revendues à d'autres criminels, ainsi qu'à des gestionnaires de sites pornographiques. On connaît les liens entre la pornographie en général et la criminalité. Entrer dans un site de jeu, par curiosité ou pour jouer, peut conduire le jour suivant à trouver sa boîte inondée de spams à caractère pornographique et inversement. Il existe des liens déjà anciens entre ce type de sites, les sites de jeux et de paris et les activités criminelles.
- La distribution de sommes à des joueurs complices favorisée par l'absence de traçage, d'archivage des connexions et des mouvements financiers (fraude et blanchiment).
- Le camouflage de l'origine des sommes investies par le joueur. L'argent peut provenir d'un pays non coopératif, même si les mises proviennent d'un compte bancaire supportant une carte de paiement, rien ne dit que le joueur est le vrai propriétaire ou qu'il a gagné légitimement ces fonds. Ces derniers peuvent provenir d'une opération intermédiaire dans le processus de blanchiment. Les fonds illégaux (en espèces) sont en partie blanchis et sont investis sur place. Le Groupe d'action financière (GAFI), déjà, dans son rapport de 2001, avait souligné le risque de blanchiment lié à l'exploitation de casinos en ligne.

Internet et la contrefaçon

Le support de la vente sur Internet a permis aux criminels d'industrialiser, tout en la facilitant, la distribution des produits contrefaits. Ils utilisent leurs propres sites de vente directe, aussitôt disparus aussitôt reconstitués, dès qu'un risque se profile. Ils peuvent aussi se servir des sites d'enchères pour distribuer des produits sans attirer l'attention, eu égard à l'immensité du marché et au caractère individuel des échanges.

En effet, la structure très souple de certaines organisations articulées autour d'échanges rapides, peu ou pas contrôlés, entre clients et fournisseurs autorise toutes les dérives, qu'il s'agisse de contrefaçon ou de commerce clandestin. La plupart des sites de vente en ligne ont accepté le principe de précaution et effectuent désormais des contrôles en amont sur la qualité des articles mis en vente ainsi que sur l'identité des vendeurs. L'un d'entre eux, pourtant, se refuse à se soumettre aux condamnations essuyées sur ce point. Une telle structure, si elle n'effectue pas les contrôles *a minima*, constitue l'un des plus beaux supports de fraudes, de contrefaçon et de blanchiment en ne pratiquant pas les démarches préventives nécessaires ou en refusant de transmettre les informations demandées par les services de contrôle.

La criminalité maîtrise depuis l'origine, et fort bien, le développement du marché de la contrefaçon qui suppose des structures logistiques importantes, des investissements considérables et une organisation à la fois rigide – quasi militaire – et très flexible, car la réactivité, la capacité d'adaptation, la souplesse d'utilisation sont devenues des caractéristiques essentielles de la grande criminalité. Si le besoin de financement est considérable – mais la criminalité n'en manque pas – le retour sur investissement est à la hauteur de la mise. L'Internet lui donne l'opportunité de distribuer ses produits presque sans risque, lui offre un stade de blanchiment lucratif et peu contrôlé, parce que difficilement contrôlable, en raison de l'éclatement des opérations entre différents pays et de multiples structures, si le site n'est pas coopératif.

Internet et les corruptions

Les montages antiques de corruption dans les jeux et les paris ont été transposés sur Internet. Ceci est confirmé par une augmentation des mises dans des pays improbables sur des compétitions atypiques comme sur des événements connus. Corrélativement, une multiplication de cas de corruption dans les sports riches est constatée. En effet, toutes les manifestations sportives, sans exception, ont fait l'objet de tentatives ou de corruptions. Le principe utilisé est assez simple, il combine les manipulations physiques et celles qui relèvent de l'Internet. Pour corrompre dans le milieu sportif, il est nécessaire de disposer d'un support – un club, un site de bookmakers – et de corrompre des joueurs. Cela ne pose pas de problème puisque les fonds ne manquent jamais et la menace physique est toujours présente. Une fois propriétaire d'une structure ou installé dans un tel cadre, il est aisé de convaincre diverses mafias de s'impliquer sur ces paris. Lorsqu'elles n'ont pas elles-mêmes organisé les montages, elles se laissent facilement persuader. Des paris « gagnant/gagnant » sont ainsi organisés depuis le lieu dans lequel leurs fonds sont stockés, et portent sur des compétitions se tenant dans n'importe quelle autre région du monde, la distance ne joue pas.

Ainsi, au cours des trois dernières années, on a pu assister à des mises importantes depuis un pays asiatique vers une équipe de troisième division belge, aux paris de gros « investisseurs », depuis Hong Kong ou depuis l'Australie, sur des compétitions africaines. On a vu ainsi se déclencher une véritable bourrasque de paris sur le tennis qui n'ont été limités que par la mise en place de procédures très contrôlées dans les plus grands tournois.

Une information récente (12 mars 2008), parue sur le site *webdopoker*, évoque une attaque externe effectuée par des hackers d'un joueur régulier. Les sommes porteraient sur des milliers d'euros. « *Un joueur a commencé à perdre régulièrement, sauf lorsque sa main était très bonne (paire d'as). Cependant, dans ce cas, les autres joueurs* foldaient *systématiquement. S'il bluffait, il était systématiquement démasqué. Les ingénieurs qui ont analysé le cas se sont aperçus que le joueur avait reçu d'un autre compétiteur un logiciel de calcul de probabilité qui contenait un Troyen. Ainsi, chaque fois que la cible jouait au poker, son opposant recevait sur son écran la main de son adversaire.* » Le « hacking » se met donc au service des fraudeurs.

Il faut cependant noter que la connaissance de ces manipulations est possible grâce à Internet et à la masse documentaire informatisée qu'il génère. Ce sont les sites de paris honnêtes qui, les premiers, ont identifié les atypismes dans les mises à partir d'analyses fines des informations figurant dans les fichiers. Ainsi, tel Janus aux deux visages, Internet peut être la pire des choses si on laisse faire, et un très bon moyen de contrôle si on utilise la documentation que chacune de ses opérations génère en respectant évidemment les libertés individuelles et les procédures légales.

Noël PONS

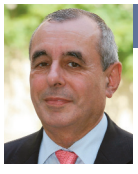
Internet et dérives sectaires

Henri-Pierre DEBORD

Le « phénomène sectaire », ensemble complexe de mouvements et de réseaux à caractère sectaire, trouve en Internet un formidable outil de promotion. Le Web devient ainsi un moyen d'amplification du risque de dérives sectaires et ce pour quatre raisons essentielles. C'est un moyen d'accélération de la mise en contact entre groupes et victimes potentielles. C'est un instrument déterminant pour le déroulement de la phase de séduction. De plus, il facilite la dilution de la menace. Et enfin, il complique considérablement l'exercice d'une vigilance par les pouvoirs publics.

The Internet and the Danger of Cults

The phenomenon of cults, complex movements and networks, has found a formidable tool with the internet. The web has become a means by which the danger of cults has increased, and for four reasons. The web speeds up the number of contacts between groups and potential victims. It is a powerful means of enticement. It also facilitates the spread of the threat. Finally, it complicates enormously the oversight of law enforcement agencies.



Henri-Pierre Debord

Fonctionnaire des Douanes, il débute comme contrôleur en 1975. En 1978, il rejoint l'École nationale des douanes en tant qu'inspecteur-élève. En 1987, il rejoint la direction du Léman comme chef divisionnaire, puis, en 1991, la direction nationale du Renseignement et des Enquêtes douanières (DNRED). En 1993, sur proposition du directeur général des Douanes, il est recruté par le ministère de la Justice pour se joindre à l'équipe de fondation du Service central de prévention de la corruption (SCPC). Conseiller de la MILS puis de la MIVILUDES (depuis Novembre 2002), en charge des questions économiques et financières, il y développe et met en œuvre des moyens de lutte contre les dérives sectaires. Il seconde également le Secrétaire général de la Mission.

Une part importante de la bataille qui oppose les États de droit aux mouvements et réseaux à caractère sectaire se joue sur Internet. L'enjeu est considérable. Au risque de ne pas effectuer un examen exhaustif des diverses zones de risques découlant de l'émergence de la menace sectaire sur le Web, il est possible de résumer cette menace en abordant trois niveaux d'analyse et de préoccupations.

Le premier niveau concerne, d'une part, le caractère séducteur des sites et, d'autre part, l'effet démultiplicateur de l'outil permettant d'augmenter considérablement les contacts avec des cibles potentielles.

Le second niveau est celui de la possibilité offerte par Internet aux créateurs de sites à finalité sectaire de présenter, de manière optimale, des projets, des prestations et des produits proposés, indépendamment du contexte d'organisation et de fonctionnement réel d'un mouvement ou d'un réseau, et donc, d'aménager de la meilleure façon possible leur irresponsabilité juridique.

Le troisième niveau, enfin, est celui du foisonnement de propositions mêlant quête de sens, développement personnel, bien-être, accomplissement de soi et management des hommes qui induit une dispersion du risque et une difficulté à déterminer celui-ci en l'absence d'une recherche plus large. En effet, seule cette recherche est à même d'attester de la cohérence d'action d'entités apparaissant distinctement sur la Toile.

Et, au-delà de ces trois niveaux de menace, une autre, plus pernicieuse se profile. Les organisations à caractère sectaire excellent dans l'usage de cette menace : il s'agit de l'exploitation de cet instrument unique de communication en vue d'entrer en conflit avec les institutions et les détracteurs.

Internet et l'effet démultiplicateur du risque sectaire

L'histoire du phénomène sectaire nous enseigne, tout d'abord, qu'il existe des constantes dans la chronologie des phases de développement des structures et organisations et dans la mise en œuvre de leurs modalités de fonctionnement.

La première étape consiste en la création, par le fondateur, d'un ou plusieurs « concepts ».

Cette étape de création est suivie de plus en plus fréquemment, et ce, très rapidement, par une deuxième phase consistant en la protection de ces concepts par des droits de propriété intellectuelle ou droits d'auteur auprès d'instituts nationaux et transnationaux de protection de la propriété intellectuelle. Cela représente un double avantage : celui de la protection de l'usage et celui d'une diffusion maîtrisée des messages et des propositions à destination des cibles potentielles.

Puis, vient l'étape de mise en place de processus de commercialisation associant conférences de promotion, séminaires, formations et développement d'un réseau de propagateurs ou de diffuseurs. Seuls quelques mouvements évitent cette étape en raison des fondements même de leur doctrine.

Dans le prolongement de cette dernière, correspondant à une diversification des activités, vient celle du cloisonnement des entités juridiques concourant à l'objet central du mouvement dans le but d'échapper, de manière optimale, à la vigilance des autorités administratives et judiciaires.

À ce titre, la connaissance de l'historique de mouvements et réseaux à caractères sectaires les plus anciens apporte de très riches enseignements sur leurs choix de protection et de préservation de leurs intérêts. Elle nous éclaire sur les instruments juridiques, commerciaux, informatiques qu'ils ont mis en place pour acquérir une opacité croissante et gêner, voire empêcher la détection des risques de dérives sectaires et l'application des lois et règlements. Toutes ces étapes sont repérables pour un analyste expérimenté. Avant comme après Internet, l'approche méthodologique reste la même.

Avant qu'Internet ne soit mis à contribution, l'étape de la présentation des concepts et, dans un deuxième temps, des pratiques et programmes d'activités et d'intégration se déroulait sous la forme de réunions d'informations, d'invitations à une première expérience de vie commune ou de conférences à l'issue desquelles une proposition de « premier engagement » était formulée.

Il peut s'agir de propositions émanant de mouvements à pratique « extra-mondaine » (communautés fermées), qui ont pour vocation de proposer une rupture physique avec l'environnement d'origine, de tenir un discours antisocial inaccessible aux enquêteurs par des moyens d'investigation classique, de formuler des exigences financières dans un but de don de soi au service de la communauté ou bien alors à vocation « intramondaine » comme le sont les mouvements psychothérapeutiques et psychologisants, ou encore les réseaux préconisant un

schéma totalisant de vie avec maintien de la personne dans la vie sociale.

Ces dérives interviennent sur le champ du développement personnel, de l'aspiration à s'accomplir humainement, socialement et professionnellement, ce qui induira des rejets non plus physiques, mais psychologiques, avec l'environnement d'origine, un discours institutionnel fondé sur la contestation des méthodes et pratiques validées et déontologiquement encadrées, et des exigences financières exorbitantes, liées à la nécessité d'acheter des prestations et produits en nombre croissant.

Avec l'utilisation d'Internet, les communautés fermées s'installent, la plupart du temps, dans une distanciation calculée, lorsqu'elles sont partie intégrante d'un réseau. Ainsi, le réseau prend en charge la présentation des « idéaux », de l'historique et des thèmes porteurs avec leurs produits et prestations associées. Quant à la communauté vers laquelle ont été guidés les « recruteurs webmestres », elle assure les phases de « séduction rétentrice » et de mise en situation de dépendance.

De leur côté, les mouvances « extra-mondaines » sont passées maîtres dans la diffusion de leurs propositions par l'intermédiaire de réseau de prestataires ou d'« adeptes professionnalisés », qui apparaissent sur la Toile, indépendamment de l'organisation en réseau elle-même. Cette dilution du risque est mise en place par des fournisseurs d'activités ou de solutions à des problèmes de vie personnelle, sociale et professionnelle.

L'internaute est donc face à un foisonnement d'offres à caractère « thérapeutique », « bien-être », « développement personnel », « accomplissement de soi », d'apparence associative ou commerciale classique, et il n'est pas en mesure de détecter le risque par des mots-clés « conceptuels » ou « doctrinaux », puisqu'il n'accède qu'aux mots-clés des praticiens. En apparence, les méthodes et pratiques proposées semblent s'inscrire dans une logique de transparence du marché du bien-être quand bien même pourrait apparaître quelque prétention à donner un sens « spiritualiste » ou « religieux » à l'éventail des propositions. Ainsi, la recherche par l'internaute de « mots-clés » comme « bien-être » ou « accomplissement de soi » s'avère fondamentalement et de manière croissante porteuse de risques en raison de la capacité des réseaux à caractère sectaire à se mouvoir dans la plupart des thèmes de société ou d'actualité, hors référencement conceptuel ou méthodologique propre dans les premières phases d'approche des personnes réceptives ou en recherche. De surcroît, l'usage de blogs ou de forums liés aux sites sensibles favorise la mise en contact d'apparence anodine avec le réseau porteur de risques.

Internet : un moyen idéal d'échapper à la vigilance

Le point de départ est la morcellisation du risque. Par la création de concepts et de méthodes nombreuses, quoique concourant au même objectif, celui de rendre des personnes dépendantes du système induit par la « consommation » de ces concepts et méthodes, l'organisation à caractère sectaire peut, grâce à Internet, approcher les futurs « adeptes consommateurs » de façon appropriée, presque individualisée, décuplant ainsi l'impact de la « phase de séduction » en favorisant l'enchaînement « séduction - séduction rétentrice ».

L'architecture la plus aboutie des organisations à caractère sectaire est fondée sur l'utilisation de copyrights et de droits d'auteur dont la gestion est centralisée et la diffusion décentralisée, et sur la recherche des « adeptes clients » ou « adeptes – consommateurs » par un marketing enseigné par les détenteurs de droits et mis en œuvre à l'aide du Web.

Il est ainsi de plus en plus fréquent d'observer et de détecter des cabinets libéraux ou associations assurant la promotion d'outils protégés liant donc ces cabinets à des propriétaires de droits d'exploitation de concepts, tout en cherchant à apparaître comme des travailleurs indépendants, professions libérales ou praticiens autonomes. La formidable diversité de leurs parcours personnels, l'hypothèse souvent confirmée d'une formation acquise auprès des formateurs liés à telle ou telle mouvance porteuse de risques, l'autoproclamation fréquente de leurs compétences et de la réussite assurée de leur pratique non validée ni soumise à examen critique pour validation sont des indices.

L'analyse impérative de sites Internet créés par les diffuseurs d'une même méthode, d'une même pratique et, en avant, leur repérage constituent les conditions *sine qua non* de la compréhension de facteurs de dépendance juridique et financière qui expliqueront, au fur et à mesure du déroulement de l'analyse de risque, la menace de dérives sectaires induite par la transmission de ces méthodes et pratiques.

Par ailleurs, l'appartenance durable d'un propagateur de risque à une même mouvance s'estompe au profit d'une pluri-appartenance en découlant, plus que d'une adhésion à des « principes », d'une dépendance contractuelle ou pseudo-contractuelle à l'égard de fournisseurs d'« opportunités commerciales » ou de méthodes d'« accomplissement de soi ».

Internet : un rempart favorable à l'expansion de la menace sectaire

À cette complication considérable des modalités de fonctionnement du sectarisme dans ses évolutions les plus récentes s'ajoute l'intervention de lobbies favorables, dits « pro-sectaires », dont la mission centrale est de contester le bien-fondé de l'action des pouvoirs publics et de faire écran entre « concepts » et « pratiques », en s'érigeant en défenseurs des « minorités spirituelles ».

L'exploitation par les groupes à caractère sectaire d'Internet, tant pour la propagation de leurs activités sensibles que pour la conduite d'une stratégie de plus en plus fine de communication fait, en effet, appel à la constitution de groupes « porte-parole » organisés juridiquement, indépendamment des mouvements et réseaux actifs. Leur moyen d'action est l'animation d'un site Internet offensif et « trompe-l'œil ».

Ainsi Internet diversifie les points d'impact du risque, dilue les responsabilités des organisateurs de ces réseaux porteurs de risques de dérives sectaires et favorise l'émergence de nouvelles zones de conflit entre mouvements organisés et États de droit. Les sites « conceptuels » valorisent un thème ; les sites « pratiques » ont la mission de développer la prise de contact et de retenir les personnes ; enfin, les sites « polémiques », véritables lobbies pro-sectaires se chargent d'attaquer les pouvoirs publics lorsque ceux-ci font preuve de clairvoyance et d'efficacité.

Un double front est en train de se constituer. Le premier concerne la montée en puissance du juridisme dans l'expansion du phénomène. Le second tient à la capacité des organisations à caractère sectaire, somme toute assez récente dans les faits, à contester le bien-fondé de l'action de l'État contre leurs agissements répréhensibles et les menaces sur les libertés individuelles que leurs activités induisent.

La montée en puissance du juridisme s'exprime de diverses façons. Internet en est l'un des révélateurs essentiels. En premier lieu, ce phénomène tient à l'accroissement exponentiel du nombre de concepts et méthodes protégés, soit par des droits d'auteurs (première étape), soit par des droits de marques ou autres droits de propriété intellectuelle (deuxième étape). Les produits et services porteurs de risques de dérives sectaires sont de plus en plus marchands, quoique certains types d'organisations restent attachés à des concepts non marchands, en apparence, ou compte tenu de leur profil typologique. La contestation de ces produits et services par des familles d'adeptes, observateurs des associations de défense des victimes ou des avocats, amène naturellement ces mêmes observateurs critiques à se référer à des biens matériels ou immatériels protégés. Qui plus est, ils peuvent faire l'objet d'une conservation confidentielle des mouvements et organisations en cause. Ceci peut conduire, et l'on peut le constater effectivement, à des conflits d'intérêt.

Concrètement, le fait qu'un intervenant critique à l'égard d'un mouvement publie des extraits d'écrits tels que des citations, des descriptions de concepts et pratiques, propriété de celui-ci ou d'un réseau à caractère sectaire, peut conduire à un conflit « commercial », voire à une procédure judiciaire. Ainsi, apparaît actuellement, dans le contexte de la lutte contre les dérives sectaires, la « procédure » d'arbitrage entre mouvement et victime et ce, notamment, en cas d'intervention des pouvoirs publics dans le conflit, dans le prolongement d'une plainte ou d'un signalement émanant de la victime ou d'un proche.

En second lieu, ces mêmes mouvements et réseaux ont de plus en plus recours à la procédure de « demande d'accès aux documents administratifs » et à celle de « plainte en diffamation ». La première démarche vise en particulier à faire reconnaître aux pouvoirs publics l'exploitation d'informations réellement ou prétendument protégées, et à révéler indirectement les sources des services sollicités au titre de cette procédure.

Aussi est-il déterminant de remarquer que nombre de décisions récentes de la Commission d'accès aux documents administratifs (CADA) viennent confirmer le bien-fondé du refus d'accéder à la demande, au nom de la sécurité des personnes ou de la sécurité publique.

Internet : un futur terrain de conflit entre mouvements, victimes et pouvoirs publics

La lutte contre les dérives sectaires s'avère être, on le voit, une tâche toujours plus délicate et complexe. Les mouvements à caractère sectaire ont un temps d'avance par rapport à tous ceux qui ont reçu mission de faire appliquer le droit et plus encore de détecter des zones de non-droit créées de toutes pièces par ces mouvements. Internet est le révélateur essentiel de cet état de fait et du « rapport de force » qui en découle.

Deux exemples permettent d'illustrer cette réalité. Le premier concerne l'usage du mot « Miviludes » par des

organisations sur lesquelles la mission interministérielle est amenée à porter son attention. L'objectif est d'apparaître le plus haut possible dans l'affichage des sites de référence à la fois pour détourner l'attention et pour gonfler artificiellement le volume des interrogations d'Internautes. Le second a trait à la souplesse infinie de cet outil de mise en relation pour constituer des blogs *ad hoc* ou des « annonces prétendument commerciales » ayant pour finalité d'établir un contact, d'engager le dialogue et de mettre en œuvre un processus d'« hameçonnage ». Le blog n'avoue pas immédiatement son origine et ses liens. Il en va de même pour le site d'annonces. Ils sont alors des lieux idéaux de recueils d'informations à caractère personnel quand bien même l'usage de pseudos offre de théoriques garanties.

D'aucuns considèrent que la partie est équilibrée entre organisations à caractère sectaire et pouvoirs publics. Il n'en est rien. L'accélération de la circulation de l'information liée à la liberté de créer, de déplacer ou de fermer des sites et forums rend la tache des pouvoirs publics de plus en plus délicate quand on sait la capacité des mouvements et réseaux à contacter de nouvelles « cibles humaines », puis à les prendre en charge en toute discrétion, hors des moyens de communication informatisés et des conférences et réunions publiques.

Néanmoins, et cela peut être un encouragement pour l'avenir, la prétention des mouvements à prendre le contrôle d'Internet en usant de l'arme juridique et de la menace est contrebalancée par les initiatives, d'une part, de détracteurs, quelquefois anciens membres, donc très au fait des stratégies de communication internes, et, d'autre part, des pouvoirs publics qui ont acquis un savoir-faire appréciable en matière de détection des évolutions de comportements sur la Toile des organisations présentant une menace sectaire.

Internet devient alors un terrain nouveau, sensible et essentiel d'investigation pour ceux qui ont la charge d'organiser et de coordonner la lutte contre les dérives sectaires.

Henri-Pierre DEBORD

Rumeurs et attaques informationnelles sur Internet

Franck BULINGE

Avec Internet, la rumeur semble avoir trouvé de nouvelles voies, formes et cibles, ainsi que des conséquences liées à la mondialisation des réseaux d'information. Cet article fait le point sur ce phénomène dans le domaine particulier de l'attaque d'image et la déstabilisation des entreprises.

Rumors and Information Attacks on the Internet

Is the rumor a reliable weapon which can be launched via Internet to strike a competitor? The aim of the article is to answer this question by defining the rumor and analyzing it in a context of hard competitive relationship between companies.

Franck Bulinge

Maître de conférences, docteur en science de l'information et chercheur au sein du laboratoire I3M de l'université de Toulon, Franck Bulinge est président et membre fondateur du réseau Analystes et Décideurs (An&D).

« *Les hoaxbusters ont constaté que régulièrement des personnes ou des sociétés étaient mises en cause nominativement dans les hoax. Compte tenu de la rapidité de la diffusion de l'information via Internet, un effet d'amplification est souvent constaté. Basé sur de fausses allégations, l'image des personnes ou des sociétés se détériore très rapidement. Les effets de cette désinformation peuvent être catastrophiques et avoir des répercussions sur la vie privée des personnes citées et sur l'image de marque des entreprises mises en cause...* » [1]. Telle serait, aujourd'hui, la problématique d'un phénomène qui n'est pourtant pas nouveau, la rumeur, mais qui, via Internet, semble avoir trouvé de nouvelles voies, de nouvelles formes, et de nouvelles cibles, ainsi que des conséquences liées à la mondialisation des réseaux d'information.

Un concept mal défini

Le Petit Robert [2000] définit la rumeur comme « *un bruit, une nouvelle de source incontrôlée qui se répand* », mais nous allons voir qu'en réalité il est difficile de s'accorder sur une définition précise de la rumeur.

Au fil de son histoire, l'expression semble changer de sens : le terme apparaît au XIII^e^ siècle pour désigner le « haro » que tout citoyen doit pousser pour signaler un délit ; au XVII^e^ siècle, elle désigne un bruit social incohérent ; au XVIII^e^ siècle, elle est un bruit émanant d'une lutte ou d'une sédition avant d'exprimer, le siècle suivant, la dénonciation publique ou la surprise devant un événement imprévu. C'est à la fin du XIX^e^ que la rumeur est liée à la notion de foule anonyme, et devient le bruit qui court, transmis par « le bouche à oreille ».

Durant la Seconde Guerre mondiale, les Américains Allport et Postman, s'inspirant des travaux de Louis William Stern [1902], définissent la rumeur comme « *une proposition liée aux événements du jour, destinée à être crue, colportée de personne en personne, d'habitude par le bouche à oreille, sans qu'il existe de données concrètes permettant de témoigner de son exactitude* » [1946]. Il convient de noter que cette approche s'inscrit dans le courant américain émanant de l'*Office of War Information*, très lié aux services secrets américains, qui présente la rumeur en opposition à l'information, dans un contexte de lutte contre la propagande et de guerre psychologique. À partir de la Seconde Guerre mondiale, on distingue ainsi deux sortes de rumeur : la rumeur littéraire qui décrit un phénomène lié à l'inconscient collectif (le bruit qui court, les légendes urbaines), et la rumeur instrumentalisée qui devient un moyen au service d'une stratégie, autrement dit une arme de guerre (le bruit qui tue).

Kapferer [1987] souligne qu'Allport et Postman n'étudient que les « fausses » rumeurs au détriment des aspects positifs du phénomène. Il ajoute qu'« *en réalité, c'est parce qu'elle peut se révéler exacte que la rumeur gêne* », alors que, selon lui, « *partout où le public veut comprendre mais ne reçoit pas de réponses officielles, il y a rumeur* ». Il ajoute que « *celle-ci est le marché noir de l'information* ». L'auteur donne alors sa propre définition de la rumeur qui est selon lui « l'*émergence et la circulation dans le corps social d'informations soit non encore confirmées publiquement par les sources officielles, soit démenties par celles-ci* » . Ce faisant, il introduit un rapport entre l'information et l'autorité politique considérée comme la source « officielle » de l'information. Dès lors, la rumeur devient un instrument de la révélation, un contre-pouvoir parfois opposé à l'information officielle.

Un cadre de recherche indispensable

Faute d'un consensus et d'une définition précise de la rumeur, on constate qu'à l'usage, le terme devient une sorte de concept fourre-tout, dans lequel se mélangent des phénomènes assez flous, liés à la manipulation de l'information en vue d'influencer l'opinion. De fait, il est difficile de distinguer clairement la rumeur de la propagande ou de la désinformation. Or, il est indispensable pour le chercheur de situer l'objet de sa recherche dans un cadre aussi précis que possible, sans toutefois se perdre dans des querelles sémantiques.

Afin de créer un cadre d'observation suffisamment stable d'un point de vue sémantique, nous entendrons le terme rumeur au sens plus général de « phénomène rumoral » que nous définissons comme une forme de communication de masse, qui se caractérise par la propagation d'informations vraies ou fausses, soit spontanément, soit à des fins instrumentales ou stratégiques (désinformation, subversion, démoralisation, déstabilisation...). Par la suite, nous utiliserons indifféremment l'un ou l'autre des termes, en distinguant au besoin la « pure rumeur », telle que la définissent les différents auteurs, dès lors qu'il en sera plus précisément question, du phénomène rumoral en général.

(1) http://www.hoaxbuster.com/hoaxcenter/dangers.php

Précisons également que l'objet de notre recherche porte plus particulièrement sur l'aspect instrumental et stratégique des phénomènes rumoraux, lesquels s'inscrivent dans le cadre plus large de ce que nous appelons les risques informationnels [Bulinge, 2002], auxquels doivent faire face les personnes physiques ou morales, dans le contexte politique, économique et social d'une société dite « de l'information ». Il en découle un parti pris que le lecteur devra garder en mémoire afin de resituer en permanence notre propos dans les limites contextuelles et expérimentales que nous nous sommes fixées.

Les bases psychologiques et sociales de la rumeur

Le phénomène rumoral, objet de notre recherche, repose sur des mécanismes psychologiques complexes, à la fois individuels et collectifs. Il s'inscrit dans un contexte plus global de manipulation, qui selon Philippe Breton [2000] joue à la fois sur les affects et sur la cognition. Dans le premier cas, le phénomène rumoral agit sur un registre émotionnel (peur, dégoût, colère, angoisse, humour...), alors que, dans le second, il influence l'objectivité de la cible, en jouant sur sa perception/analyse d'une situation.

Disons d'emblée qu'il est difficile de parler de victime dans le cas de la rumeur et des phénomènes rumoraux, car il apparaît qu'en réalité chacun s'en saisit librement, voire volontairement, parce que la rumeur répond généralement à une attente émotionnelle ou cognitive. Pour Kapferer [1987] : « l*a circulation de la rumeur est une succession de persuasions* », et pour que germe une rumeur, il faut un terreau fertilisé par l'opinion elle-même. La rumeur, lorsqu'elle germe (souvent de manière incontrôlable), s'inscrit instantanément et en profondeur dans un réceptacle de croyances, et c'est parce qu'on veut croire à la rumeur qu'elle se propage et qu'on devient soi-même propagateur, voire « jardinier » de la rumeur. L'exemple le plus typique de cette connivence face à la rumeur est ce qu'on appelle la théorie du complot, basée sur une culture paranoïaque qui facilite l'ancrage des croyances, les plus fondées comme les plus absurdes, induisant des raisonnements par inférences sophistiques (exemples : tel chanteur est mort, la preuve c'est qu'on ne le voit pas sur la pochette de son dernier album ; telle compagnie est accusée de faire travailler des enfants, la preuve, c'est que son démenti n'est pas convaincant...). Généralement, démentir la rumeur ne fait qu'amplifier le phénomène, parce qu'il le dramatise et multiplie le nombre de « récepteurs » qui sans cela, n'en auraient pas été informés.

Rumeur en haute mer

Lors de la guerre du Kosovo en 1999, le porte-avions Foch fut déployé en mer Adriatique durant quelques mois. Pour des raisons liées à la mise en œuvre opérationnelle du porte-avions nucléaire Charles de Gaulle, il fut décidé de tester l'équipage aux conditions de navigation de longue durée. Le Foch resta ainsi cinquante-trois jours sans toucher terre et les deux mille membres d'équipages se trouvèrent dans une situation de confinement et de stress particulièrement éprouvante. Pour pallier le manque de loisir, la télévision de bord diffusait en boucle des clips musicaux. Avec le temps, on entendait toujours les mêmes enregistrements, dont une série de chansons de Johnny Halliday, au point que l'équipage commença à se lasser. Au cours d'un repas au carré des officiers mariniers supérieurs, alors qu'un marin se plaignait de toujours entendre Johnny, un collègue affecté à l'état-major renseignement (lieu de concentration de l'information), répondit qu'il s'agissait d'un hommage suite au décès du chanteur. C'est ainsi que la rumeur se répandit, sur fond de censure des e-mails et de contrôle de l'information, et persista jusqu'au retour du navire en France.

Internet est-il un accélérateur de rumeur ?

Par l'intermédiaire du courrier électronique, des listes de diffusions et du Web, Internet permet de véhiculer une quantité vertigineuse d'informations. Cette surabondance pose le problème du choix, mais également du discernement et de la capacité de traitement. C'est sans doute à cause de cette infinité de choix que l'on pourrait percevoir *a priori* Internet comme un « accélérateur » de rumeur. On constate, de fait, un fort développement des « rumeurs électroniques », selon Emmanuel Taïeb [2002] qui souligne, au passage, l'identité de nature entre la rumeur et Internet. L'une comme l'autre obéissant à une « *nécessité de circulation* », Internet apparaît dès lors comme le véhicule idéal pour la diffusion des rumeurs. Pour Pascal Froissart [2002, a], « *Parce qu'Internet propose une orgie de textes dans tous les genres, parce que le réseau des réseaux semble gouverné par tout le monde ou personne, parce que n'importe qui se connecte à n'importe quoi, parce qu'aussi Internet est une mécanique complexe, on a pu dire qu'Internet était le médium rêvé de la rumeur* »

Le réseau mondial, ou Web, à travers les sites, blogs, Wiki, forums, listes, chats, permet d'émettre des hypothèses,

des théories qui peuvent être présentées, perçues ou interprétées comme des certitudes. « *Toute personne qui a une théorie possède maintenant un mégaphone* » [2]. Il est intéressant de noter que toutes les situations angoissantes ou de tensions mondiales peuvent susciter une vague de fantasmes sur Internet, lesquels se nourrissent et alimentent la théorie du complot. En ce sens, Internet ne fait qu'amplifier des états socio-psychologiques provoqués par les crises, lesquelles se caractérisent par une augmentation de l'état d'incertitude et des facteurs anxiogènes, très fertiles en termes de rumeur.

L'idée qu'Internet est un réseau anarchique où circulent des informations douteuses est communément répandue. Internet, identifié comme l'espace de toutes les dérives et de tous les dangers, est rapidement montré du doigt jusqu'à devenir l'emblème spectral de la manipulation des masses. Ainsi, Internet favoriserait la rumeur tandis que l'information fiable serait communiquée par d'autres médias.

Cette condamnation est-elle réellement fondée ? Ne cache-t-elle pas, dans certains cas, une réaction aux progrès des technologies de l'information et de la communication, face à la remise en cause possible du rôle prédominant de la presse en matière d'information ?

Il est certain qu'Internet offre des possibilités de trucages et de manipulation susceptibles d'engendrer la rumeur. Cependant, les autres médias, à commencer par la presse, sont-ils plus fiables ? Dans un contexte d'industrialisation de la presse, les journalistes n'apparaissent plus, aux yeux du public, comme les garants d'une information propre et fiable. L'information de presse, répondant à des critères économiques, tend à devenir uniforme. Dans certains cas, la rumeur franchit même la barrière déontologique des journalistes et se répand dans la presse.

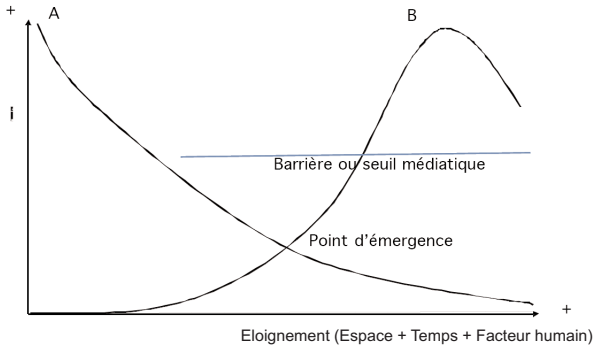
Pascal Froissart considère que, loin de se diffuser accidentellement via les médias, la rumeur « *se meut via les médias d'abord et avant tout* ». Cela serait d'autant plus vrai pour les rumeurs d'ordre économique qui n'ont de sens que lorsqu'elles touchent un public extrêmement ciblé (salles de marchés, actionnaires, décideurs...).

Le cycle de vie de la rumeur

Il semble qu'il existe une relation, d'une part, entre la fiabilité de l'information représentée par la courbe A dans le schéma ci-dessous, et le niveau de propagation de la rumeur, et, d'autre part, entre ce niveau de propagation et le franchissement d'un seuil médiatique au-delà duquel la presse transmet elle aussi la rumeur.

La courbe A illustre le fait que plus nous nous éloignons de la source d'information (témoin direct), plus celle-ci devient invérifiable et, par conséquent, peu fiable. La rumeur, dont le cycle de vie est représenté par la courbe B, germerait dans cet état de flou informationnel, au moment où l'information devenue invérifiable mais suffisamment vraisemblable devient un facteur de lien social, sous forme d'un événement informationnel soudain digne d'être repris, porté et partagé par une chaîne d'acteurs. Kapferer cite Shibunati [1966] pour qui la rumeur trouve son origine dans l'interrelation entre l'importance et l'ambiguïté d'un événement : « *si son importance est nulle ou si l'événement n'est pas du tout ambigu, il n'y aura pas de rumeur* » [Kapferer, 1987].

Dès lors la rumeur prend vie et forme, grandit, s'enrichit, jusqu'à atteindre un niveau de maturité, puis entame une phase de déclin, sans qu'il soit possible de dire si elle meurt véritablement ou si elle couve comme le feu sous la cendre, ce que semblent confirmer les chercheurs qui observent un phénomène de récurrence / résurgence. Sur ce point, Internet favorise la remémoration des rumeurs qui, une fois émises sur la toile, sont stockées et accessibles sans limite dans le temps.



(2) « Anybody With a Theory Now Has a Megaphone », USA Today, 18 septembre 1996, cité in Campion-Vincent (V.), Renard (J-B.), 2002, *De Source sûre, Nouvelles rumeurs d'aujourd'hui*, Paris, Payot.

Typologie des rumeurs sur Internet

Il est nécessaire, à ce stade, d'esquisser brièvement une typologie des différents types de rumeurs que l'on peut rencontrer sur Internet. Si l'on se réfère à la typologie de Campion-Vincent et Renard [2002], on peut distinguer sept types de messages « rumoraux » : les alertes aux virus informatiques, les chaînes magiques ou superstitieuses, les chaînes de solidarité, les pétitions, les rumeurs proprement dites ou canulars, les légendes urbaines, les histoires drôles, et les photos ou dessins humoristiques. De son côté, Heiderich [2004], outre les légendes urbaines, distingue la désinformation à but commercial, l'attaque politique, l'attaque directe d'une offre commerciale, les fausses offres commerciales, la désinformation financière, la diffamation, les opérations de décrédibilisation, l'alerte panique pour semer la terreur... Les deux auteurs résument assez bien les deux facettes de la rumeur, littéraire d'un côté, et instrumentalisée de l'autre. C'est, bien entendu, le second qui nous intéresse ici.

La prophétie du 11 septembre 2001

Un très bon exemple de rumeur circule depuis les attentats du 11 septembre 2001. Il s'agit de la conversion alphabétique d'une soi-disant immatriculation d'un des appareils qui a percuté le WTD. Le message invite le lecteur à convertir Q33 NY en alphabet windings sur Word. Cela donne :

Q33 NY = ✈▤▤ ☠✡

La démonstration est stupéfiante, et la plupart des individus réagissent « positivement » en transmettant le message à leurs amis. Ici, les éléments de manipulation sont concentrés dans l'expression graphique et la symbolique qui s'en dégage. Dans cet exemple, on associe un fond d'antisémitisme historiquement très fertile (voir le mythe du Protocole des sages de Sion), à des affects liés au drame, l'ensemble se renforçant mutuellement au point de faire oublier la question essentielle : à aucun moment, les « victimes » de ce hoax s'interrogent sur la réalité de cette immatriculation. L'esprit critique est inhibé et l'ancrage renforcé par un effet de répétition / massification dû à la propagation rumorale. Au final, il devient évident qu'un mystère plane sur le 11 septembre, mais ce mystère est, en réalité, une construction collective, un mythe qui s'inscrit désormais dans la mémoire de l'humanité, et deviendra régulièrement le lieu d'émergence de nouvelles rumeurs.

La rumeur, arme de guerre économique ?

Dans le domaine économique, la compétition exacerbée à laquelle se livrent les entreprises, mais également certains États, a donné lieu à une littérature qui s'attache à illustrer le concept de guerre économique, notamment à travers l'étude des rumeurs instrumentalisées. On parle ainsi d'attaque par la rumeur, où la rumeur serait utilisée comme une arme et deviendrait un outil stratégique utilisé pour survivre face aux exigences de compétitivité du marché mondial. Dans le cadre de la compétition qui oppose Airbus et Boeing, on note ainsi qu'Airbus est régulièrement taxé de problèmes de mécaniques, de commandes de vol approximatives, de « dumping », de détester les pilotes de certains pays, etc. [Heiderich, 2004].

En l'absence d'un cadre sémantique stable, il est cependant difficile de définir avec précision le terme d'attaque par la rumeur, c'est pourquoi nous lui préférons le terme plus général d'attaque informationnelle de type rumoral, définit comme un phénomène rumoral visant à nuire intentionnellement à une entité identifiable (personne physique ou morale, marque, technologie, etc.), ou à ses intérêts, et ce, quelles que soient les motivations qui fondent l'intention de son auteur.

La question stratégique

Le concept d'attaque informationnelle rumorale pose un certain nombre de questions, notamment celle de l'objectif stratégique visé, le ciblage de l'attaque, la stratégie et les techniques adoptées.

Les objectifs stratégiques

On peut supposer, au regard de la littérature de la guerre économique, qu'ils visent l'affaiblissement de l'adversaire (à défaut de l'anéantir), selon deux voies :

- la déstabilisation qui vise à casser la dynamique interne de l'entreprise par la mise en doute et l'injection virale de facteurs anxiogènes (les militaires appellent cela une atteinte au moral des troupes) ;

- l'atteinte à l'image qui vise à affaiblir la relation client ; c'est, en quelque sorte, une démarche de contre-marketing.

Dans les deux cas, l'attaque vise l'émergence d'une crise informationnelle centrée sur l'entreprise, qui entraîne de fait une consommation d'énergie pénalisante.

Le ciblage de l'attaque

En fonction des objectifs stratégiques, l'attaque peut viser deux types de cibles : l'opinion publique qui constitue l'ensemble des consommateurs/clients, ou les « stakeholders » (parties prenantes) qui participent à la gouvernance de l'entreprise. Selon le cas, la rumeur ne véhiculera pas les mêmes informations : dans un cas, il s'agira, par exemple, de détourner les consommateurs d'une marque (boycott), dans l'autre de semer le trouble parmi les employés, ou ternir l'image d'un dirigeant, ou d'influencer les actionnaires.

Les techniques

Généralement, dans le premier cas, l'attaque informationnelle restera au niveau d'Internet parce qu'elle vise un public large et facile à duper. Les techniques employées seront celles liées à la manipulation des affects (émotions, sentiments). Ce sont notamment les légendes urbaines (peurs, angoisses primaires), les hoax (curiosité, sensationnel), le détournement de logo et les fausses publicités (humour, dérision).

Dans le cas des attaques visant la manipulation des stakeholders, les techniques viseront essentiellement la manipulation cognitive, via la désinformation, en vue de court-circuiter la capacité d'analyse rationnelle des acteurs, au profit d'une perception biaisée de la réalité. Le succès de ce type de manipulation repose sur les tensions qui résultent de la compétition économique, et qui entraînent des états de moindre vigilance chez les spécialistes eux-mêmes. Il n'est pas rare de voir les journaux économiques et financiers publier des rumeurs parce qu'elles activent des réflexes cognitifs (heuristiques) liés à une perception erronée de l'urgence et de la gravité d'une situation.

Une idée reçue pourrait laisser penser que le manque d'éducation est un facteur de vulnérabilité, or il n'en est rien. Au contraire, selon Froissart [2002, b], « *l'intelligentsia est bien plus sensible à la rumeur que le reste de la population* » et « *non seulement les milieux aisés sont ceux où l'on consomme davantage d'informations médiatiques, mais en plus ils sont les plus "connaisseurs" de rumeurs* ».

Deux études de cas

Nous avons choisi deux exemples de phénomènes rumoraux liés à des entreprises. Précisons, au passage, que les exemples ne sont pas aussi nombreux que semble le laisser penser la littérature.

La rumeur de Procter & Gamble

Cet exemple de pure rumeur est aujourd'hui un classique du genre. Depuis 1981, selon Kapferer, et même depuis les années 1960 selon certains sites, Procter & Gamble est accusée de pactiser avec le diable, comme le prouverait son logo qui comporterait plusieurs symboles sataniques. Le président de P&G aurait même déclaré au cours d'un talk-show qu'il versait une partie des bénéfices de l'entreprise à l'Église de Satan. En 2005, alors que P&G négociait la fusion avec la société Gillette, un collectif de chrétiens américains tentait de s'opposer à l'opération auprès du département d'État. L'exemple est intéressant non seulement parce qu'il traite d'une pure rumeur, mais également parce que cette rumeur est récurrente dans un laps de temps assez long, et bien avant qu'Internet n'existe.

On notera, certes, que la rumeur resurgit sur la Toile à un moment critique de la vie de l'entreprise et que le mouvement déclenché vise apparemment à influencer le département d'État. Pour autant, l'origine de cette attaque semble clairement identifiée, puisqu'il s'agirait, selon Kapferer, d'une communauté de religieux fondamentalistes, connue sous le nom de *Bible Belt*, dont les pasteurs sont connus pour leur intégrisme moyenâgeux et notamment leur rejet à l'égard de la société de consommation.

L'attaque informationnelle contre Areva

Areva est régulièrement la cible d'attaques informationnelles. C'est d'autant moins surprenant que l'entreprise développe son activité dans le secteur nucléaire, très fertile en facteurs rumoraux. La palette des effets est assez complète, entre la peur que suscite le nucléaire, la désinformation dont ce secteur est l'objet, le secret et l'opacité qui entourent cette activité et, bien entendu, l'activisme dont font preuve les opposants au nucléaire, chacun des acteurs étant passé maître en matière de manipulation. Areva apparaît, de fait, comme une cible idéale, et son existence est par nature, intimement liée au phénomène de rumeur.

En avril 2007, lors d'une conférence de presse organisée par la CRIIRAD [3] et Médecins du Monde, Areva est accusée de polluer l'eau d'un village nigérien proche d'une mine d'uranium que l'entreprise exploite. Dès lors, se déclenche un phénomène rumoral, qui se traduit par la propagation d'un corpus informationnel où il est notamment question de la mort d'un certain nombre de personnes, par ailleurs, non dénombrées et non identifiées, suite à une exposition prolongée à la radioactivité des mines d'uranium proches.

La trame rumorale repose ici sur l'utilisation d'informations dont on connaît en partie l'origine (CRIIRAD), et sur les sentiments de colère et de révolte que suscite immédiatement la perception du contraste entre la toute puissance présumée d'Areva, qui serait indifférente à la santé des populations, et ces dernières qui subiraient les conséquences désastreuses de l'exploitation de leur sous-sol. En seulement trois jours sur Internet, et sur cette extrême schématisation, une toile d'information se tisse autour de l'entreprise, entre les organisations accusatrices, les sites prenant le relais, suivis de la presse et, en toile de fond, les opposants traditionnels au nucléaire.

Areva réagit immédiatement en annonçant la création d'un observatoire de la santé, et apporte des éléments d'informations censés rétablir de manière rationnelle un fond de vérité. Pour autant, l'attaque a bien eu lieu et restera définitivement sur la toile, comme tâche indélébile.

Il est intéressant de noter, là encore, que cette « attaque » s'inscrit opportunément dans le cadre d'une bataille qui oppose, à cette époque, Areva aux entreprises chinoises, canadiennes et australiennes, pour ne citer qu'elles, alors que le gouvernement nigérien s'apprête à prononcer la fin du monopole d'Areva dans la région et à redistribuer les concessions. Faut-il en conclure qu'il existe un lien entre la rumeur lancée contre Areva et le contexte dans lequel elle s'inscrit ? Bien que tentante, cette conclusion ne repose sur aucune donnée factuelle, si ce n'est la concordance chronologique des événements. S'agit-il d'une attaque informationnelle s'inscrivant dans une stratégie générale d'atteinte à l'image en vue de peser sur les négociations en cours ? Ou bien la CRIIRAD a-t-elle profité de la situation stratégique pour médiatiser cette affaire, en s'appuyant au même moment sur le succès du Défi Areva dans l'*America's Cup* ? La situation est complexe et il est difficile de trancher, d'autant que deux ans plus tôt, la même accusation avait eu lieu de la part des mêmes acteurs. On est ici réduit à des conjectures, à des hypothèses qu'il conviendrait de confirmer avant d'émettre une quelconque conclusion. Seules Areva et la CRIIRAD connaissent la vérité, mais ce qui est sûr, c'est que la concordance des événements ne suffit pas à constituer la preuve d'une stratégie délibérée. Toute conviction exprimée dans ce domaine, fondée sur ces seules conjectures, relèverait de la désinformation.

Les limites du concept d'attaque rumorale

Rumeur et phénomène rumoral reposent sur une propagation de type « réaction en chaîne » dont on ne peut prévoir le développement et connaître par avance les effets. Cela est d'autant plus vrai que les rumeurs émergent dans des situations à la fois complexes et chaotiques, où l'entropie l'emporte sur la cohérence informationnelle.

De fait, on peut poser la question de la pertinence du terme « attaque rumorale » puisqu'il revient à évoquer un phénomène de propagation instrumenté (par exemple : désinformation, hoax, marketing viral), qui suppose une origine, une cible et un contenu informationnel. Or, dans les deux cas, et si l'on fait l'analogie avec une arme, on n'est jamais sûr d'atteindre la cible et de surcroît, on ne connaît ni ne contrôle son pouvoir de nuisance, et encore moins ses effets secondaires ou collatéraux. Ainsi une attaque par la rumeur peut-elle être aussi bien une bombe dévastatrice qu'un pétard mouillé, voire un boomerang. Dans le cas de P&G ou d'Areva, la rumeur entraîne la mobilisation d'une équipe de gestion de crise, certes coûteuse, mais il ne semble pas qu'elle ait nui en profondeur au développement de ces entreprises. On peut dès lors avancer, faute d'exemple précis, que la rumeur ne constitue pas une arme létale dans l'arsenal de la compétition *versus* guerre économique.

Conclusion

Il semble intéressant de resituer l'étude des rumeurs dans un contexte plus général, et d'en mesurer les enjeux et la portée réels. Considérant le nombre d'attaques informationnelles rumorales visant les entreprises, au regard de leur nombre et du volume d'activité concurrentielle, il semble que le phénomène soit relativement limité. De fait, la recherche sur les phénomènes rumoraux, dans le domaine de l'intelligence économique, doit éviter deux écueils : celui d'une focalisation excessive (effet de

(3) Commission de recherche et d'information indépendante sur la radioactivité.

loupe), au risque de lui donner une ampleur illusoire, voire trompeuse ; et celui d'une dramatisation qui donnerait à la rumeur et aux phénomènes rumoraux une importance qu'en réalité ils n'ont pas.

Une autre question se pose, celle de l'intérêt de rechercher l'origine de la rumeur, qui, dans le contexte de la maîtrise des risques informationnels, apparaît comme un faux problème puisqu'une fois la rumeur en circulation, la priorité n'est pas de rechercher le pyromane, mais de gérer l'incendie. Ceci est d'autant plus vrai qu'il est hasardeux de vouloir attribuer coûte que coûte une source et une intention à la rumeur, qui selon Kapferer est « *le plus souvent une production sociale spontanée* », lequel ajoute que « *le mythe de la source tapie en stratège persiste intensément, car il est à la fois agréable et utile* [...] *il nous plonge dès la moindre rumeur dans l'univers imaginaire du complot, de la manipulation, de la désinformation, de la guerre économique et politique* ».

L'analogie aux feux de forêts conduit à évoquer un dernier problème, celui des pompiers pyromanes fascinés par la guerre économique, qui tentent de créer des rumeurs pour « voir ce que ça fait ». Cette année, un concours de rumeur a même été lancé au profit des étudiants en intelligence économique... Il est heureux qu'une réaction en chaîne rumorale ne s'obtienne pas aussi aisément que voudraient le laisser croire d'obscurs apprentis sorciers, mais cela reste tout de même inquiétant, ne serait-ce que d'un point de vue déontologique. À croire que le vrai danger de la rumeur serait de nous placer face à nos propres ambiguïtés, au point d'en perdre notre bon sens collectif, quand ce n'est pas la raison.

Franck BULINGE

Bibliographie

Akoun (A.), « Rumeur », *Encyclopedia Universalis*, DVD-ROM version 7.

Allport (G.W.), Postman (L.), 1946, «An Analysis of Rumor», *Public Opinion Quaterly*, 10, Winter 1946-1947, p. 501-517.

Breton (P.), 2000, *La parole manipulée*, Paris, La Découverte.

Bulinge (F.), 2002, *Pour une culture de l'information dans les petites et moyennes organisations : un modèle incrémental d'intelligence économique*, thèse pour le doctorat en sciences de l'information et de la communication, université du Sud, Toulon, Var.

Campion-Vincent (V.), Renard (J.-B.), 2002, *De source sûre. Nouvelles rumeurs d'aujourd'hui*, Paris, Payot.

Froissart (P.), 2002a, « Rumeurs sur Internet », *in Les Cahiers de Médiologie*, 13, p 27-35.

Froissart (P.), 2002b, *La rumeur sur Internet, Histoire et fantasmes*, Paris, Belin, coll. « Débats ».

Heiderich (D.), 2004, *Rumeurs sur Internet*, Paris, Village Mondial.

Kapferer (J.-N.), 1987, *Rumeurs. Le plus vieux média du monde*, Paris, Seuil coll. « points ».

Shibunati (T.), 1966, *Improvised News : A sociological Study of Rumor*, Indianapolis, Bobbs Merill.

Taïeb (E.), 2003, « Des rumeurs de guerre et de quelques rumeurs après le 11 septembre », *Quaderni*, n° 49 & 50.

Webographie

www.hoaxbuster.com : le site français sur les rumeurs, les chaînes, les pétitions, les parodies circulant sur le Net.

Cybercriminalité identitaire

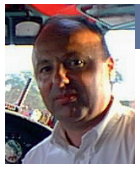
Christophe NAUDIN

© Fotosearch

La cybercriminalité identitaire est désormais l'une des infractions qui connaît une forte croissance mondiale. Elle s'appuie sur l'anonymat procuré par les technologies numériques. Tous les états occidentaux sont touchés par ce phénomène criminel, lequel déstabilise fortement le fonctionnement de la société. Deux solutions existent : la biométrie et la signature électronique.

Identity Theft

The cybercrime of identity has become one of the fastest growing in today's world. It relies on digital technologies that provide anonymity. All Western countries have been hit by this kind of criminal phenomenon, destabilizing the functioning of society. Two solutions exist: biometrics and digital signatures.



Christophe Naudin

Chercheur au Département de recherche sur les menaces criminelles contemporaines (DRMCC), Université Paris II, et à l'Observatoire géopolitique des espaces nationaux et internationaux (OGENI), université Paris IV, Christophe Naudin est aussi formateur au Service de coopération technique internationale de police (SCTIP) et consultant international, spécialiste de la sûreté du transport aérien ainsi que de la fraude documentaire.

Dans le monde virtuel, l'identité n'est pas encore attribuée par l'autorité publique. Certains n'ont pas oublié d'en profiter...

Les hors-la-loi ont presque toujours eu le souci de se dissimuler aux yeux des autres. Chacun se souvient évidemment de l'histoire d'*El Zorro* [1], un bandit masqué de Californie, qui prenait fait et causes pour le peuple, contre l'occupant militaire espagnol. L'histoire a été romancée et embellie par la télévision, mais l'existence de Zorro est avérée. Plus tard, *desperados* et *gringos* nord-américains nouaient un foulard de *cow-boy* sur le bas de leur visage, non pas pour éviter de respirer la poussière soulevée par le bétail, mais pour ne pas être reconnus ou poursuivis par une justice locale très expéditive. Bien que nous disposions aujourd'hui de moyens techniques beaucoup plus performants, comme la vidéosurveillance à reconnaissance faciale, les meilleures méthodes criminelles subsistent. Ainsi, après l'époque des braqueurs recouverts d'un bas sur la tête, après le « gang des postiches [2]», les conférences de presse corses en cagoule, les sweat-shirts à capuche complètent désormais le parfait uniforme du délinquant moyen de nos cités sensibles. Pas seulement ! Car depuis vingt ans, l'ordinateur est le nouveau masque de Zorro. Quoi de plus anonyme en principe qu'une machine, qui opère à distance pour escroquer, tromper, usurper en toute impunité ? Si la criminalité identitaire est à la jonction de tous les trafics, la cybercriminalité identitaire est une nouvelle menace à laquelle il convient désormais de réfléchir. Du masque de Zorro à l'adresse IP aléatoire l'objectif reste le même : dissimuler ses activités criminelles...

L'état-civil d'un internaute

Depuis l'apparition de l'état-civil dans les pays de tradition judéo-chrétienne, le nom patronymique est attribué à chaque personne à sa naissance, soit de manière autoritaire (jusqu'à présent par la seule filiation paternelle), soit sous le contrôle étroit de l'administration. Nul ne peut s'attribuer à lui-même une identité complète reconnue des autorités publiques.

Dans le monde virtuel, les attributs de la personnalité sont libres de choix sans que l'administration vienne s'y intéresser. Chaque personne désireuse d'accéder à Internet doit se créer une ou plusieurs adresses personnelles permettant d'être destinataire des informations qui la concerne. Or, ces adresses peuvent varier en fonction de nombreux facteurs : le fournisseur d'accès, et la façon dont la personne souhaitera elle-même être identifiée. En ce sens, la plus grande liberté est laissée aux internautes qui choisissent eux-mêmes les attributs de leur identification, soit un nom suivi de la lettre @ et du fournisseur d'accès ou du propriétaire d'un nom de domaine, soit une suite numérique mnémotechnique.

- Jean.dupont@wanadoo.fr
- chnaudin@drmcc.org
- 55254A74F@hotmail.com
- etc.

Chaque internaute décide de lui-même de la naissance d'une adresse d'identification, mais aussi de la fin de son utilisation. La Commission nationale de l'informatique et des libertés (CNIL), a qualifié en 2006 l'adresse électronique de donnée à caractère personnel identifiant de manière effective des individus personnes physiques. En effet, il circule dans les courriels des informations à caractère personnel, qui sont du ressort de la vie privée. Les intercepter serait une atteinte à la vie privée comme l'article 226-1 du Code pénal en dispose.

Dès lors, il est possible, et peut-être tentant, de se créer de nombreux identifiants. Ces nouveaux identifiants se trouvent à mi-chemin entre l'identité réelle et le nom de fantaisie, librement choisi par une personne physique dans l'exercice d'une activité particulière afin de dissimuler au public son nom véritable. Les internautes recourent donc régulièrement aux pseudonymes, se constituant ainsi un nombre important d'identifiants numériques, c'est-à-dire autant d'identités différentes, ce qui leur permet de segmenter leurs activités personnelles, (professionnelles, privées, associatives, etc.), mais aussi se libérer des contraintes

(1) *El Zorro* : le renard en espagnol, signifiant également le rusé. À cette époque, la Californie est encore sous la coupe de la couronne d'Espagne qui espère récupérer du jeune gouvernement américain un tiers des terres sauvages (du Mexique jusqu'à l'État actuel du Montana – Montañas). À son retour d'Europe, Don Diego de la Vega découvre un Los Angeles tyrannisé par l'armée espagnole. Il décide alors de devenir Zorro le justicier masqué, afin de soulager le peuple des abus d'une gestion militaire.

(2) Tourancheau (P.), 2004, *Les Postiches. Un gang des années 80*, Paris, Fayard, 310 p. Le gang des postiches est une célèbre équipe de braqueurs qui opéra à Paris entre 1981 et 1986. Ils s'attaquèrent à une trentaine de banques avec une rare audace. Ils entraient tout simplement dans l'agence, habillés en bourgeois et portant des perruques et de fausses moustaches ou barbes, d'où leur nom.

des fournisseurs d'accès peu respectueux des clauses contractuelles [3] qui les lient à leurs clients. Aucune limitation technique ni juridique n'existe à cet égard et il se crée parfois même autant de personnalités qu'il y a d'identifiants.

La forme ludique de la fausse identité numérique, c'est le pseudonyme, cultivé désormais par chacun de nous. Et c'est bien pratique, d'autant que c'est également parfaitement légal ! Notamment sur les sites de rencontres ou les forums d'opinions, au sein desquels le dialogue peut être plus direct sans les arrière-pensées que la bienséance, l'honneur ou l'éducation nous interdisent généralement.

La naissance de la cybercriminalité identitaire

En matière criminelle, comme on l'imagine, l'adresse mail n'est donc pas une barrière à la dissimulation de ses activités. La forme criminelle de la fausse identité numérique consiste à user d'identités fictives, ou à récupérer, par tout moyen technique, le mot de passe ou le code personnel d'une personne, ses coordonnées bancaires, des informations numériques personnelles, aux fins de commettre une infraction pénale.

La seule identification effective sur Internet est l'adresse de chaque machine connectée au réseau, dite adresse IP (*Internet Protocol)*, constituée d'une suite numérique qui permet, en principe, de situer géographiquement une machine dans un pays. C'est là la première faille du système, rapidement découverte par les cyberdélinquants qui usent désormais de générateurs aléatoires d'adresses IP qui leur permettent de changer d'adresse en permanence et d'éviter ainsi d'être repérés trop précisément. Bien entendu, il existe déjà de nombreux précédents au cours desquels les infractions sont constatées, sans que leurs auteurs puissent être poursuivis. Sans utiliser de techniques trop complexes et risquer d'éveiller les soupçons d'enquêteurs, la méthode la plus simple consiste à opérer d'un cybercafé et de se livrer anonymement à ses activités depuis un poste appartenant à un tiers dupe, avec une adresse IP fixe.

Richard Reid 21 décembre 2001 Terrorisme

L'un des exemples les plus intéressants en ce sens est celui de Richard Reid [4], alias Abdel Rahim, alias Abdul Rauff, qui a tenté d'embarquer le 21 décembre 2001 à bord du vol American Airlines AA063 avec des chaussures piégées. Alors qu'il était refoulé par le contrôle de sûreté pour un problème de passeport, il s'est rendu dans un cybercafé parisien du 18e arrondissement de Paris, a contacté ses donneurs d'ordre par mail en leur précisant qu'il n'avait pas pu embarquer. Ces derniers lui ont alors répondu aussitôt de retenter d'embarquer le lendemain, ce qu'il a fait le 22 décembre 2001. Chacun connaît la suite de l'histoire. À l'époque, la direction de la Surveillance du territoire [5], en charge de l'enquête française, avait fait le maximum pour identifier le donneur d'ordre à partir de son adresse, sans pouvoir réussir à le faire.

Facebook et le roi du Maroc Usurpation d'identité

Fouad Mourtada, un jeune informaticien marocain de 26 ans, a créé, le 15 janvier 2008, un profil sur le site *Facebook* [6] dans lequel il se fait passer pour le frère du roi du Maroc. C'est évident, les propositions des plus jolies filles du monde entier ont abondé rapidement, et notre ami Fouad jusque-là considéré comme un garçon insignifiant, s'est instantanément transformé en un apollon sans égal. Cette cybermétamorphose lui a permis de passer quelques agréables soirées, le temps que les soupirantes réalisent, trop tard, l'étroitesse d'envergure financière du frère du roi du Maroc, alors que ces dernières avaient déjà payé rubis sur l'ongle, de leur propre corps. Seul le roi Mohammed VI n'a pas goûté la plaisanterie de potache. Fouad a été arrêté le 5 février 2008 et condamné le 22 du même mois à trois ans de prison. Un bel exemple destiné à refroidir les ardeurs de ceux qui trouvent amusant d'usurper l'identité de quelqu'un sur Internet. Pour sa défense, Fouad a plaidé : « *Je pensais que cela ferait prendre conscience à notre gouvernement que Facebook pourrait être un bon moyen de communication pour le cabinet royal, pour être plus proche du peuple comme le font déjà Barack Obama ou le maire de Paris par exemple* ». De tels exemples d'usurpation d'identité sont plus fréquents qu'on ne l'imagine, et causent de réels préjudices aux victimes.

(3) Fréquentes interruptions de services pendant des durées indéterminées, alors que le paiement de la prestation s'effectue par avance. C'est le cas de la société Noos Numéricable qui a été condamnée le 16 septembre 2008 par le tribunal correctionnel de Meaux à 150 000 € d'amende pour publicité mensongère et non-respect de ses engagements.

(4) Naudin (C.), 2005, *Alias*, Paris, Éditions de la Table Ronde, 218 p.

(5) Depuis le 1er juillet 2008, un service de renseignement intérieur unique a été créé : la direction centrale du renseignement intérieur (DCRI).

(6) www.facebook.com

Cybervengeance

En 2006, Lori Drew, une mère de famille de 49 ans, souhaite se venger d'une jeune fille de 13 ans, avec laquelle sa propre fille s'est disputée [7]. Sachant que les adolescentes sont des adeptes du site de socialisation et de rencontres *MySpace*, elle décide, avec quelques autres adultes, de créer le profil d'un garçon de 16 ans, baptisé « Josh ». La jeune voisine tombe dans le panneau. Lori Drew et ses complices multiplient mots doux, compliments et rencontres virtuelles. Le flirt dure trois semaines. Mais brutalement, Lori Drew et ses complices décident de mettre un terme à la relation et envoient un message à l'adolescente. Le garçon imaginaire lui dit que tout le monde se porterait mieux sans elle. Le canular se termine de façon dramatique : une heure plus tard, la jeune fille se pend dans sa chambre. Sur *MySpace*, le profil de « Josh » est rapidement effacé par la mère de famille. Lori Drew a été inculpée pour son rôle dans ce tragique canular, accusée de « complot et accès sans autorisation au réseau de *MySpace* dans le but d'infliger une souffrance émotionnelle à la jeune fille. »

Identités fictives et Spam nigérians

De nombreux spams envahissent aujourd'hui nos machines avec des propositions, venant généralement d'Afrique, d'hébergement de ressources bancaires considérables, en attendant qu'elles puissent être transférées. Ce sont les fameux spams nigérians ou spam 234 [8].

Les techniques diffèrent : vous pouvez être le gagnant d'une tombola miraculeuse, ou être contacté par le dernier proche parent de l'ex-président Mobutu, désireux de rapatrier sa fortune en Europe via votre compte bancaire. En jouant sur la corde sensible et sur l'appât d'un gain facile, certains internautes tombent dans le panneau.

Aucune statistique n'étant publiée par les organisations criminelles, nous ignorons aujourd'hui l'impact de ces méthodes. Mais ce qui est certain, c'est qu'elles fonctionnent et qu'elles rapportent. Peu de victimes portent plainte... par souci de dignité personnelle.

```
-----Message d'origine-----
De : [redacted]
Envoyé : mardi 9 septembre 2008 13:32
À : unlisted-recipients:; no To-header on input
Objet : Bonjour,

Bonjour,
Je rentre en contact avec vous pour que nous puis son entre prendre une affaire, mais tout d'abord
j'aimerais que vous me dites si vous etre intéressé.Il s'agit d'une assistance de grande importance.j'ai
la somme de $45m que j'aimerais transférer dans un pays étranger ou je peuriez allez en exile parce
que je perdu mes parents cela faire 1 ans,ces fonds se trouve dans des caisse au siens d'une compagnie
de sécurité et nous avons besoins de votre accord pour vous donne lecontact de la compagnie de sécurité
pour que vous puissez entre en contact avec eux pour avoir plus informations. Nous attendons votre
réponse.

Que Dieu vous bénisse et nous garde.
David B.
```

(7) *Washington Post*, 17 mai 2008.
(8) Indicatif téléphonique du Nigéria.

-----Message d'origine-----
De : [redacted]
Envoyé : samedi 26 janvier 2008 21:08
À : infos_contacts_biao@latinmail.com
Objet : Bonne Nouvelle.

Honorable Correspondant,
A l'occasion de l'expansion de ses activités Commerciales et Marketing, l'Etablissement financier dénommé BIAO Sis à Abidjan Côte d'Ivoire a organisé une Tombola en faveur de toute personne physique ou morale résidant ou non en Côte d'Ivoire et possédant une adresse électronique.
Pour cette tombola organisée les prix étaient les suivants :
- Ier Prix : Une Villa SIPIM située à Abidjan d'une valeur de 52.500 €
- 2è Prix : une somme de 40.000 €
La carrera hacia la Casa Blanca, a un click de distancia http://www.starmedia.com/noticias/especiales/gobiernousa.html

-----Message d'origine-----
De : mohamed kone [mailto:konem4@yahoo.com]
Envoyé : [redacted]
À : info@drmcc.org
Objet : BONJOUR
DE:MOHAMED K.
Abidjan, Cote d'Ivoire. +22507654995

Bonjour,
Permettez-moi de vous informer de mon désir d'entrée dans le rapport d'affaires avec vous.J'ai beaucoup prié et après cela j'ai choisi votre nom entre d'autres noms je pense que vous êtes digne de la recommandation de ma prière donc une personne honorable de confiance avec qui je peux faire des affaires. ainsi je n'ai eu aucune hésitation à me fier à vous pour des affaires simples et sincères.
Je suis M. MOHAMED K. le seul fils défunt de M. et Mme MOUSTAPHA K. Mon père était un négociant de cacao et exploitant d'or à Abidjan la capitale économique de la Côte d'Ivoire, mon père a été empoisonné à la pénurie par ses associés d'affaires au cours d'une de leurs promenades en voyage d'affaires.
Ma mère est morte quand j'étais un bébé et depuis lors mon père m'a pris a sa charge. Avant la mort de mon père en novembre 2001 dans un hôpital prive ici à Abidjan, il m'a secrètement appelé au chevet de son lit et m'a indiqué qu'il a la somme de huit millions, cinq cents mille dollars unis d'état. USD ($ 8,500.000) dans un compte d'ordre fixe/ordre dans une banque principale ici à Abidjan.Il m'a également expliqué que c'était en raison de cette richesse qu'il a été empoisonné par ses associés d'affaires. Il à aussi souhaité que je cherche un associé étranger dans un pays de mon choix où je transférerai cet argent et l'emploierai dans des investissements tel que la gestion de biens immobiliers ou la gestion d'hôtel. Monsieur, je cherche honorablement votre aide des manières suivantes :
(1) pour fournir un compte bancaire sur lequel transférer cet argent.
(2) pour servir de gardien de ces fonds puisque je suis encore tres jeune.
(3) Pour m'aider a immigrer dans votre pays avec une attestation de résidence afin que je puisse y poursuivre mes études.
Ainsi dit, Monsieur je suis disposé à vous offrir 15 % de toute la somme qui représente mon héritage en compensation pour vos efforts après le transfert de ces fonds sur votre compte.
En outre, vous indiquerez vos options pour m'aider sachant en ce qui me concerne, j'ai foi que cette transaction peut se faire le plus vite possible. J'aimerai avoir votre point de vue sur la question et cela selon votre disponibilité.
Vous pourrez me joindre dès réception du présent message a mon e-mail.
Merci, que Dieu vous bénisse immensément.
MOHAMED K.

Le pire, c'est que cela fonctionne ! Monsieur R., un Nantais de 40 ans, en a fait l'amère expérience en 2006. Alléché par les retombées financières sur son compte bancaire, il a accepté d'entrer en contact avec les présumés parents d'un ancien roitelet africain. Malheureusement, pour accueillir les fonds (130 millions de dollars), il faut verser par avance les droits de transfert, lesquels s'élèvent à 20 000 euros, une paille en comparaison des 1 % que devrait lui rapporter sa commission. Il se rend donc en Espagne pour rencontrer le banquier africain, lequel le presse d'effectuer immédiatement un virement vers un compte au Nigeria, en attendant le transfert final. Au bout de quelques jours, sans nouvelles de ses nouveaux amis, il réalise qu'il a été abusé. Toutes ses économies familiales ont été englouties dans l'arnaque.

La cyberusurpation d'identité

Les motivations des usurpateurs sont multiples. Il peut s'agir d'un simple canular, de s'identifier à sa star préférée, de prendre la parole de manière anonyme dans un forum de discussion, d'approcher l'être cher sous couvert d'anonymat ou plus simplement de conserver un anonymat prudent. Il peut servir à soutirer de l'information : la technique consiste alors à se faire passer pour une autorité et obtenir toutes sortes d'informations sur une personne dénommée. Mais, il peut aussi s'agir de commettre des forfaits, d'accéder à des systèmes sans y être autorisés, d'user d'une fausse carte bancaire sous un faux nom, etc. L'usurpation d'identité vient alors aider à la constitution d'une infraction [9].

L'usurpation d'identité devient un délit pénal dès l'instant où « *le fait de prendre le nom d'un tiers, dans des circonstances qui ont déterminé ou auraient pu déterminer contre celui-ci des poursuites pénales* [10]». Dans ce cas, elle est punie de cinq ans d'emprisonnement et de 75 000 euros d'amende. La condition, pour que le délit soit constitué, tient à ce qu'ait été pris « le nom d'un tiers ». À ce jour, il n'existe pas de jurisprudence qui puisse affirmer que « prendre » une adresse IP ou une adresse e-mail soit assimilable au « nom » de l'article 434-23.

Si l'usurpation d'identité vient au soutien d'une infraction de droit commun, elle caractérisera souvent le délit lui-même. On pourrait aussi retenir, dans certains cas, le délit de faux de l'article 441-1 du Code pénal. Selon ce texte : « *Constitue un faux toute altération frauduleuse de la vérité, de nature à causer un préjudice et accomplie par quelque moyen que ce soit, dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques* ».

L'interception de données bancaires

Le risque existe, comme l'a expliqué à de nombreuses reprises Daniel Martin du Cybercrimeinstitut [11], spécialiste incontesté des utilisations déviantes des nouvelles technologies de l'information et de la communication (NTIC). Selon ses propres termes, dès l'instant qu'une donnée est numérique, elle peut être copiée si les sécurités sont déjouées.

Mais à ce jour, peu d'exemples concrets ont été portés à notre connaissance. Il semble, et je m'exprime sous toute réserve, que l'interception des données de carte bancaires soit très faible. En revanche, il est exact que le nombre de tentatives de fraudes avec des faux numéros de cartes bancaire connaît une forte croissance, n'en déplaise aux organismes qui créent et gèrent ces moyens de paiement.

Déjouer les sécurités numériques est toujours possible, mais cela demande du temps et une grande puissance de calcul. Ces moyens manquent généralement aux organisations criminelles, même les plus performantes. C'est pour cette raison que ces sécurités doivent évoluer en permanence, au même titre que les antivirus sont mis à jour une fois par semaine.

Une réponse : la signature électronique et la biométrie

La signature électronique [12] pourrait être la réponse adéquate puisqu'elle se fixe comme objectif, entre autres, de garantir l'authenticité de l'identité de celui qui contracte.

(9) Olivier Iteneau, *Le journal du Net*, 9 mars 2004.
(10) Article 434-23 du Code pénal.
(11) http://www.cybercriminstitut.com
(12) Article 1316-4 du Code civil.

Si la signature électronique paraît envisageable pour certains actes de la vie sociale, tels que les achats en ligne, les déclarations, elle ne couvre pas cependant tout le spectre des faits et gestes possibles en ligne.

Une autre technique pourrait également être d'une grande utilité, la biométrie. Cette technique seule permettrait d'authentifier à distance une personne émettrice d'ordres ou de contrats. Une nouvelle forme de recommandations du courrier qui pourrait faire concurrence à la Poste. Pourtant, il n'est pas pensable de ne pas laisser à chacun la liberté de se dissimuler quand il le souhaite, pourvu qu'il n'y ait pas d'atteinte au droit. Internet reste un espace de liberté important qu'il ne faut pas détruire.

Il est parfaitement envisageable de créer un dispositif sur les claviers ou d'adjoindre un périphérique qui permettrait, dans certains cas, d'identifier et d'authentifier un internaute lors d'opérations contractuelles, achat en ligne, ou émission de messages avec certains de ses correspondants. Cela résoudrait beaucoup de problèmes, et empêcherait probablement les techniques de « fisching », aujourd'hui diaboliquement efficaces.

Les difficultés existent, ne nous voilons pas la face. Elles résident dans l'intégrité du système biométrique, car si un tiers s'approprie numériquement une identité biométrique du type des empreintes digitales, morphologie de la main, ou autre, il peut ainsi, au moyen de ces identités biométriques, passer tout type d'actes au nom de la victime. « *Comment la victime pourrait-elle alors révoquer sa propre empreinte digitale ou identité visuelle ? Lesexperts en sécurité que nous avons interrogés sont partagés. Tous y reconnaissent cependant là une difficulté au passif de cette protection technique* [13]», s'interroge à juste titre l'avocat Olivier Itenau. Une question difficile à laquelle les ingénieurs essaient aujourd'hui de répondre par des aménagements technologiques.

Coupler la biométrie avec la signature électronique semble une solution acceptable que les spécialistes devront creuser dans les années à venir. Technologiquement, les outils sont prêts. Ce sont surtout les capacités de calculs des systèmes qui sont à même d'assurer une sécurité de bonne qualité avec cryptage et scellement numérique des données, unique dispositif capable d'assurer l'intégrité d'une transaction.

Conclusion

La cybercriminalité identitaire n'est pas un fantasme. C'est un phénomène mondial, mal appréhendé, qui connaît une croissance importante. Cette nouvelle menace criminelle contemporaine trouve son fondement dans notre dispositif identitaire très récent et dans la liberté que l'on a de choisir sa propre identité sur la toile. Elle touche chacun de nous, car en tant qu'Internaute nous recevons de nombreux courriers émanant de personnes incertaines, sans compter les achats qui sont effectués en ligne, et pour lesquels des risques existent.

Face à l'usurpation d'identité dans le monde virtuel, les victimes font face à une situation juridique incertaine, à des réponses techniques balbutiantes. La cybercriminalité identitaire semble avoir de beaux jours devant elle.

L'identité, même numérique, est un droit qu'il faut protéger. Les libertés fondamentales au XXI[e] siècle ne peuvent faire l'économie de la première sécurité du citoyen : celle de son identité unique dans la société.

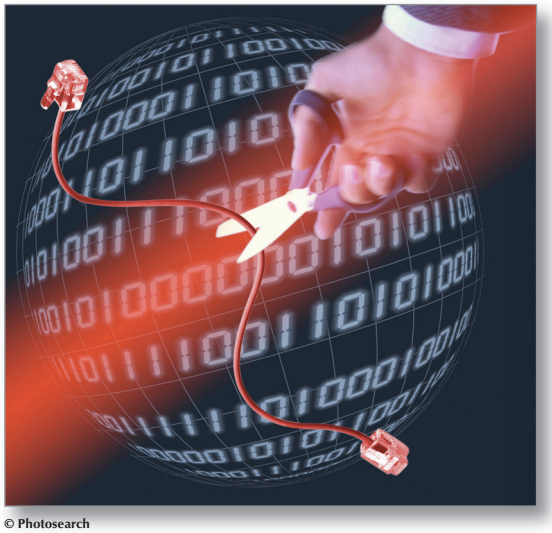
Christophe NAUDIN

(13) Olivier Itenau, *ibid.*

Cyberattaques - Cyberdéfense

Les Baltes en première ligne

Dominique DUBARRY



La cyberguerre est en marche. Ordinateurs infestés par hackers = e-mails avec virus = incursions non désirées. Espions et terroristes sont aux aguets. Les cyberattaques ont pour but la déstabilisation des structures étatiques ou d'entreprises privées. Comment la cyberdéfense peut-elle réagir dans un monde virtuel ?

Cyber Attacks and Cyber Defense : The Baltic States on the Front Line

We are already engaged in cyber war. Computers and e-mails are penetrated by hackers and infected with viruses. Spies and terrorists are on the look-out. Cyber attacks attempt to undermine state structures as well as private enterprises. How are cyber defenses to be mounted in the virtual world?

Dominique Dubarry

A fait une partie de sa carrière dans les produits de défense et de sécurité à l'exportation vers les États-Unis et les pays du Nord de l'Europe. Ancien auditeur de l'Institut des hautes études de Défense nationale (IHEDN) et du Centre des hautes études en armement (CHEAr). Il a publié, en 2006, un ouvrage sur les relations de la France avec les États baltes, *Les rencontres franco-baltes. 800 ans d'histoires partagées*, chez Romain Pages Éditions.

Les relations russo-baltes n'ont jamais été marquées du sceau de la simplicité. Si Moscou s'est résigné à accepter l'indépendance de ces pays dans les années 1990, elle ne fut tolérée que du bout des lèvres. Puis, l'intégration des trois États dans l'OTAN, en mars 2004, a eu le don d'agacer Moscou qui a réagi peu après en arrêtant l'approvisionnement pétrolier de la Lettonie. La Lituanie subit le même sort en juillet 2006, et l'Estonie se voit privée d'importation charbonnière. En juillet 2007, le ministre russe des Transports, Igor Levitin, va plus loin en annonçant que son pays allait arrêter tout transit pétrolier vers les ports estoniens au profit des nouveaux ports russes. Les survols d'avions militaires russes sont devenus plus fréquents. Un Sukkoi 27 a violé l'espace aérien et s'est abattu en Lituanie en septembre 2005. Ces incursions ont pour but de tester les réactions des pilotes de l'OTAN basés à Siauliai en Lituanie, mais elles préoccupent essentiellement les populations, les États baltes ne possédant pas d'avions de chasse à réaction.

Cyber-attaques pour le déplacement d'une statue

En avril 2007, le gouvernement estonien décide de déplacer la statue en bronze représentant un soldat soviétique ; elle est placée en plein centre de Tallinn et commémore la libération de 1944 contre le nazisme. Il faut reconnaître que ce monument était plutôt considéré par les Estoniens comme le symbole des cinquante années d'occupation soviétique.

Dans les heures qui suivent, des manifestations imprévues vont se dérouler dans la capitale les 26 et 27 avril : des bandes de jeunes issus de la minorité russophone considèrent que le déplacement de la statue est un affront à la mémoire des soldats soviétiques. Devant une police totalement dépassée, de nombreux édifices et boutiques sont saccagés et les dégâts représentent plusieurs centaines de milliers d'euros. Un homme y laissera la vie et plus d'une centaine de blessés se retrouvent dans les hôpitaux. Tallinn est sous le choc. Depuis son indépendance, elle n'a pas vu une telle violence et autant de dégâts. Les autorités mettront en cause le groupe des jeunes *Naschi* (Les Nôtres), considéré comme inféodé au Kremlin et chargé de s'opposer, entre autres, à de nouvelles « révolutions orange ». Ce même groupe sera encore impliqué peu après dans une cyberattaque coordonnée et dirigée contre les sites internet des autorités, ministères, administrations, banques, centres de communication, organismes de presse.

Durant le week-end du 24 au 25 novembre, des rumeurs (totalement infondées) de dévaluation de la couronne estonienne furent diffusées en langue russe sur les sites web. La dévaluation annoncée dépasse 63 % de la valeur légale. Ceci a de quoi inquiéter tous les citoyens du pays et des files d'attente se forment devant les banques (*Hansabank* et *Seb Uhisbank*). Le quotidien *Postimees* précise alors que les vendeurs de couronnes contre des devises étrangères sont essentiellement des russophones résidant dans le nord-est de l'Estonie près de la frontière russe. Cette tentative de sabotage informatique avait pour but manifeste de provoquer une panique dans le public avec le risque d'entraîner une dévaluation de la couronne. Il est prouvé que l'origine de cette spéculation au motif politique reposait sur un faux rapport apparu sur le site web du groupe radical *Naschi* qui s'était érigé en défenseur du monument à la gloire du soldat soviétique. Ces groupes à la typologie particulière se distinguent par leur caractère fermé, embrigadé et asservi au pouvoir étatique par des courroies de transmission occultes. Ils sont considérés par le journaliste Edward Lucas comme des « *fanatiques dont les actions démontrent une dérive manifeste vers le totalitarisme* » [1].

Il est utile de rappeler que la Lettonie avait elle aussi fait face à des rumeurs de dévaluation de sa devise – le *lats*, en mars 2007 – diffusées par des messages SMS. Là encore, l'opération a échoué car les banques centrales de Lettonie et Estonie ont pu réagir très rapidement.

Raid contre la Lituanie

Le dimanche 29 juin 2008 à 18 heures, les *hackers* exécutent une nouvelle cyberattaque. Ils infiltrent 300 sites web des autorités gouvernementales lituaniennes, ainsi que des groupes privés dans l'automobile ou la grande distribution. Les messages en langue russe sont accompagnés du drapeau de l'ex-Union soviétique. L'un des textes est adressé au siège du parti social-démocrate lituanien, le *Baltic Times* [2] nous en livre un extrait : « *Vous les rancuniers, vous êtes tous des cinglés, vous considérez-vous comme la plus généreuse des nations ? Les gens généreux font tout ce qu'ils peuvent pour leur pays plutôt que de le détruire comme vous le faites... Votre destin est clair, la rancune et*

(1) *The New Cold War: How the Kremlin Menaces Both Russia and the West*, 2008 , Edward Lucas, journaliste spécialiste de l'Europe de l'Est pour *The Economist*.

(2) *The Baltic Times*, juillet 2008

le fiasco, mais vous continuerez à engendrer encore plus de dégénérés et de voyous. »

L'inconvenance des propos est accentuée par l'incohérence du raisonnement. Faut-il tenter de décoder ? Ou les termes utilisés par l'auteur sont-ils mal maîtrisés ? Dans tous les cas, leur incongruité dénote une manifestation de violence délibérée. Il apparaît que ce genre de cyberattaques survient généralement à la suite d'une décision politique déplaisante pour les nostalgiques de l'ex-URSS. L'émeute d'avril 2007 à Tallinn faisait suite au déplacement de la statue du soldat soviétique. La cyberattaque de juin 2008 à Vilnius s'est déclarée lorsque le Parlement lituanien a décrété l'interdiction des représentations, symboles et signes distinctifs d'origine nazie ou soviétique.

À la même époque, le Secrétaire général des Nations unies, Ban Ki Moon, avait d'ailleurs déclaré : « *l'Internet est devenu la colonne vertébrale de notre monde globalisé, pour les Nations unies il est devenu un outil puissant dans sa mission pour promouvoir la paix et la sécurité.* »

L'OTAN et la cyberdéfense

Ces cyberattaques, imprévisibles, répétées, sous-estimées au départ, ont néanmoins sensibilisé le gouvernement estonien à la vulnérabilité du pays. Il fait appel au ministre de la Défense Jaak Aaviksoo qui décide de mettre sur pied une structure appropriée au niveau international, et va même jusqu'à affirmer que « *les cyberattaques peuvent causer des dégâts comparables aux armes conventionnelles.* »

Face à cette menace susceptible de détruire les intérêts vitaux d'un pays, l'Estonie, par les attaques qu'elle a subies, a acquis une connaissance et une capacité de réaction qu'elle offre de coordonner au niveau des pays de l'OTAN. Elle propose la création d'un centre d'études des cyberattaques, dirigé sur les nouvelles cybermenaces technologiques que les gouvernements occidentaux doivent se préparer à affronter. Un Centre d'excellence sur la cyberdéfense vient d'être installé à Tallinn pour être opérationnel rapidement. Il comportera deux départements, l'un en charge de la formation et de l'entraînement, le second pour la recherche et le développement. Les méthodologies viseront à accroître les opérations et à se défendre dans le cyberespace. Petit clin d'œil de l'histoire : le centre de cyberdéfense de l'OTAN installé à Tallinn se trouve dans un bâtiment qui fait face à un jardin... où se trouve le soldat en bronze de l'armée soviétique qui a déjà fait couler beaucoup d'encre.

L'OTAN prévoit la mise sur pied d'un centre d'alerte et de réaction aux attaques informatiques (CERT [3]) pour protéger les systèmes existants, mais aussi mettre en œuvre des contre-attaques face à ce type d'agression. Dès sa création, sept pays ont décidé d'y apporter leur concours : Allemagne, Espagne, Italie et les trois pays baltes. Les autres pays de l'OTAN y participent à titre d'observateur.

L'Organisation pour la sécurité et la coopération en Europe (OSCE) a aussi réagi rapidement, elle comprend 56 pays et les pays baltes en font partie depuis 1992. Une résolution [4] a été adoptée le 3 juillet par l'Assemblée parlementaire (seule la Grèce a voté contre). Elle souligne le grand discernement de ses membres devant l'obligation inéluctable d'une coopération qui doit être globale pour faire face à ces nouvelles menaces dans un monde en perpétuelle évolution.

La résolution fait appel à une collaboration rapide avec le Conseil européen pour la cybercriminalité et le terrorisme. Elle demande instamment une coopération entre les gouvernements, les organisations internationales, le secteur privé et les citoyens pour unifier les moyens sur les plans moral, légal et politique des utilisations abusives du cyberespace.

Le Secrétaire général de l'OTAN, Jaap de Hoop Sheffer, a précisé que la cyberdéfense reste une « *priorité nationale* », mais aussi que l'Alliance est prête à aider les membres qui seraient attaqués ou nécessiteraient une assistance, en mettant sur pied des moyens de contre-réaction. Cette déclaration rappelle fort logiquement l'article 5 du Traité de l'OTAN qui prévoit l'assistance aux membres de l'Organisation si l'un d'eux subit une agression.

Voici une nouvelle tâche à laquelle l'OTAN doit s'atteler, mais son domaine d'application dépasse la seule vision militaire des intérêts stratégiques. Elle couvre aussi l'ensemble du secteur civil, économique et financier de chaque nation. Les exemples de cyberattaques évoqués sont une menace à prendre en compte dans les multiples agressions à attendre sur le champ de bataille planétaire que nous réserve le futur.

Dominique DUBARRY

....

(3) Computer Emergency Response Team.

(4) *The Baltic Times,*16 août 2008.

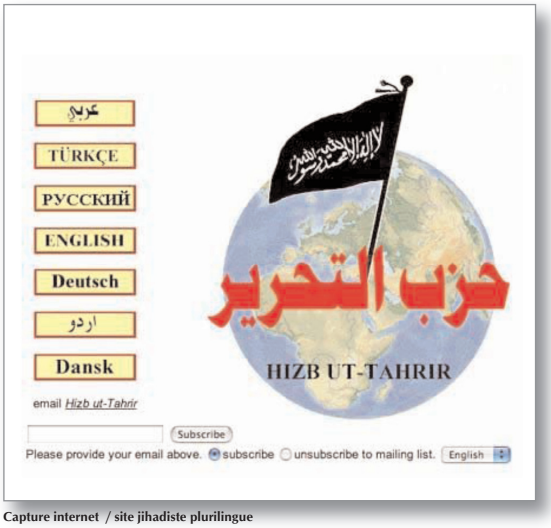
Post-scriptum

Si l'agression russe en Géorgie a été amplement couverte par la presse internationale, peu de médias ont relevé qu'elle fut précédée par une cyberattaque généralisée. Il est curieux de constater que plusieurs heures avant le franchissement de la frontière par les troupes russes, les sites web de l'État géorgien ont été infestés. L'accès aux sources officielles d'information étant coupé, certains sites gouvernementaux se sont réfugiés sur d'autres serveurs à travers le monde. C'est ainsi que le site du ministère des Affaires étrangères géorgien est devenu l'hôte de l'Estonie.

Mart Laar, ancien Premier ministre estonien, a précisé le 25 août 2008 « *durant les premiers jours de l'invasion, l'information russe était devenue dominante, décrivant la Géorgie comme un agresseur et la Russie, la victime. Dans la guerre de l'information, le plus important demeure la vitesse et l'ingéniosité. L'effort doit être dirigé vers l'information* [des gens] *qui évoluent dans le cyberespace russe.* »

La propagande jihadiste sur Internet : diagnostic et perspectives

Walter AKMOUCHE, Henri HEMERY



Capture internet / site jihadiste plurilingue

Lorsque l'on parle de cyberterrorisme ou de cybercriminalité, l'une des premières pensées est le risque potentiel d'une attaque informatique majeure contre les infrastructures réseaux. Or, il existe déjà des risques réels et avérés, car les salafistes de la mouvance al Qaïda utilise déjà Internet pour la formation, les communications, et la propagande. Cette propagande, en particulier, est souvent très instructive, car au XXIe siècle, même une mouvance terroriste a besoin de communiquer et de diffuser ses messages de fond, révélateurs de sa stratégie.

Jihadist Propaganda on the Internet

Whenever cyberterrorism and cybercrime are mentioned, the potential risk of a major information attack on the net comes to mind. The risk is real. The Salafist movement of Al-Qaeda already is using the internet for training, communication and propaganda. In the 21st century even a terrorist movement needs to communicate and broadcast its basic message on the net. However, this available propaganda is particularly instructive since it also reveals a group's strategy.

Walter Akmouche

Intervenant au sein de Département de recherche des menaces criminelles contemporaines (Université Paris II Panthéon-Assas) et titulaire du diplôme universitaire d'analyse des menaces criminelles contemporaines (Paris II). Il est également membre du bureau du Club sécurité globale de la Société des électriciens et électroniciens.

Henri Hemery

Docteur ès Sciences et consultant en sécurité au sein d'un grand groupe industriel français. Il a suivi le diplôme universitaire d'analyse des menaces criminelles contemporaines (Paris II). Il est membre du Comité directeur et responsable du Comité d'étude Risk Management de l'ANAJ-IHEDN (Association nationale des auditeurs jeunes de l'IHEDN).

Internet : un vecteur de propagande idéal

L'Internet se prête très bien à la diffusion de la propagande. En effet, sur le fond, toute rumeur peut être véhiculée et demeure, de fait, invérifiable. Cette information se prête parfaitement à la théorie du complot : défiant les informations officielles, tout démenti est interprété comme la preuve de la véracité (puisqu'on se défend, c'est qu'il y a bien un secret à protéger) et toute absence de communication prouve que les assertions sont bien vraies. De plus, sur la forme, Internet est un média adapté car il permet simultanément de toucher une vaste population de millions d'internautes grâce à son développement dans le monde, et de s'adresser à chaque internaute individuellement derrière sa console d'ordinateur.

En considérant que le taux de réussite de la propagande reste toujours faible, cette large capacité de diffusion est primordiale : sur 1,3 milliard de musulmans, on estime le nombre de jihadistes à 30 000, soit 0,002 % de cette population, c'est-à-dire une population extrêmement marginale et minoritaire. Concrètement, cela signifie que, statistiquement, pour rallier un jihadiste, il faut démarcher, en moyenne, 45 000 personnes.

En outre, paradoxalement, chaque internaute est touché individuellement, sans possibilité de réfléchir. C'est le cadre idéal d'une vaste théorie du complot adressée à des millions d'internautes, dont chacun a le sentiment d'être le seul destinataire de cette information invérifiable. De plus, ce moyen de communication est accessible à domicile, au travail, dans des cybercafés, et, désormais, sur des téléphones mobiles. Enfin, compte tenu des colossaux volumes de données échangées, même leurs traitements automatiques rendent très fastidieuse une surveillance efficace du Net : l'abondance de données sert aussi, d'une certaine façon, à garantir l'anonymat.

Une propagande efficace et polymorphe

La technique seule d'Internet ne saurait suffire. Les salafistes et jihadistes ont su concevoir, structurer et mettre en œuvre une propagande très efficace, en recourant parfois à des personnes compétentes. On peut citer, par exemple, Abou Mayssara al Iraqi qui a su transformer Abou Moussab al Zarkawi en un leader terroriste charismatique de stature internationale alors qu'il n'était, à l'origine, considéré que comme un simple criminel sans grande envergure. On peut également citer les membres de l'agence de communication Al Sahab qui ont su mettre en scène les discours d'Oussama Ben Laden et Ayman al Zawahiri. Derrière cette mise en scène et ces discours se cachent de redoutables propagandistes qui s'inspirent des mécanismes les plus efficaces de cette discipline : la notion de caractère commun d'individus afin de les guider vers un but ultime, ici, l'Oumma, sur le modèle de Gustave Le Bon [1895]. Le lecteur pourra se référer à l'ouvrage de Jacques Ellul, *Propagandes* [1962] pour en saisir tous les ressorts.

La propagande jihadiste exploite très régulièrement une dualité schizophrène, « victime-vainqueur », révélatrice de la théorie du complot : les moudjahiddins sont à la fois les victimes de l'humiliation et des massacres des Occidentaux, et, en même temps, les « redoutables combattants » qui infligent des pertes terribles à ces mêmes Occidentaux présentés comme des incompétents et des faibles. Les nouveaux moyens techniques permettent à ces propagandistes de proposer des images, photos ou vidéos de leurs opérations en Irak, en Afghanistan ou en Tchétchénie. Ces moyens multimédias s'adressent manifestement à un public jeune, souvent avide de sensations, pour qui ces actions militaires accompagnées d'une musique glorifiante (parfois même sous forme de rap) peuvent représenter un attrait. Grâce aux moyens techniques, cette communication peut être diffusée avec une célérité incomparable dans l'histoire, sans moyen efficace et rapide de contrôle.

Une propagande usant des techniques du marketing

Dans une stratégie marketing, il convient de distinguer le marketing « stratégique » du marketing « opérationnel » et du marketing mix. Au final, il conviendra de rédiger une *copy strategy* [1], avec une promesse, une justification, un ton et un style. Il est largement reconnu que la clef de voûte du marketing est le positionnement, ce qui implique de connaître les attentes du « client » (ici la population musulmane, ce qui peut s'avérer difficile compte tenu de sa diversité), d'identifier ses concurrents (les mouvements concurrents tels que le Hezbollah, le Hamas, etc.) et de connaître ses propres caractéristiques

(1) La *copy strategy* est un élément classique du marketing. C'est un document de travail, généralement établi entre l'annonceur et l'agence, afin de définir le cadrage d'une campagne publicitaire. Il sert de cahier des charges. Ce document synthétique comprend la description de la promesse, des arguments (preuves de la promesse), du bénéfice et du ton, ainsi que tout autre élément nécessaire à la campagne publicitaire.

(capacités de recrutement, objectifs, etc.). De ce point de vue, Oussama Ben Laden, et ses conseillers, peuvent être considérés comme très performants et très efficaces.

Considérons l'exemple du discours d'Oussama Ben Laden du 29 décembre 2007 : il se réfère à l'Irak, où les troupes américaines sont en difficulté, et à la Palestine, plus qu'à l'habitude. Or, plus que l'Irak, la Palestine est un sujet qui passionne les foules arabes et musulmanes, un sujet sur lequel les Occidentaux n'ont guère réussi à avancer, et un sujet sur lequel la nébuleuse Al Qaïda (au sens large) a encore peu fait et dispose d'un fort potentiel. D'où ce nouveau positionnement. Cela peut également signifier que, d'une certaine façon, les « segments » Irak et Afghanistan sont considérés comme gagnés, et sur lesquels on maintient un investissement minimal. La *copy strategy*, contenue dans ce discours, reprend les éléments classiques : une promesse, à savoir que, désormais, la Palestine est un enjeu. Cela est justifié par le fait que la Palestine est la victime des « sionistes » et des « croisés », et désormais sont possibles, et même autorisés, un combat en martyr ; un style suffisamment énergique, voire assez militaire, ainsi qu'un ton grave, sérieux et quasi prophétique. Dans sa vidéo sur Internet, diffusée le 22 avril 2008, Ayman al Zawahiri s'est également inspiré des méthodes marketing actuelles exploitant le web 2.0 ou web contributif, répondant à des questions préalablement postées sur un forum Internet (attentes des « clients » clairement identifiées, puisqu'émanant des clients eux-mêmes), il a cependant orienté son discours sur ses propres préoccupations et notamment sur les combats en Irak, l'instauration d'un état islamique en Irak et les conséquences d'une défaite américaine sur place. On peut noter, au passage, que le fait de répondre, certes en différé, à des messages postés sur un forum, presque en chattant, est une provocation, voire un camouflet infligé aux Occidentaux, incapables de repérer sur Internet avec leurs puissants systèmes d'interception le numéro deux d'Al Qaïda dont la tête est mise à prix pour 25 millions de dollars.

On peut d'ailleurs se rappeler qu'en 2004, l'Irak n'était pas considéré par les spécialistes comme un enjeu majeur, contrairement à l'Afghanistan, et à compter de cette année, Oussama Ben Laden a également modifié ses discours pour se positionner sur ce théâtre de guerre qu'il pressent alors intéressant. Ayman al Zawahiri s'est inscrit également dans cette perspective. En définitive, la stratégie est certes pertinente et très pragmatique, mais on ne peut pas la qualifier d'imaginative

La propagande : un danger sous-évalué

Le préalable au recrutement

Sur un terreau *a priori* fertile de frustration, d'humiliation ressentie ou, plus simplement, de désœuvrement, l'abondance et la force de conviction de cette propagande peuvent conduire des jeunes sans lien direct avec la mouvance salafiste à adhérer à cette idéologie. Pour certains, une minorité, un recrutement physique par des groupes salafistes locaux devient possible, et, pour une plus faible minorité encore, le passage à l'acte devient une potentialité.

En soit, ces perspectives de recrutement et de passage à l'acte peuvent déjà être considérées comme particulièrement préoccupantes. Mais, plus inquiétant, il est possible que des ressortissants nationaux, internautes quasiment indiscernables et indétectables, sans lien direct avec les salafistes, puissent se grouper et passer à l'acte. D'une certaine manière, les attentats de Londres du 7 juillet 2005 préfigurent ce type de risque de « génération spontanée de menace ». L'émergence spontanée de groupes salafistes indépendants permet alors efficacement de frapper au cœur des métropoles occidentales.

Internet et sa propagande ne sauraient suffire. Ils ne sont que des conditions nécessaires et des prérequis. Une mise en relation humaine est indispensable.

Une menace humaine, matérielle et économique

En 2004, la projection du film *Submission* de Théo Van Gogh avait conduit à de nombreuses réactions très virulentes sur les sites islamistes et jihadistes, certains appelant même à son assassinat. Et, de fait, un islamiste était effectivement passé à l'acte. Ce type de passage à l'acte est rarissime, car si les sites islamistes diffusent chaque année des centaines d'appels à la violence, le nombre d'assassinats effectifs reste très faible.

Mais, s'étant déjà produites, même de manière statistiquement très marginale, et pouvant potentiellement survenir, ces menaces sur Internet obligent les gouvernements à prendre parfois des mesures très contraignantes. En 2004, le site Internet www.islamic-minbar.com avait diffusé une large campagne de menaces d'attentats contre l'Italie, conduisant à un large déploiement de carabiniers dans

les rues. En 2006, plusieurs sites avaient évoqué des menaces contre la Suisse. Lors des caricatures portant sur le prophète, le site http://alekhlaas.com avait diffusé des incitations au meurtre contre les dessinateurs et, plus généralement, contre le Danemark. En avril 2008, des menaces présumées sérieuses contre les représentations diplomatiques danoises en Algérie et en Afghanistan se soldent par la fermeture des bâtiments et la protection des personnels. À chaque fois, des mesures de sécurité sont prises, impliquant un coût financier parfois non négligeable. Néanmoins, aucun dirigeant ne pourrait prendre le risque de l'inaction face à des menaces sans équivoque.

Les pays principalement visés par le prosélytisme et la propagande salafiste sont les États-Unis, déclarés coupables d'humilier et d'asservir le monde arabo-musulman ; Israël, systématiquement désigné comme le pays des sionistes ; et les gouvernements arabes, considérés comme vassaux des États-Unis, et par conséquent, impies. Il serait cependant faux de croire que la France et l'Europe échappent à cette campagne de menaces et de prosélytisme. Conscients de la relativement faible connaissance de l'arabe par les jeunes générations européennes, des sites clairement islamistes et même jihadistes n'hésitent pas à proposer des versions françaises, allemandes, anglaises, etc.

Or, ces surcoûts, dans un contexte mondial tendu, ne sont pas sans effets. Des mesures concrètes et donc financièrement coûteuses sont prises en cas de menaces virtuelles ou potentielles d'un coût quasi nul. Et à ce jeu, le bouclier implique bien plus d'efforts que le glaive.

Des formations à distance

L'inconvénient est qu'il existe aussi sur Internet des sites proposant des formations à la guérilla (urbaine notamment, comme les revues au format pdf *Camp al Battar* ou *Zarouat as-sanam*), à la fabrication d'explosif à partir de composants du commerce, au maniement des armes à feu, etc. Ces fichiers à l'origine en pdf sont de plus en plus remplacés par des fichiers multimédias vidéo, avec explication sonore et sous-titres, zoom sur les séquences les plus délicates, etc.

La propagande est complétée par des capacités de former à distance (« e-learning ») des internautes susceptibles de passer à l'acte, et en mesure, en quelques clics de souris, de passer d'un site de propagande à des sites de formation très efficaces.

À la lumière de tout ce qui précède, on serait tenté d'interdire les sites jihadistes tant leur dangerosité paraît prouvée. Néanmoins, ce serait aussi méconnaître l'intérêt de ces sites pour étudier et caractériser la mouvance salafiste internationale Al Qaïda et pour anticiper le niveau de menace réel des groupes ou groupuscules terroristes.

La nécessaire surveillance des sites de propagande

Surveiller ou fermer ces sites ?

Lors de menaces ou d'insultes particulièrement graves et virulentes, la tentation est grande de décider la fermeture de ces sites jihadistes. Les autorités sont d'ailleurs souvent soumises à la demande populaire qui ne comprendrait pas qu'aucune réaction ne puisse avoir lieu.

Toutefois, hormis pour des sites mineurs et, en définitive, peu nuisibles, ces fermetures de sites s'avèrent au moins inefficaces, voire contre-productives. Inefficaces, car pour les sites les plus pertinents et les plus virulents, les responsables du site ont prévu à l'avance des noms de domaine de remplacement, des sites miroirs, des adresses IP supplémentaires, etc. De fait, un site fermé réapparaît sur le web dans les 48 à 72 heures sous un autre nom. On peut citer l'exemple du site www.assabyle.com fermé après avoir menacés, en 2004, le ministre de l'Intérieur Nicolas Sarkozy, et ouvert, sept jours plus tard, sous le nom www.ribaat.org. On peut également citer le site www.al-ansar.biz, fermé après avoir diffusé le film de la décapitation de l'otage Nick Berg en Irak en 2004, et qui devint successivement geocities.com/al-ansar, www.ansarnet.ws, www.inn4news.net, etc. On peut également citer le site www.islah.org, qui disposait de nombreux sites miroirs : www.islahi.net, www.islah2000.org, www.alislah.net, etc.

En pratique, un site fermé réapparaît donc rapidement, de sorte que la fermeture semble bien dérisoire et complique un peu plus le travail des services de renseignement. Sur le fond, certains sites jihadistes peuvent être de précieux outils d'analyse.

Le contenu des sites jihadistes est bien évidemment condamnable. Il ne s'agit donc pas ici de justifier le contenu de ces sites, mais seulement de montrer l'intérêt que peut offrir ce contenu pour déterminer la menace (dans cet article, nous n'entrerons pas dans les détails pour des raisons de sécurité).

En premier lieu, la ou les langues employées donnent des indications utiles. Ainsi, le site www.prohijab.net propose des versions en arabe, en français, en anglais et en néerlandais. De même, le site www.hizbuttahrir.org est accessible en ourdou, en arabe, en turc, mais aussi en

russe, en anglais, en allemand et en polonais. Pour certaines langues, peu développées au niveau mondial (néerlandais, polonais, etc.), ces sites ne font donc pas mystère des populations visées. Quant au site www.albasrah.net, site de soutien à la « résistance sunnite irakienne », il a reçu 169 849 connexions depuis la France, entre le 13 novembre 2003 et le 18 avril 2006 [2]. Cela place la France en cinquième position des pays consultant ce site, devant l'Égypte ou l'Arabie Saoudite.

Les différents sites jihadistes ne représentent pas tous la même menace. Les sites ribaat.org, hizbutahrir.com ou prohijab.net ont clairement, en raison des choix de langues qui sont faits, des visées sur les internautes européens. Cela peut même être plus précis car la langue néerlandaise s'adresse manifestement à une population particulièrement spécifique.

Par ailleurs, certains sites sont clairement mieux informés, voire en avance. Ils constituent des sortes de « sites référents » du jihadisme international. Cela était le cas du site www.ansarnet.ws, sur lequel ont été diffusés en exclusivité les discours audio d'Abou Moussab al Zarkawi. On peut aussi citer le site www.qal3ah.net qui avait publié le texte de la revendication des attentats de Londres. Ces sites référents fixent les grandes tendances des menaces et peuvent constituer une sorte de baromètre de la menace.

Une communication révélatrice des groupes et des stratégies

On parle de communication d'Al Qaïda. Il convient cependant de préciser qui, personne physique, parle ou écrit sur Internet. Car, sauf mention contraire, il n'existe pas de porte-parole officiels d'Al Qaïda, en droit de s'exprimer au nom de toute l'organisation. Pas même Oussama Ben Laden, qui ne revendique ni ce titre, ni même celui de chef quelconque.

Il conviendrait donc d'analyser avec précision celui qui parle, ce dont il parle et de qui il parle. Par exemple, dans la lettre d'Ayman Al Zawahiri à Abou Moussab Al Zarkawi du 11 octobre 2005, on peut s'étonner de la traduction de la presse. Zawahiri soutient les groupes jihadistes en Irak et leur adresse sa bénédiction... mais pas plus à Zarkawi qu'à un autre. Alors qu'Oussama Ben Laden avait fait de Zarkawi, quelques mois auparavant, son émir en Irak. En effet, Zarkawi avait des résultats en Irak, et avait réussi à médiatiser ses actions grâce aux sites Internet, réussissant même la prouesse de faire passer au second plan les actions pourtant bien plus nombreuses et efficaces de la résistance baasiste. Mais, dans son combat, Zarkawi n'a jamais respecté les recommandations prônées par le « cheikh » Oussama Ben Laden, en particulier en s'en prenant violemment à la communauté sunnite.

Ainsi, dans son discours audio du 12 septembre 2004, Abou Moussab al Zarkawi se place sous l'autorité morale du cheikh Oussama Ben Laden, autorité morale d'un sage, mais sous réserve à peine voilée de la reconnaissance de la stratégie militaire employée en Irak. Le 27 décembre 2004, Oussama Ben Laden fait effectivement l'éloge de la conduite des opérations en Irak par Zarkawi.

On pourrait étendre ces remarques à l'ex groupe salafiste pour la prédication et le combat (GSPC) devenu Al Qaïda au Maghreb islamique.

Comme tout groupe, au sens large, Al Qaïda ne devrait pas être exempte de conflits et de jeux de pouvoirs, comme toutes les structures multinationales, publiques ou privées. De fait, à la lumière des atermoiements, de ces échanges, de remarques parfois très surprenantes, certains spécialistes ont avancé l'idée que certains textes pouvaient être des faux, et selon leurs hypothèses des faux fabriqués par les Américains qui auraient tout intérêt à prolonger cette lutte. Cette analyse ne doit pas être négligée. Mais, il est également possible que ces messages soient vrais et qu'ils soient des révélateurs de dissensions ou de conflits d'intérêts au sein d'une mouvance non hiérarchisée et aux stratégies multiples. Certes, il s'agit de combattre l'Occident et les infidèles pour reconstituer l'Oumma originelle, mais pour les détails et la pratique, les stratégies sont très diverses, et même parfois opposées.

Plusieurs stratégies peuvent être distinguées.

- La première pourrait être dénommée « stratégie afghane », qui consiste à créer un État pilote pour le Jihad. Cette stratégie est assez proche d'une structure fasciste classique pour lequel une avant-garde éclairée, structurée et hiérarchisée doit mener la lutte, définir la propagande, et conduire les foules. Cette catégorie semble aujourd'hui incarnée par Ayman Al Zawahiri, et, plus généralement, par les jihadistes égyptiens issus notamment des frères musulmans.
- La seconde stratégie pourrait être définie comme la stratégie irakienne, une sorte d'Internationale du Jihad, anarchique et chaotique, avec une structure assez souple et dont le seul objectif consiste à affronter un ennemi (quitte à en créer un de toutes pièces s'il n'en existe plus). Il s'agit de professionnels de la guerre, qui ne savent plus rien faire d'autre que combattre. Zarkawi en Irak ou Muqrin en Arabie Saoudite étaient le reflet de cette stratégie.

....

(2) En moyenne, cela représente environ 200 connexions par jour.

- Une troisième stratégie pourrait être qualifiée de « stratégie marketing », à la fois pragmatique et dépendant du « marché » potentiel accessible. Cette stratégie est actuellement en train de se développer fortement.

Conclusion

La propagande jihadiste est devenue incontournable sur Internet. La nébuleuse Al Qaïda utilise la Toile parce que c'est un moyen souple, peu coûteux et simple d'utilisation, mais aussi parce que toute information est par définition invérifiable. Compte tenu de la violence verbale de cette propagande, et de sa relative capacité de persuasion, il peut être tentant de chercher à fermer ces sites. Cela serait parfaitement justifiable et justifié.

Cependant, il faut aussi considérer le fait, antinomique, que ces mêmes sites sont également des sources d'information privilégiées désignant les populations visées, les cibles potentielles, etc. Ils sont aussi le révélateur des stratégies internes d'Al Qaïda, des divergences et des antagonismes. A ce titre, ils contribuent à comprendre un ennemi souvent insaisissable et qu'il convient de neutraliser avant le passage à l'acte terroriste.

En définitive, il n'existe pas de posture adéquate ou de conduite à tenir simple : d'une certaine façon, et c'est une forme de victoire, les jihadistes nous ont enfermés dans un paradoxe.

Walter AKMOUCHE, Henri HEMERY

Bibliographie

AKMOUCHE (W.), 2006, « La mouvance salafiste internationale et Internet », *Revue Défense nationale et sécurité collective*, n°8-9, août-septembre.

BAUER (A.), RAUFER (X.), 2005, *L'énigme Al-Qaïda*, Paris, Lattès.

BROWN (L.), 2006, *Cyberterrorism And Computer Attacks,* New York, Novinka Books.

BUNT (G.), 2003, *Islam in the Digital Age: E-Jihad, Online Fatwas and Cyber Islamic Environments, Londres,* Pluto Press.

DEROY (F.), 2008, « La stratégie de communication d' Al-Qaïda », *Revue de la Défense nationale et de la sécurité collective*, mars 2008.

DUNNIGAN (J.), 2003, *The Next War Zone: Confronting the Global Threat of Cyberterrorism,* New York, Citadel.

ELLUL (J.), 1962, *Propagandes*, Paris, Armand Colin, réédition Economica, collection Classiques des sciences sociales, 1990.

LE BON (G.), 1895, *La psychologie des foules*, Paris, Ed. Felix Alcan, réédition PUF, collection Quadrige, 2003.

Les nouvelles menaces criminelles numériques

Laurence IFRAH

© Gettyimages

La menace numérique n'a jamais été si préoccupante. Aujourd'hui, les médias communiquent régulièrement sur ce fléau et les utilisateurs sont beaucoup mieux informés des risques qu'ils encourent à surfer sur la toile. Pourtant, les organisations criminelles qui opèrent sur Internet n'ont jamais été aussi puissantes. Elles ne visent plus seulement l'ensemble des internautes, mais des utilisateurs ciblés selon un profilage précis du type de victime auquel correspond une forme d'attaque spécifique.

The New Threats of Electronic Crime

The threat of electronic crime has never been so preoccupying. Today's media regularly communicate to the public the nature of this scourge and citizens are much better informed of the risks they run when surfing on the net. Nevertheless, the criminal organisations that operate on the net have never been so powerful. They no longer target all users, but now aim at particular categories of the population that have been carefully profiled as vulnerable victims.

Laurence Ifrah

Criminologue spécialisée en criminalité numérique au Département de recherches sur les menaces criminelles contemporaines (DRMCC) de l'Institut de criminologie de Paris, Université Paris II Panthéon-Assas, consultant en sécurité des systèmes d'information, expert en recouvrement de données et en analyse de supports numériques. Elle a été auditeur de la 19e session nationale de l'INHES. Elle intervient auprès des étudiants de 3e cycle du DRMCC sur la criminalité numérique et auprès de l'Institut d'études judiciaires.

La communauté internationale commence enfin à prendre conscience de l'urgence à mettre en place des moyens de protection contre le cybercrime. Des pays comme les États-Unis et l'Estonie ont mis en œuvre des structures offensives et défensives capables d'analyser et de répliquer à de nombreuses formes d'attaques, après avoir subi des offensives répétées et parfois massives. Les moyens utilisés seront forcément les mêmes d'un côté comme de l'autre, ce qui implique que les éditeurs d'antivirus devront éviter de reconnaître certaines signatures de « malwares » pour permettre aux États d'infiltrer à distance des ordinateurs ciblés. Il ne reste qu'à espérer que les organisations criminelles ne profitent pas de cette aubaine pour mieux développer leurs activités car leurs moyens budgétaires sont bien souvent supérieurs à ceux des administrations, au quotidien en tout cas.

La progression du crime numérique

Quelques faits récents

Voici quelques faits récents qui démontrent l'inquiétante progression du crime numérique en 2008, tant au niveau de la technologie qu'au niveau des vecteurs de diffusion.

Avril 2008

L'achat de périphériques de stockage de données devient risqué, et il est désormais préférable de passer un antivirus et de formater le matériel avant de l'utiliser. Des disques durs et des clés USB ont été altérés pendant leur production en Chine et diffusés sur le marché occidental à l'insu des marques et des distributeurs. Fait nouveau depuis novembre 2007, des éditeurs d'antivirus ont constaté la présence de chevaux de Troie sur des disques durs et des clés USB neufs. Après enquête, il s'est avéré que les infections de ces matériels avaient eu lieu sur les sites de production dans des usines basées en Chine. L'éditeur Kaspersky a été le premier à faire état du problème sur les disques durs Maxtor de Seagate qui contenaient un cheval de Troie chargé, entre autres, de désactiver et de récupérer les mots de passe des joueurs en ligne pour les expédier sur un serveur basé en Chine et de désactiver les antivirus. L'entreprise a confirmé la situation sur son site Web et fait immédiatement rappeler 3 600 disques durs de 500 Go. Puis, c'est au tour de Hewlett-Packard, en Australie, d'apprendre que des clés USB de 256 Mo et de 1 Go offertes à ses nouveaux clients (acheteurs d'imprimantes) avaient également été corrompues, à leur insu, par un code malveillant. En janvier, c'était l'importateur hollandais qui proposait à la vente des lecteurs médias de la marque Victory LT-200, également fabriqués en Chine. Ces périphériques propageaient un ver sur les machines connectées à un réseau de partage de fichiers [1].

Mai 2008

Les moyens de compromission des ordinateurs sont plus sophistiqués et il devient difficile de différencier la mise à jour d'un produit licite de celle d'un code malicieux. L'affichage est identique et paraît le plus souvent légitime. En mai 2008, plus d'un demi-million de pages Web ont été compromises par Zlob Trojan (figure 1), un cheval de Troie déguisé en décodeur vidéo. Les internautes étaient invités à télécharger un utilitaire pour visualiser les vidéos proposées sur les sites Internet. En cliquant dans la fenêtre affichée, ils installaient le malware qui permettait au pirate de prendre le contrôle à distance de leur ordinateur.

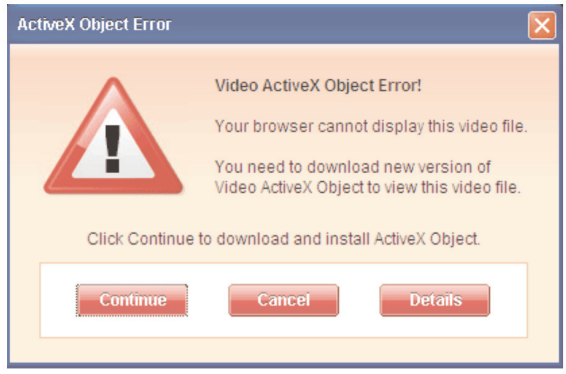


Figure 1 - Zlob Trojan

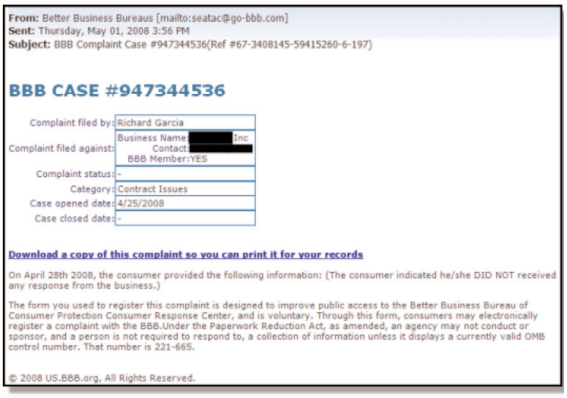
Les nouvelles versions de « spams » infectés par des chevaux de Troie ne sont plus envoyées en masse à n'importe quel destinataire, ils sont à présent conçus pour des victimes préalablement sélectionnées en fonction de leur activité dans l'entreprise qui les emploient. Des cadres supérieurs de très grands groupes américains ont été visés par un e-mail frauduleux prétendant émaner du Better Business Bureau [2] aux États-Unis, et qui ouvre les systèmes d'information de leur entreprise aux pirates [3]. L'e-mail précisait le nom du destinataire, sa fonction et les coordonnées de la société qui l'employait. Le texte indiquait

(1) www.viruslist.com

(2) Le Better Business Bureau est un conseil d'éthique commercial chargé des relations entre les entreprises et les consommateurs. Il est présent aux États-Unis et au Canada dans plus de 140 villes.

(3) www.f-secure.com

qu'une plainte avait été déposée à l'encontre de son entreprise et l'invitait à télécharger le document en cliquant sur un lien qui demandait de télécharger une mise à jour du logiciel Acrobat de l'éditeur Adobe ainsi qu'un contrôle ActiveX. Ce dernier, une fois installé, ouvrait une « backdoor » [4] qui donnait accès au système d'information et permettait de collecter des données personnelles et confidentielles. Autre détail, le lien dirigeait l'internaute vers le site www.us-bbb.com alors que l'adresse véritable du Better Business Bureau est www.us-bbb.org (figure 2).


From: Better Business Bureaus [mailto:seatac@go-bbb.com]
Sent: Thursday, May 01, 2008 3:56 PM
Subject: BBB Complaint Case #947344536(Ref #67-3408145-59415260-6-197)

BBB CASE #947344536

Complaint filed by: Richard Garcia
Complaint filed against: Business Name: [redacted] Inc
Contact: [redacted]
BBB Member:YES
Complaint status: -
Category: Contract Issues
Case opened date: 4/25/2008
Case closed date: -

Download a copy of this complaint so you can print it for your records

On April 28th 2008, the consumer provided the following information: (The consumer indicated he/she DID NOT received any response from the business.)

The form you used to register this complaint is designed to improve public access to the Better Business Bureau of Consumer Protection Consumer Response Center, and is voluntary. Through this form, consumers may electronically register a complaint with the BBB.Under the Paperwork Reduction Act, as amended, an agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number. That number is 221-665.

© 2008 US.BBB.org, All Rights Reserved.

Figure 2 - e-mail frauduleux ciblé

Autre exemple, un pirate chilien a publié sur deux sites internet les informations personnelles de six millions de ses compatriotes après les avoir récupérées sur des bases de données du gouvernement. Ces données comportaient entre autres, les noms, prénoms, adresses et numéros de téléphone des victimes [5].

Juin 2008

Un gang de pirates exploite actuellement les événements de l'actualité internationale en diffusant de faux flashs d'information via des spams infectés [6]. L'éditeur d'antivirus Sophos a intercepté des e-mails dont les titres sont liés à la présence des forces armées américaines au Moyen - Orient :

- la troisième guerre mondiale a débuté ;
- 20 000 soldats américains en Iran ;
- l'armée américaine a franchi la frontière iranienne.

Juillet 2008

Une faille DNS [7] découverte en début d'année par Dan Kaminsky, expert en sécurité des systèmes d'information chez IOActive, aurait pu être à l'origine d'un véritable désastre économique sur Internet. Les serveurs DNS assurent la correspondance entre un nom de domaine (par exemple : www.google.fr) et son adresse IP (209.85.135.99), un système mis au point pour simplifier la saisie des adresses d'un site Internet car il est plus facile de se souvenir de www.google.fr que de 209.85.135.99. Les serveurs DNS disposent de caches pour garder en mémoire les adresses saisies par les internautes, ceci permet de diriger l'utilisateur directement sur le site de son choix en réduisant le temps d'attente et sans avoir à solliciter constamment les autres serveurs DNS. La faille décelée (aussi connue depuis 2004 [8] sous le nom de DNS « pharming » ou encore de DNS cache « poisoning ») permet à un pirate de modifier ces caches à distance pour rediriger les internautes sur des sites de « phishing ». Ces derniers, alors convaincus d'être sur des sites légitimes, communiquent sans hésitation leurs informations personnelles.

Ce sont là quelques-uns des faits marquants de l'année 2008. Dans la société de l'information, le vrai danger c'est ce que l'on n'a pas vu, pas su ou pas pu voir. Nous ne reprendrons pas ici les poncifs et sempiternels exemples ressassés partout, mais ce qui se passe vraiment aujourd'hui, en 2008, avec pour perspectives les nouvelles menaces informatiques, celles qui seront dominantes et qui émergent aujourd'hui.

L'explosion des malwares [9]

Le premier million de malwares (dont 60 % de chevaux de Troie), en circulation sur Internet, sera atteint et même largement dépassé au courant du deuxième semestre 2008, soit plus du double depuis le début de l'année. Quelle que soit la technique employée pour permettre la diffusion de ces codes malicieux, il n'existe que deux moyens de les transmettre sur un ordinateur :

- la vulnérabilité système ou applicative ;
- le « Social Engineering » [10].

....

(4) Porte dérobée.
(5) www.TheRegister.co.uk
(6) Sophos antivirus.
(7) *Domain Name System*.
(8) www.idg.net
(9) Contraction des mots *malicious* (pour code malicieux) et *software* (pour logiciel).
(10) L'art de la manipulation de personnes tierces, souvent crédules, qui représentent le point central d'une attaque afin d'obtenir des informations confidentielles permettant d'accéder à des ressources protégées.

La vulnérabilité système ou applicative

La vulnérabilité système est toutefois moins exploitée que l'applicative ; le « Drive-by download » est une technique qui utilise les failles présentes dans les logiciels tels que les navigateurs Internet pour y insérer des codes malveillants qui s'installent automatiquement et en toute transparence sur les ordinateurs des internautes, sans intervention de leur part. Pour infecter le plus d'internautes possible, les pirates injectent du code malveillant (JavaScript) sur les pages des sites web les plus populaires comme les moteurs de recherche ou les magazines en ligne. Les éditeurs s'efforcent de publier des mises à jour correctives dans les meilleurs délais pendant que les organisations criminelles offrent des sommes allant jusqu'à 75 000 dollars pour obtenir l'information et l'exploiter le plus longtemps possible.

Le Social Engineering

Le social engineering, utilisé depuis des années, prend aujourd'hui une tournure plus perfide. Ce mode opératoire, particulièrement prisé par les organisations criminelles (majoritairement situées en Russie, en Ukraine, en Roumanie et dans d'autres pays d'Europe de l'Est), est utilisé pour installer des codes malveillants destinés à leur permettre de prendre le contrôle à distance des ordinateurs des utilisateurs. Le professionnalisme dont ces organisations font preuve se remarque dans cette formidable capacité à tromper l'utilisateur et à améliorer en permanence les techniques d'approche, en réalisant un ciblage précis de leurs futures victimes grâce à des leurres de plus en plus sophistiqués. Ainsi, de nombreux e-mails ont été envoyés à des cadres supérieurs dans des entreprises. Les messages indiquent précisément le nom, le poste de la victime et celui de sa société. Ils émanent d'organismes d'État comme le FBI, le fisc ou la Cour de Justice et semblent parfaitement crédibles (figure 3).


From: United States District Court [subpoena@uscourts.com]
To: Steve Kirsch
Cc:
Subject: Subpoena in case #28-755-YCH

AO 88(Rev. 11/94) Subpoena in a Civil Case

Issued by the
UNITED STATES DISTRICT COURT

Issued to: Steve Kirsch
Propel Software Corporation
408-571-6300

SUBPOENA IN A CIVIL CASE

Case number: 28-755-YCH
United States District Court

YOU ARE HEREBY COMMANDED to appear and testify before the Grand Jury of the United States District Court at the place, date, and time specified below.

Place: United States Courthouse
880 Front Street
San Diego, California 92101

Date and Time: May 7,2008
9:00 a.m. PST

Room: Grand Jury Room

Figure 3

Des attaques politiques

Les attaques motivées par l'actualité politique sont également en nette progression. Lors du conflit récent entre les militaires chinois et les Tibétains, de nombreux e-mails piégés ont envahi les forums des organisations humanitaires qui soutenaient « la libération » du Tibet. Les internautes, soigneusement ciblés en fonction de l'importance de leur soutien aux « rebelles », recevaient des e-mails au contenu parfois illustré par des photos de Tibétains malmenés par des militaires chinois. Ces e-mails semblaient être expédiés par des personnes de confiance, parfaitement connues des destinataires (figure 4). Les chevaux de Troie présents dans les fichiers joints aux formats standards des logiciels de bureautique permettaient à ses expéditeurs d'espionner les ordinateurs de leurs victimes à leur insu. Selon F-Secure, des malwares similaires ont été repérés dans des attaques contre des entreprises, ce qui porterait à croire que les auteurs de ces codes offensifs seraient motivés par des raisons politiques mais également intéressés par les activités de l'industrie liées au secteur de la Défense.

50 % des attaques sont réalisées pour des motifs idéologiques. Les partis politiques, leurs candidats et certains départements d'États subissent régulièrement des défacements de leurs sites Web sur lesquels les opposants laissent des messages de propagande. On note une hausse sensible de ces défacements à l'approche d'élections.

```
All,
Attached here is the update Human Rights Report on Tibet issued by
Department of State of U.S.A on March 11, 2008.
You may also visit the site:
Tashi Deleg,
Sonam Dagpo
Secretary of International Relations
Department of Information & International Relations
Central Tibetan Administration
Dharamshala -176215
H.P., INDIA
Ph.: [obfuscated]
Fax: [obfuscated]
E-mail: [obfuscated]@gov.tibet.net or diir-pa@gov.tibet.net
Website: http://www.tibet.net/en/diir/
```

Figure 4 - E-mail piégé

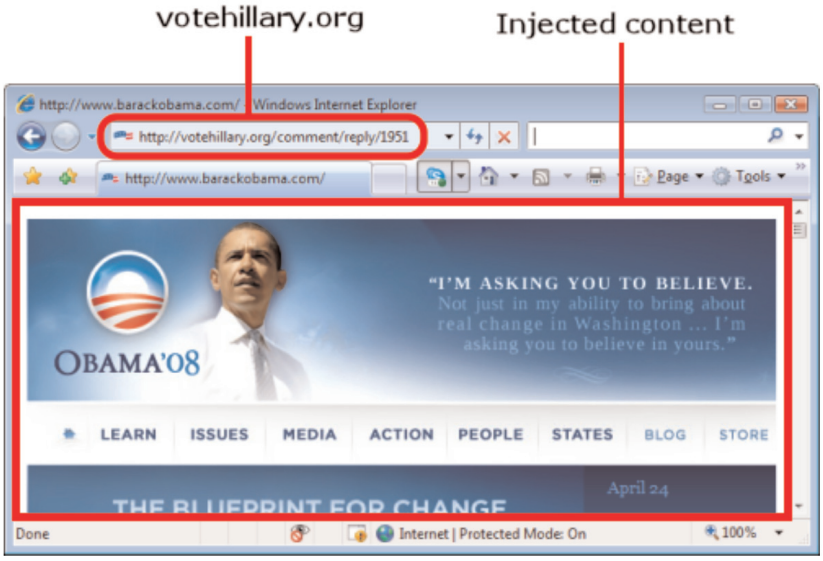


Figure 5 - Redirection du site d'Obama vers celui de Clinton
Source : www.barackobama.com

En avril 2008, le site de Barrack Obama a été attaqué par une injection de code qui lors de la saisie de l'url de son site web, redirigeait les internautes vers celui de sa rivale Hillary Clinton (figure 5).

Les nouveaux « Botnets »

À l'origine de la diffusion de tous ces maux, se trouve une technique d'attaques massives, les botnets. Jusqu'en 2006, on pouvait détruire un botnet en supprimant le poste de contrôle et de commande du pirate que l'on tentait de retrouver plus ou moins aisément. Aujourd'hui, et ce depuis l'apparition au début de l'année 2007, d'une nouvelle forme de Botnet dont Storm Worm (conçu par la tristement célèbre organisation criminelle RBN [11]), qui se propage sur les réseaux Pair-à-pair (*Peer2Peer*), il est impossible de localiser ce poste de commande. Entre juin et juillet 2007, 1 700 000 machines étaient infectées contre 2 817 entre mai et juin 2007. 71 342 attaques ont pu être bloquées les cinq premiers mois de 2007 ; elles sont passées à plus de 20 millions entre juin et juillet [12]. Le 24 juillet 2007, sur 46,2 millions de spams détectés, plus de 99 % contenaient le ver Storm [13].

Technique et stratégie

Le système pair-à-pair permet de nommer un ensemble constitué d'utilisateurs (en nombre pas forcément défini, ni fixe, mais plutôt de manière générale), du protocole qui leur permet de communiquer (Gnutella, BitTorrent, CAN, etc.), et du fonctionnement du protocole entre ces machines. Le terme de « réseau pair-à-pair » permet de désigner les machines et leur interconnexion à un moment donné, avec un nombre défini de machines/utilisateurs.

Dans un système pair-à-pair, les postes utilisateurs ne jouent pas exclusivement les rôles de client ou de serveur mais peuvent assurer parallèlement les deux fonctions. Ils sont en effet simultanément clients et serveurs et jouent aussi le rôle de routeur, en passant les messages de recherche, voire les données vers leurs destinataires. Cette architecture réseau permet ainsi aux Botnets de se déployer, sans qu'il soit possible de localiser le poste de contrôle et de commande principale, chaque ordinateur infecté étant un porteur du virus indépendant, si un poste est supprimé, un autre prend immédiatement la relève. À ce jour, il n'a pas été possible de quantifier précisément le nombre de PCs compromis par Storm, mais on a évalué le Botnet à environ 20 millions de machines, au plus fort de sa

(11) Le *Russian Business Network* est aussi l'auteur de nombreux logiciels offensifs dont MPack qui a été mis à disposition dans une version commercialisée à 700 dollars l'unité, sur les forums russophones lors des attaques contre l'Estonie, en avril 2007.
(12) *SecureWorks*.
(13) *Cf.* Postini, spécialiste de la messagerie hébergée sécurisée.

performance. Aucune parade n'a été mise en place, et les experts en sécurité des systèmes d'information affirment qu'aucune forme de protection disponible actuellement ne pourrait stopper une attaque de déni de service lancée par Storm. Un groupe de chercheur finlandais a cependant tenté de tuer le vers en infectant le code malveillant, une tentative réussie temporairement car une des particularités de Storm est sa capacité à mettre à jour ses propres failles en quelques heures. Storm est le premier botnet intelligent, il sait sélectionner les ordinateurs bénéficiant du haut débit pour diffuser ses spams infectés afin d'agrandir son réseau, soit environ 30 000 à 40 000 spams par heure et par ordinateur zombie. Outre l'envoi de spams, il est utilisé pour diverses formes d'attaques, le phishing, le Ddos (Déni de service distribué), les attaques sur messageries instantanées, etc. Storm est également pourvu de capacité de défense et s'attaque violemment aux organisations spécialisées dans la lutte contre les botnets en activant son réseau de PCs zombies pour lancer des connexions simultanées - par centaines de milliers - sur leurs serveurs, afin de les rendre indisponibles.

Mais rappelons-le, le spam n'est que la partie visible de l'iceberg, les botnets ont beaucoup de ressources et sont générateurs de revenus substantiels, parmi les nombreuses activités, les plus courantes sont :

- le « Pump and Dump » ;
- la vente de produits illicites en ligne ;
- le chantage, la menace et l'extortion (casinos et *book-makers*) ;
- l'nstallation à distance d'outils offensifs (« Keyloggers ») ;
- la collecte d'informations personnelles (fraude bancaire et identitaire) ;
- la corruption de réseaux sensibles pour accéder à des données confidentielles (espionnage industriel) ;
- les attaques de Ddos (Déni de service distribué, dans le cas de l'Estonie ou des entreprises spécialisées dans la lutte contre le crime numérique).

Le Pump and Dump est une escroquerie bien connue des marchés boursiers qui consiste à gonfler artificiellement le cours d'une entreprise avant de vendre d'un coup toutes les actions dont le détenteur majoritaire dispose, et de la mettre généralement en faillite. Grâce à son réseau d'ordinateurs zombies, Storm a diffusé des millions de spams aux internautes pour les inciter à acheter des actions de sociétés sélectionnées pour ce type d'opération. Des prix attractifs et une bonne communication semblaient rendre l'affaire prometteuse. Les futures victimes ont fait monter le cours de l'action jusqu'au jour où les malfaiteurs ont vendu en masse et se sont retirés en empochant une plus value conséquente. Ainsi, le 7 août 2007, Sophos, éditeur d'antivirus, a détecté plus de 500 millions d'e-mails conseillant aux internautes d'investir dans la société Prime Time Stores Inc., domiciliée à Puerto Rico. Cette campagne a généré, en 24 heures, une hausse spectaculaire de 30 % du nombre de spams dans le monde.

Storm est, entre autres, utilisé pour promouvoir la vente de médicaments en ligne via des pharmacies virtuelles qui délivrent au client des produits de contrefaçon originaires de Russie et d'Inde. Selon IronPort [14], filiale de Cisco, ces revenus seraient dédiés au développement du Botnet et d'autres malwares. Pour éviter la localisation de ces sites illicites, Storm utilise les techniques de fast-flux DNS qui permettent d'attribuer des milliers d'adresses IP à un même nom de domaine. Le système fonctionne de la façon suivante. Un individu possède un site dont le nom de domaine est, imaginons, www.pharmacie.com. Pour que les internautes puissent s'y connecter, il faudra leur attribuer une adresse IP, par exemple 80.246.10.132. Il est possible de bloquer cette IP pour que personne ne puisse s'y connecter. Pour éviter de se faire repérer, les malfaiteurs utilisent une technique parfaitement légale de répartition de charge de serveurs DNS afin d'empêcher une saturation en cas de connexions multiples. À la seule différence qu'au lieu d'effectuer cette répartition de charge sur des serveurs DNS, ils vont utiliser leurs Botnets et les milliers d'ordinateurs infectés pour attribuer autant d'adresses IP à leur nom de domaine. Ces IP seront alors celles des ordinateurs compromis des utilisateurs qui ignorent totalement l'activité se déroulant sur leurs machines. Cela permet ainsi de changer l'adresse IP toutes les trois minutes, une fois l'IP du site sera localisée en France, une autre fois en Suède ou en Chine. Le Fast-Flux DNS est une technique qui évite aux malfaiteurs de se faire localiser et leur offre une redondance optimale.

Storm est extraordinairement créatif en matière de Social Engineering, son vecteur d'infection favori. Depuis sa création, il a diffusé des dizaines de versions de spams infectés sur des thèmes continuellement adaptés à l'actualité, aux événements sportifs, aux fêtes de Noël, du jour de l'An, de la Saint-Valentin et même à la sécurité informatique, en promouvant la vente de logiciels « antispyware » qui, bien-sûr, étaient chargés de corrompre les ordinateurs des internautes crédules.

••••

(14) *Special Report* – 2008 Internet *malwares trends*.

Depuis, cette technique a fait des émules et les malfaiteurs s'en sont inspirés pour créer des botnets, toujours plus performants et plus malveillants. Bobax, Kraken, Mayday et Mega-D sont les nouvelles versions en circulation sur la toile. Kraken aurait infecté en avril 2008, cinquante des entreprises du Fortune 500 et serait indétectable par plus de 80 % des antivirus [15].

Quelques réflexions prospectives

Il s'agit désormais de prendre conscience de l'étendue des compétences de très haut niveau dont disposent les organisations criminelles. Il n'y a pas « seulement » l'aspect technique informatique, mais un ensemble de professionnels issus de la finance, du domaine juridique, du marketing et de la communication et, dans certains cas, (médicaments, stupéfiants et autres produits illicites) de la logistique. Plus récemment, on note la présence de traducteurs et de rédacteurs (souvent des « correspondants locaux »), chargés de rédiger des textes convaincants dans la langue du pays ciblé (rarement le même que celui d'où l'attaque est originaire), ces derniers sont parfois des acteurs de l'intelligence économique, experts dans l'art de la manipulation.

Ces nouvelles tendances prennent des proportions alarmantes, d'autant plus que les internautes mieux informés sur les risques qu'ils encourent notamment par e-mail, se fient à des points de reconnaissance qui leur ont été répétés depuis des années, à savoir n'ouvrir qu'un e-mail qui provient d'une personne connue, qui leur est adressé nominativement et dont le sujet les concerne. Des éléments qui ne correspondent désormais plus à la réalité.

Les États seront amenés à court terme à créer des cellules réunissant les mêmes compétences, c'est-à-dire des experts du blanchiment d'argent et de la finance, de l'intelligence économique, de la géopolitique, de la logistique, du trafic de stupéfiants et de la contrefaçon, du terrorisme, de l'énergie, des stratèges (militaires), des criminologues et des avocats pour lutter efficacement contre l'envahissement de la toile par les malfaiteurs qu'ils soient criminels, terroristes ou hacktivistes. S'en tenir exclusivement aux aspects techniques serait une coûteuse erreur.

Laurence IFRAH

(15) http://www.darkreading.com/

Les technologies numériques du futur :
Nouvelles menaces, nouvelles vulnérabilités

Michel RIGUIDEL

Doit-on craindre un Hiroshima numérique, une future guerre impitoyable des réseaux ? Doit-on redouter un Tchernobyl numérique où des apprentis sorciers provoqueraient une panne cataclysmique ? Peut-on imaginer la conjugaison d'attaques et de pannes entremêlées ? Cet article présente un état des lieux, analyse les menaces et les vulnérabilités futures, remet en question quelques dogmes en sécurité numérique et ouvre des perspectives de recherche.

The Digital Technologies of the Future: New Threats and New Vulnerabilities

Should we fear a digital Hiroshima, an unsparing network war? Should we be wary of a digital Chernobyl where any sorcerer's apprentice may provoke a cataclysmic breakdown? Is it possible to imagine a combined attack and breakdown? It is important to analyze our current situation, future threats and vulnerabilities so as to call into question some of our security dogmas in order to open new perspectives and fields of research.

Michel Riguidel

Michel Riguidel est chef du département Informatique et Réseaux à Télécom ParisTech, anciennement, École nationale supérieure des télécommunications. Il enseigne la sécurité et les réseaux avancés. Il consacre sa recherche à la sécurité des réseaux du futur, avec un engagement fort dans la Communauté européenne. Il a publié *Le téléphone du futur* (Pommier, 2004), dirigé la publication *La sécurité à l'ère numérique* (Hermès, 2004) et le chapitre sur la sécurité des systèmes et des réseaux de *L'encyclopédie informatique et des systèmes d'information* (Vuibert, 2006).

La fragilité du Village virtuel violent

Le cyberespace : deux gros nuages enchevêtrés

La dépendance de l'humanité envers les fragiles édifices numériques est devenue inquiétante. Les édifices numériques sont Internet et le Web, les réseaux de télécoms, de diffusion de télévision, de constellations satellites, les systèmes d'information des entreprises, des administrations et des institutions, les systèmes informatiques critiques de contrôle des infrastructures nucléaires, électriques, routières, hospitalières, logistiques, les systèmes de contrôle-commande (alarme, climatisation des immeubles, électronique des voitures), les réseaux WiFi à la maison.

Le Village virtuel violent des citoyens et des entreprises constitue un halo intangible, une enveloppe composée de deux nuages intriqués : le nuage actif dispersé des programmes informatiques de plus en plus opaques, mobiles et devenus incontrôlables, et le nuage passif éparpillé des informations volatiles ou persistantes. Ce cyberespace s'est réincarné en une vulnérabilité béante dans nos sociétés développées, ouvert à tous les vents agressifs ou subversifs, dans lesquels peuvent s'immiscer et se dissimuler ceux qui vivent en marge des lois de nos sociétés, et ceux qui combattent les valeurs de nos civilisations. Le danger majeur de ce règne numérique, récemment installé aux côtés des règnes animal, végétal et minéral, dans sa complexité inextricable et dans son usage critique, résulte essentiellement, pour son volet technique, de la faiblesse architectonique des infrastructures, de l'obscurcissement du nuage des logiciels d'une part, et de l'expansion envahissante du nuage des données disséminées, d'autre part.

En effet, les logiciels sont de plus en plus obscurs : secret de fabrication oblige, cette éclipse partielle marque l'échec du mouvement des logiciels libres qui rêvait d'un monde dématérialisé, ouvert et transparent. Par ailleurs, dans un univers de compétition, la valeur d'un pays se mesure, entre autres, par la valeur de ses biens intangibles : droits de propriété intellectuelle, logiciels, bibliothèques, musées, contenus vidéo et cinéma, organisations numérisées. Enfin, le volume des données double chaque année, croissance encouragée par la baisse du prix des supports de stockage qui diminue dans ce même rapport. Chaque individu possède en moyenne un patrimoine de dizaines de gigaoctets, masse considérable de logiciels boursouflés, d'informations fongibles, surabondantes, magma de bits pléthoriques quand on le compare aux quelques centaines de mégaoctets qui suffisent à conserver toute l'œuvre de Jean Sébastien Bach, de Victor Hugo ou aux quelques téraoctets pour mémoriser tout le cinéma muet ! [Riguidel, 2006, p. 83].

L'usage numérique en évolution rapide

La résistance des infrastructures numériques a dû se renforcer ces dernières années pour faire face aux sollicitations croissantes d'échanges massifs en temps réel. Leur seuil de tolérance aux pannes et aux attaques a augmenté lorsque l'on considère les variations sévères de flux, l'immédiateté des requêtes d'internautes, l'impatience des adeptes de SMS ou du téléphone mobile, l'addiction des adolescents envers des applications ludiques multijoueurs. La technologie numérique soutient les infrastructures vitales, supporte l'urgence d'une alarme, étaye la défense d'un pays. Cette clef de voûte façonne aussi le divertissement et contribue à l'ampleur de la société du contact et du spectacle.

L'usage numérique s'est profondément modifié du côté des citoyens et des entreprises : la messagerie, l'affichage, la recherche d'informations sur le Web ont été supplantés par le commerce électronique, par des services plus appropriés, avec des objectifs de performance et d'instantanéité, une exigence d'urgence au détriment de la réflexion, de la vraie communication et d'une vision à long terme. Le dimensionnement de ces infrastructures anticipe, avec une avance de quelque dix-huit mois seulement, la lente et sûre progression des ressources informatiques, ce qui permet d'absorber toutes les requêtes des utilisateurs : ressources de trafic sur les réseaux optiques, de bande passante radio, de stockage des serveurs et de puissance de calcul. Mais le paysage informatique, autrefois filet diffus de routes et de serveurs informatiques, se modifie en autoroutes pratiquement congestionnées, en centres stratégiques d'aiguillages (comme le *Global Internet eXchange*, nœuds d'interconnexion de réseaux d'Amsterdam), en pôles archi-concentrés de serveurs (comme le site de Google). Les flux gigantesques (100 Gigabits/s) de données entre Systèmes autonomes fusionnent et se concentrent : une congestion de ces infrastructures est à craindre [1].

(1) Le 24 février 2008, le site web *YouTube* a été inaccessible, suite à une action délibérée venant du Pakistan, par un détournement d'adresse IP sur le protocole BGP (Border Gateway Protocol), le protocole de l'Internet pour les interconnexions entre opérateurs, à cause de vidéos blasphématoires.

En outre, le Web, tissu déchiqueté d'utilisateurs novices, constitue un monde angélique de coopération, les protocoles de communication étant aujourd'hui employés loyalement. Mais, si un nombre significatif, pas forcément élevé, d'utilisateurs détournait la fonction normale des logiciels de base et des protocoles en téléchargeant et installant un ersatz malveillant à partir du Web, rien ne fonctionnerait plus [2].

La responsabilité excessive des utilisateurs otages

Le patrimoine numérique, entrelacs d'infosphères

Chaque bit du cyberespace est la propriété [3] d'une personne physique ou morale. L'ensemble des bits (données et logiciels) dont on est possesseur, constitue l'infosphère personnelle [Riguidel, 2004]. Ce peut être l'infosphère d'un utilisateur standard (ses données personnelles sous son contrôle, ses données hors de sa portée dans les bases de données de ses fournisseurs, les traces de géolocalisation chez son opérateur de télécoms), mais ce peut être aussi l'infosphère d'un éditeur de logiciel, laquelle s'étend sur des millions d'ordinateurs d'usagers.

Chaque bit du cyberespace est utilisé par un usager principal. L'ensemble des bits (données et logiciels) que l'on utilise, constitue le patrimoine numérique personnel. L'usager est aujourd'hui responsable de son patrimoine. Ce patrimoine, en général, ne lui appartient pas, car l'usager final utilise de nombreux logiciels, dont il n'est pas propriétaire, mais dont il acquiert seulement la licence d'utilisation. Les deux notions de patrimoine et d'infosphère s'entrecroisent puisque chaque utilisateur exploite de nombreux fragments d'infosphères qui appartiennent à de multiples propriétaires. L'usager standard est de plus en plus prisonnier des logiciels qu'il utilise. Sa vie privée est menacée, car il possède une infosphère personnelle visible par les infosphères opaques des propriétaires de logiciels qui recueillent des données directes ou indirectes, à son insu. Et pourtant, quand l'usager commet une erreur sur son patrimoine, il est le seul responsable.

La souveraineté perdue de l'infosphère personnelle

La souveraineté numérique du cyberespace est mise à mal, ce qui soulève une inquiétude majeure dans nos sociétés démocratiques fondées sur la responsabilité des personnes physiques ou morales. Les usagers, qui sont responsables des actions et des préjudices provoqués par l'utilisation des logiciels dont ils ont payé la licence, ne contrôlent plus l'exécution de ces logiciels. Un ordinateur personnel, sous la responsabilité de son utilisateur, exécute des centaines de processus que le novice, ou même l'expert, ne maîtrise absolument plus, comme la mise à jour des applications, des antivirus, du système d'exploitation. On lui demande seulement de cliquer ! L'usager responsable maîtrise de plus en plus mal son patrimoine numérique, modifié en temps réel et en flux tendus par les différents propriétaires, sans que le gestionnaire de ce patrimoine soit réellement informé.

La dignité évincée de l'infosphère personnelle

La dignité numérique [Riguidel, 2006, p. 521] des usagers responsables risque d'être bafouée si on ne réagit pas rapidement, en émettant des règles dans le monde virtuel, règles similaires aux principes du monde réel, et en renouvelant les outils de prévention et de régulation de l'écosystème. Les utilisateurs sensibilisés (personnes ou entreprises) savent protéger la partie de leur infosphère privée, engendrée de leur plein gré et sous leur contrôle. En revanche, la partie de l'infosphère intime des individus et des entreprises, qui est hors de leur portée et enregistrée à leur insu, leur échappe totalement. Toute leur vie privée est fragilisée par une intrusion potentielle de leur infosphère, en dehors de leur contrôle et par l'enregistrement des traces numériques de leur comportement, qu'ils laissent à leur insu, via leur attirail numérique ou leur avatar sur l'espace virtuel. Chaque individu écrit, sans le savoir, un journal intime éclaté, dans les registres des opérateurs, des fournisseurs d'accès à Internet, des sites web, des moteurs de recherche, que des « biographes », sortes de *big brother* ou détective masqué, risquent de reconstituer à des fins d'inquisition numérique ou de filature électronique, en dehors de toute législation.

(2) Corruption de TCP (Transmission Control Protocol), le protocole de transport fiable permettant à deux applications d'échanger des donnés, par exemple : pour éviter de « redémarrer à froid », suite à une congestion sur le réseau, rien n'empêcherait de modifier les protocoles de son ordinateur à des fins d'utilisation égoïste.

(3) La propriété numérique est complexe : dans le cas du dossier médical personnel, les données du dossier appartiennent au médecin, et non au patient qui ne peut qu'accéder à ses données de santé à caractère personnel.

La forme des attaques

Les deux chemins de la violence des attaquants

La violence numérique, prolongement naturel de la violence dans notre société, s'exprime de deux façons :

- en utilisant normalement de manière banale le support informatique afin de communiquer et d'échanger dans l'ombre (communauté de gens mafieux qui se retrouvent discrètement sur Internet, sectes qui utilisent le support informatique comme outil de propagande, de recrutement, marché noir, blanchiment d'argent sale, diffusion de fausses informations) ;

- en s'attaquant à des cibles désignées ou aveugles par l'exploitation des failles et vulnérabilités du système informatique (réseau distribué de robots logiciels furtifs offensifs, propagation de virus ou de messages intempestifs, utilisation ou création de failles informatiques pour gagner de l'argent et tromper des utilisateurs candides, blanchiment de code informatique sale via des logiciels téléchargeables, craquage de comptes informatiques de systèmes d'information peu protégés pour communiquer sournoisement sous une identité usurpée).

Les trois dimensions des cyberattaques

Les menaces informatiques s'inscrivent dans les trois dimensions, réelle, symbolique et imaginaire :

- L'attaque réelle, la délinquance informatique : on agresse, de manière aveugle ou ciblée, pour obtenir un gain réel de manière frauduleuse, récupérer ou falsifier une information dans un but criminel (fraude sur les cartes bancaires, les cartes SIM de téléphone ou les cartes de boîtiers de TNT, vol de mot de passe pour extorquer de l'argent, déverrouillage de consoles vidéos, usurpation d'identité, saisie ou falsification d'information pour de l'espionnage industriel).

- L'attaque symbolique, médiatique : on attaque l'image de la cible par la médiatisation même de l'agression et par ses répercussions sur l'opinion publique (défiguration de site web, pénétration dans un serveur informatique, guerre informatique). La publicité autour de ces attaques fait naître le doute et perdre confiance.

- L'attaque imaginaire, fictive ou simulée : on frappe l'imagination des utilisateurs à travers leur méconnaissance des systèmes. On intimide par des révélations, on gèle le comportement, on déstabilise. L'agresseur crée une peur irraisonnée ou fait semblant d'attaquer, la menace étant pire que l'exécution. On néglige trop souvent l'influence de ces attaques imaginaires. Les attaques dévoilées à grand renfort de tapage médiatique proviennent parfois des acteurs économiques, comme la supercherie du bug de l'an 2000, dans les années 1997 à 1999, contribuant à doper le marché, premier effet d'emballement avant la bulle Internet [4].

Un mélange des genres ou une combinaison de ces attaques est évidemment possible : leurre ou site attrape-nigaud, désinformation, déguisement de site web sous forme de cause noble pour récolter des fonds, saturation du trafic réseau pour empêcher une utilisation réelle d'un serveur (saturation des serveurs gouvernementaux d'Estonie en mai 2007, de Géorgie au début août 2008). L'attaque en déni de service pendant quelques heures des serveurs *Yahoo* et *Amazon* en février 2000, événement parfaitement anodin, fut le signal de l'éclatement de la bulle Internet en mars 2000. Ce sont aussi les inventions ou les alarmes d'informaticiens qui exposent des attaques hypothétiques, comme la faille dans les annuaires, début juillet 2008, du DNS (*Domain Name System*) par l'expert Dan Kaminsky [www.doxpara.com], qui a fait exagérément la une de journaux français.

Les nouvelles menaces, les nouvelles vulnérabilités

Les menaces et vulnérabilités actuelles

Depuis quinze ans, les grandes pannes informatiques d'infrastructures sont toujours dues, à l'origine, à des fautes de procédure dans des mises à jour irréversibles de logiciels : réparation à la hâte sans possibilité de revenir à l'état initial, déploiement d'un nouveau service réalisé sans mesurer les conséquences sur le reste des applications.

(4) La mystification du bug de l'an 2000, avec un battage médiatique incitant à remplacer les ordinateurs et un marketing orchestré par les éditeurs de logiciel, fut relayée par les pouvoirs publics.

La faille principale de l'Internet provient de l'usurpation d'identité. On se cache le visage avec un masque dans le dessein d'être anonyme ou de prendre la silhouette d'un autre. Les agressions de ce genre ont de multiples variations : usurpation d'adresse d'ordinateur (« spoofing »), de site web (« phishing », « pharming »), invasion par déni de service (à partir d'un « botnet »), effraction de l'annuaire DNS. Par ailleurs, il ne faut pas négliger la commercialisation des attaques avec l'émergence d'une économie parallèle des producteurs-distributeurs-consommateurs organisés, avec de véritables contrats d'utilisation de botnets.

Pourtant, les vulnérabilités et les attaques informatiques ont finalement un impact assez faible. Peu de pannes gigantesques affectent la réalité. Un virus informatique n'a jamais tué personne. Le coût des dommages créés par un bug ou un virus est souvent surestimé. Les chiffres de perte des entreprises, qui figurent sous les dommages, mélangent tout : trop d'argent est dépensé par manque de compétence informatique et méconnaissance des logiciels utilisés. Il n'existe d'ailleurs pas d'assurance tout risque en dommages de système d'information, pour la composante intangible, logiciels et données.

L'image des vulnérabilités actuelles, données par certains experts ou la presse, est différente. On parle de cybercriminalité, de cyberterrorisme, de grands périls, sans jauger avec exactitude la réalité des faits. Les éditeurs de logiciel accentuent cet effet : le marché de l'antivirus en France est florissant. L'épouvantail [5] des virus fut un message bien compris par ces éditeurs dont le mécanisme vampirise les processeurs, alors que l'intelligence des algorithmes antivirus est bien minime [Filiol, 2007].

Les menaces et vulnérabilités à venir

Les contenus illicites (pédophilie, racisme) du Web risquent d'être bientôt détrônés par des calculs illicites sur le réseau, plus dangereux encore pour le respect des individus (moteur de recherche pour fureter la sphère privée et répertorier des internautes) et la paix dans notre société (déni de service régionalisé). Des applications tentaculaires emprunteront bientôt pendant quelques minutes la puissance de votre ordinateur, tourneront à saute-mouton, sur des millions d'ordinateurs différents, pendant des années, sans que les réels propriétaires de ces ordinateurs soient informés. Les responsables de ces applications pourront lancer des applications bienveillantes (des calculs astronomiques sur la galaxie, des applications de surveillance de tsunamis) ou des applications de cryptanalyse pour casser des codes. Ces calculs pourront être plus malsains, cruels ou destructeurs : calculs d'une bombe A pour une organisation terroriste, calculs et dissémination de milliards de virus informatiques tous distincts que les logiciels traditionnels d'antivirus ne pourront contrecarrer.

Les attaques se renouvellent ou se métamorphosent en général tous les trois ans. Tour à tour, les générations d'attaques par virus sur support physique, par virus sur fichiers attachés dans des messages, ont quitté le palmarès et laissé place à une génération de virus plus intrusive en 2003. Cette génération correspond à l'arrivée de l'ADSL en France, génération qui s'est convertie vers 2006 en des assauts de messages de désinformation et des dénis de service distribués, favorisés par l'émergence de nouveaux pays d'internautes et une nouvelle vague d'internautes néophytes, chez nous. Ces menaces se transformeront en 2009 en d'autres actes malveillants incités par les attaques des applications en pair à pair, les applications géographiques (en utilisant des applications du type *GoogleEarth* et le géoréférencement), les téléphones plus ouverts aux applications distribuées, l'interconnexion plus forte du téléphone et de l'Internet, la télévision mobile personnelle. Nul ne peut deviner quel angle d'attaque sera popularisé parmi les communautés actives des pirates.

La cybercriminalité et le cyberterrorisme

Alors que l'on discrimine bien délinquance, criminalité et terrorisme, il existe un certain flou dans l'utilisation du vocabulaire qui fait que l'on mêle dans la presse à sensation délinquance informatique ou cybercriminalité avec cyberterrorisme. Il faut faire la part des choses, l'informatique n'est pas encore intrinsèquement un support de terreur ou une arme de destruction [6]. La cybercriminalité choque les mœurs, porte atteinte à la tranquillité, et à la sûreté des citoyens tandis que le cyberterrorisme fait trembler la société.

La cybercriminalité est apparue très tôt, dès que l'utilisation informatique s'est répandue auprès d'un large public dans les années 1960. Elle n'a cessé de croître.

....

(5) Installer une défense avec pare-feu, antivirus dans chaque ordinateur est une stratégie équivalente à dissoudre notre armée et notre police, en disant à chaque Français : « *Armez-vous, payez-vous une milice personnelle ou payez des mercenaires qui agiront sans garantie de l'étranger* ».

(6) On a déjà tué de manière ciblée, grâce à la géolocalisation : personnes cibles utilisant des téléphones par satellite, repérage de terroristes dans la jungle et frappe chirurgicale de ces objectifs.

Le cyberterrorisme n'existe pas encore véritablement en 2008, mais il deviendra une arme nouvelle contre nos sociétés le moment venu, si on n'y prend garde : des nuages de programmes et de données s'engouffreront alors dans une spirale violente pour tuer, ignorant les frontières des ordinateurs et des réseaux car ils atteindront fatalement les infrastructures physiques et les activités humaines.

Les conditions techniques du cyberterrorisme

Pour qu'une organisation terroriste puisse préparer de tels attentats et faire surgir ces événements sinistres, il faudrait réunir deux conditions [7] qui conjugueraient leurs puissances néfastes :

- Il faudrait, d'une part, être capable de déployer, sur la friche informatique du réseau mondial, une infrastructure virtuelle, spontanée, transcontinentale, furtive et cohérente, c'est-à-dire mettre en mouvement des applications malveillantes anonymes sur des millions d'ordinateurs en réseau, subrepticement, de manière dynamique et continue, pendant une durée de l'ordre d'une semaine au moins, avec une puissance informatique de quelques « pétaflops [8]». Les grilles informatiques actuelles ne sont pas encore capables de mettre en œuvre ces propriétés de puissance, de continuité et de furtivité. Pour anonymiser leurs assauts, les attaquants mettent une cagoule sur les protocoles ; pour surprendre l'adversaire, les attaques informatiques se propagent à la vitesse de la lumière sur les réseaux en fibre optique, pour compliquer les enquêtes et les poursuites, les scénarios d'attaques sont internationaux, les interconnexions des réseaux transgressent les frontières, la discrétion dans les attaques devenant une propriété plus fréquente depuis que la surveillance du réseau s'organise. Mais l'intelligence des attaques artificielles est faible : ce sont des dénis de services, bruts avec une frappe massive, sans apprentissage ou adaptabilité, incapables de modifier leur comportement *in vivo*.

- Il faudrait, d'autre part, que les flux des ordinateurs interagissent directement avec la réalité physique et l'activité humaine. Ce n'est pas encore le cas en 2008. Les humains sont toujours détachés de leurs ordinateurs : entre la réalité physique et les ordinateurs, il existe encore un maillon humain qui permet de court-circuiter la relation directe, suite à un dysfonctionnement ou une anomalie. Ce verrou risque de sauter bientôt suite à l'immersion de l'informatique dans le monde vivant, aux personnes cyberdépendantes du réseau (stimulateur de malade cardiaque, connecté à Internet), et à l'irrigation toujours plus grande de l'informatique dans l'activité quotidienne : flotte de véhicules télécommandée via le réseau [9], téléassistance de personne fragile, surveillance des personnes géolocalisées par bracelet électronique, applications industrielles de surveillance composées de réseaux autonomes de capteurs et d'actuateurs, dispersés dans la nature.

La mise en place de caméras dissuasives de surveillance dans les lieux publics risque de chasser de la rue les terroristes qui finiront par se réfugier dans leur domicile. On risque de voir éclore dans le secret de caches privées, une communauté de cyberterroristes qui pilotera en réseau, à partir de leurs ordinateurs, une immense toile anonyme de nœuds virtuels et piégés. Les actuels botnets ne sont qu'une amorce de ce genre d'arme.

Le règne numérique chaotique

Le métasystème numérique, dans son exploitation quotidienne et dans son évolution à long terme, échappe aux technologues et aux industriels du laisser-faire, apprentis sorciers d'un nouveau *Far West*. Le profil des attaquants est souvent l'objet de fantasmes, nourris par l'appréciation ambiante, si bien que l'on a tendance à restreindre le catalogue des menaces et des scénarios d'attaques. Mafia russe pour la délinquance informatique ou « hacker » islamiste pour le cyberterrorisme sont des exemples de schématisation.

La violence légale, économique et scientifique

À côté de la violence illégale et féroce, il existe aussi un affrontement légal, la compétition brutale entre les entreprises toujours plus internationales (intelligence économique). Il ne faut pas non plus ignorer la rivalité scientifique entre les centres de recherche, la concurrence entre les pays (gestion de l'opinion publique), voire la

(7) Le but de cet article est de prévenir objectivement, de solliciter des initiatives de recherche ; il n'est pas de susciter un vent de panique ou de mettre de l'huile sur le feu.

(8) Un Pétaflops : un million de milliards d'opérations par seconde : le flops (*FLoating point Operations Per Second*) est la mesure de la puissance de calcul des ordinateurs.

(9) On sait déjà intercepter une voiture volée, lorsqu'elle est équipée d'un antivol à télécommande.

guerre de l'information via des services divers d'institutions légales ou des associations « sans frontières ».

Le marché de l'informatique, première industrie au monde (2 500 milliards d'euros), suscite des batailles à l'échelle des continents. Les chercheurs sous-estiment souvent cette influence majeure sur le destin des infrastructures numériques : tassement de la recherche scientifique à cause de mauvaises orientations, ralentissement des innovations dans les architectures de base à cause de l'immobilisme du marché, frein dans certains secteurs de l'informatique à cause d'une industrie dominante qui tient à conserver sa primatie et asphyxie les succès prometteurs de petites entreprises, assèchement des financements de recherche dans des secteurs innovants pour protéger des produits informatiques déjà en place.

Bien sûr, il ne faut pas confondre la violence illicite des cybercriminels avec la compétition normale des entreprises ; néanmoins si l'éthique des uns et des autres diverge, les méthodes employées se ressemblent souvent. Si les procédés sont analogues et si les pratiques ne le sont pas, les unes étant criminelles et illégales et les autres normales et admises, comment distinguer une entreprise qui affronte une autre entreprise d'un pirate qui agresse une personne privée et comment surveiller et contrôler cette surveillance ? C'est tout le problème de la politique et de l'éthique de la police du réseau.

La perte du contrôle de l'espace numérique

Tout le monde a perdu le contrôle de l'informatique, en général. Ce n'est pas le cas des industries sensibles (nucléaire, énergie, transport, agriculture, santé) qui fonctionnent avec l'informatique, car ces systèmes numériques sont très fermés aux communications extérieures et sérieusement contrôlés par des procédures rigoureuses à l'intérieur. La maîtrise de l'informatique, science de l'organisation des symboles, fait partie des grands défis de ce siècle, au même rang que l'écologie avec la maîtrise de l'énergie, la démographie et la lutte contre la misère.

Le règne numérique n'est plus contrôlé, foncièrement à cause des bugs inhérents à l'informatique actuelle, et subsidiairement à cause de l'opacité des services. D'abord, les erreurs dans les logiciels sont dues à la pauvreté de la sémantique des langages informatiques et à la faiblesse des environnements de fabrication et de validation des logiciels. Ensuite, les éditeurs de logiciels pratiquent la non-transparence au motif de garder les secrets de fabrication. Les codes-sources des logiciels hégémoniques sont habituellement confidentiels : système d'exploitation, moteur de recherche, téléphonie sur Internet, logiciels de sécurité. La technologie informatique, bâtie sur des limons récents, est déstabilisée en permanence, par un modèle économique de l'informatique qui favorise l'innovation des services, voire la fuite en avant, plutôt que la sécurité et la sûreté de fonctionnement.

Si on sait à peine réaliser des logiciels conformes et corrects avec les langages informatiques actuels, on sait encore moins construire et faire utiliser des logiciels inoffensifs [10]. Un logiciel peut être parfaitement correct, conforme à sa spécification et à sa documentation, et se révéler dangereux (c'est justement le cas des vers informatiques). Un logiciel peut être incorrect et demeurer inoffensif. Il ne faut pas confondre la sécurité ou la sûreté avec les exigences de correction, de validation et de vérification, les objectifs de ces disciplines sont distincts. En sécurité, il est vain de comprendre toutes les subtilités et les effets de bord de l'horlogerie inextricable des systèmes numériques, il suffit de contrecarrer leurs actions périlleuses et les pannes par des boucliers robustes, avec des mécanismes résistants, conformes à une politique de sécurité, mais de complexité nettement plus réduite que celle du système. Enfin, les modèles de sécurité de type « bac à sable » sont insuffisamment exploités. On pourrait imaginer la mise en place de ces filets de sécurité profilés pour les utilisateurs novices, ce qui les immuniserait contre des fautes occasionnelles.

Une exploitation étendue des vulnérabilités

Les menaces résultent de tous les acteurs qui interviennent dans les édifices numériques. Ce sont des attaques intentionnelles ou simplement des erreurs, dans les deux phases distinctes de conception ou d'exploitation des systèmes. Les attaques intentionnelles proviennent statistiquement des utilisateurs du Web, mais on aurait tort de se borner à ces assaillants. Les infractions et les erreurs humaines, à l'intérieur des entreprises par du personnel autorisé, sont plus importantes que les attaques anonymes issues de l'extérieur. La panoplie des acteurs susceptibles d'engendrer ces menaces est large :

- ce sont des concepteurs de système, qui engendrent des fautes de conception par inadvertance, ou qui laissent des faiblesses après une évolution des usages ;

....

(10) Y remédier devrait être une priorité, mais la recherche en sécurité est paupérisée : on masque l'indigence de ses budgets propres, en y rattachant les budgets de la recherche en conformité du génie logiciel.

- ce sont des pupitreurs qui engendrent des fautes d'exploitation, suite à des défauts de procédure, par manque de formation suffisante ;

- ce sont des développeurs informatiques de logiciel libre ou propriétaire, qui incrustent des bombes logicielles ou laissent des portes dérobées dans un programme informatique dans la prévision d'un déclenchement ultérieur ;

- ce sont des acteurs voyous : opérateur de télécoms résolu à déstabiliser la chaîne de confiance des opérateurs de téléphone mobile [11]; fournisseur d'accès borderline décidé à attirer les clients en leur offrant des services douteux ; fournisseur de services qui héberge des contenus illicites ou qui examine le contenu de leurs clients avec l'intention de leur offrir des publicités profilées ; éditeurs de logiciels qui profitent de l'opacité de leurs logiciels pour épier le comportement des utilisateurs ; ou simplement des utilisateurs malveillants ou inconscients réalisant des téléchargements illicites ;

- c'est une obscurité dans la gestion et la gouvernance des systèmes. La répartition inéquitable et la disette des adresses de l'Internet sont entretenues pour gêner l'Asie. La gouvernance hégémonique de l'Internet avec la mainmise transatlantique est une question ouverte qui risque de faire basculer tôt ou tard le réseau mondial vers une balkanisation de l'Internet. « L'harmonie » actuelle du Village global risque de se dissoudre dans une confrontation plus brutale, au profit d'un paysage moyenâgeux où l'on verra se dresser de nouvelles murailles protectionnistes.

L'abandon de la souveraineté

Les États ont perdu leur souveraineté numérique. Les éditeurs de logiciel qui vendent un système d'exploitation, un logiciel d'antivirus, les fournisseurs qui proposent gratuitement un moteur de recherche, interviennent dans le patrimoine numérique des utilisateurs. Ils ont pris en charge les utilisateurs, leur comportement (traces numériques géolocalisées par un éditeur), voire leur intimité (mots clés volés sur les moteurs de recherche). Alors que la finalité première est d'offrir un service direct (comme fournir un système d'exploitation, un logiciel pour téléphoner sur Internet, une protection antivirus) à l'utilisateur final selon une spécification précise, l'éditeur du logiciel récupère une information collatérale qui n'est pas inscrite dans la finalité première du logiciel. Avec l'étendue massive du marché informatique auprès des citoyens, l'éditeur de logiciel, leader dans son domaine, s'octroie, statistiquement à l'échelle d'un pays, une information indirecte qui n'était pas acquise au départ. Ce point de vue à deux niveaux transforme, secondairement mais stratégiquement, cet éditeur en un acteur de métrologie informatique : statistique de l'activité digitale des utilisateurs dans une région, météo des virus ou spams du Web en France, trafic sur Internet à l'échelle d'un pays. La surveillance du monde numérique, d'ordre régalien, est maintenant sournoisement concurrencée, exploitée et accompagnée par des éditeurs privés, souvent étrangers. Une inquisition numérique sur les autoroutes de l'information occupe une place privilégiée à côté des autorités compétentes, dans tous les pays. La loi Informatique et Liberté de 1978 aurait besoin d'une sérieuse révision afin de s'adapter aux pratiques actuelles de finalité et de proportionnalité. Enfin, on devrait prohiber l'insolence des contrats inintelligibles de licence d'utilisation qui apparaissent dans les minuscules fenêtres avant une installation logicielle, que l'on doit accepter sans conditions face à des éditeurs logiciels qui ne s'engagent à rien quand on achète leur licence.

Le déficit de sensibilisation des usagers

Le marché de la sécurité informatique est difficile. Les utilisateurs, et même les entreprises, négligent ou bien ignorent les dangers potentiels. Les utilisateurs ne veulent pas s'embarrasser d'outils de sécurité trop lourds, ils dédaignent les avertissements tant qu'ils n'ont pas été confrontés à la réalité d'un dommage. Le risque d'un préjudice est jugé faible devant les opportunités si intéressantes du réseau. La législation rend en général responsable et coupable l'utilisateur final si bien que les éditeurs de logiciels sont peu enclins à améliorer la sécurité de leur produit. Dans la chaîne de confiance, la loi devrait responsabiliser davantage de manière proportionnée tous les acteurs qui contribuent à la chaîne de communication : le fournisseur d'accès, l'éditeur de logiciel qui a vendu sa licence d'utilisation. Il existe une non-responsabilité, une impunité généralisée dans le monde numérique, qui remonte à l'introduction du *copyright* en informatique. La loi qui fait porter le fardeau sur le seul utilisateur final, implique que personne ne se sent responsable de cette déficience. Cependant, il n'existe pas d'opposition entre l'économie et l'écologie numérique, entre une informatique qui serait performante et innovante et une informatique qui

(11) Tous les opérateurs GSM du monde sont interconnectés et inter-opèrent pour qu'un abonné connu d'un seul opérateur de télécoms puisse téléphoner de n'importe quel point de la planète.

respecterait les utilisateurs dans leur souveraineté et leur dignité.

Le déplacement de la prépondérance cryptographique

L'outil fondamental de la sécurité est la cryptographie. Ce pilier sur lequel repose toute la sécurité se fissure à cause des interconnexions robustes et massives de l'informatique ubiquitaire. En outre, sur un plan géo-stratégique, la suprématie scientifique occidentale dans cette discipline est en train de se déplacer vers l'Asie. La science cryptographique vacille, attaquée sur plusieurs fronts. Les fondements de la discipline sont basés sur la notion de secret et sur la mesure quantitative de la résistance d'un algorithme.

Sur le front de la connaissance, la cryptographie a été longtemps une science fermée, calfeutrée chez les militaires. Elle était, sur le plan technologique, essentiellement américaine grâce à la suprématie des algorithmes du RSA, du DES. Elle s'est ensuite disséminée dans le monde civil, à tel point que la cryptographie s'est déplacée sur l'échiquier politique. L'AES, le dernier algorithme de chiffrement par blocs est belge (université de Louvain). Le dernier théorème sur les nombres premiers a été démontré en Inde, à Kanpur, en août 2002, (sur le caractère polynomial du calcul pour déterminer la primalité d'un nombre entier) [Agrawal, 2004, p. 781], et Xiaoyun Wang de l'université de Shandong en Chine a montré des attaques par collision des fonctions de hachage MD5 et SHA-0 à la conférence CRYPTO'04, et cassé, en février 2005, les algorithmes de hachage qui sécurisent l'Internet actuel.

Sur le front des moyens informatiques, il faut posséder, pour casser un code secret, une puissance informatique extraordinaire, démesurée vis-à-vis des adversaires. Cette puissance était l'apanage des gouvernements ; ils pouvaient mesurer leur force à l'aune de la puissance informatique, cette force brute qui permet de percer un secret, en y mettant les moyens. Ce temps sera bientôt révolu pour deux raisons essentielles.

D'une part, certaines applications civiles, comme les moteurs de recherche pour l'indexation des mots, requièrent une concentration exceptionnelle de serveurs informatiques, à tel point que des fermes d'ordinateurs pullulent sous des hangars, expansion visible sur l'évolution temporelle des images de *Google Earth*. Deux ou trois entreprises informatiques monopolisent à elles seules plus du tiers de la puissance de calcul et de stockage des serveurs de la planète. Cette puissance concentrée pourrait être détournée le moment venu. D'autre part, un individu quelconque pourra bientôt, à partir de sa chambre, se connecter et fabriquer un tissu d'arlequin de serveurs connectés pour calculer ses propres applications.

La cryptographie risque de n'engendrer bientôt que des secrets de Polichinelle. Il est temps que la science cryptographique se renouvelle, arrête de n'utiliser que la force brute des ordinateurs, et s'ancre aussi sur la réalité : l'histoire, le passé ou l'évolution dans le temps des secrets, la géographie ou la place des réseaux, la configuration des ordinateurs, bref des secrets réels laissés çà et là sur la lande informatique. La cryptographie quantique paraît être aussi une promesse intéressante pour distribuer ces secrets.

Le chantier d'une nouvelle urbanisation numérique

L'Internet s'est brisé

Ce que les spécialistes savaient déjà depuis longtemps, David Clark l'a révélé en décembre 2005 au grand public : « *Internet is broken* » [2005]. L'Internet s'est fracassé à cause de son architecture trop ancienne et son gigantisme ; il ne s'est adapté ni à la mobilité, ni à une sécurité moderne. Les outils de protection existent, mais ils ne sont pas ou peu utilisés, n'ont pas le succès escompté ou bien coûtent trop chers. Les infrastructures de gestion de clés publiques sont peu déployées puisque le marché de l'administration des certificats est faible, la signature électronique n'est quasiment jamais utilisée malgré les directives européennes, le déploiement de la biométrie nécessite un énorme investissement de départ d'enregistrement canonique de confiance. Seuls les antivirus ont du succès, trop sans doute. La cryptographie est peu utilisée pour le chiffrement de données, dans les applications normales. Les échanges téléphoniques sont en clair, le GSM chiffre, seulement dans certains pays, le segment des communications dans l'air. Les échanges par messagerie électronique sont en clair, si bien que des communications chiffrées deviennent suspectes. Cependant, il ne faudrait pas grand-chose pour que tout bascule. La téléphonie sur Internet via *Skype* est chiffrée. Les applications P2P pourraient bientôt être chiffrées. Mais ces chiffrements de données, s'ils protègent la transmission, ne vont pas forcément rassurer les interlocuteurs des échanges, qui ne partagent pas les secrets de ce codage. C'est évidemment celui qui exploite le service qui maîtrise tout.

Un Internet polymorphe et multipolaire

Dans le futur, on va assister à une informatique de plus en plus abstraite. On ne pourra plus raisonner en termes de monotechnologies. L'Internet du futur sera polymorphe, créé à partir de plusieurs infrastructures différentes, fragmenté géographiquement selon une gouvernance multipolaire. On sera probablement dans un schéma de recouvrement de l'ubiquité de l'espace informatique, un peu comme des tapis successifs de feuilles d'automne qui recouvrent le sol de la forêt. Il existera un premier socle de transmission avec la fibre optique et la radio. Il existera une deuxième couche de communication, avec non pas des routeurs ou des commutateurs, mais de véritables ordinateurs différents, spécialisés, selon leur emplacement dans le réseau. Il existera enfin un troisième socle, celui des applications et des services, avec les données.

L'enjeu principal de l'Internet du futur est donc de maîtriser ces infrastructures de communication : gouvernance de l'Internet, maîtrise des opérateurs de télécoms, de télévision, souveraineté sur les infrastructures de géolocalisation, contrôle de l'Internet des Choses.

Un nouvel horizon pour des paradigmes modernes

L'actuelle vision des chercheurs américains GENI [www.geni.net] ou européens FIRE [cordis.europa.eu/fp7/ict/fire/] tient dans l'idée établie qu'il faut construire des systèmes toujours plus complexes, plus interconnectés, entrelacés mais sans couture, supportant sans difficulté une forte hétérogénéité, presque auto-administrables, baignant dans une ambiance mobile, intelligente, peuplée de logiciels ubiquistes, saturés d'informations omniprésentes, avec des utilisateurs capables de se connecter presque partout et en permanence, nomades, sans contrainte de sédentarité, actualisant leurs programmes informatiques en ligne, téléchargeant les mises à jour de sécurité.

Il faut d'abord dépasser la démarche de l'informatique, une conception incrémentale des réseaux du futur, et notamment de l'Internet, empreinte d'optimisme comme une méthode Coué et d'une orthodoxie conservatrice. Un bouleversement éventuel (en termes géostratégiques, économique, technologique) est une variable à intégrer, car une rupture historique, concevable dans les deux décennies à venir, pourrait conduire jusqu'à un désordre international majeur.

Il faut enfin incorporer la rupture, la nature dynamique et évolutive des systèmes numériques. Nos repères informatiques actuels sont en train de se dissoudre. Les dichotomies entre l'ordinateur et le réseau, le matériel et le logiciel, les applications et les services, le plan logique et le plan virtuel, les logiciels et l'information, sont en train de s'estomper, ou, plus exactement, les termes de la césure changent radicalement de signification. La feuille de route de l'architecture des réseaux suit le même itinéraire que l'histoire des langages informatiques, avec une complexification du typage des abstractions,

Modèle, contre-modèle, alter-modèle

Dans la recherche informatique internationale [www.inco-trust.eu], il faut susciter une pensée intercontinentale. Les pensées du monde sont sans doute localisées : il faut donc penser la différence, les modèles de l'altérité. Avec la mondialisation, il faudra accepter les innovations mais aussi les détournements et les reprises d'inventions. Il faudra alors concevoir d'autres références avec des modèles, des contre-modèles et des alter-modèles et inventer des passerelles entre ces modèles, suite à l'arrivée sur la scène informatique de la Chine et de l'Inde. On dit parfois que le XIX^{e} siècle fut européen, le XX^{e} fut américain, le XXI^{e} sera asiatique. Il se produit indubitablement une mutation des préoccupations, à la fois démographiques et de développement, un déplacement de pouvoirs dont il faudra tenir compte, y compris dans la science et la technologie. Il faudra aussi intégrer les mouvements de contestation, à la fois des mouvements pseudo-libertaires (les « naïfs de l'Internet ») et des purs et durs de la répression (les gouvernements autoritaires). On verra se greffer sur le réseau physique mondial, universel, sans frontières, une multitude de services, à l'intérieur de murs virtuels, avec des propriétés à la carte : infrastructure de confiance laxiste, réseau marchand, réseau sécuritaire. Tout ne sera pas résolu avec cette fragmentation du filet de l'interconnexion, loin s'en faut.

Dans une perspective de laisser-faire la technologie, on risque de rester descriptif de l'ordre : on ne maîtrise pas l'évolution, la régulation est autoréflexive, on évite ainsi de passer au normatif. Gouverner, c'est définir un ordre. En matière de technologies, on décrit trop souvent ce qui est, et pas assez ce qui devrait être ou ce qui pourrait être, sans même s'ouvrir à des démarches qui acceptent l'utopie : un « ONU numérique » rentrerait dans le champ de cette utopie.

La balkanisation du Village

Avant la convergence, les infrastructures de communication étaient séparées. Les cloisons étanches entre l'Internet, le téléphone et le téléviseur diminuaient la probabilité de panne en cascade des trois systèmes.

De nouvelles infrastructures vont naître. Les infrastructures de géolocalisation (Galileo en Europe, GPS aux États-Unis, Glonass en Russie, Beidou-2 en Chine, IRNSS en Inde) se mettent en place, et esquissent le nouveau Yalta numérique du XXIe siècle : Amérique du nord, Europe, Russie, Chine, Inde, Brésil. Dans l'avenir, l'heure et la position de confiance vont fortement structurer l'informatique et leurs services avec des services géolocalisés. Les infrastructures de géolocalisation sont un atout supplémentaire de la sécurité : on remet les pendules à l'heure et l'on pointe les boussoles au même nord. Les millions d'ordinateurs qui avaient des horloges différentes et peu fiables vont désormais utiliser la même heure. On va pouvoir acheminer des paquets d'informations selon la latitude et la longitude, on va pouvoir déployer des protocoles cryptographiques et authentifier un sujet, un objet en fonction de son identité, mais aussi de sa position à l'heure dite : cet attribut va permettre de crédibiliser un échange commercial, authentifier une personne qui veut se connecter à l'ordinateur de son entreprise à partir de son domicile. Cette fonction inédite va créer des alibis par l'enregistrement du trajet. L'informatique va réinvestir le monde réel.

La pollinisation des services

Les services aujourd'hui sont attachés et verrouillés à leur infrastructure. On va assister à un déverrouillage des services et des applications qui vont se libérer de leur infrastructure originelle. Telle application qui se déployait jadis sur la télévision va se déployer sur l'Internet ou le téléphone. Mais plus encore, on va assister à la création de nouveaux services qui seront à califourchon sur plusieurs infrastructures : des services virtuels spontanés vont se créer en prenant l'heure et la position sur Galileo, des tags de l'espace environnant sur l'Internet des Choses, une application par un programme Java sur un site Web2 de l'Internet courant, des données personnelles sur la carte SIM du téléphone portable, et utiliseront des éléments d'une émission de télévision interactive. Les nouveaux services informatiques seront des bulles intangibles qui surnageront sur le maquis des infrastructures de communication. On va assister à une pollinisation des services qui vont opérer une fertilisation croisée : la difficulté sera de maîtriser ces boutures informatiques. La sécurité et la sûreté du système devront reposer sur une approche holistique, pour empêcher des effets dominos [Riguidel, 2003].

Par-delà l'inéluctable

L'interdépendance de la vie quotidienne envers les infrastructures vitales est préoccupante. Le cyberespace, assemblage délicat et dynamique de deux ensembles dispersés de logiciels et d'informations, constitue une vulnérabilité majeure dans nos sociétés. Les attaques et les pannes dans ce règne numérique découlent de l'architecture en pièces rapportées, des logiciels opaques et fragiles, et des données en expansion continue. Ces faiblesses sont exploitées par la violence des délinquants, des criminels ou des terroristes. Elles sont favorisées par le manque de sensibilisation des utilisateurs, et accentuées par une gouvernance déficiente, une jurisprudence absente. Comme les technologies deviennent globales, les menaces se mondialisent, elles aussi. Sans décèlement précoce, une attaque distribuée, peu dangereuse au premier abord, mais prenant de l'ampleur avec son évolution, comme une vague qui déferle lentement, pourra se révéler désastreuse. L'identification *in vivo* de l'attaque sera impossible. Il faut donc inventer dès maintenant, des instruments de sécurité, opérés par des instances légales comme un dispositif réticulaire robuste qui s'autocicatrise en rétrécissant ses tuyaux automatiquement afin de ne véhiculer que les messages urgents, et qui se protège en ripostant de manière graduée par des contre-attaques. Comme pour toute prévention, il faut renforcer le renseignement informatique légal (infiltration, écoute), contrôlé démocratiquement, couplé avec le travail classique sur le terrain. Le travail sur ces menaces futures ne doit pas affaiblir les luttes plus concrètes sur les fléaux actuels : marché de la drogue, prostitution, sectes en tout genre attirées par l'argent facile, organisations criminelles camouflées sous des allégations politiques, gerbe de mondes parallèles qui se recoupent tout près de nous, dans l'ombre. La confrontation à la barbarie numérique à venir ne pourra être séparée de la lutte acharnée contre le terrorisme et le rude combat contre la criminalité. Dans un monde violent et globalisé, le repère de nos valeurs, la défense de nos principes et de notre modèle devront guider notre action afin d'organiser sainement le renseignement numérique et protéger l'indépendance, la souveraineté et l'intégrité du patrimoine numérique des citoyens, des entreprises et de notre pays, en parallèle avec la lutte offensive contre la criminalité, le trafic de drogue et la corruption.

Michel RIGUIDEL

Bibliographie

AGRAWAL (M.), KAYAL (N.) SAXENA (N.), 2004, «Primes Is in P», *Annals of Mathematics*, 160: p 781-793.

CLARK (D.), TALBOT (D.), 2005, «The Internet is broken», *MIT Technology review*, Dec 2005, http://www.technologyreview.com/InfoTech-Networks/wtr_16051,258,p1.html

FILIOL (É.), 2007, *Les virus informatiques : techniques virales et antivirales avancées*, Springer, coll. IRIS.

RIGUIDEL (M.), 2003, « Les infrastructures critiques et leurs interdépendances », *Revue de l'Électricité et de l'Électronique*, Paris, Société de l'électricité, de l'électronique et des technologies de l'information et de la communication.

RIGUIDEL (M.), 2004, « La sécurité à l'ère numérique », Paris, *Les cahiers du numérique*, Vol. 4, n° 34, Paris, Hermès Lavoisier.

RIGUIDEL (M.), 2006, «The Twilight of the Despotic Digital Civilization», *Transactions on Computational Systems Biology*, LNCS 3939, Springer, p 83-98.

RIGUIDEL (M.), 2006, « La sécurité des réseaux et des systèmes », *Encyclopédie de l'informatique et des systèmes d'information*, Paris, Vuibert, p 521-548.

Internet : Champ de bataille pour l'entreprise

Jean-Marc ZUCCOLINI

Le réseau Internet représente un risque avéré, mais de quelle nature et dans quelles proportions ? Cette question a conduit le Commissariat à l'énergie atomique (CEA) à mettre en œuvre, en 2006, une série d'équipements dont l'objectif est de superviser les communications provenant d'Internet et à destination de notre réseau d'entreprise. Force est de constater que la situation est loin d'être apaisée.

The Internet: New Battlefield for Business Enterprises

The internet network represents a known risk. But how great is it? In 2006 this risk led us to adopt a series of measures whose objective was to supervise business communications originating on the net. It must be admitted that the situation remains far from reassuring.

Jean-Marc Zuccolini

Responsable du groupe Sécurité des systèmes d'informations au pôle Maîtrise des risques du Commissariat à l'énergie atomique (CEA).

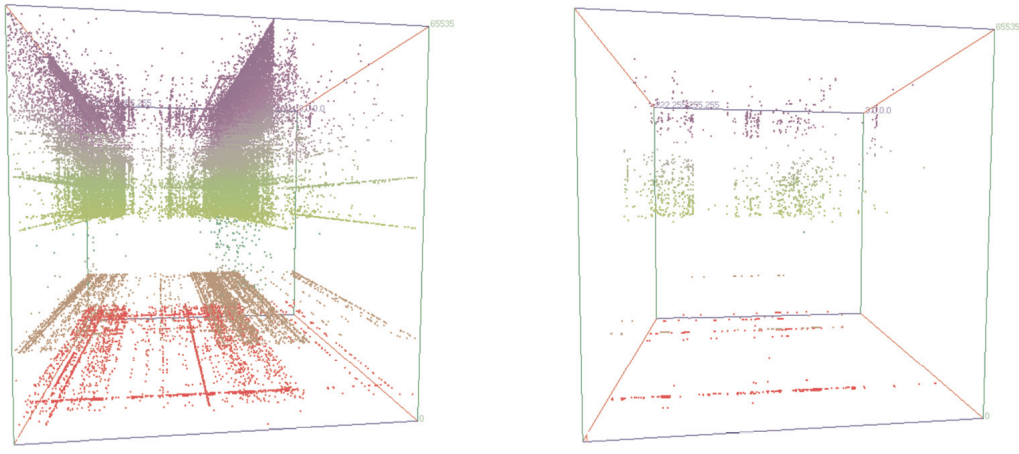
A contrario des autres équipements de sécurité, placés de manière classique derrière les premières lignes de défense, les outils de supervision que l'on a mis en œuvre pour tâter le pouls d'Internet, ont été placés le plus en amont possible. Ils écoutent et analysent en temps réel le flot continu d'activité réseau avant que ces derniers ne soient filtrés. Ces postes avancés offrent une visibilité surprenante sur la réalité des menaces subies avant que ces dernières ne soient interceptées par la politique sécurité de l'entreprise.

Que montre la supervision réseau d'Internet ?

Quel est le taux de communications réseaux accepté en provenance d'Internet par rapport au nombre total de communications ? 3 %. Sur les 800 flux qui arrivent en moyenne chaque seconde à la porte de notre réseau, seuls 3 % sont admis à établir une communication avec la ressource demandée, les autres sont tout simplement rejetés (*fig.1*). Cette activité, en terme de consommation de la précieuse bande passante, est quantité négligeable, si bien qu'elle ne dérange pas l'utilisation légitime du réseau. De plus, certaines techniques d'exploration sont suffisamment lentes pour ne déclencher aucune alerte de sécurité, mais c'est bien ce ratio de 3 % que l'on constate depuis plusieurs années. On peut reconnaître dans ce bruit de fond plusieurs types de recherche massive de nos vulnérabilités ou points d'accès potentiels. La première est une tentative d'accès systématique aux services de communication Microsoft depuis tout l'Internet, c'est une signature caractéristique de tous ces postes zombies, enrôlés à l'insu de leur propriétaire légitime, dans des réseaux de stations, sous le contrôle d'un acteur indélicat (on parle de « botnet »). L'activité récurrente de ces postes zombies, lorsqu'ils ne sont pas loués ou utilisés pour mener des attaques de type spam ou déni de services, est d'étendre le cheptel de postes compromis en tentant de se propager. Ceci se traduit par le fait qu'une bonne partie d'Internet cherche à contacter l'ensemble de notre réseau d'entreprise sur un service particulier, généralement lié à un service Microsoft.

Parmi les autres signatures d'activités dangereuses, on constate généralement des balayages systématiques de l'ensemble de nos machines sur un service donné comme un serveur de base de données ou une application annoncée récemment comme vulnérable. Cette signature provient le plus souvent de trois ou quatre sources Internet différentes dans la journée et traduit l'apparition récente d'une vulnérabilité sur un applicatif réseau, mais aussi, parfois, la réminiscence d'une ancienne vulnérabilité (on constate encore des traces du ver slammer de 2003). On a donc, au choix, tous les fournisseurs d'accès de l'Internet qui tentent de vous compromettre sur un service Microsoft, ou quelques individus qui cherchent à exploiter la nouvelle ou pourquoi pas ancienne vulnérabilité d'un service réseau que vous mettez à disposition.

Fig.1 - Représentation graphique de deux heures d'activité en provenance d'Internet



Activité totale (sans aucun filtre)

Activité normale (uniquement les demandes d'Internet abouties)

Chaque point représenté dans le cube traduit une activité réseau en provenance d'une adresse d'Internet à destination d'une ressource du réseau d'entreprise. On constate habituellement que seule 3 % de l'activité réseau globale est autorisée à travers les dispositifs de protection.

Une dernière signature quotidienne consiste en une cartographie exhaustive de notre réseau à la recherche des services offerts sur Internet. C'est une adresse Internet qui tente d'entrer en communication avec l'ensemble de nos postes et serveurs sur l'ensemble des services disponibles, mais ceci, de manière pseudo-aléatoire et relativement lente. On considère qu'en moins d'une journée, une adresse Internet peut ainsi établir un diagnostic complet de l'ensemble des services mis à disposition. Détail amusant que nous avons pu constater, les adresses à l'origine de cette recherche exhaustive, n'établissent généralement aucune communication ou tentatives d'attaques, les éclaireurs ne participent donc pas à l'offensive.

Que nous a appris cette supervision ?

Le premier constat est que le droit à l'erreur n'est plus permis sur Internet (si tant est qu'il l'ait été un jour). Mettre en œuvre un service vulnérable ou un poste sans protection sur Internet n'est pas une question de jours mais de secondes avant que ce dernier ne soit compromis. Le balayage est peut-être aveugle mais il est permanent et redoutablement efficace. Si ceci ne pose pas de problème dans le cas du réseau d'entreprise où les ressources bénéficient d'une protection par défaut, cela demeure un risque important pour toutes les ressources nomades qui ne cessent de faire des allers - retours entre des réseaux protégés et des réseaux plus ouverts. On peut s'en remettre à des protections de type poste isolé (antivirus et *firewall* personnel) mais elles ne seront jamais comparables aux protections redondantes et administrées de manière permanente dans l'entreprise.

Le deuxième constat a été la nécessité de revoir notre politique de supervision de la sécurité. L'analyse de toutes les alertes générées par les équipements de sécurité placés devant Internet n'est plus une priorité. Il ne faut pas se concentrer sur ce qui est filtré ou bloqué, mais au contraire sur ce qui est autorisé, car c'est là que le risque existe. C'est une distinction notable entre la supervision des artères de communication avec Internet où on s'intéresse à l'ensemble des flux autorisés au détriment des alertes, par rapport à des réseaux internes à l'entreprise où la supervision des alertes demeure prioritaire. Sur l'Intranet d'une entreprise, les tentatives d'attaques peuvent annoncer la possible compromission d'une ressource interne et elles restent pertinentes. *A contrario*, lorsque l'on est confronté à la supervision d'un réseau exposé à Internet, l'analyse des alertes ou des flux réseaux interdits ne révèle pas grand-chose, si ce n'est le taux de charge des équipements de sécurité et le nombre important de postes compromis à l'extérieur.

Le troisième constat a conduit à compléter les outils de sécurité existants par des équipements plus basiques dans l'analyse, mais exhaustifs dans leur mode de conservation des traces. Les équipements de sécurité reposent le plus souvent sur une politique de journalisation basée sur un compromis entre le niveau des traces, la performance et la capacité d'exploitation. Ce compromis conduit rarement à une conservation exhaustive des traces mais à un choix favorisant le plus souvent les alertes. De plus, les outils qui fonctionnent sur des encyclopédies d'attaques connues (IDS, Antivirus) doivent confronter l'activité réelle avec leurs bases de références en opérant une fouille approfondie des données transmises. Cette opération se révèle, d'une part, très consommatrice en terme de ressource et, d'autre part, inopérante sur les informations chiffrées. Bien que les moyens de protection mis en œuvre constituent une barrière indispensable vis-à-vis d'Internet, il n'est pas rare que certaines attaques, ne générant aucune alerte sur ces systèmes, ne laissent aucune trace pour une analyse *a posteriori*. Compléter ces dispositifs par des sondes passives, dont l'objectif n'est pas d'analyser le contenu mais juste de conserver une trace de toutes les communications établies, constitue un atout réel dans la supervision. Il ne s'agit pas de conserver une copie complète de l'activité, mais juste les informations normalement dévolues à la métrologie réseau : qui d'Internet communique avec mes ressources. À quelle période et pour quelles durées ? Quels volumes d'information ? Dans quel sens de communication ? Les volumes d'information générés permettent une conservation de plusieurs mois, avec des équipements appropriés, et constituent une mémoire exhaustive de toutes les communications, qu'elles aient occasionné des alertes ou pas.

Comment détecter l'indétectable ?

La protection vis-à-vis d'Internet a beaucoup porté sur la sécurisation des ressources et des utilisateurs de l'entreprise, soit en bloquant les attaques connues en multipliant le nombre de passerelles de sécurité entre un attaquant et une ressource, soit en augmentant la résistance intrinsèque des services mis à disposition (mise à jours des correctifs de sécurité, tests intrusifs, analyse de code). Cette stratégie de défense en profondeur qui consiste à construire plusieurs lignes de défense autour des

ressources, et de s'attacher à ce que les plus exposées soient aussi les plus résistantes, porte ces fruits, car, malgré une volumétrie constante des attaques, peu de compromissions sont à déplorer et elles ne portent pas sur des ressources stratégiques.

La nature des attaques a évolué en conséquence, bien que les attaquants cherchent toujours à pénétrer les protections de l'entreprise, maintenant ils attendent aussi dehors que leur victime vienne à eux. Cette tendance, favorisée par l'utilisation d'Internet en entreprise, est beaucoup plus délicate à détecter. Parallèlement, les attaques ont aussi quitté le monde du prêt-à-porter pour celui du sur-mesure, elles se veulent plus discrètes et elles répondent à des intérêts plus cupides que ludiques. Ces attaques sont, dorénavant, conçues dès l'origine pour ne pas faire trembler l'ensemble d'Internet, mais pour se concentrer sur une population restreinte, comme les clients d'une banque ou quelques individus dont on a pris soin, au préalable, de connaître les centres d'intérêts et les interlocuteurs privilégiés. Cependant, si les attaques sont de plus en plus ciblées, les solutions de sécurité demeurent, quant à elles, génériques, et font rarement l'objet d'un paramétrage personnalisé par utilisateur.

Par analogie avec le domaine médical, dans lequel la sécurité informatique puise certaines références, nos utilisateurs et nos ressources sont correctement vaccinés, et relativement résistants aux infections diverses et variées, mais qui s'inquiète aujourd'hui de ceux qui toussent ou ont un peu de fièvre ? Quel patient consulte son médecin en lui disant « *j'ai contracté la souche espagnole du virus de la grippe hier soir entre 23h12 et 23h14 au cinéma* » ? Le dispositif actuel ne peut empêcher que les utilisateurs de l'entreprise, et, indirectement, les ressources auxquelles ils accèdent, soient en contact avec des attaques inconnues, à moins d'interdire toute communication avec Internet. La protection doit partir du principe que certaines attaques ont pu aboutir et s'attacher davantage aux symptômes pour y remédier qu'à une identification de la cause.

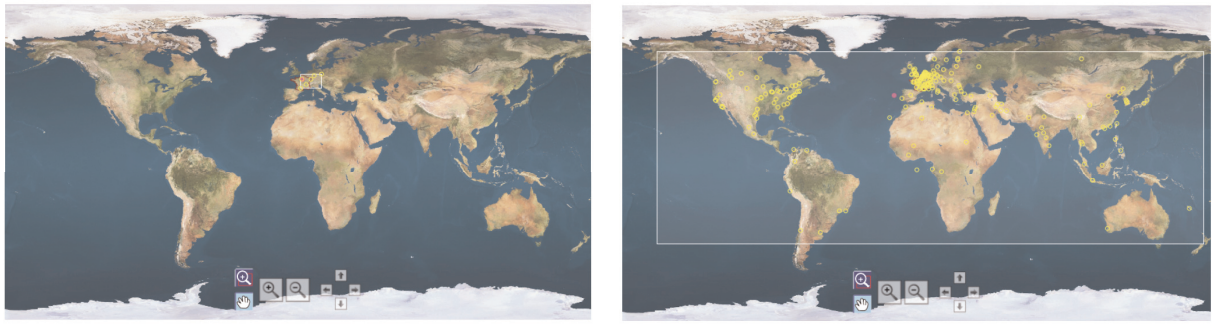
Supposons qu'un poste de l'entreprise héberge une application malveillante qui permette sa prise de contrôle à distance depuis Internet, et faisons volontairement abstraction des causes qui ont pu conduire à cette situation. On peut espérer que ce poste déclenche une signature d'attaque connue (le virus Zorglub a été détecté sur votre poste de travail) ou qu'il décide de saturer le réseau, mais ce type de comportement a tendance à se faire rare. *A contrario*, l'attaquant a besoin d'échanger depuis Internet avec le poste compromis et, à cette fin, il est nécessaire d'établir un canal de communication discret pour prendre le contrôle ou extraire des informations. Comme ce canal caché est établi depuis le cœur du réseau d'entreprise vers Internet, il est souvent traité avec moins d'attention par les mécanismes de protection et il est de toute façon conçu pour être discret : il n'utilise pas de protocole particulier (la messagerie ou le web suffisent amplement), il n'est pas gourmand en terme de bande passante (il n'est pas nécessaire de saturer un réseau qu'on a l'intention d'exploiter), il est résistant à l'analyse de ses données en transit (il utilise des mécanismes de camouflage, ou mieux, des mécanismes de chiffrement si ces derniers sont autorisés).

L'analyse du trafic réseau évoquée précédemment est exhaustive, elle garde donc une trace de l'activité de ce tunnel caché. On peut espérer que ce dernier soit atypique par rapport au comportement habituel de la victime (*fig. 2*). Les premières caractéristiques que l'on a pu constater comme étant les symptômes d'une compromission sont un accroissement significatif dans l'usage du réseau fait par un utilisateur, ou l'utilisation d'un protocole anecdotique. Malheureusement, des écarts aussi faciles à détecter ont par nature tendance à disparaître. Il est nécessaire de rechercher d'autres caractéristiques comme la corrélation avec l'activité des autres utilisateurs : il est, en effet, peu commun que quatre ou cinq utilisateurs de l'entreprise se mettent en même temps à communiquer avec un serveur d'Internet selon la même fréquence et la même durée, pour enfin s'arrêter et répéter le même scénario sur un autre serveur. L'heure de l'activité peut aussi être significative : il peut se produire que le tunnel caché (comme il n'est pas lié à l'activité de la victime mais davantage à la personne qui a pris le contrôle de son poste) agisse à des heures inhabituelles par rapport au profil de la victime. En effet, il nous est arrivé de constater qu'une communication camouflée en navigation web s'établisse à des heures où l'utilisateur n'est pas là pour naviguer.

Comme pour l'établissement d'un diagnostic, un indicateur n'est pas pertinent à lui seul, mais la conjugaison d'un ensemble d'indicateurs peut conduire comme l'analyse des symptômes à l'identification d'une pathologie. L'avantage de la sécurité informatique est que l'on n'est pas obligé de guérir le patient et, pour se faire d'identifier la maladie. On peut détruire le porteur (le poste de travail et les programmes associés, pas l'utilisateur) et on en fabrique un tout neuf. Les outils de supervision doivent être capables d'identifier les variations même peu significatives, mais ceci suppose, d'une part, que ces indicateurs soient définis, et que l'on soit capable de conserver leurs évolutions dans le temps pour identifier un changement de comportement alarmant.

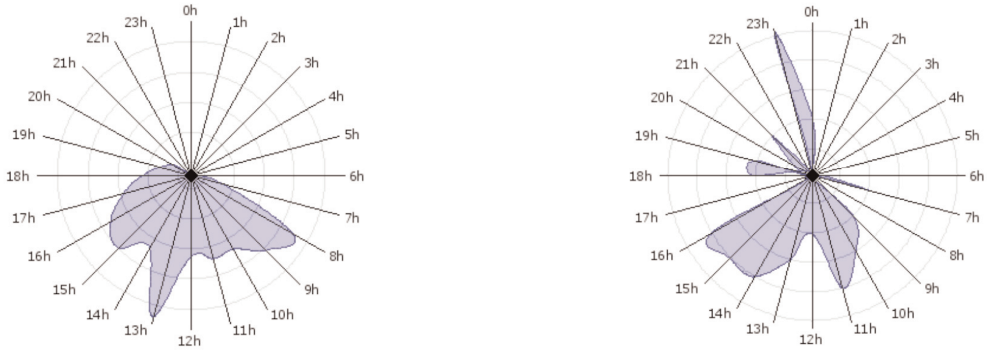
Fig.2 - Indicateurs traduisant l'activité nouvelle et atypique d'un poste

Évolution de la couverture géographique de l'activité Internet d'un poste



Évolution de la répartition horaire de l'activité d'un poste

On constate une activité nocturne atypique



Qu'est-ce qui pourrait changer ?

Depuis plus de deux ans que la supervision de l'activité réseau est effective, rien ne semble démontrer une quelconque diminution dans le risque que constitue l'Internet. Qu'est-ce qui pourrait changer ? Une baisse de l'activité malveillante sur Internet ? Une meilleure prise en compte de la sécurité par les internautes ? Une plus grande diversité dans les systèmes d'exploitation et navigateurs utilisés qui rendrait plus difficile et plus onéreuse la conception des attaques ? Tous les scénarios qui tablent sur une diminution de la menace ou sur une augmentation notable de la sécurité des ressources Internet semblent peu réalistes à court ou moyen terme. La qualité des attaques et leur diversité rendent de plus en plus difficile la découverte d'une compromission par le simple fait que l'on connaît l'attaque et qu'on l'ait identifiée. Alimenter des encyclopédies de virus ou de signatures de codes malveillants est une chose, mais on en oublie presque que la finalité est moins d'éviter la compromission que ses conséquences. La thérapie n'est plus de confronter l'ensemble du système d'information à l'ensemble des maladies connues pour identifier les éléments contaminés, mais, plutôt, d'identifier les symptômes d'une contamination et, en particulier, l'échange d'information directe et sans contrôle entre le réseau d'entreprise et l'Internet. Si la supervision réseau d'Internet conforte dans la nécessaire protection vis-à-vis de ce formidable outil, elle doit aussi évoluer vers une meilleure identification des symptômes d'une compromission. La supervision se doit de considérer les postes aussi bien dans leur comportement individuel que dans leur comportement collectif et de confronter systématiquement l'activité présente avec le trafic historique, ces outils doivent apprendre à utiliser leur mémoire et leur connaissance antérieure à des fins d'analyse.

Jean-Marc ZUCCOLINI

Cybersécurité

Protection des systèmes d'information et résilience des organisations

Gérard PESCH

© Thales

Dans le sillage du *Livre blanc* sur la Défense et la Sécurité nationale, l'auteur met en évidence la vulnérabilité de nos systèmes d'information critiques confrontés à l'ouverture des réseaux de données et au caractère imprévisible des cyberagressions. La mobilisation de toutes les compétences passe par le rapprochement des mondes civils et militaires, publics et privés. Au sein des organisations elles-mêmes, seul un management transversal de la sécurité pourra relever les nouveaux défis. Il est urgent d'appliquer les bonnes pratiques et de déployer de nouveaux modèles de systèmes d'information sécurisés, ainsi que des nouveaux concepts d'organisations résilientes.

Cybersecurity

Following the publication of France's White Paper on defence and national security, the author highlights the vulnerability of our critical information systems as data networks become increasingly open and cyber attacks ever more unpredictable in nature.
To respond effectively to these threats, we must combine all the expertise at our disposal in a process of convergence between the civil and military worlds and between the public and private sectors.
Within organisations themselves, a transverse approach to security management with the support of competent service providers (the combined expertise of consultants, system architects and engineers) is needed as we step up to the challenges ahead.
Now is the time to apply best practices and deploy new models of secure information systems, as well as new concepts of resilient organisations as a matter of urgency.

Gérard Pesch

Directeur de l'activité Conseil en sécurité et évaluation de l'équipe dédiée à la sécurité des systèmes d'information et de communication au sein du Groupe Thales. Ingénieur agro-alimentaire, maître ès Sciences en biologie, sa formation dans le domaine du vivant lui a donné le goût de l'ingénierie des systèmes complexes. Il a complété son expertise par un DEA de Gestion industrielle. Il est diplômé du CPA/HEC et auditeur de l'INHES. Sa carrière s'est déroulée au sein de grands groupes d'ingénierie (SERETE, SGN), de services (AREVA) et de conseil (ARTHUR ANDERSEN), principalement tournée vers l'amélioration de performances des ressources opérationnelles et la maîtrise des risques.

L'exposition des applications critiques aux cyberagressions s'est accrue dans des proportions exponentielles avec l'ouverture des systèmes d'information et le développement de menaces polymorphes. Il est urgent de juguler cette double complexité. Au-delà de l'indispensable rappel aux bonnes pratiques, il nous faut imaginer de nouveaux modèles de systèmes d'information intrinsèquement sécurisés et forger de nouveaux concepts d'organisations résilientes.

Internet et le nomadisme : le point de rupture

En ouvrant leurs systèmes d'information au grand public, fournisseurs et partenaires dans un environnement de nomadisme et de mutualisation des données, les organisations ont franchi un point de rupture entre leurs dispositifs traditionnels de protection et les risques encourus.

Les services en ligne

C'est au moment même où les fonctions critiques des institutions et entreprises se déployaient totalement dans leurs systèmes d'information que les nouvelles technologies de l'information et de la communication, tout en décuplant leur puissance, les ont rendues vulnérables. L'idée si féconde d'un dialogue en ligne entre le grand public et les applications les plus sophistiquées des services – administrations, transports, finances, etc. – conduit évidemment à un accroissement considérable des risques d'intrusion ludiques ou malveillants dans les systèmes. Or, les services sont pourtant utiles pour les fonctions économiques, sociales, administratives, et même pour la protection territoriale de la nation.

La dématérialisation

L'idée, si productive pour l'administration, la santé, les transactions commerciales, de dématérialiser les échanges de documents, conduit à exposer aux prédateurs des informations sensibles pour les personnes comme pour les organisations.

L'externalisation

En outre, Internet a facilité l'externalisation d'un grand nombre de services des entreprises chez leurs prestataires, en ouvrant des espaces illimités de partage d'information. Pour organiser leurs *supply chains*, les industriels multiplient les liens avec des partenaires, en amont et en aval de leurs chaînes de production, en leur donnant accès à leurs systèmes de gestion des commandes et des programmes de fabrication : formidable progrès dans l'anticipation des flux et l'optimisation des transports, mais qui conduit des données sensibles hors du périmètre des entreprises.

À l'instar de la logistique, de nombreuses fonctions sensibles ont été externalisées par les entreprises qui souhaitent s'en décharger sur des spécialistes pour concentrer leurs forces et leurs ressources informatiques sur leur cœur de métier. Citons la paie et la gestion des ressources humaines, sous-tendues par des milliers de données individuelles confiées aux bons soins des prestataires, voire les mouvements de fonds qui vont chaque mois des banques aux salariés : dématérialisés, donc exposés aux aléas des autoroutes de l'information.

Les interconnexions et interfaces

Ces rapprochements de partenaires sont d'autant plus porteurs de performances économiques que leurs systèmes d'information peuvent s'interconnecter. Le métabolisme des données s'étend à des ensembles de plus en plus vastes d'entreprises en synergie, participant d'une économie négentropique, toujours plus riche en information, structurante pour les échanges et la création de richesses. Mais ces ensembles interconnectés sont souvent constitués de systèmes d'information préexistants, héritiers de générations technologiques diverses, hétérogènes dans leurs modèles de données, leurs architectures, leurs protocoles de communication. Des milliers d'interfaces informatiques ont été développés au cours des dernières années. Aussi différentes les unes que les autres et aussi diverses qu'ingénieuses, elles ouvrent autant de points de fragilité à la jonction entre les systèmes d'information.

La mobilité

L'impératif de mobilité s'est imposé à tous les cadres de l'administration et des entreprises, alors que l'ordinateur individuel et les réseaux avaient multiplié leur productivité par quatre. Dès lors, l'information doit être disponible partout et immédiatement. Sans fils, les ordinateurs portables captent les réseaux dans les lieux publics où le trafic d'informations confidentielles est plus dense que le trafic automobile dans les métropoles aux heures de pointe.

La télémaintenance

Abolie, la distance l'est également pour le contrôle des *process* industriels, des infrastructures énergétiques, des équipements publics. La télémaintenance contrôle, relève

des données, diagnostique des dysfonctionnements, pénètre au cœur des systèmes de commande, modifie les paramètres, met à jour les logiciels, pilote des installations, arrête et relance les machines et les *process*.

Très performante, l'informatique industrielle a intégré tous les progrès du nomadisme sans bénéficier des investissements sécuritaires réservés aux applications administratives, de défense ou financières. Contrôle à distance des équipements publics, voire individuels. Des appareils d'assistance cardiaque peuvent être reliés à des systèmes d'information et d'alarme, voire de pilotage. Un *hacker* « ludique » a récemment prouvé sa capacité à prendre le contrôle d'un tel dispositif indispensable à la survie d'une personne.

La fin des bastions

L'arrivée d'Internet et la nomadisation des équipements pour l'informatique et les télécommunications marquent le point de rupture dans l'équilibre entre la protection des systèmes d'information et les risques encourus. C'est la fin des bastions, systèmes d'information fermés dans un périmètre topographique dont les accès, physiquement et électroniquement contrôlables, étaient réservés à un personnel identifié. Bastions physiques mais aussi technologiques : les systèmes d'exploitations et les logiciels « propriétaires » ne livraient leurs sources qu'aux initiés qui les avaient développés au sein de tel ou tel secteur - l'énergie par exemple. Vient le jour où la maintenance de ces forteresses s'avère trop coûteuse : on les remplace par des standards du marché dont les mises à jour sont amorties à des centaines, voire des milliers d'exemplaires.

La standardisation

Des plateformes de gestion intégrée ont imposé leurs standards sur les marchés internationaux, offrant aux pirates des conditions idéales pour optimiser leur courbe d'expérience au fil de leurs intrusions dans des environnements technologiques qui leur deviennent familiers.

La mutualisation des réseaux

Tandis que s'accroît l'exposition des réseaux aux menaces d'intrusion, les risques encourus s'étendent à l'ensemble des fonctions qui, de plus en plus, s'y concentrent. Très économique, la téléphonie sur IP mutualise les réseaux entre l'informatique et les télécommunications, exposant ces deux fonctions vitales au déni simultané des services vocaux et des services de données.

Les menaces imprévisibles et polymorphes

Pour autant, il serait faux de penser que les actions offensives sont toujours effectuées par des individus situés à l'extérieur des organisations. Bien au contraire, les études montrent que la majorité des dommages sont déclenchés au sein même des entreprises ou des administrations, et que leurs auteurs sont, la plupart du temps, inscrits au registre des personnels, ou tout simplement admis dans leurs murs en qualité de stagiaires, voire de sous-traitants.

On est donc fondé, dans une certaine mesure, à corréler la fréquence et la nature de ces agressions avec le climat social, comme on a pu le faire à propos des dégradations matérielles, voire de l'absentéisme. Mais cette approche reste insuffisante si l'on néglige les influences extérieures, les subornations ou, pire encore, les stratégies de pénétration des effectifs par des agents malveillants.

Climat social et immunité naturelle

Le climat social peut rendre les populations vulnérables à ces influences, dont la nature et les objectifs restent, bien entendu, à déterminer. On peut inversement établir qu'un climat social sain et un fort sentiment d'appartenance accroissent les capacités « naturelles » de résistance à ces influences.

De l'indélicatesse individuelle à l'attaque organisée

Il arrive qu'un salarié s'estimant frustré aliène des données confidentielles. Les directeurs des ressources humaines et les directeurs des systèmes d'information ont été saisis de tels cas et les mesures de protection sont dans l'ensemble identifiées. Plus préoccupants sont les cas de personnalités entrées dans la dépendance idéologique d'organisations malveillantes, parfois très déterminées dans leurs objectifs et leurs modes opératoires.

La constellation des puissances occultes

À chaque agression se pose la question de savoir quelle la nature de l'organisation extérieure qui est parvenue à pénétrer un système d'information, directement ou par la subornation d'un collaborateur ? Le récent rapport de la Commission des Affaires étrangères, de la Défense et des Forces armées du Sénat, met l'accent sur « *la réalité d'attaques informatiques dont la nature et les formes* [sont] *encore mal perçues en Europe* », évoquant « *la paralysie qui a affecté durant plusieurs semaines, au printemps 2007, les sites du*

gouvernement, des banques et des opérateurs téléphoniques en Estonie, puis l'annonce des tentatives d'intrusion informatiques ciblant des diplomates français et divers services occidentaux ».

Un premier repérage permet de distinguer les activistes, les terroristes et les États eux-mêmes. Les méthodes peuvent être les mêmes, voire les objectifs, mais les organisations et les finalités seront aussi différentes que la lutte contre l'expérimentation animale, la destruction de la civilisation, la guerre économique. L'agresseur peut donc avoir une assise militante identifiable, mais aussi relever d'un réseau polymorphe et mutant, voire s'appuyer en dernières instances sur des services d'un État. On voit que la frontière entre public et privé, civil et militaire, doit être franchie pour repenser l'impact des cyberagressions et les nouvelles approches, plus solidaires, de notre protection.

Un éventail illimité de menaces

On a vu que des collaborateurs d'une entreprise ou d'une administration peuvent entrer sous le contrôle d'influences extérieures.

Il en va de même pour les ressources informatiques qui peuvent passer, à l'insu de leurs propriétaires, sous le contrôle d'une organisation extérieure. Elles peuvent alors être utilisées à leur tour pour saturer un système cible et le mettre hors service en se connectant à lui de manière répétitive et intempestive. Il faut citer en outre l'expédition de courriels piégés véhiculant des utilitaires clandestins capables de pénétrer les systèmes pour en exfiltrer les données, en petits convois discrets, vers les sites de leurs commanditaires. Les objectifs de telles manœuvres peuvent évidemment relever de l'intelligence économique comme de l'espionnage.

Bien entendu, ces opérations peuvent être concertées pour compromettre les échanges économiques, entraver la vie sociale, voire inhiber des réseaux vitaux pour la nation, réseaux d'eau, d'énergie, de transport, de télécommunications civiles ou militaires. Il ne semble pas déraisonnable d'imaginer des cyberagressions majeures dans le monde spatial, telles que l'attaque et la neutralisation de satellites, visant à priver la nation de certaines fonctions vitales de contrôle et de surveillance. Sans aller jusqu'au pire, les dommages pourraient être considérables sur les entreprises atteintes dans leur capacité de services et/ou leur image.

Du ludique à l'agressif : l'insaisissable ambiguïté

Les *hackers* s'inscrivent bien souvent dans une ambiguïté particulièrement insaisissable, parfois même à leurs propres yeux. Dans la plupart des cas, la dimension ludique ou sportive de leurs effractions ne fait pas de doute au départ. Mais lorsque le succès est obtenu, intervient une survalorisation à la fois narcissique et économique de la performance qui peut en décider autrement. Le héros peut valoriser son savoir-faire sur le marché de la sécurité en embrassant une carrière de « *hacker* éthique ». Mais si l'on sort du champ des valeurs morales, la corruption dispose évidemment d'arguments convaincants, surtout si les enjeux d'intelligence économique, voire de terrorisme, sont importants aux yeux de ceux qui les manipulent

Les hauts lieux de l'ambiguïté

Il faut souligner l'existence même des congrès de *hacking*, rendez-vous de l'ambiguïté où se retrouve, dans ses composantes les plus diverses, la communauté des hackers. Citons la *Black Hat*, grand-messe californienne dédiée à la sécurité informatique, le *Defcon*, qui a fait parler de lui lorsque des journalistes en ont été exclus : on leur reprochait d'être munis de « renifleurs », pour capturer les données confidentielles dans les réseaux locaux. C'est également au Defcon, congrès international de *hacking* qui a lieu chaque année à Las Vegas, qu'après avoir violé le système RFID du métro de Boston, des étudiants ont voulu témoigner de leur performance. Mais un juge fédéral les en a empêchés. À tort, pensent les partisans de la divulgation intégrale ; à juste titre, affirment les tenants du « responsible disclosure », qui réservent leurs révélations.

Anticiper : le rôle clé des *hackers* éthiques

Le débat, on le voit, se déplace au niveau déontologique et montre, par sa vivacité même, l'existence d'une communauté de *hackers* éthiques, qui utilisent leur savoir-faire pour anticiper les cyberagressions et préconiser des solutions pour s'en prémunir. Le meilleur moyen d'aguerrir les systèmes d'information n'est-il pas de mettre leurs failles au grand jour ? Contre la pratique spectaculaire du « *full disclosure* », les *hackers* éthiques professionnels réservent, bien entendu, leurs révélations à leurs clients. Le *hacking* éthique relève aujourd'hui des sociétés de conseil en sécurité des systèmes d'information et se conforme à leur déontologie. C'est un métier nouveau qui attire des passionnés, réservant leurs savoir faire à leur entreprise et à ses clients.

La double complexité

La nouvelle complexité des systèmes d'information, qui en accroît la vulnérabilité, a donc pour équivalent la complexité des menaces qui s'exercent sur eux. La combinaison de ces deux complexités nous conduit aujourd'hui

à un niveau de risque inconcevable ou inimaginable, exigeant une réforme de nos concepts et de nos organisations à tous les niveaux.

Une nouvelle approche créative et réaliste

L'actualité des dernières années conduit à élargir à l'ensemble du corps social, institutions, entreprises et citoyens, la réflexion et les pratiques sécuritaires afin d'élaborer et d'affronter un concept de catastrophe inconcevable ou inimaginable. Les nouveaux concepts de sécurisation des systèmes d'information devront s'élaborer à deux niveaux, celui de la réduction des risques et celui de la résilience face aux chocs extrêmes. Il paraît réaliste aujourd'hui d'assigner aux organisations un objectif de 80 % de risques maîtrisés, les efforts consentis pour les mesures de résilience étant proportionnés aux 20 % de risques incontrôlables.

Réduire le niveau de risque

Les incidents graves qui ont secoué récemment le monde des *brokers* ont mis en évidence l'écart entre les règles et leur application, sans remettre fondamentalement en cause les premières. Il faut tirer parti de cette observation pour mettre l'accent sur les insuffisances dans la généralisation des bonnes pratiques de contrôle et de sécurité, ainsi que de leur mise en application.

Appliquer les bonnes pratiques

Il est urgent d'appliquer toutes les règles déjà définies et de les appliquer sans faille. L'écart entre les pratiques, d'une part, et les standards et référentiels, d'autre part, constitue à lui seul un gisement de sécurisation qui est à la fois important et facile d'accès, d'autant que les fonctions existent dans les organisations, celles des directions des systèmes d'information en particulier, celles des responsables de la sécurité des systèmes d'information également.

Les actions d'audit, de sensibilisation et de formation sont, dans ce contexte, de nature à faire baisser rapidement le niveau de risque. Elles feront notamment la lumière sur les pratiques ordinaires de confidentialité telles que le choix des mots de passe et leur renouvellement, l'usage des clés, la gestion des comptes d'administrateurs, enfin les habitudes des dirigeants en demande d'informations et d'échange sur le mode du « tout, tout de suite ». Dans l'ensemble des missions conduites à ce jour, les failles les plus couramment observées se situent à des niveaux d'évidence tels que la faiblesse des mots de passe, les retards dans la mise à jour des systèmes d'exploitation, le lancement de requêtes imprévues.

Bien entendu, l'audit devra inspecter les outils et solutions comme les pare-feu (*firewall*) et, quand ils existent, les systèmes de détection d'intrusion, d'authentification forte, de cryptographie, etc. Des technologies de pointe permettent en outre d'envisager des systèmes de surveillance des applications dans le monde entier, détectant les vulnérabilités et déclenchant des alertes en temps réel. Mais cette première action portera autant sur les facteurs humains que sur les systèmes eux-mêmes et préparera ainsi une nouvelle phase, dans laquelle les fonctions et l'organisation vont être repensées, ainsi que l'ingénierie des projets. La culture sécurité est en marche.

Rapprocher civils et militaires, public et privé

Avant d'aborder les rapprochements fonctionnels qui s'imposent dans les organisations, il paraît nécessaire d'en appeler à des rapprochements institutionnels, entre le civil et le militaire, d'une part, entre le public et le privé, d'autre part. Les retombées des technologies militaires, notamment dans le domaine de la cryptographie, ont déjà été exploitées avec profit, en particulier dans les applications financières et les systèmes de paiement électroniques. La fécondation peut être encouragée dans les deux sens, les secteurs bancaires et assurantiels ayant pris une réelle avance sur certains axes. On ne saurait trop encourager le partage des approches méthodologiques (Ebios, Critères communs, etc.), ainsi que des outils et produits, mais aussi le renforcement mutuel des capacités d'analyse des flux, en particulier de détection de flux sortants signalant des manœuvres de pirates, voire des logiques prospectives de défense offensive.

« Personne n'y parviendra seul »

Comment ne pas souhaiter une politique nationale d'émulation des initiatives privées ? Le modèle déjà éprouvé par le ministère de la Défense pour fédérer les compétences, lancer des programmes de R&D, centraliser les appels d'offres ne sera-t-il pas un jour adopté par le ministère de l'Intérieur ? Pourquoi ne pas imaginer un partenariat État-entreprises sur un objectif de normalisation, enfin, et surtout, l'intégration systématique de la sécurité dans le code des marchés publics ? « *Personne n'y parviendra seul* », tel est le leitmotiv recueilli au cours d'une enquête récente [1] dans les administrations et les grandes entreprises françaises.

(1) Enquête sécurité réalisée par l'activité conseil en sécurité de Thales auprès d'une centaine de décideurs en sécurité de grands groupes privés et publics et en administrations.

Certaines filières ont été identifiées dès l'origine, ou très rapidement, comme des filières à risque. Il semble souhaitable d'identifier aujourd'hui des filières émergentes dans cette catégorie et de leur faire bénéficier des approches qui ont fait leurs preuves. Nous avons su nous doter d'un Institut de protection et sûreté nucléaire et d'un Institut de veille sanitaire. L'État a montré, dans ces domaines, sa capacité à créer des organes de régulation, à établir des normes et imposer des règles. Il pourrait en être de même dans des domaines aussi nouveaux et aussi divers que la logistique des produits sensibles, la distribution de l'eau, etc.

Le gouvernement a déjà mis l'accent sur la nécessité de créer une Agence interministérielle chargée de la sécurité des systèmes d'information et dépendant directement du Premier ministre. Cette politique s'esquisse déjà au niveau européen, comme le souligne une récente intervention du ministre de l'Intérieur au Forum international de la cybercriminalité, appelant de ses vœux « la création d'une plate-forme européenne d'échanges d'informations sur la cybercriminalité, dans le cadre d'Europol ».

Créer une fonction nouvelle

À la transversalité institutionnelle doit correspondre une transversalité dans les organisations. La sécurité est aujourd'hui une contrainte dispersée dans de multiples fonctions. Très rares sont les organigrammes qui en individualisent la responsabilité globale. Celle-ci devrait être assumée par un directeur de la sécurité, rattaché à la direction générale comme toute fonction vitale ou stratégique et interlocuteur des pouvoirs publics. Ce manager serait chargé de conduire une politique cohérente de sûreté/sécurité, mission transverse à l'ensemble des fonctions, des services généraux à la direction des systèmes d'information, en passant par la R&D, les RH et l'ensemble des services utilisateurs des technologies de l'information et de la communication. Après la conformation aux bonnes pratiques, la deuxième phase verra donc interroger l'organisation, avec l'ambition d'installer à terme et de faire reconnaître cette fonction transverse.

Fédérer les talents

Ces managers d'un nouveau type devront appréhender la réalité des risques dans leurs dimensions à la fois technologiques et humaines, mais aussi juridiques. Ils auront à faire converger autour d'eux des talents aussi divers que ceux des sociologues, des informaticiens, des ergonomes, des conseillers en organisation et communication, et l'on ne saurait trop leur recommander de multiplier les échanges et les réseaux de partage d'expérience.

Repenser les organisations

On peut s'interroger sur les technologies, les outils, les pare-feux, et on doit le faire. On peut aussi, n'en déplaise aux écoles, questionner les modèles d'organisation matriciels, en mutation permanente, qui auront fait florès au XX^{e} siècle, avec leurs avantages non contestés mais aussi la difficulté à les traverser d'un éclairage cru dans une optique de contrôle. Gageons que le débat va s'ouvrir à nouveau avec les tenants des hiérarchies à deux dimensions et des chaînes de commandement et d'actions claires et efficaces.

Prendre en compte le climat social

On devra enfin sonder le climat social et les pratiques managériales qui ont autant d'influence sur les comportements déviants que sur d'autres variables qui ont pu être analysées par ailleurs, comme l'absentéisme ou les dégradations matérielles.

Encourager l'ingénierie simultanée

La mission de ces nouveaux managers sera à la fois corrective et structurante. Corrective, parce qu'ils auront à expertiser toutes les failles des systèmes d'information pour les combler.

Structurante surtout, car il s'agira d'intégrer la dimension sécurité au départ de tout nouveau projet. En un mot, ils auront à projeter autant qu'à protéger. On se trouve là dans une situation comparable à celle de la fonction qualité, voire celle de la fonction « développement durable » [2]. Elles ont été perçues au départ comme exerçant des contraintes négatives sur les cycles de conception et de développement, puis elles sont devenues des contraintes positives et structurantes des concepts. Enfin, la maturation du marché a suivi son cours.

Ainsi les solutions intrinsèquement, structurellement sécurisées apparaîtront bientôt comme celles qui affichent

(2) « Le développement durable est passé en quelques années du statut de sujet obscur pour spécialistes, à un concept flou, à la mode et principalement destiné à nourrir la communication des entreprises, avant d'émerger [...] comme un thème enfin sérieux, à la fois au centre des préoccupations politiques et sociales des gouvernements de beaucoup de pays développés et au cœur des stratégies de croissance de nombreuses des plus grandes entreprises mondiales. Il est à espérer qu'en matière de sécurité, l'obsession de continuité et de l'impératif d'image, mais aussi la nécessité de faire de la sécurité un avantage concurrentiel conduisent à une mobilisation similaire et concertée des gouvernants, des actionnaires et des dirigeants ».
INHES, 18^{e} session nationale d'études : État et entreprises, quelles synergies de sécurité pour quelle efficience ? Groupe de diagnostic de sécurité(GDS 7) - Mai 2007.

des avantages concurrentiels. Leur design avancé sera une barrière défensive, non seulement contre les pirates, mais... contre la concurrence ! Il faut donc encourager les approches d'ingénierie simultanée des systèmes et de leurs protections en associant les utilisateurs et les métiers à l'ensemble de la problématique.

Il est clair que les nouveaux défis de la sécurité sont des défis de créativité. Ici comme ailleurs, l'innovation viendra des rapprochements et, parfois des rencontres inattendues. On a déjà évoqué celles de la banque et du militaire. Mais si l'on approfondit un peu le concept de lutte contre l'invisible qui caractérise la nouvelle problématique sécuritaire, on est aussitôt renvoyés à des domaines apparemment incongrus comme le nucléaire et l'agroalimentaire. Dans le premier, l'invisible est ce qui peut émaner du produit, la radiation. Dans le second, l'invisible est ce qui peut l'affecter : le virus ou la bactérie. Contamination centrifuge, contamination centripète. Le nucléaire a disposé de beaucoup de moyens pour développer ses protections. Les systèmes d'information en ont tiré profit et les retombées en matières de technologies sécuritaires sont, ici aussi, à prendre en compte, notamment en matière de traçabilité. L'agroalimentaire a dû faire beaucoup avec peu de moyens, développant des réponses créatives dont on peut tirer des leçons. Quand on ne peut s'offrir une salle blanche, on est obligé de penser son *process* comme intrinsèquement propre. Il s'agira donc, sur le même modèle, de maîtriser les contaminations en passant de l'intrinsèquement propre à l'intrinsèquement sûr.

Étendre le concept de résilience aux organisations

Le moment est venu d'élargir le concept de résilience. Bien au-delà de la seule capacité des systèmes à continuer de fonctionner en cas de panne, il faut l'étendre à l'organisation elle-même pour la rendre capable de « manager la surprise ». Les comités de direction et le management doivent pouvoir se déployer rapidement avec une capacité intacte à recueillir, traiter et échanger des informations, quelles que soient la nature et l'ampleur des chocs. Les capacités physiques et psychologiques des personnels eux-mêmes à circuler et à reprendre les opérations seront anticipées, sans exclure aucune hypothèse, notamment sur l'axe de la délocalisation d'urgence des fonctions en mode télétravail.

Rapprocher continuité d'activité et gestion de crise

Il conviendra donc de rapprocher deux fonctions trop souvent distantes, celle qui s'engage sur la continuité d'activité et celle qui anticipe la gestion des crises. La continuité d'activité est trop souvent considérée dans la seule sphère des ressources informatiques, voire dans l'hypothèse que l'énergie et les télécommunications subsisteront dans tous les cas. Les consignes comportementales et actions psychologiques prennent toute leur place dans ce concept élargi.

Repenser les logiques immobilières

On interrogera les logiques immobilières qui conduisent à loger sous le même toit les centres de pilotage et les centres de traitement, bien qu'ils soient déjà cloisonnés dans la plupart des cas. On pointera naturellement le voisinage éventuel de ces derniers avec les équipements de *back up.* La même question se posera sur la proximité des centres de management et des salles de secours, dont les moyens de communication, en outre, sont souvent vulnérables : la menace NRBC (nucléaire, radiologique, biologique, chimique) notamment est généralement occultée.

Partager des modèles

Le partage d'expériences et de technologies est le chemin le plus court pour offrir aux organisations les moins avancées des réponses de haute performance et des coûts acceptables. Les rapprochements avec le militaire et le nucléaire notamment seront fructueux. On pourra en importer des modèles de type « war room » et de « bastions » informatiques, de « dispositifs mobiles » – espaces de repli nomades –, d'infrastructures de télécommunications spécialisées et interopérables, de redéploiement des organisations aux domiciles des salariés.

Toutes ces approches devront être concevables en environnements propriétaires ou partagés, voire accessibles à travers des offres de services.

Globaliser les approches

Réseaux, topographie, organisation : les approches doivent être globales, technologiques, multiflux, immobilières et humaines. Leur cohérence doit être garantie par des « chefs de projets résilience », la cohésion des cellules de crise et l'efficacité des procédures d'urgence dûment testées par des exercices, aujourd'hui encore très insuffisants.

Vers l'intelligence collective de la sécurité

La complexité des menaces est telle que les modèles traditionnels de réponses centralisées doivent être dépassés. La résilience des organisations doit être pensée en termes

d'intelligence collective de la sécurité. En clair, cela signifie qu'aucune intelligence individuelle ne pourra totaliser le concept de la solution sécuritaire, qui se trouvera en revanche diffracté dans la communauté des personnes concernées. L'organisation pourra dès lors démontrer une intelligence résiliente non seulement supérieure aux capacités individuelles de ses meilleurs éléments, mais aussi supérieure à la somme de ses parties. À une échelle plus vaste ces concepts pourront à leur tour être appliqués à la résilience citoyenne, voire à l'échelle des mégalopoles. Ce nouveau territoire conceptuel, qui reste à conquérir, contient peut-être des éléments de réponse essentiels à la problématique qui ébranle aujourd'hui nos démocraties en profondeur, celle de la compatibilité entre leur propre survie comme espaces de liberté et leur protection contre des menaces imprévisibles et inimaginables.

Le décret « Secteurs d'activité d'importance vitale » (SAIV) du 23 février 2006, les Directives nationales de sécurité (DNS) qui ont suivi, enfin le *Livre blanc* de la Défense et de la Sécurité ont montré la volonté des pouvoirs publics de mobiliser les énergies et les compétences, tout particulièrement en direction des activités critiques pour la nation dans les secteurs de l'énergie, du transport public, de l'aéronautique et de l'industrie. La prise de conscience se propage dans l'administration civile et le secteur privé, tandis que le monde militaire se montre ouvert aux synergies.

Reste à positionner, sur le marché de la sécurité des systèmes critiques, des prestataires capables de mobiliser en leur sein (à l'exemple de Thales) des équipes pluridisciplinaires de consultants, d'architectes systèmes et d'ingénieurs. Ces acteurs globaux seront d'autant plus précieux qu'ils pourront proposer une approche à la fois technologique et organisationnelle – et fédérer le meilleur des quatre mondes, civil et militaire, public et privé.

Gérard PESCH

Interview de Didier DUVAL, Contrôleur général,
Chef du Pôle de la lutte contre la délinquance financière
et de la protection du patrimoine
de la direction centrale de la Police judiciaire

PHAROS, la plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements

Quelle est la mission dévolue à cette plateforme ?

Cette plateforme située au sein de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), l'un des offices centraux de la sous-direction en charge de la lutte contre la criminalité organisée et la délinquance financière de la direction centrale de la Police judiciaire, a été créée en 2005, et sera finalisée en fin d'année 2008, dans le cadre du plan de renforcement de la lutte contre la cybercriminalité de Michèle Alliot-Marie, ministre de l'Intérieur, de l'Outre-mer et des Collectivités territoriales. Cette plateforme a pour objectif de recenser ce qui apparaît comme illégal sur Internet en vue de son traitement judiciaire par un service de police ou de gendarmerie territorialement compétent, et après avis de l'autorité judiciaire.

De qui est composée cette plateforme ?

Cette plateforme est composée d'une équipe mixte de policiers et gendarmes actuellement au nombre de dix personnes et susceptible, à terme, en fonction du volume de son activité de voir ses effectifs s'étoffer en conséquence.

Pourquoi une telle structure ?

La loi du 21 juin 2004 sur la confiance dans l'économie numérique a déchargé les fournisseurs d'accès à Internet d'une partie de leur responsabilité pénale et civile du fait des contenus illicites dont ils ignorent la mise en ligne sur leurs supports. En contrepartie, elle leur a imposé une triple obligation d'agir promptement pour supprimer l'accès à ces contenus quand ils en ont connaissance, de les signaler aux autorités publiques lorsqu'ils relèvent de la xénophobie, de la pédophilie ou de la diffusion d'images à caractère violent ou pornographique susceptibles d'être vues par des mineurs, et de mettre à la disposition du public un moyen de rapporter facilement ces contenus.

L'État se devait donc de mettre en place une structure capable de recevoir et de traiter de tels signalements. Le ministre de l'Intérieur, de la Sécurité intérieure et des Libertés locales, dans son discours prononcé le 13 avril 2005, à l'occasion de la présentation des travaux du Chantier de lutte contre la cybercriminalité, avait donc annoncé « *la mise en place d'un centre national de signalement, afin d'éviter qu'une même information consultée par une multitude d'internautes ne génère une démultiplication des plaintes et des signalements* ».

Le centre était ainsi défini :

- un point d'entrée national, unique et clairement identifié ;
- pour le signalement des contenus illicites de l'internet ;
- distinct de l'activité de veille (travail d'initiative qui vise à rechercher de manière proactive les infractions) ;
- composé à parité de policiers et de gendarmes et placé auprès de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC).

La plateforme nationale de signalement prendra sa pleine dimension dès que les autorisations administratives de nature juridique le permettront. Elle donnera concrètement accès pour le public à un portail, sous l'adresse www.internet-signalement.gouv.fr qui autorisera tout internaute à signaler en ligne l'existence d'un contenu illicite, dans tous les domaines de la criminalité, et non plus dans le seul domaine de la pédopornographie.

Quels sont les perspectives d'évolutions de la plateforme ?

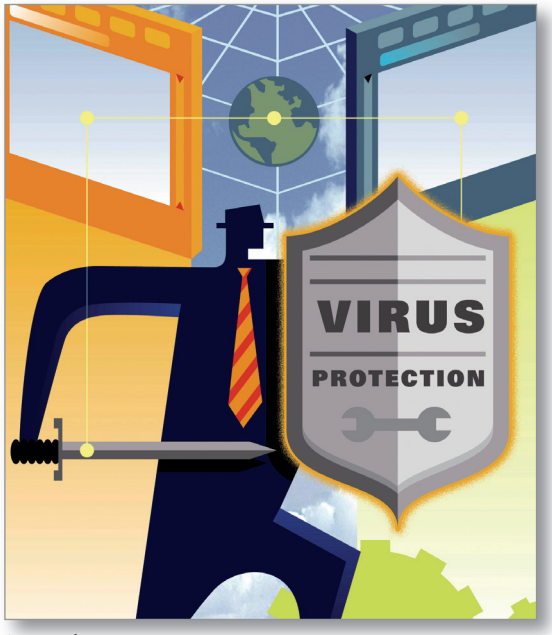
Cette plateforme, qui assurera donc une présence forte et visible des pouvoirs publics en termes de prévention et de poursuite des actes illicites sur Internet, pourrait également servir de support de communication à destination des internautes, souvent mal informés des risques liés à la cybercriminalité. Des informations sur les méthodes de protection des ordinateurs individuels ainsi que sur les modes opératoires les plus couramment employés par les fraudeurs pourraient aussi être diffusées sur ce portail.

Par ailleurs, la mise en place d'une solution de filtrage des sites pédopornographiques s'appuiera nécessairement sur le dispositif PHAROS, seule entité étatique capable de générer une liste de contenus illicites en temps réel.

Enfin, il convient de souligner que dans le cadre des activités de la Présidence française de l'Union européenne du second semestre 2008, l'OCLCTIC a organisé, du 3 au 7 juin 2008 à Reims, un séminaire européen réunissant les spécialistes de la lutte contre la cybercriminalité de l'Union européenne, ainsi que du Maroc et du Sénégal, ayant pour thème l'idée de l'extension d'une plateforme de signalement à l'échelle européenne, dont la mission consisterait à fédérer des plateformes nationales et mutualiser leurs informations dans une démarche de coopération policière et judiciaire accrue.

L'Europe, un atout pour la France dans la lutte contre la cybercriminalité

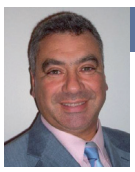
Christian AGHROUM



La cybercriminalité est globale. L'Europe, forte de pays riches et industrialisés, en est une cible privilégiée. La France ne peut lutter seule, même au sein de ses propres frontières. La lutte ne peut se concevoir sans une approche organisée et cohérente des 27 États membres. L'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) de la direction centrale de la Police judiciaire, service à vocation tout à la fois stratégique et opérationnelle, assure la lutte au plan interministériel. Christian Aghroum, qui en est le chef, nous propose là une approche paneuropéenne de réponse au phénomène.

European Institutions: An Opportunity for France in its Struggle against Cybercrime

Cybercrime is global. The rich industrialized countries of Europe are prime targets. France cannot counter this crime alone, even when it is perpetrated within its own borders. It must rely on an organized and coherent approach with the 27 other members of the European Union. The Central Office of the Prevention of Crime Related to the Technologies of Information and Communication, part of the Central Direction of the Judicial Police, is a service whose goal is strategic and operational, as well as inter-ministerial. The Commissaire Divisionnaire Christian Aghroum is its head. He proposes a pan-European approach to the new phenomenon.



Christian Aghroum

Commissaire divisionnaire, chef de l'OCLCTIC. Entré dans la Police nationale en 1982, en tant qu'inspecteur à la préfecture de Police de Paris (brigade de protection des mineurs, puis brigade des stupéfiants), admis au concours de commissaire de police en 1991, il a exercé toutes les activités de police judiciaire confondues, en province et à Paris, notamment dans la lutte antiterroriste, aux différents niveaux de responsabilité. Il est également professeur associé à l'École nationale supérieure de la police et à l'École nationale de la magistrature. Il occupe la fonction de président du groupe « statistiques » de l'Observatoire national de la sécurité des cartes de paiement.

Internet n'a pas de frontières. Cette réalité s'impose à tous et, tout particulièrement, aux services en charge de la sécurité de nos concitoyens. Parallèlement, le respect des souverainetés nationales ne saurait être un frein à la protection des internautes. Dans un monde où le maillon faible fragilise l'ensemble du dispositif, seule une action solidaire européenne permettra aux 27 États membres d'atteindre l'équilibre nécessaire à une lutte conjointe. Il convient donc, pour lutter efficacement contre la cybercriminalité, de promouvoir les outils de mutualisation nationaux, mais aussi européens qui permettront à l'espace des 27 de se protéger au mieux. Il faut être innovant, proactif et solidaire.

La France dispose d'outils de lutte efficaces. L'Hexagone s'est rapidement mis en situation de lutter contre la cybercriminalité. La loi informatique et libertés, dès le 6 janvier 1978, pose les fondations de l'arsenal juridique français. La loi pour la confiance dans l'économie numérique du 21 juin 2004 assied la réalité du droit de l'Internet et les bases d'une nouvelle manière de commercer.

Parallèlement, dès la fin des années 1980, les autorités françaises mettent en place un groupe d'enquêteurs spécialisés qui allaient faire florès. Environ 350 fonctionnaires de police et militaires de gendarmerie constituent à ce jour la flotte dont disposent les services de sécurité intérieure pour lutter efficacement contre la cybercriminalité. Leur mission est facilitée par les compétences en police technique et scientifique déployées au sein de la sous-direction de la Police technique et scientifique de la direction centrale de la Police judiciaire à Écully près de Lyon, pour la Police nationale, et à Rosny-sous-Bois pour la Gendarmerie nationale. La perméabilité des deux forces est, à cet égard, un atout considérable. L'appui des attachés de sécurité intérieure déployés dans les ambassades de France à l'étranger par le Service central technique international de police est indispensable et de grande qualité. Les nombreuses formations de polices étrangères sur site sont significatives à cet égard, nonobstant la plus grande fluidité des informations d'ordre opérationnel quotidiennement échangées.

L'action des forces répressives françaises sur le territoire national s'enrichit aussi de celle des institutions policières européenne et mondiale que sont Europol et Interpol à travers les différents offices centraux de police judiciaire dont l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication. L'apport d'Europol à la lutte contre la cybercriminalité est indéniable et se concrétise à travers les fichiers d'échange de données qui évoluent, en ce sens, sous la pression des pays membres. Eurojust complète ce dispositif.

Les axes de la lutte contre la cybercriminalité

Le plan annoncé par Michèle Alliot-Marie, ministre de l'Intérieur, de l'Outre-mer et des Collectivités territoriales progresse. La mise à niveau des outils statistiques, à disposition des services de police et de gendarmerie, et, à travers l'Observatoire national de la délinquance, à disposition des chercheurs et de la presse, affinera notre connaissance de l'impact de la cybercriminalité en France et de son évolution. Une étude objective permettra de mesurer l'impact sur la population à l'heure où le taux de pénétration dans les foyers français ne peut que croître du fait du développement de la micro-informatique à des prix de plus en plus accessibles, des liaisons de troisième génération, de l'arrivée de la Wi MAX et des réseaux de fibre optique, de la téléphonie support de télévision et des jeux en ligne, du « push mail ». L'assistant personnel, le bureau mobile, la console multimédias sont dorénavant les outils nomades incontournables du cadre, du retraité, de l'adolescent.

La législation française s'adapte aux pratiques contemporaines de la cybercriminalité. L'obligation de conserver durant une année les données de connexion sera clarifiée pour prendre en compte les accès aux bornes Wi-Fi et ceux aux points d'accès publics. Les possibilités de captation de données à distance sous contrôle d'un juge, dans le cadre de la lutte antiterroriste et contre la criminalité organisée, sont à l'étude. L'usurpation d'identité sur Internet, infraction pivot d'une grande part des nuisances connues sur la toile, devrait prochainement être poursuivie. Ces progrès s'accompagnent d'avancées administratives et culturelles nécessaires au sein du dispositif répressif.

La France dispose historiquement de deux forces de police complémentaires : Police nationale et Gendarmerie nationale. Au 1er janvier 2009, les deux forces seront placées sous l'autorité du ministre de l'Intérieur. Chacune possède déjà de réelles compétences dans la lutte contre la cybercriminalité. La synergie des services de police et de gendarmerie permettra, à travers une formation commune, la mise en place d'un réseau d'experts. Des cursus à vocation technologique dans les services sont en voie d'être définis. Les formations assurées par Europol sont à cet égard exemplaires et seront encouragées. La recherche et le développement d'instruments partagés assureront une meilleure efficience des enquêteurs spécialisés dont il est prévu, à l'horizon 2012, de doubler le nombre actuel, permettant ainsi d'atteindre le nombre de 700 spécialistes.

Au même titre que la lutte contre la cybercriminalité doit être coordonnée au plan national, les États membres

européens doivent continuer à travailler de concert. Les services français doivent s'appuyer sur une meilleure coopération internationale. Elle passe d'abord par une entraide et une compréhension mutuelle en Europe.

La création d'un groupe de lutte contre les escroqueries sur Internet au sein de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication, dès septembre 2008, permet de mieux protéger nos concitoyens en échangeant avec nos partenaires. Il complétera le dispositif de protection de la carte de paiement en France, assurant le développement serein du commerce en ligne.

Le développement d'instruments techniques facilitant les perquisitions et constatations distantes autorisera la France à accroître sa compétence avec ses partenaires européens dans une logique partenariale et de réciprocité. La création d'équipes communes d'investigation et d'enquête est encouragée. Comment pourrait-il en être autrement dès lors que plusieurs pays européens sont victimes d'une même équipe organisée de cyberdélinquants ?

Une plateforme européenne de signalements

L'idée d'une plateforme européenne de signalements répond à cette évidence. La France dispose, en effet, au sein de l'OCLCTIC, d'une plateforme nationale en charge de recueillir les signalements des contenus illicites. La démarche est obligatoire pour les fournisseurs d'accès internet, elle est naturellement facultative pour les particuliers et répond à une démarche citoyenne. La plateforme ouverte en septembre 2006 ne traitait principalement que de signalements relatifs à la pédopornographie, l'incitation à la haine raciale et à la xénophobie. Sur 24 193 signalements traités de septembre 2006 à juin 2008 inclus, 3 320 ont fait l'objet d'une procédure dont 585 en France et 2 735 à l'étranger, soit 13,7 % des signalements. Le fort nombre de signalements non traités prouve l'intérêt d'un système centralisateur permettant d'éviter sur le terrain la redondance de services de police. L'idée de décliner à l'identique ce modèle, mais au plan européen, est née de ce constat, d'autant que sur 1 464 messages transmis par le BCN-Interpol à l'étranger, durant le premier semestre 2008 (la discrimination n'avait pas été opérée précédemment), 142 l'ont été à destination de pays européens soit environ 10 %.

Un traitement centralisé européen permettra donc d'éviter les redondances de traitement pour des signalements intéressant plusieurs pays en Europe, ce qui ne peut être que régulier, Internet ne connaissant pas de frontières.

Des plateformes identiques existent dans la plupart des pays européens. Seize pays européens sont déjà équipés d'une plateforme étatique, quatre d'une structure mixte [1] (État/privé) et sept n'en sont pas dotés [2]. Chacune reflète les enjeux légaux, sociaux et culturels de son pays, mais toutes ont la même ambition : apporter une réponse simple et rapide aux exigences de nos concitoyens en évitant la redondance des services saisis d'un même fait. Il importe que chaque pays européen en soit muni. Le constat national pourra ainsi se répéter au plan européen. La création d'une plateforme européenne, point central d'échanges des plateformes nationales, évitera la répétition de signalements identiques, inutilement croisés lors de liaisons intracommunautaires jusqu'alors principalement bilatérales. Elle favorisera la connaissance commune et enrichira l'Europe d'un nouvel outil de cybersécurité.

La plateforme européenne sera aussi le dispositif commun nécessaire à l'égard des pays extra-européens hébergeurs de cybercriminels ou de réseaux zombies. Elle sera un parfait exemple du partenariat privé-public indispensable à la lutte contre la cybercriminalité en concordance avec les travaux menés par la France au sein du Conseil de l'Europe et de la Commission européenne, travaux de consolidation du dispositif menés lors du séminaire tenu à Reims début juin 2008. Les vingt-sept États membres et quatre pays extra-européens choisis car représentatifs de leur continent ou de leur culture (Canada, Japon, Maroc, Sénégal) ont concouru à la définition de ce nouvel outil. Cette plateforme européenne sera hébergée par Europol.

La compétence des divers États membres dans la lutte contre la cybercriminalité est diverse et inégalement partagée alors même que tous les pays européens sont concernés. La solidarité est là aussi indispensable ; la sécurité de tous repose sur la force de chacun, la mutualisation des compétences et le soutien combiné des différentes forces en présence. Une politique de sécurité intérieure au sein même des frontières européennes est garante d'une lutte efficace contre la cybercriminalité.

(1) Finlande, Irlande, Lettonie, Malte.
(2) Espagne, Estonie, Hongrie, Pays-Bas, Pologne, Portugal, Slovaquie.

La France assure la présidence de l'Union européenne de juillet à décembre 2008. Renforcer la lutte contre la cybercriminalité en Europe est bien l'un des objectifs qu'elle s'est fixé.

Un plan ambitieux sur des bases européennes solides

L'Union Européenne n'a fort heureusement pas attendu 2008 pour s'organiser dans la lutte contre la cybercriminalité. La Convention de Budapest du Conseil de l'Europe, en date du 23 novembre 2001, est l'outil racine de lutte contre la cybercriminalité. Elle n'est signée et ratifiée que par une partie des pays européens et pourrait l'être par tous.

Des mesures proprement européennes sont par contre en vigueur, et précisent les moyens d'action de l'Union européenne. La décision-cadre 2005/222/JAI relative aux attaques des systèmes d'information en est une. La décision-cadre 2004/68/JAI sur la protection des enfants contient, pour sa part, un chapitre précis sur l'utilisation d'Internet. La directive 2002/58/CE « Vie privée et communications électroniques » porte obligation pour les fournisseurs d'accès de garantir la sécurité de leurs services.

La création en 2004 d'une Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) [3] est un atout de sécurisation des systèmes d'information en Europe d'autant que l'enjeu est rappelé par le 7e programme-cadre de recherche de l'UE.

La Commission poursuit ses projets de recommandations en matière de partenariat public-privé et de formation d'enquêteurs spécialisés de haut niveau. La Commission, enfin, a lancé, le 25 mai 2007, au Parlement européen, au Conseil et au Comité des Régions une communication intitulée « Vers une politique générale en matière de lutte contre la cybercriminalité », base de doctrine européenne.

Le Conseil européen des 8 et 9 novembre 2007 a, pour sa part, rappelé l'intérêt de l'ensemble de ses mesures et tout particulièrement de la recommandation de la Commission, appuyant sur les aspects de formation des autorités policières et judiciaires, le dialogue nécessaire entre le secteur public et le secteur privé et l'importance de la Convention du Conseil de l'Europe du 23 novembre 2001.

Plusieurs axes sont poursuivis. Mieux se connaître, partager, anticiper en sont les maîtres mots.

Améliorer la connaissance mutuelle et la formation des acteurs

La mise en place d'un réseau des chefs de service de lutte contre la cybercriminalité est à encourager. Une réunion annuelle des différents chefs de service européens permettrait, outre une meilleure connaissance des 27 dispositifs de lutte contre la cybercriminalité, la mise en place d'une synergie de lutte, l'échange de bonnes pratiques et l'aide au développement des services des pays les moins bien équipés.

Dans la même logique, il faudrait réunir un groupe d'experts chargés de réfléchir aux éléments prospectifs utiles à une meilleure compréhension des risques futurs, de manière à mieux former et armer les services enquêteurs.

Un groupe de veille technologique européen chargé de tester les outils d'investigation et de police technique et scientifique, au profit des unités d'investigation, aurait toute sa place. L'objectif étant d'éviter les redondances et de rechercher les meilleurs coûts d'acquisition. Un « label » police pourrait être attribué qui contribuerait à des cofinancements européens, l'intérêt étant à nouveau d'aider les pays les moins bien équipés et de soutenir les autres dans leur programmation d'acquisition.

Le dispositif de formation commun actuellement engagé en partenariat par Europol et l'université de Dublin doit être poursuivi : la cybercriminalité n'a pas de frontière, la formation des différents acteurs de lutte doit être identique en Europe, et basée sur les mêmes processus de recherche et d'acquisition de la preuve. La création à terme d'une « académie de lutte contre la cybercriminalité » doit être soutenue.

Encourager le partenariat public-privé

Le Conseil de l'Europe, les 1er et 2 avril 2008, lors de sa conférence Octopus, a proposé la mise en place d'une recommandation visant à améliorer le partenariat public-privé dans le cadre de la lutte contre la cybercriminalité. Cette recommandation est en fait une charte des bonnes pratiques à mettre en place pour fluidifier les rapports entre acteurs et, tout particulièrement, entre forces de police (Law enforcement agencies - LEA), opérateurs, fournisseurs d'accès, hébergeurs, etc. La Commission

(3) http://europa.eu/agencies/community_agencies/enisa/index_fr.htm

européenne, pour sa part, travaille à la déclinaison de ce texte dans l'espace des 27 États membres. Cette idée est à soutenir impérativement, les éléments nécessaires à la lutte contre la cybercriminalité étant au plan technique essentiellement détenus par les partenaires privés.

La conservation des données, point clef de la lutte contre la cybercriminalité, fait l'objet d'une directive dont l'application doit être suivie. Les travaux sur l'itinérance téléphonique (*roaming*) doivent être poursuivis et mis en application.

Rechercher des outils juridiques adaptés

La perquisition à distance est une conséquence inéluctable du mode de fonctionnement d'Internet. La notion de souveraineté territoriale est battue en brèche par l'universalité de l'Internet et l'extraterritorialité des actes criminels y afférents. De même, l'émergence d'acteurs mondiaux (*Microsoft*, *Google*, *eBay*, *MySpace*, *U-Tube*, *Facebook*...) a contribué à une gestion à l'extérieur de nos frontières de données personnelles relatives aux utilisateurs de ces services. Ces données sont ainsi difficilement accessibles aux services d'enquête, alors qu'elles concernent souvent des ressortissants de leur propre pays.

La perquisition en ligne constitue, dès lors, l'unique moyen d'accéder rapidement à ces informations. Le Code de procédure pénale français a intégré une disposition en son article 57-1 qui permet, sous certaines conditions, l'accès distant à un système informatique. De même, la Convention de Budapest prévoit une telle possibilité entre pays signataires. Il convient donc d'encourager la mise en œuvre de ces dispositions au niveau européen et la généralisation de ces pratiques.

L'usurpation d'identité est l'infraction pivot du vol de données sur Internet. Une étude européenne des différentes législations est en cours. Il convient d'encourager cette initiative, et d'aboutir à l'adoption d'une incrimination spécifique dans l'ensemble des États membres.

Le blocage des sites pédopornographiques ne peut se faire isolément. Plusieurs États ont déjà adopté de telles solutions (Norvège et Royaume-Uni notamment) et la France s'apprête à adopter un texte législatif obligeant les fournisseurs d'accès à prendre de telles mesures. Cette idée doit être généralisée à l'ensemble des États membres. La plateforme européenne de signalement (*cf. infra*) pouvant être l'outil d'établissement d'une liste noire commune.

Le recours à la cyberpatrouille est un outil moderne de lutte contre la criminalité sur Internet. Cette méthode ne peut être utilisée dans l'unique enclave nationale, de peur que des cyberpatrouilleurs, issus de pays différents, ne se retrouvent à se piéger mutuellement. L'information sur les pseudonymes doit donc être partagée au niveau européen, ainsi que la formation spécifique sur ce domaine.

Mettre en place rapidement la plateforme européenne de signalement des contenus illicites

Les conclusions du séminaire de Reims ont fait apparaître la nécessité de créer une plateforme européenne de signalement des contenus illicites. Au-delà de l'aspect purement opérationnel, la plateforme européenne pourra servir d'outil statistique, de coopération et de fondement de négociation. En effet, il est nécessaire que l'Europe puisse s'exprimer d'une seule voix, face aux pays hébergeurs de cybercriminels ou jouant un rôle majeur dans la gouvernance mondiale de l'Internet.

Aider les pays émergents à lutter contre la cybercriminalité

Aider les pays émergents est nécessaire au renforcement de tous les maillons de la chaîne d'entraide internationale, indispensable à la lutte contre la cybercriminalité. La cybercriminalité est un fléau mondial dont l'Europe est particulièrement victime. Il est dans son intérêt de contribuer au développement des compétences et des moyens juridiques et techniques des pays émergents. Ces derniers constatent un taux de pénétration élevé des technologies de l'information et de la communication, mais demeurent impuissants à juguler les phénomènes criminels liés à ces évolutions. Les réseaux organisés sont, en effet, mobiles et s'installent où les faiblesses législatives et d'organisation leur sont le plus favorables.

Christian AGHROUM

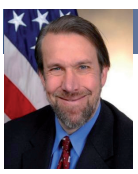
Combattre le cybercrime : défis et perspectives, nécessité d'une coopération internationale

Christopher PAINTER

La menace que représente le cybercrime a terriblement augmenté durant ces dix dernières années, alors que la société est sans cesse plus dépendante des réseaux informatiques, et les criminels toujours plus inventifs et tenaces dans l'usage abusif de cette technologie. Cet article est centré sur cette menace changeante, les types de mesures qui devraient être prises au sein de chaque pays pour la combattre – y compris la formation de magistrats et d'officiers de police – et examine la nécessité d'une coopération internationale sans précédent, compte tenu de la nature sans frontières de cette criminalité.

Combating Cybercrime : Challenges And Opportunities And The Need For International Cooperation

The threat posed by cybercrime has increased dramatically over the last ten years as society has become ever more dependent on computer networks and criminals have become ever more inventive and persistent in abusing this technology. This article focuses on this changing threat, what steps should be taken within each country to combat it – including training and education of Magistrates and law enforcement officers – and discusses the need for unprecedented international cooperation given the borderless nature of these crimes.



Christopher Painter

Christopher Painter est actuellement conseiller du vice-ministre de la Justice pour la Division criminelle au Département américain de la Justice (DOJ), spécialisé dans les questions de cybercrime. Il a précédemment participé à la direction de la Section criminalité informatique et de la Propriété intellectuelle du DOJ, et a été procureur fédéral à Los Angeles. Il poursuit la criminalité informatique depuis 16 ans et a instruit certaines des affaires les plus célèbres aux États-Unis, comme celle du « hacker » notoire Kevin Mitnick. Il préside aussi le Sous-groupe sur le Crime high-tech du G8 et co-préside le Groupe de coordination « *National Cyber Response* » américain.

Apparemment, depuis les débuts de l'histoire humaine, chaque avancée technologique s'est accompagnée de son exploitation par des criminels qui cherchent à l'utiliser pour servir leurs vils projets. Cela s'est vérifié avec la poste, les réseaux téléphoniques et maintenant, à un degré sans précédent, les réseaux informatiques et Internet. La criminalité informatique est saisissante par son étendue et sa diversité, comprenant non seulement de nombreux délits traditionnels perpétrés grâce à un nouveau et puissant moyen – le prétendu « vieux vin dans de nouvelles bouteilles » - comme la fraude, l'escroquerie et la diffusion de pornographie enfantine, mais aussi de nouveaux types de délits comme le hacking, l'attaque des ordinateurs par des virus, et la diffusion d'attaques par déni de service, où c'est l'ordinateur même qui est la cible du délit. La dépendance croissante de la société envers les ordinateurs et les réseaux informatiques accroît la portée des attaques et des perturbations sur ces systèmes, ainsi que la nécessité d'une enquête efficace et d'une dissuasion des individus susceptibles d'entreprendre de telles attaques. De plus, comme les ordinateurs sont maintenant utilisés pour contrôler des infrastructures essentielles, telles que les réseaux électriques, de télécommunications, d'eau ou d'autres systèmes vitaux, les conséquences de la piraterie informatique revêtent une dimension qui va bien au-delà d'une simple perte économique.

Évidemment, l'augmentation de l'exploitation criminelle des nouvelles technologies a aussi entraîné un jeu du « chat et de la souris » entre les services de police et les criminels dans lequel chacun cherche à être plus malin que l'autre. L'avènement d'Internet et des réseaux informatiques en général a donné de nouvelles dimensions à cette bataille : de nouvelles méthodes pour traquer les conduites criminelles ont été mises en œuvre, mais cela a aussi posé des défis d'envergure aux enquêtes des services de police. La criminalité informatique est, de par sa nature, fondée sur la technologie et, par conséquent, exige une compréhension et une maîtrise de celle-ci pour que les enquêtes et poursuites judiciaires soient efficaces. De plus, ce type de criminalité présente une « menace asymétrique » permettant aux criminels d'atteindre un nombre de victimes infiniment plus grand et de causer de très gros dégâts financiers ou autres, avec un investissement modeste en termes de ressources et de savoir-faire. Cela se double de l'apparent anonymat qu'offre Internet, et du fait que ce système ainsi que la criminalité informatique sont véritablement sans frontières. À la différence de la plupart des domaines de la criminalité traditionnelle, la criminalité informatique n'a souvent pas de frontières juridiques - les criminels peuvent attaquer leurs victimes dans plusieurs régions et pays différents. Un criminel malin opérant sur Internet va intentionnellement acheminer ses communications et attaques à travers plusieurs pays. À vrai dire, il y a eu des affaires dans lesquelles le criminel et la victime étaient localisés dans la même ville, cependant les attaques impliquaient de nombreuses juridictions nationales et internationales. Cette absence de juridiction unique a de sérieuses conséquences sur l'efficacité des enquêtes et des poursuites judiciaires. De surcroît, la nature internationale de ces délits complique l'unique aspect le plus important de toute enquête criminelle, à savoir la désignation du coupable pour le traduire en justice. La désignation d'un coupable de délit sur Internet est en soi une question difficile en raison de la nature technique du traçage des manœuvres électroniques et du caractère souvent éphémère des preuves électroniques. Le traçage d'un seul délit électronique peut nécessiter un processus se divisant en plusieurs phases impliquant l'obtention d'informations chez de nombreux fournisseurs de services internet et d'autres parties en cause. Obtenir une preuve permettra probablement de fournir les informations nécessaires pour remonter vers le maillon suivant de la chaîne des FAI (Fournisseurs d'accès internet), mais chaque étape prend du temps. Malheureusement, les divers FAI et autres entités ont des politiques différentes quant à la longueur du délai pendant lequel ils conservent des fichiers cruciaux et autres archives. Par conséquent, les traces digitales qui constituent la piste dans la délinquance informatique peuvent disparaître et l'enquête se trouvera alors très rapidement dans une impasse.

Tout cela est aggravé par la nature internationale de cette criminalité. Pour que les enquêtes aboutissent, les données doivent demeurer disponibles dans les multiples juridictions où ont lieu les délits. Cependant, les divers pays ont des régimes juridiques différents et parfois hétérogènes quant à la durée de sauvegarde des données par les fournisseurs de services. Cela renforce l'importance d'enquêtes fiables et rapides sur le plan national autant qu'international. Le calendrier classique d'enquêtes complexes qui peuvent parfois prendre des années ne sera pas adapté pour contrer le cybercrime ou même la criminalité classique dans laquelle les preuves électroniques volatiles sont désormais primordiales.

Pour que les enquêtes dans le domaine du cybercrime soient fiables et efficaces, un certain nombre d'éléments s'avèrent indispensables. En premier lieu, tous les pays doivent avoir une législation et une procédure solides punissant le cybercrime et permettant le dépistage des conduites criminelles. En second lieu, les enquêteurs, procureurs et juges doivent être formés de manière adéquate afin de bien comprendre ce type d'affaires. Et enfin, il

faut mettre sur pieds une coopération internationale solide et opérationnelle.

Dans ce bref article, j'examinerai tout d'abord l'évolution de la nature du cybercrime à partir de l'expérience des États-Unis. Je décrirai ensuite quelques méthodes de formation et autres dispositions structurelles adoptées aux États-Unis afin de combattre ce nouveau fléau – en particulier la construction de réseaux d'enquêteurs et de procureurs. J'analyserai enfin certains des efforts internationaux essentiels – comme la construction d'infrastructures juridiques, la formation et la coopération internationale – en insistant particulièrement sur la Convention sur le Cybercrime du Conseil de L'Europe et le G8 24/7 *High Tech Crime Point of Contact Network* (réseau d'information du G8 accessible vingt-quatre heures sur vingt-quatre pour la lutte contre la criminalité liée à la haute technologie).

L'Évolution de la menace du cybercrime

Depuis que j'ai commencé à engager des poursuites judiciaires contre les cybercrimes en 1992, bien des choses ont changé. Au début des années 1990, les réseaux internet restaient le domaine des grandes entreprises, des institutions éducatives et des passionnés d'informatique. La plupart des gens s'intéressaient peu aux réseaux informatiques et n'en dépendaient pas beaucoup. La criminalité informatique était assez circonscrite, plus motivée par le défi intellectuel (ou à tout le moins prétendument) que par l'appât du gain, et les aspects internationaux en étaient limités. Bien que Kevin Mitnick ait causé de gros préjudices aux nombreuses victimes auxquelles il avait volé des informations personnelles, il a toujours prétendu qu'il n'avait pas été motivé par le profit. De nos jours, Internet constitue un élément vital de notre vie quotidienne et c'est, dans une très large mesure, là où se trouve l'argent. De manière similaire, la criminalité sur Internet a explosé en volume et diversité, et les mobiles aussi bien que l'organisation des criminels informatiques a changé de manière spectaculaire. Là où on trouvait naguère des escrocs informatiques qui agissaient en solo pour des motifs peu conventionnels, on trouve aujourd'hui des groupes organisés de criminels en ligne dont les motivations sont explicitement financières et qui souvent se répandent et opèrent au-delà des frontières. Dans le document récemment rendu public par le Département américain de la Justice « Law Enforcement Strategy to Combat International Organized Crime » (Stratégie policière pour combattre le crime organisé international), les organisations criminelles utilisant le cyber - espace pour cibler des victimes et infrastructures américaines ont été identifiées comme l'une des menaces principales : « *Le crime organisé international utilise une variété infinie de combinaisons du cyber-espace pour voler des centaines de millions de dollars au détriment des consommateurs et de l'économie américaine. Ces procédés malhonnêtes menacent aussi la sécurité des informations personnelles, des entreprises et des infrastructures gouvernementales, ainsi que la sécurité et la solvabilité des marchés d'investissements financiers* ».

De nouvelles formes très inventives de conduites criminelles fleurissent. Ceux qui attaquent les réseaux informatiques ont employé des techniques de plus en plus sophistiquées non seulement pour perpétrer leurs crimes, mais aussi pour cacher leur identité. Ces techniques sont de surcroît aisément disponibles pour les gens ayant peu d'expérience – les outils pointer-cliquer des hackers étant très répandus et facilement accessibles sur le Web. Les attaques « tape-à-l'œil », « m'as-tu vu » ont cédé la place à des comportements délibérément masqués car la motivation est désormais la recherche du profit et non la célébrité. Si une victime réalise qu'elle a été visée, cela peut conduire à démasquer le criminel et l'empêcher d'utiliser le système visé pour voler des secrets commerciaux ou causer des dommages supplémentaires. La criminalité facilitée par l'informatique a aussi explosé, avec des vols d'identité sophistiqués et des manipulations financières malhonnêtes. On observe, par ailleurs, un glissement du paradigme concernant les auteurs de ces crimes. Dans les débuts, les pirates du Net sophistiqués et les fraudeurs qui utilisaient simplement le Net pour atteindre de nouvelles victimes, mais qui manquaient de savoir-faire technique élaboré, constituaient deux groupes distincts. On assiste désormais à une fusion et un partage rapide des savoir-faire entre ces acteurs – entraînant des défis plus grands encore pour les services de police au fur et à mesure que la communauté des fraudeurs adopte des techniques lui permettant de masquer des forfaits qui étaient précédemment l'apanage de seulement quelques membres futés de la communauté des pirates du Net. Presque chaque affaire a une dimension internationale. Un certain nombre d'entre elles illustrent la menace grandissante et le défi que représentent les cybercrimes.

En février 2000, une attaque *Distributed Denial of Service* (DDoS), une attaque par déni de service fut lancée contre de nombreux sites de commerce en ligne parmi les plus connus aux États-Unis, comme *Yahoo*, *Ebay*, *CNN* et *E*Trade*. Ce type d'attaque se caractérise par une intrusion dans des milliers d'ordinateurs, les transformant en « esclaves » ou « zombies », et qui les met sous les ordres

de la personne contrôlant le réseau, provoquant ensuite l'envoi par ces « esclaves » d'informations à un ordinateur ciblé sur Internet. Cela entraîne en même temps le blocage de sa connexion à Internet. L'enquête est remontée vers le Canada, et a pu aboutir uniquement grâce à la coopération étroite entre les autorités canadiennes et américaines. Il s'est avéré que le coupable était un jeune garçon de 14 ans dont le surnom sur Internet était « *mafiaboy* » et qui lui-même n'était pas particulièrement compétent en informatique, mais qui utilisait des outils développés par d'autres pour causer des dégâts substantiels. Les attaques et les méthodes DDoS ont progressé de manière significative. Celles-ci – désormais appelées communément « botnets » – impliquent maintenant des millions d'ordinateurs esclaves dans le monde entier et des mécanismes de contrôle sophistiqués qui rendent très difficile l'identification de l'auteur. L'utilisation de ces « *bot armies* » a aussi évolué, devenant de véritables couteaux suisses pour tous les genres de criminalité informatique, de l'escroquerie à la diffusion de spams en passant par le vol d'identité. Tandis que le mafiaboy causait certes des dégâts, les nouveaux pourvoyeurs de botnets gagnent de l'argent en opérant à l'échelle mondiale. Dans une affaire relativement récente, United States v. Anchetta, l'accusé rassemblait des armées d'ordinateurs esclavagés et les vendait ensuite à d'autres escrocs du Web, afin qu'ils puissent utiliser ces armées de robots pour démolir leurs concurrents, forcer les sociétés à payer en les menaçant de démolir leurs sites internet, ou commettre des vols d'identité en interceptant des informations sur les ordinateurs réduits en esclavage. À vrai dire, les affaires de botnet sont devenues si envahissantes et d'une telle portée que le FBI est en train de mettre en place un plan spécial (appelé « opération Bot Roast ») et il existe une équipe internationale spécifique dotée de pouvoirs de police contre les botnets.

De nombreux groupes organisés sont impliqués dans l'obtention et la diffusion de données financières personnelles comme les numéros de cartes de crédits. Une organisation criminelle de ce type, appelée « *Shadowcrew* » (« Équipe de l'ombre »), possédait des milliers d'effectifs dans le monde entier et gérait un site web qui fut utilisé pendant deux ans pour la vente d'informations volées, avant que le groupe ne soit finalement neutralisé à la suite d'une enquête secrète menée par le gouvernement américain. Cette organisation était structurée de façon plutôt classique avec des capitaines, des lieutenants et des fantassins qui avaient chacun des tâches particulières. La différence résidait dans le fait que le groupe était organisé de façon virtuelle, avec des membres ne connaissant leurs complices qu'à travers leurs liens internet et communiquant par le biais d'un serveur sécurisé (ou au moins considéré comme tel par les criminels). De plus, il y avait dans cette affaire des preuves que les escrocs utilisaient les méthodes employées par des hackers aguerris pour protéger leur identité et empêcher leur arrestation. Fin 2004, le Département de la Justice et ses services, à la suite d'une enquête secrète qui avait duré un an, ont coordonné l'arrestation de 28 membres de *Shadowcrew* situés dans huit États américains et six pays étrangers, et ont procédé par la même occasion à de nombreuses perquisitions. Pour ce faire, les services de police américains ont travaillé avec leurs homologues de Bulgarie, Biélorussie, Pologne, Suède, Pays-Bas et Ukraine, du Royaume-Uni et du Canada. (On pourra noter qu'après les arrestations, les services de police ont remplacé le portail web de *Shadowcrew* par un autre, représentant la photo d'un homme derrière les barreaux et informant les membres du réseau qu'ils feraient mieux de se rendre (c'est ce que plusieurs d'entre eux ont fait). Il ne s'agit ici que de l'un des nombreux efforts des services de police mis en œuvre pour contrer les groupes criminels organisés en ligne. Plus récemment, le gouvernement américain a travaillé avec les autorités roumaines qui ont réussi à neutraliser des membres du crime organisé impliqués dans un bon nombre d'escroqueries en ligne visant les citoyens américains.

Dans le cadre d'une autre affaire récente, un ancien employé d'une société de services de santé fut poursuivi pour avoir placé une « bombe logique » - une forme de logiciel malveillant configuré pour « exploser » à une date ultérieure, effaçant les fichiers ou causant d'autres dommages – dans le système informatique de l'entreprise qui gérait, entre autres choses, une base de données sur les médications des patients. La base de données était utilisée de manière habituelle par des pharmaciens pour vérifier si une ordonnance envisagée serait susceptible de présenter une contre-indication avec des médicaments déjà prescrits au patient. De la même manière, un entrepreneur de la U.S Navy fut poursuivi pour avoir placé une bombe logique dans un ordinateur de la Marine localisant les bateaux et sous-marins au sein du Commandement européen de la *U.S. Navy.*

Au début de ma carrière, j'ai instruit la première affaire de manipulation boursière sur Internet aux États-Unis. Une page web factice de *Bloomberg News* faisait faussement état de la vente d'une société appelée *PairGain* avec une très grosse plus-value. Cette fausse nouvelle a été diffusée et a fait l'objet d'un battage publicitaire sur des sites de chat en ligne consacrés au courtage en bourse. Dans cette affaire, le prix des actions a spectaculairement grimpé avant de s'effondrer quand il fut révélé que l'histoire était fausse. Le coupable fut repéré grâce à ses traces électroniques, bien qu'il ait cherché à camoufler ses pistes en employant de fausses informations et en établissant les comptes

gratuits et supposément anonymes. Il n'avait lui-même jamais fait de transactions ou réalisé de profits, mais ses manœuvres ont entraîné la perte de sommes d'argent conséquentes pour des milliers de particuliers. Il n'est pas surprenant que les fraudes boursières sur Internet aient continué à évoluer. Dans le cadre d'une récente arnaque, des escrocs opérant depuis la Thaïlande et l'Inde ont été accusés d'infiltrer des comptes boursiers en ligne, en utilisant des noms d'usagers et des mots de passe volés ou en créant de nouveaux comptes à partir d'identités volées. L'acte d'accusation les inculpe pour avoir ensuite utilisé ces comptes afin d'acheter des actions peu demandées, ce qui a par conséquent augmenté la valeur de ces titres, qu'ils revendaient ensuite avec profit. Les accusés ont été arrêtés par des services de police hors des États-Unis, et le procès est actuellement en instance.

Il existe bien d'autres affaires qui permettent toutes d'illustrer comment la criminalité sur Internet est devenue plus massive, envahissante et coûteuse, et qui montrent que les escrocs sur le Net sont toujours plus organisés, sophistiqués et tenaces, car animés par des motivations financières. Les services de police doivent eux aussi progresser en termes de sophistication, organisation et formation, si nous ne voulons pas nous contenter de contenir cette criminalité, mais réussir à punir et dissuader ces crimes. Beaucoup d'éléments entrent en ligne de compte pour réussir dans cette entreprise, mais je me concentrerai ici sur la formation, l'organisation et la coopération internationale.

La lutte contre le cybercrime : organisation, collaboration et formation

Trois piliers essentiels sont nécessaires pour combattre le cybercrime :

- une législation procédurale solide et importante ;

- Une capacité d'investigation et d'instruction ;

- Une coopération internationale d'envergure.

Les États-Unis possèdent une législation très solide réprimant une large gamme de cybercrimes. À l'échelon fédéral, le *Computer Fraud and Abuse Act* punit les crimes dans lesquels l'ordinateur est la cible du crime, et une autre catégorie de lois punit les crimes traditionnels facilités par Internet. Chacun des cinquante États fédérés américains possède aussi sa propre législation contre la criminalité sur Internet. Notre législation procédurale autorise le traçage, l'interception et la perquisition des données et communications d'un ordinateur, avec des garanties statutaires appropriées, et autorise aussi les enquêteurs – et cela est important – à demander la sauvegarde de données informatiques souvent volatiles, pendant que la procédure judiciaire est en cours. Nous nous sommes efforcés de rendre nos lois « technologiquement neutres » afin qu'il ne soit pas nécessaire de les modifier lorsqu'apparaît un nouveau procédé technologique dans la perpétration des crimes, même si la législation a été amendée ces quelques dernières années. Mais une législation solide demeure inefficace si elle ne se double pas d'une capacité à enquêter sur les crimes et à appliquer ces lois. Pour les États-Unis, la mise en place de cette capacité s'est traduite par la création d'unités et de réseaux très performants dans le domaine informatique. Il a aussi fallu former des services de police, des procureurs et des juges, même s'ils ne sont pas spécialisés dans le cybercrime. Il a également été nécessaire d'encourager les enquêteurs et procureurs à travailler ensemble, en équipe, ainsi qu'avec le secteur privé.

Compte tenu de la complexité du cybercrime et du caractère technique du traçage des comportements sur les réseaux informatiques, les enquêteurs doivent comprendre comment fonctionne la technologie afin de faire leur travail. De plus, enquêteurs et procureurs doivent répondre à des exigences potentiellement contradictoires : les enquêtes sur les réseaux informatiques doivent impérativement être rapides, compte tenu de la nature volatile des données électroniques, mais, parallèlement, les exigences procédurales doivent être respectées dans le déroulement de l'affaire. C'est la raison pour laquelle enquêteurs et procureurs doivent être formés pour faire face à ce dilemme. À vrai dire, en raison de la nature nécessairement très réactive de ces enquêtes, une intensité de communication sans précédent s'impose entre les enquêteurs et le procureur au fur et à mesure que l'enquête et le procès avancent. À partir de mon expérience personnelle, je peux affirmer que les affaires que j'ai été amené à instruire avec le plus de succès sont celles qui ont bénéficié de ce type de coopération très intense – où chaque participant peut apporter un point de vue unique permettant d'avancer plus rapidement dans un contexte très mouvant. De plus, les enquêteurs autant que les procureurs doivent être en mesure de transcrire ces savoirs techniques dans un langage accessible aux profanes. Dans notre système, si une affaire arrive en justice devant un jury, les membres de ce dernier sont vraisemblablement peu à même de comprendre ces technologies souvent complexes et ont besoin d'être éclairés de manière concrète. Cela vaut aussi pour la plupart des

juges qui instruisent une large variété d'affaires et n'ont pas nécessairement les connaissances techniques suffisantes.

Compte tenu du déplacement de tous les types de criminalité vers les réseaux internet, la plupart des enquêteurs et des procureurs ont besoin d'une compréhension plus avancée ainsi que d'un personnel spécialement formé pour combattre le cybercrime. Un certain nombre d'initiatives à cet effet sont en cours. Au FBI, le cybercrime a été désigné comme la troisième plus haute priorité (dépassée seulement par le terrorisme et la sécurité nationale). Le siège du FBI possède une Division cybercrime, des équipes cyber dans chacune de ses différentes antennes à l'échelon des états fédérés, et presque cent équipes spéciales et groupes de travail avec des forces de police aux différents échelons des états dans tout le pays. Ces cyber-agents reçoivent une formation spécifique sur les enquêtes dans le domaine du cybercrime, et ils ont la possibilité de prendre des cours plus spécialisés sur des aspects variés de l'investigation et de l'analyse des données informatiques. De la même manière, le *United State Secret Service* a créé l'*Electronic Crimes Special Agent Program* qui fournit une formation renforcée, et a établi l'*Electronic Crimes Task Forces*, comprenant des investigateurs fédéraux et des États fédérés dans vingt-quatre villes.

Le Département de la Justice a mis sur pieds, au sein de son siège, le *Computer Crime and Intellectual Property Section* en 1992, et un réseau spécial de procureurs, *Computer Hacking and Intellectual Property Network* (CHIP) en 1995. Ce réseau CHIP compte maintenant 220 procureurs issus de chacun des bureaux régionaux du ministère de la Justice, et spécialement formés pour enquêter dans le domaine du cybercrime. Ces derniers sont désignés non seulement pour faire face à la criminalité sur Internet dans leurs services respectifs, mais aussi pour assurer eux-mêmes les fonctions de formateurs et d'experts auprès de tous les autres membres de leur équipe. Cette approche en termes de « formation des formateurs » permet de garantir que l'expertise et les ressources, limitées, soient maximisées et que tous les procureurs puissent bénéficier d'une initiation aux problèmes posés par les enquêtes électroniques. Les procureurs du CHIP, et beaucoup d'autres non spécialisés dans la criminalité sur le Net, reçoivent une initiation dans le cadre d'un enseignement particulier de « *Basic Cybercrime* » qui traite, entre autres choses, du fonctionnement d'Internet, des techniques permettant de retrouver des preuves sur les réseaux d'ordinateurs, et des méthodes d'enquêtes et d'instruction dans une affaire de crime informatique. Les procureurs du CHIP reçoivent chaque année une formation approfondie supplémentaire qui couvre des questions spécifiques d'ordre juridique ou technique. Par exemple, durant ces deux dernières années, cette formation approfondie s'est déroulée conjointement à la réunion de formation *Government Forum of Incident Response and Security Teams* (les spécialistes gouvernementaux de la sécurité informatique) afin de permettre aux procureurs de s'informer sur les nouvelles technologies et techniques criminelles. Cette formation facilite aussi les échanges et mises en relation des participants afin qu'ils puissent ultérieurement partager les leçons techniques et juridiques tirées de leurs expériences au cours des enquêtes. Cela donne aussi des opportunités aux agents et procureurs pour se former ensemble afin de mieux se comprendre et adopter une approche d'équipe plus cohérente.

Au-delà de la formation, le réseau CHIP Network remplit d'importantes fonctions opérationnelles. En raison de la nature transfrontalière de la criminalité informatique, beaucoup de ces crimes relèvent de plus d'une juridiction. Le CHIP Network propose une approche en réseau d'un problème en réseau, permettant à des procureurs spécialement formés dans différentes parties du pays de collaborer de façon efficace sur des enquêtes qui doivent être menées rapidement dans plusieurs juridictions à la fois. Les avocats du CHIP servent aussi de passerelle entre les procureurs fédéraux et locaux. Souvent les cybercrimes peuvent être des violations tant de la loi fédérale que de celle d'un état fédéré et le CHIP, ainsi que les fonctionnaires locaux, peuvent coordonner leurs efforts. Enfin, une des fonctions du CHIP consiste à se rapprocher du secteur de l'industrie.

Le secteur privé est souvent victime du cybercrime, mais est aussi lui-même constitué de fournisseurs de technologie, logiciels et services internet qui jouent un rôle essentiel dans les enquêtes sur la criminalité informatique. En tant que victime, en particuliers d'affaires de hacking, le secteur privé se montre souvent réticent à signaler les intrusions frauduleuses aux forces de police. Établir une relation solide et confiante encourage les entreprises à signaler les escroqueries dont elles sont victimes et permet à la police de mieux protéger le public, en particulier lorsqu'une société n'est qu'une victime parmi d'autres. Le secteur privé, qui possède une meilleure compréhension des nouvelles technologies de pointe, peut aider la police à mieux les comprendre, et par conséquent aider à mieux anticiper les tactiques criminelles émergentes, fournissant dans le même temps des opportunités de formation que le gouvernement n'aurait pas été en mesure de proposer. Par conséquent, le rapprochement des secteurs public et privé est une fonction importante du CHIP et une priorité pour les enquêteurs. Par exemple, le programme *InfraGard*, une alliance des secteurs privé et public créée par le FBI, crée des canaux d'échanges d'informations formels et informels qui rassemblent plus de 20 000 participants.

Bien sûr, ces différentes formations et structures organisationnelles sont propres au gouvernement fédéral. Chaque État fédéré et localité s'occupent aussi de créer des groupes d'enquêteurs et procureurs bien formés, en collaboration avec les autorités fédérales. De la même manière, chaque pays devrait parvenir à adopter son approche propre, en fonction de ses ressources, ses institutions gouvernementales et policières. Quoi qu'il en soit, l'éducation et la formation des enquêteurs, procureurs et même des juges sont vitales pour assurer le succès d'un programme de lutte contre le cybercrime. Mais en raison des progrès continuels de la technologie, cette formation ne peut pas demeurer statique. C'est pour cette raison que des réseaux et des unités spécialisés dans le cybercrime revêtent une importance capitale, même si, de plus en plus, ce sont là des compétences dont tous les enquêteurs et procureurs auront besoin, même à un niveau élémentaire.

La nécessaire coopération internationale

En raison de la nature transfrontalière de la criminalité informatique et des preuves électroniques, la nécessité d'une coopération internationale est primordiale. Plusieurs des affaires décrites plus haut, y compris celle de *Shadowcrew* qui a entraîné des arrestations presque simultanées dans sept pays, illustrent la nécessité de travailler ensemble par-delà les frontières. Cependant, une véritable coopération internationale exige préalablement que les pays du monde entier disposent d'une législation adéquate et d'une capacité juridique à coopérer. À la différence de nombreux crimes de nature physique qui sévissent dans le monde entier, il est souvent facile et banal pour les criminels informatiques de profiter de pays qui n'ont pas de structures juridiques très solides, ni la capacité de coopérer aux enquêtes policières. Par exemple, si un pays A possède une législation solide contre le cybercrime, le criminel peut faire passer son attaque par un pays B qui ne possède pas cette législation, ou encore lancer son attaque depuis ce pays, sachant qu'il sera difficile de le retrouver et de l'arrêter. De plus, en l'absence d'une forte législation, il pourrait être possible de créer des « paradis » du cybercrime. Rappelons-nous que, il y a plusieurs années, bien que le tristement célèbre virus « *I love you* » ait été retrouvé chez un particulier aux Philippines, aucune loi ne pouvait être invoquée dans ce pays pour y intenter une procédure judiciaire (leur législation a par la suite été revue). En raison de la nature globale du cybercrime, et des conséquences potentielles si le problème n'est pas envisagé à l'échelle mondiale, plusieurs initiatives internationales importantes ont été prises.

En 1997, les pays du G8, parmi lesquels la France et les États-Unis, ont rendu public un ensemble de dix Principes et un Plan d'Action en dix points pour faire face au défi du crime high-tech, et ont créé un sous-groupe permanent au sein du Groupe de Lyon sur la criminalité transnationale, afin de réfléchir spécifiquement au problème. Ces Principes et ce Plan d'Action ont constitué la base de deux Résolutions de l'Assemblée générale des Nations unies et fourni des principes de base tels que la nécessité d'une législation adéquate et d'une coopération transfrontalière [1].

La nécessité pour tous les pays de se doter d'une législation adaptée contre le cybercrime a été très efficacement prise en compte par la Convention sur le cybercrime du

••••

(1) www.cybercrime.gov/intl.html#vc6

Les dix principes :

I. Il n'y aura aucun refuge sûr pour ceux qui fraudent grâce aux technologies de l'information ;

II. Les enquêtes et poursuites des crimes high-tech internationaux doivent être coordonnées entre tous les États concernés, quel que soit l'endroit où les dommages ont été commis ;

III. Les personnels de police doivent être entraînés et équipés pour faire face au crime high-tech ;

IV. Les systèmes juridiques doivent protéger la confidentialité, l'intégrité et la disponibilité des données et systèmes de toute dénaturation non autorisée, et garantir que tout abus grave sera pénalisé ;

V. Les systèmes juridiques devraient autoriser la sauvegarde et l'accès rapide aux données électroniques, qui sont souvent essentielles pour le succès d'une enquête criminelle ;

VI. Les régimes d'assistance mutuelle doivent garantir le recueil et l'échange des preuves en temps opportun dans les affaires ayant trait au crime high-tech international ;

VII. L'accès aux données électroniques ouvertes au public par les forces de police ne doit pas nécessiter d'autorisation de la part de l'État où se trouvent ces données.

VIII. Les normes d'analyse approfondie des ordinateurs pour retrouver et authentifier les données électroniques dans le cadre d'enquêtes et poursuites criminelles doivent être développées ;

IX. Dans la mesure du possible, les systèmes d'information et de télécommunications devraient être conçus pour faciliter la prévention et la détection de la fraude sur le Net, et devraient aussi faciliter le repérage des criminels ainsi que le recueil des preuves.

X. Le travail dans ce domaine devrait être coordonné avec celui des autres tribunes internationales compétentes afin de se prémunir contre d'inutiles dispersions et doubles emplois des efforts.

Conseil de l'Europe. Cette Convention historique, conclue et signée en 2001, est le seul instrument international qui détaille les exigences nécessaires à une législation efficace contre le cybercrime, les procédures, et les dispositions en matière d'assistance juridique mutuelle. La Convention exige des pays qu'ils criminalisent certains comportements, comme le hacking, et demande aux nations signataires de mettre sur pieds des outils procéduraux pour les services de police, permettant des enquêtes criminelles efficaces contre les délits sur le Net. La Convention exige aussi que les pays s'engagent à améliorer la rapidité de l'assistance juridique afin de faciliter le nombre toujours plus élevé de requêtes internationales. Elle est suffisamment flexible pour permettre aux pays dotés de différents systèmes juridiques de parvenir aux mêmes buts. Les pays membres mais aussi extérieurs au Conseil de l'Europe, ayant des traditions juridiques différentes ont participé à la rédaction de la Convention en fixant les buts à atteindre, tout en laissant à chaque pays signataire la latitude nécessaire pour adapter les principes et les faire coïncider avec leur propre système juridique. Quarante-cinq pays ont maintenant signé la Convention et vingt-trois l'ont ratifiée, dont la France et les États-Unis. Plus encore, de nombreux pays dans le monde entier sont en train de changer ou de rédiger leur cyber-législation afin de se mettre en conformité avec la Convention. En raison de la nécessité d'un cadre juridique solide dans chaque pays, les États-Unis ont fait de l'adhésion à cette Convention la pierre angulaire de leur stratégie internationale contre le cybercrime. Une sévère législation dans les pays du monde entier permet de garantir que les criminels, où qu'ils se trouvent, ne pourront pas agir impunément. Cela aide aussi les services de police de chaque pays à remplir leur mission plus efficacement.

À un niveau plus opérationnel, le G8 *High-Tech Crime Subgroup* (HTCSG), composé des fonctionnaires des ministères de l'Intérieur et de la Justice de chacun des pays du G8 et de la Commission européenne, s'est réuni régulièrement depuis sa création en 1997 et s'est imposé comme leader face aux problèmes croissants induits par le cybercrime. Entre autres choses, le Sous-groupe a proposé des principes de base d'analyse approfondie des données informatiques, principes ayant trait aux enquêtes transfrontalières ; recommandations pour le traçage des communications terroristes transfrontalières ; création de critères pour la conservation des données et élaboration de principes relatifs à leur disponibilité ; tenue de trois conférences réunissant conjointement des représentants du secteur industriel et des policiers afin d'améliorer la coopération avec le secteur privé, et publication de principes sur la protection des infrastructures cruciales détentrices d'informations.

Le HTCSG a créé, et peut-être est-ce là encore plus important, un réseau disponible 24 heures sur 24 et 7 jours sur 7 (24/7 Contact), le *High Tech Crime Point of Contact Network*, conçu pour faciliter une coopération internationale rapide, en particulier dans la sauvegarde et la sécurisation des preuves électroniques dans des affaires de cybercrime de haute importance. Ce réseau, dont la France et les pays du G8 ont été les membres fondateurs, s'est maintenant étendu à plus de cinquante pays du monde entier. Il est destiné à compléter, et non remplacer, les canaux de coopérations déjà existants, il encourage une importante coopération opérationnelle dans des affaires en cours, et cherche à éviter la disparition des fragiles traces électroniques. De plus, il est intervenu dans des affaires nombreuses et variées – aidant même à assurer l'arrestation d'un individu ayant tué un policier en Europe. Il a fait figure de modèle du type de coopération internationale nécessaire à la poursuite des criminels transfrontaliers. Le Network a en fait servi de base à la mise en place de dispositions au sein de la Convention sur le cybercrime du Conseil de l'Europe, et le HTCSG travaille en étroite collaboration avec le Conseil de l'Europe pour créer un réseau unique sous les auspices des deux organisations. De plus, deux sessions de formations d'unités du cybercrime participent au Network (et une troisième est prévue). Ces formations communes à plusieurs pays favorisent une meilleure collaboration dans les investigations et permettent de partager les expériences et approches.

Le Network est un système volontaire dans lequel chaque membre tente de fournir une assistance selon les circonstances d'une affaire particulière. Supposons que des d'enquêteurs mènent une investigation aux États-Unis dans une affaire de hacking, impliquant une infiltration dans les réseaux d'une institution financière à New York. Une analyse des données informatiques indique que l'attaque provient d'Espagne. Les États-Unis, à travers le U.S. 24/7 contact, pourraient contacter le même service espagnol (24/7 Contact Point) et demander que les données relatives à cette adresse IP espagnole soient sauvegardées et, si possible, partiellement divulguées, pour aider l'enquête. Le contact espagnol 24/7 établit, après avoir passé en revue les données qu'il obtient, que l'Espagne a seulement servi de lieu de transit pour l'attaque, et que celle-ci semble provenir d'Allemagne. L'Espagne pourrait contacter directement le Contact Point allemand (par ailleurs, il semblerait qu'une escroquerie ait été également commise en Espagne) ou pourrait simplement transmettre l'information aux États-Unis, qui peuvent ensuite eux-mêmes contacter le Contact Point allemand. L'Allemagne sauvegarde et obtient des données indiquant que le hacker est sur son territoire. En travaillant avec les autorités

policières américaines, les services allemands sont en mesure de procéder à l'arrestation des malfaiteurs. Tout cela peut se dérouler, et c'est souvent le cas, de manière exceptionnellement rapide. À chaque étape, dans cet exemple, et dans d'autres exemples réels impliquant encore plus de pays, les preuves pourraient disparaître si elles n'étaient pas, au minimum, sauvegardées. S'il avait fallu ne serait-ce que plusieurs semaines pour obtenir les informations en provenance d'Espagne, pour apprendre que l'escroquerie provenait en fait d'Allemagne – délai assez rapide si l'on se réfère aux standards normaux de coopération internationale – les preuves électroniques en Allemagne auraient pu être détruites et l'enquête aurait abouti à une impasse. Bien entendu, les différents Contact Points ont des capacités diverses, et ce qui peut être fait varie selon le contexte de l'affaire, mais le réseau 24/7 a vraiment permis de faire la différence dans de nombreuses affaires. Dans les conclusions qui ont fait suite à la réunion des ministres de l'Intérieur et de la Justice du G8 à Munich durant la présidence allemande en 2007, et cette année encore durant la présidence japonaise, les ministres ont recommandé que le Network continue à s'étendre et se renforcer. Ils ont de plus pris acte du fait que ce Network est soutenu par les actuels pays membres. Souvent, dans certains pays, la police n'est pas informée de l'existence du Network et de ses capacités. Si vous n'avez pas d'informations sur le Network, il faut alors vous mettre en relation avec le Contact Point adéquat.

D'autres organisations internationales se sont aussi montrées actives. Interpol a créé un certain nombre d'« équipes de travail » régionales spécialisées dans les questions de criminalité high-tech – dont une équipe de travail européenne qui a produit bon nombre de documents utiles. Interpol a aussi organisé beaucoup de sessions de formation, mis en relation des enquêteurs de criminalité sur le Net (dernièrement en Inde) et des spécialistes high-tech attitrés. Les forums de l'Organisation des États Américains et de l'APEC (*Asian Pacific Economic Cooperation*), ont chacun adopté des stratégies de cyber sécurité qui promeuvent des législations et structures plus solides. La Commission européenne a publié une communication sur le cybercrime intitulée : *Vers une stratégie générale dans la lutte contre le cybercrime*, exposant les priorités opérationnelles, notamment la lutte contre le matériel pédophile sur le net, des actions pour contrer les attaques massives contre les systèmes d'informations et des actions contre la fraude d'identités. Entre autres choses, la stratégie de la Commission européenne demande la promotion de partenariats public/privé dans ce combat, et l'OCDE, l'Union internationale des télécommunications (UIT) et d'autres ont commencé à réfléchir sérieusement au problème.

Aux États-Unis, la participation à des réseaux internationaux est une priorité. Le Département de la Justice est un membre actif du réseau G8 24/7, et aide à en administrer le fonctionnement. Le FBI possède un réseau d'agents internationaux qui s'occupent de plus en plus du cybercrime. Le FBI, le *Secret Service*, et le Département de la Justice participent tous aux activités de formation à l'échelon international. Cela peut aller de la conduite d'ateliers en matière de législation, dans le cas des pays réfléchissant à moderniser la leur pour contrer le cybercrime, à l'aide aux pays pour la mise en place et la formation d'unités spécialisées en la matière. Tout cela confirme que nous ne pouvons pas accomplir notre travail efficacement sans la coopération de nos homologues. Au-delà de ces activités, nous travaillons activement, et de manière suivie, voire quotidienne, sur des affaires avec nos homologues étrangers. Ce dispositif a permis de procéder à plusieurs enquêtes et arrestations – aux États-Unis, ou dans des juridictions étrangères. Les auteurs de ces crimes sont désormais soumis à des sanctions pénales, c'est là le point le plus important.

Conclusion

La criminalité électronique prolifère, de plus en plus sophistiquée, nuisible, et d'envergure internationale. Les criminels du Net sont mieux organisés, déterminés et motivés par le profit. La police doit affronter ce défi en créant des équipes efficaces et opérationnelles contre le cybercrime, mettre en place une formation permanente adaptée, et promouvoir une coopération internationale rapide. Le but ultime de tous ces efforts est de parvenir à la poursuite des cybercriminels d'envergure, à la protection du public et à un fort message dissuasif envers ceux qui croient trop souvent que leur conduite criminelle restera impunie.

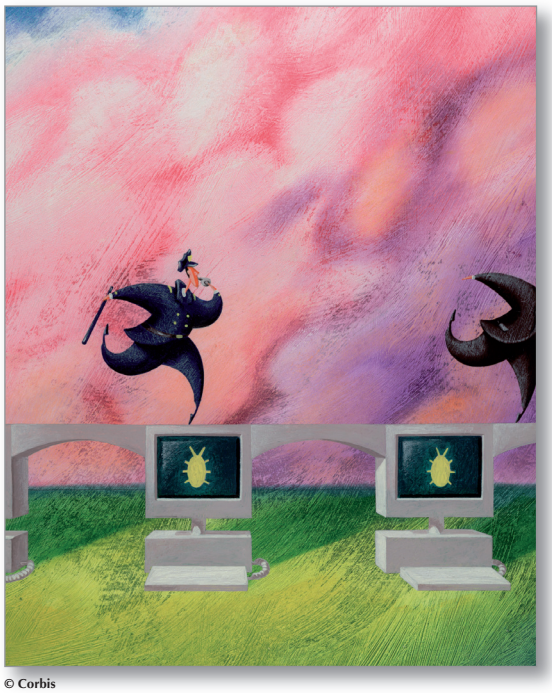
Christopher PAINTER

Cet article contient les opinions personnelles de l'auteur et ne reflètent pas nécessairement les vues du Département de la Justice ou du Gouvernement américain.

La sécurité des systèmes d'information

De la prise de conscience collective à la mobilisation publique

Serge PERRINE



© Corbis

L'article concerne la sécurité des systèmes d'information. Il rappelle les enjeux croissants dans le domaine au fur et à mesure du développement du réseau Internet. Il donne des exemples des risques correspondants. Mais son objet est surtout de faire un point sur l'essentiel des mesures de protection prises à l'issue du rapport Lasbordes. Celui-ci a déclenché une véritable prise de conscience collective, suivie d'actions concrètes. Restent la sécurité de l'État et les infrastructures vitales pour lesquelles le rapport Romani actualise le diagnostic, mais où la création du réseau ISIS a apporté un progrès substantiel.

The Security of Information Systems: Public Awareness and Mobilization

In view of the growing concern for the security of information systems, and the high stakes related to the development of the internet, the risks involved as presented by the Lasbordes Report, and the measures proposed and undertaken, are dealt with here. The report played a significant role in raising awareness, which then led to the adoption of concrete responses. The Romani report updated the diagnosis in relation to national security and the vital infrastructures of the government. The creation of the ISIS brought substantial progress.

Serge Perrine

Ancien élève de l'École polytechnique, de Sup Télécom Paris, titulaire d'un DEA d'histoire du droit, et docteur en mathématiques, il a mené une carrière alternant des activités administratives, opérationnelles et de recherche. Il est actuellement secrétaire du Conseil scientifique de France Télécom, mais est aussi chargé du contrôle interne de sa division Marketing stratégique. Il a coordonné l'ouvrage collectif *Intelligence économique et gouvernance compétitive* publié, en 2006, par l'INHES à La documentation Française.

Le 26 novembre 2005, le député Pierre Lasbordes rendait son rapport, intitulé *La sécurité des systèmes d'information – Un enjeu majeur pour la France* [1]. Il indiquait, dans son introduction, s'attaquer à un champ large allant des virus et vers qui submergent Internet au vol des secrets commerciaux en constante augmentation. Pour les États-Unis, cette dernière menace a créé un préjudice sur les mille premières entreprises de 59 milliards en 2001. La révélation d'une affaire importante en 2005 a mis en évidence comment des chevaux de Troie pouvaient être utilisés à cet effet. Elle a aussi permis de prendre conscience que les outils nécessaires aux pirates étaient parfois disponibles en ligne, et que l'ouverture des réseaux et leur complexité croissante renforçaient la vulnérabilité des systèmes d'information connectés.

Au demeurant, la connexion à Internet s'impose d'elle-même pour des raisons de coûts : pas facile pour une entreprise de ne pas se connecter quand les concurrents le font et diminuent ainsi leurs frais d'exploitation. Cette réalité technologique et économique inéluctable déplace l'équilibre entre les avantages et les inconvénients. Parmi les avantages, il y a évidemment le fait que les systèmes d'information concourent directement à la préservation et au développement des emplois. Parmi les inconvénients, l'accroissement de la vulnérabilité informatique est significatif et requiert une attention permanente ; le risque d'atteinte à l'indépendance nationale par cyber-attaque majeure restant un scénario imaginable depuis l'attaque de 2007 contre l'Estonie. D'ailleurs, une remarque importante formulée dans le rapport est que « *le caractère fortement évolutif de l'objet de l'étude appellerait à une actualisation permanente* ». Et sans doute, cette réactualisation est-elle engagée pour les menaces principales par deux publications récentes : *Le Livre blanc* sur la Défense et la Sécurité nationale [2], présenté le 17 juin 2008 par le président de la République, et le rapport d'information du sénateur Roger Romani, *Cyberdéfense, un nouvel enjeu de sécurité nationale* [3], publié le 8 juillet 2008.

Une prise de conscience progressive

Le rapport Lasbordes a contribué à une véritable prise de conscience des enjeux de la sécurité sur Internet. Il est vrai qu'il a été rédigé près de quinze ans après le début de la révolution technologique sans précédent, qui a complètement bouleversé le réseau mondial des communications. Cette révolution a généralisé le recours à la numérisation des signaux d'information. Elle a connecté réseaux téléphoniques et équipements électroniques en commençant par les micro-ordinateurs, permettant aussi, dans la période récente, la convergence des réseaux fixes et des réseaux mobiles. Elle a accru les débits dans des proportions telles que l'utilisation de services d'images est désormais possible dans de bonnes conditions de confort et de qualité ; ces dernières vont encore être améliorées avec le déploiement de la fibre optique à domicile. Les réseaux informatiques (réseaux locaux d'entreprises, réseaux publics, réseaux individuels, etc.) se connectent progressivement par l'Internet aux réseaux de communication (réseaux de téléphonie, réseaux mobiles, réseaux sans fils, etc.), plus récemment aux réseaux de diffusion (radio et télévision), voire à n'importe quelle machine comprenant un dispositif électronique.

En fait, les gains de productivité qui résultent de cette connectivité par Internet sont tels que cette dernière devient irrésistible pour des processus développés dans un environnement de plus en plus concurrentiel où la réduction de coûts à tous les niveaux est désormais une contrainte incontournable. Pour notre seul pays et fin 2007, l'enquête « L'homme en réseau » de Médiamétrie [4] terminée en mars 2008, indiquait que 93,4 % des foyers avaient accès au haut débit, et que sur les 30,3 millions d'utilisateurs d'Internet, 77,2 % se connectaient tous les jours, restant en ligne au domicile ou au travail pendant plus d'une heure par jour en moyenne. Pour le niveau mondial, les dernières statistiques disponibles [5] laissent penser que 747 millions de personnes de plus de 15 ans sont connectées, avec un taux de croissance de 10 % entre 2006 et 2007 (les chiffres correspondant pour la France sont de 24,6 millions de personnes de plus de 15 ans, et de 4 % entre 2006 et 2007 pour le taux de croissance).

L'accroissement des débits a permis de développer des services de plus en plus riches, que ce soit au niveau des personnes (banque en ligne, achats en lignes, etc.), des entreprises (télétravail, entreprises étendues, téléconférences, etc.), des États (e-administration, e-santé, etc.). Il en est résulté une dynamique économique de création de services nouveaux rendus possibles autour du réseau Internet.

(1) http://www.lasbordes.fr/article.php3?id_article=166
(2)http://www.premierministre.gouv.fr/information/les_dossiers_actualites_19/livre_blanc_sur_defense_875/livre_blanc_1337/livre_blanc_1340/
(3) http://www.senat.fr/noticerap/2007/r07-449-notice.html
(4) http://www.relationclientmag.fr/ALaUne/ConsultALaUne.asp?ID_Article=502&t=L-annee-Internet-2007-l-homme-en-reseau__
(5) http://www.comscore.com/press/release.asp?press=1242

Mais parallèlement, de nouvelles menaces sont apparues. Ces menaces se situent à différents niveaux, sont de natures variées, et font courir des risques divers allant de la propagation des vers ou virus qui affectent le fonctionnement des terminaux, à l'intrusion dans des systèmes d'information raccordés ou la captation de données personnelles, en passant par l'accès à des contenus illégaux ou leur transmission, etc. Ces risques se manifestent régulièrement et la presse s'en fait écho. Le dernier événement en date [6] est une faille de sécurité révélée mi-juillet 2008 sur les serveurs DNS (*Domain Name System*), mais découverte plus de six mois avant par un expert américain mondialement reconnu, Dan Kaminsky. Les six mois ont été mis à profit par les grandes entreprises informatiques mondiales pour mettre au point des logiciels de correction. Mais la brèche aurait pu permettre des opérations de « phishing » de grande ampleur, c'est-à-dire de récupération de données personnelles comme des numéros de cartes bancaires.

Pour information, les escroqueries à la carte bancaire ont représenté en France un total de 268 millions d'euros en 2007, et sont en croissance de 6,3 % par rapport à l'année précédente. Mais elles ne représentent que 0,062 % du total des transactions faites par carte, et, dans cet ensemble, les transactions frauduleuses utilisant l'Internet représentent 50 millions d'euros. Mais, on peut aussi rappeler que, selon l'Organisation mondiale de la santé, la contrefaçon des médicaments représente, dans le monde, une activité de 45 milliards d'euros [7], c'est-à-dire 10 % du marché pharmaceutique mondial, dont une grande partie de la vente s'effectue désormais par l'intermédiaire d'Internet.

On peut donc résumer en disant qu'Internet se trouve situé au cœur d'une dynamique technologique considérable, porteuse d'enjeux de performance économique essentiels (que l'on évoque dans le rapport Lasbordes [p. 35] par un objectif de 0,5 point de croissance du Produit intérieur brut, c'est-à-dire la moitié de ce qui est proposé avec l'ensemble des mesures du rapport Attali [8]), mais qu'il se trouve également confronté à des enjeux désormais incontournables de confiance et de souveraineté. Bien entendu, une prise de conscience parallèle à cette évolution s'est développée au fil du déploiement de l'infrastructure, et notre pays et l'Europe disposent ainsi de tout un arsenal juridique et administratif, ainsi que de moyens mis en place progressivement, pour réguler toute l'activité qui en découle.

La mise en œuvre du rapport Lasbordes

L'impulsion donnée par ce rapport s'est traduite par de nouvelles mesures dont la plus significative est la création du secrétariat d'État à l'économie numérique, où a été nommé Eric Besson. Mais le rapport a donné lieu à d'autres réalisations, et on va faire le point sur les six axes de recommandations qu'il contenait, sans nécessairement être exhaustif.

Sensibiliser et former à la sécurité des systèmes d'information

Une grande campagne de communication médiatique a été faite pendant plusieurs mois, et, dans ce cadre, est intervenue la sensibilisation à la mise en place d'un portail Internet pour mettre à la disposition des utilisateurs - citoyens, administrations et entreprises - des informations d'actualité, des guides de bonnes pratiques, des contacts, des alertes sur les menaces, etc. Ce portail est désormais accessible [9]. Il informe les utilisateurs particuliers ou entreprises, notamment les plus petites. Il comprend des fiches techniques, un module d'autoformation, un lexique spécialisé, ainsi qu'une revue de l'actualité des événements affectant Internet et des liens vers des portails à destination de publics plus spécifiques (protection des jeunes [10], logiciels libres [11], droit et déontologie [12], sécurité [13], conseil [14], etc.). À partir de ce portail remarquable, sont

....

(6) Emmanuel Grasland avec Jean-Christophe Féraud, 10 juillet 2008, « Une faille de sécurité sans précédent mobilise les grands de l'Internet », Les Échos.

(7) La lettre de Prometheus [*lettre@fondation-prometheus.org*] juillet-août 2008.

(8) http://lesrapports.ladocumentationfrancaise.fr/BRP/084000041/0000.pdf

(9) http://www.securite-informatique.gouv.fr/

(10) http://www.internetsanscrainte et http://www.actioninnocence.org/

(11) http://www.inl.fr/ et http://www.april.org/

(12) http://www.foruminternet.org/ et http://www.cnil.fr/

(13) http://www.interieur.gouv.fr/sections/a_l_interieur/la_police_nationale/organisation/dcpj/cyber-criminalite/ et http://www.cert-ist.com/, et encore http://www.ssi.gouv.fr/fr/index.html

(14) http://www.afa-france.com/ et http://www.clusif.asso.fr/

dorénavant facilement accessibles des informations précises sur les risques principaux encourus, sur les points de vigilance pour tout utilisateur, sur les recommandations types à mettre en œuvre (exemple : activer un pare-feu, protéger et changer régulièrement son mot de passe, etc.). Il est complété par quelques outils de diagnostic, comme le logiciel Ansmo mis ainsi à disposition du public. La création de cet outil à disposition de tous constitue un progrès très significatif, tout comme l'ouverture du portail « surfez intelligent » [15], courant février 2008.

Responsabiliser les acteurs

Des modèles de chartes à l'usage des utilisateurs ont été rendus disponibles sur les sites que l'on vient d'évoquer. Elles peuvent être annexées au contrat de travail - public et privé - ou aux règlements intérieurs des entreprises. La labellisation des entreprises fournisseurs de produits ou services de sécurité des systèmes d'information (SSI), qui respectent un cahier des charges de sécurité à établir, semble être encore un projet à concrétiser, mais les informations accessibles par le portail cité précédemment donnent des pistes potentielles aux entités intéressées par cette démarche.

Sur le thème particulier de la protection des enfants, le plan gouvernemental Confiance [16], démarré en novembre 2004, a été poursuivi jusqu'en 2007. Destiné à sensibiliser aux enjeux et risques de l'Internet pour les enfants, et impliquant l'ensemble des acteurs concernés, il a permis de développer et diffuser des outils d'information afin de permettre aux parents et aux éducateurs d'adopter un comportement responsable pour mieux protéger les mineurs qui peuvent, dans leur usage de plus en plus quotidien de l'Internet, être exposés à des contenus violents, des contenus incitant à la haine raciale, de la pédopornographie, des risques de conditionnement de type sectaire ou idéologique, des contenus détournés par manipulation de données et d'images, des spams et jeux d'argent. Ceci s'est traduit par la signature d'un accord le 26 avril 2006 avec les fournisseurs d'accès à Internet (FAI) pour la mise à disposition gratuite de logiciels de contrôle parental. De plus, à l'automne 2006, a été mis en place un « label famille » permettant de repérer les contenus sans risque, après le lancement en juillet 2006 d'un label « confiance en ligne » attribué aux prestataires de services candidats à être jugés sur leur capacité à protéger les mineurs, à sécuriser les équipements informatiques des clients, à lutter contre le spam et les escroqueries, à coopérer avec les autorités policières et judiciaires. L'atelier « Protection de l'enfance sur Internet » [17], tenu dans le cadre des Assises d'Internet de juin 2008 a été l'occasion pour la secrétaire d'État à la famille, Nadine Morano, de faire un point sur ce thème, et de proposer la poursuite des actions dans un cadre nouveau, le projet « Internet sans crainte » soutenu par la Commission européenne dans le cadre de son plan Safer+.

Renforcer la politique de développement de technologies et de produits de SSI et définir une politique d'achat public en cohérence

De nombreuses actions sont intervenues à ce niveau depuis le début 2006, et, par exemple, pour ce qui concerne le développement des financements publics de recherche et développement (R&D), la simplification et le déplafonnement du Crédit d'impôt recherche constituent une réponse spectaculaire à cette proposition. Permettant de couvrir en particulier des dépenses de normalisation, cette mesure permet concrètement d'accroître la présence et l'influence française dans les groupes de standardisation et les comités de normalisation.

Dans une autre direction, l'ouverture du portail de la sécurité informatique [18], en février 2008, permet d'accéder à des informations sur les produits de sécurité nationaux qualifiés et des produits européens adaptés aux différents niveaux de sécurité à assurer, même si la réponse collective à cette proposition du rapport peut être encore meilleure.

En ce qui concerne la définition d'une politique d'achat public, fondée sur le principe d'autonomie compétitive, et l'incitation des grandes entreprises à travers le pacte PME à faire confiance aux PME SSI, les chantiers restent ouverts, mais le projet européen de *Small Business Act* [19] progresse, et surtout la loi de modernisation de l'économie en cours d'adoption ouvre des pistes nouvelles.

(15) http://www.ddm.gouv.fr/surfezintelligent
(16) http://www.internet.gouv.fr/information/information/dossiers/rendre-plus-sure-navigation-enfants-sur-internet/plan-confiance-268.html
(17) http://assisesdunumerique.fr/actualites/atelier-%C2%AB-protection-de-l%E2%80%99enfance-sur-internet-%C2%BB-12-juin-2008/
(18) http://www.securite-informatique.gouv.fr
(19) http://www.premier-ministre.gouv.fr/chantiers/entreprises_852/les_propositions_lionel_stoleru_59835.html

Rendre accessible la SSI à toutes les entreprises

La diffusion aux PME sous une forme adaptée des informations de veille, d'alerte et de réponse disponibles au niveau des CERT [20] (*Computer Emergency Response Team*) nationaux, est désormais facilitée par les portails que l'on a cités. On peut très facilement trouver à partir du portail général [21] les adresses internet où lancer des alertes, contacter les CERT nationaux, etc. Quant aux forums thématiques publics ou privés favorisant la circulation d'informations, les retours d'expériences, le partage des bonnes pratiques, il s'en tient couramment. Et il serait difficile, sauf à travailler dans une instance spécialisée comme le Club informatique des grandes entreprises françaises (CIGREF) [22] d'en actualiser la liste.

Accroître la mobilisation des moyens judiciaires

Il reste certainement des choses à faire pour reconnaître la spécificité des contentieux liés aux systèmes d'information, mais en terme d'atteintes à la propriété intellectuelle sur Internet, le débat a fait rage avec les travaux préparatoires au projet de loi Olivennes [23]. Le 12 juin 2008, le Conseil d'État a validé les différentes options retenues par le gouvernement pour concrétiser les « Accords de l'Élysée » du 23 novembre 2007, signés par 47 entreprises ou organismes représentatifs du cinéma, de la musique, de l'audiovisuel et de l'Internet préoccupés par le piratage en ligne. Le projet de loi rebaptisé « Création et Internet » entre dans son parcours législatif [24], après présentation en Conseil des ministres le 18 juin dernier.

Pour ce qui est du renforcement des moyens judiciaires et policiers, on peut rappeler que mi-février 2008, Michèle Alliot-Marie, ministre de l'Intérieur, annonçait le doublement du nombre de cyber-enquêteurs dans la police et la gendarmerie, ainsi que la modernisation de leurs formations, et le renforcement de la coopération internationale avec des pays tels que la Russie ou les États-Unis qui hébergent nombre de sites illicites. L'OCLCTIC a été ainsi renforcé. Il est désormais possible de porter à leur connaissance des faits relatifs à la cybercriminalité, via Internet [25], notamment en matière de pédophilie, de haine raciale, d'apologie du terrorisme, d'escroquerie à la carte bancaire, de vente aux enchères fictive, de piratage informatique, etc. Rappelons aussi que, peu de temps avant, avait été annoncée la création d'un réseau IP hautement sécurisé reliant les 4 300 sites de la Gendarmerie nationale. Sur cet axe de propositions du rapport des efforts incontestables ont donc permis de progresser.

Assurer la sécurité de l'État et des infrastructures vitales

Comme on le rappelait en introduction, cet axe de propositions présente une grande actualité, avec *Le Livre blanc* sur la Défense et la Sécurité nationale [26] et le rapport Romani [27], et nécessite encore des efforts. Le contexte de la Révision générale des politiques publiques a pu constituer un cadre pour mettre à jour les politiques de SSI et les schémas directeurs de chaque ministère et les valider. Néanmoins, pour les infrastructures vitales, les objectifs de validation de la politique de sécurité et la conduite d'inspections et de tests d'intrusion proposés par le rapport Lasbordes demeurent essentiels. Ceci est d'autant plus important que des événements récents sont intervenus, qui sont évoqués dans le rapport Romani :

« *Les attaques dites "chinoises", dont plusieurs gouvernements occidentaux ont indiqué avoir été la cible au cours des années 2006 et 2007, font référence à des tentatives menées dans plusieurs pays selon un mode opératoire identique : l'envoi à des hauts responsables ou des fonctionnaires, ainsi qu'à des dirigeants d'entreprises, de courriers électroniques apparemment légitimes, mais dont la pièce jointe, piégée, comportait un "cheval de Troie",* [....] *En France, ces attaques ont visé le ministère des Affaires étrangères, et en particulier des diplomates en poste en ambassade. Elles se présentaient sous la forme de messages anodins, en relation avec l'actualité ou les centres d'intérêt des destinataires. La pièce jointe était susceptible d'installer sur l'ordinateur visé un programme forgé spécifiquement, et donc non détectable par les protections habituelles (pare-feux, anti-virus), dans un but de récupération et de transfert des informations vers un serveur étranger... Il est à noter que lors de la présentation de son dernier bilan sur la maîtrise des risques publié au mois de juin, le Commissariat à l'énergie atomique (CEA) a donné des indications précises sur les attaques informatiques dont il a fait l'objet en*

....

(20) http://www.certa.ssi.gouv.fr/certa/cert.htm/
(21) http://www.securite-informatique.gouv.fr/
(22) http://cigref.typepad.fr/
(23) http://www.culture.gouv.fr/culture/actualites/index-olivennes231107.htm
(24) http://www.culture.gouv.fr/culture/actualites/conferen/albanel/2008-06-18-Art-Creation-et-Internet.html
(25) http://www.interieur.gouv.fr/sections/contact/police/questions-cybercriminalite
(26) http://www.premierministre.gouv.fr/information/les_dossiers_actualites_19/livre_blanc_sur_defense_875/livre_blanc_1337/livre_blanc _1340/
(27) http://www.senat.fr/noticerap/2007/r07-449-notice.html

2007, en soulignant que les attaques aveugles et récurrentes marquaient le pas au profit d'attaques plus ponctuelles dans le temps (de quelques heures à quelques jours) et plus précises en termes de cibles visées. La diversité de ces infections met en défaut les systèmes de détection classiques qui travaillent sur la base d'attaques connues. Le CEA a indiqué que ces attaques provenaient fréquemment de Chine ».

Et le rapport Romani de poursuivre : « *Une analyse exhaustive de la situation de la France au regard de la sécurité des systèmes d'information a été publiée au début de l'année 2006, dans le cadre de la mission qui avait été confiée à notre collègue député Pierre Lasbordes. Le rapport de ce dernier dresse un constat sévère, tant en termes d'organisation que de moyens. En effet, si des avancées incontestables ont été effectuées ces dernières années, elles demeurent insuffisantes au regard des enjeux. La France accuse ainsi un réel retard par rapport à nos principaux partenaires, en premier lieu l'Allemagne et le Royaume-Uni... La France participe à diverses enceintes internationales dans ce domaine, mais les coopérations en sont encore à un stade peu développé, notamment en ce qui concerne l'Union européenne* ».

Le sénateur Romani insiste sur le besoin de créer une agence interministérielle chargée de la sécurité des systèmes d'information, projet inscrit dans le *Livre blanc*, et à cette occasion de renforcer les moyens. « *Leur niveau actuel, cinq fois inférieur à celui de nos partenaires principaux, ne permet déjà pas aux structures existantes de faire face dans des conditions satisfaisantes aux missions qui leur ont été confiées* ».

Indiquons cependant, malgré les constats assez sombres que l'on vient d'évoquer, que le Secrétariat général de la Défense nationale (SGDN) a annoncé officiellement, en novembre 2007, le lancement d'un intranet interministériel hautement sécurisé baptisé ISIS [28]. Mis en place depuis plus d'un an déjà, ce réseau permet le partage d'informations classifiées, notamment en situation de crise entre acteurs gouvernementaux. Des sites tels que l'Élysée, Matignon, les ministères de l'Équipement, de l'Intérieur, des Affaires étrangères, de la Santé et de la Défense sont reliés à Isis par l'intermédiaire d'un portail permettant de consulter et d'enrichir en temps réel une base documentaire d'informations sensibles et classifiées. Ce réseau offre la possibilité de créer un espace de travail en commun, accessible grâce à une carte d'authentification personnelle, d'accéder à un annuaire interministériel de crise, et d'échanger via une messagerie sécurisée. Il répond aux exigences élevées qu'imposent le secret de défense et la conduite de l'action gouvernementale en cas de crise.

Conclusion

Le rapport Lasbordes a permis de prendre conscience qu'une attention nationale insuffisante à la sécurité des systèmes d'information risquait de limiter les bénéfices qu'Internet est susceptible d'apporter à l'économie et au bien-être dans notre pays. Cette prise de conscience a recueilli un large écho au niveau international. Elle est désormais relayée par un organisme tel que l'Organisation pour la coopération et le développement économique. C'est ainsi que lors de la conférence de Séoul du 18 juin 2008 sur le futur de l'économie Internet, les représentants présents des membres de cette organisation se sont engagés à mener une politique de renforcement de la confiance et de la sécurité [29]. Ils ont déclaré vouloir notamment « *protéger les infrastructures d'information critiques aux niveaux national et international contre les atteintes à la sécurité* [...] *réduire l'activité malveillante en ligne par une coopération nationale et internationale renforcée entre toutes les communautés d'acteurs grâce aux mesures qu'elles prennent pour une action efficace de prévention, de protection, d'échange d'information, d'intervention et de maintien et de rétablissement de l'activité* [...] *garantir la protection des identités numériques et des données à caractère personnel ainsi que de la vie privée des personnes en ligne* [...] *encourager la collaboration entre les gouvernements, le secteur privé, la société civile et la communauté technique de l'Internet pour comprendre l'impact de l'Internet sur les mineurs et mieux protéger et aider ces derniers quand ils utilisent l'Internet* [...] *encourager la recherche pour faire face aux menaces émergentes pour la sécurité* ».

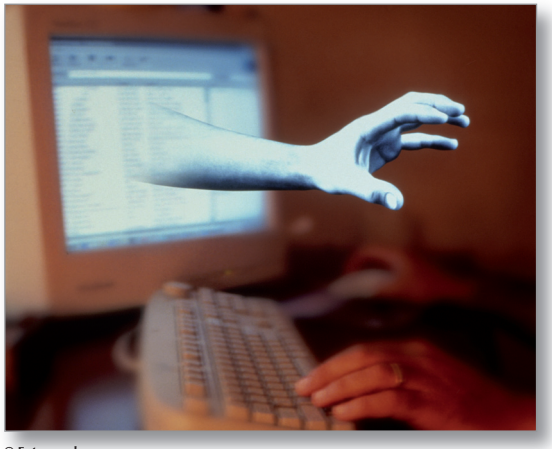
Le rapport Lasbordes a donc permis des avancées incontestables. Cependant, sur le plan des recommandations qu'il faisait en matière de sécurité de l'État et des infrastructures vitales, la mise en application reste d'actualité. Les moyens de progresser restent à notre portée, et une ambition de se hisser au niveau d'autres pays comme l'Allemagne ou le Royaume-Uni semble parfaitement réaliste. Le rapport Romani le rappelle opportunément, comme il souligne le besoin que la coopération se développe au sein de l'Union européenne, thème que la Présidence française est susceptible de faire avancer. Gageons que nous allons encore progresser dans la prise en compte collective de la sécurité des systèmes d'information aux niveaux national et européen.

Serge PERRINE

(28) http://www.ssi.gouv.fr/isis/
(29) http://www.oecd.org/document/33/0,3343,fr_21571361_38415463_38415521_1_1_1_1,00.html

Cyberdéfense : un nouvel enjeu de sécurité nationale

Roger ROMANI



© Fotosearch

Les attaques informatiques de nature diverse, qui ont touché plusieurs pays européens en 2007, ont matérialisé la réalité d'une nouvelle menace sur les intérêts stratégiques de nos sociétés. La France doit rapidement réagir en redéfinissant le cadre de sa politique de sécurité des systèmes d'information et en renforçant les moyens, aujourd'hui insuffisants, qu'elle consacre à leur protection.

Cyber Defense: The New Stakes of National Security

The various digital attacks that hit several European countries in 2007 brought to the fore the reality of a new kind of threat to the strategic interests of our societies. France must rapidly react by redefining the framework of its information system security policy. It must reinforce the currently insufficient means that it has devoted to this threat.

Roger Romani

Vice-président du Sénat, Sénateur (UMP) de Paris, ancien ministre, Roger Romani est membre de la Commission des Affaires étrangères, de la Défense et des Forces armées du Sénat. Il a effectué, au nom de cette dernière, un rapport d'information consacré à la « cyberdéfense » publié en juillet 2008.

Au printemps 2007, alors qu'une vive tension diplomatique l'oppose à la Russie à propos du déplacement d'un monument commémoratif de l'armée soviétique, l'Estonie est victime d'une vague d'attaques informatiques submergeant les sites internet du Gouvernement, des banques, des opérateurs de téléphonie mobile et des organes d'information, avec pour effet immédiat de les rendre indisponibles. Les attaques et perturbations, dont l'origine ne peut être établie avec certitude, se poursuivent durant un mois et demi. Bien qu'aucune fonction vitale ne soit interrompue, l'impact psychologique et les incidences sur la vie courante sont considérables, dans un pays où l'usage des communications électroniques est particulièrement répandu.

Quelques semaines plus tard, en septembre 2007, les autorités françaises révèlent que des services de l'État ont fait l'objet d'attaques ciblées visant à s'introduire dans leurs systèmes d'information, vraisemblablement à des fins d'espionnage. Sur une période d'environ six mois, plusieurs diplomates ont reçu des courriers nominatifs, apparemment légitimes et en relation avec leur activité professionnelle, mais les pièces jointes, piégées, devaient installer un programme permettant à l'expéditeur de pénétrer dans l'ordinateur du destinataire et d'y récupérer des données. Dans le même temps, de nombreux pays occidentaux – États-Unis, Canada, Allemagne, Royaume-Uni, Pays-Bas, Suisse, Australie, Nouvelle-Zélande – signalaient avoir fait l'objet d'intrusions similaires, bâties sur le même modèle. Qualifiées d'attaques « chinoises », elles provenaient toutes de Chine, sans que l'on puisse pour autant en déterminer précisément les auteurs.

Ces deux événements ont matérialisé de manière très concrète une menace encore mal identifiée en Europe et singulièrement en France. La vulnérabilité des réseaux informatiques n'est certes pas une préoccupation nouvelle, mais l'existence d'un risque pesant plus spécifiquement sur les États et la sécurité nationale demeurait, dans les esprits, assez théorique. À la différence des États-Unis, qui s'y référaient dans plusieurs documents stratégiques, l'Europe ne semblait pas en mesurer la réalité jusqu'aux incidents de l'an passé.

Au mois de février dernier, la Commission des affaires étrangères, de la défense et des forces armées du Sénat a jugé nécessaire d'établir un rapport d'information sur les enjeux liés à la sécurité des systèmes d'information, sujet dont *Le Livre blanc* sur la défense et la sécurité nationale, publié au mois de juin 2008, a lui aussi souligné le caractère stratégique.

De ce rapport d'information [1] découlent trois conclusions principales :

- les menaces de nature informatique susceptibles de mettre en cause la sécurité et la défense du pays sont une réalité et ne peuvent aller qu'en s'accentuant ;
- la France est encore insuffisamment préparée et organisée face à ces menaces ;
- pour s'en protéger, une impulsion politique forte, assortie de moyens humains et techniques beaucoup plus conséquents, est indispensable.

Une menace aux manifestations de plus en plus évidentes

L'usage des technologies informatiques figure désormais clairement dans la panoplie des méthodes de mise en cause des intérêts stratégiques des États.

Déni de service et intrusion : deux modes d'attaque privilégiés

Le déni de service, qui vise à stopper le fonctionnement d'un système informatique, et l'intrusion en vue de détourner des informations constituent les deux principales formes de menaces pesant sur les systèmes gouvernementaux ou d'entreprises sensibles.

Les attaques par déni de service, dont les événements d'Estonie représentent l'exemple type et qui ont également été signalées en Géorgie lors du conflit d'août 2008, visent à saturer un site internet ou un système informatique par des dizaines ou des centaines de milliers de connexions simultanées. Comment est-il possible de coordonner autant de connexions en aussi peu de temps ? Grâce à des réseaux d'ordinateurs (« botnets »), constitués de machines contaminées par un virus informatique (ordinateurs « zombies »), qui sont passées sous le contrôle d'un pirate informatique (« hacker »). Une partie du volume considérable du courrier électronique indésirable que nous recevons (les « pourriels » ou spams) contient de tels virus susceptibles d'infecter notre ordinateur et de le faire entrer dans un botnet où il sera utilisé, à notre insu, à des

(1) *Cyberdéfense : un nouvel enjeu de sécurité nationale*, rapport d'information n°449 (2007-2008) de M. Roger Romani, publié le 8 juillet 2008 : http://www.senat.fr/noticerap/2007/r07-449-notice.html

fins généralement illicites : ventes frauduleuses, escroqueries ou attaques par déni de service.

Ces réseaux d'ordinateurs contaminés sont sous le contrôle de pirates informatiques qui, généralement, agissent en groupes constitués. Le détenteur du réseau est rarement le commanditaire de l'attaque. Il monnaye sa capacité d'envoi massive à des « clients » animés de préoccupations diverses. S'agissant de l'Estonie, les regards se sont tournés vers les services russes, mais aucun lien n'a pu être établi. En tout état de cause, il est extrêmement difficile de remonter à la source de l'attaque, car il est aisé pour l'agresseur de masquer ou de déguiser son identité et d'utiliser par « rebonds » une multitude d'adresses successives pour brouiller les pistes. L'attaque par déni de service n'est qu'une des applications possibles. Son corollaire est le chantage au déni de service, c'est-à-dire l'extorsion de fonds auprès des entreprises ou organismes en échange d'une levée des attaques de saturation.

S'agissant des intrusions sur les systèmes d'information par des voies informatiques, la principale technique utilisée est celle du cheval de Troie, c'est-à-dire d'un programme informatique ou d'un fichier comportant une fonctionnalité cachée, connue de l'attaquant seul, et lui permettant de prendre le contrôle de l'ordinateur compromis, puis de s'en servir à l'insu de son propriétaire. Un cheval de Troie se cache en général dans un programme d'aspect inoffensif ou usuel, et son activation implique l'intervention de l'utilisateur (ouverture d'une pièce jointe, utilisation d'un lien de connexion à un site internet). À la différence des virus propagés à une très grande échelle, les chevaux de Troie relèvent le plus souvent d'attaques ciblées, adaptées à la victime choisie, qui ne peuvent être détectées automatiquement par les antivirus. Ils s'installent durablement sur la machine compromise.

Le cheval de Troie peut installer des programmes enregistrant la frappe de l'utilisateur sur le clavier (« keylogger ») ainsi que des logiciels espions (« spyware ») en vue de récupérer, par des envois fractionnés et discrets, tout le contenu de l'ordinateur. Il pourra également mettre en place des outils de dissimulation d'activité (« rootkits ») permettant d'effacer les traces de l'intrusion et du vol de données.

Une grande variété de cibles potentielles

Les sites et services accessibles au public offrent la cible la plus évidente pour une attaque informatique potentielle. Provoquer l'indisponibilité du site internet d'une institution ou d'une administration, comme on l'a vu en Estonie, répond essentiellement à un objectif politique, de même que la défiguration (*defacement*) du contenu et son remplacement par des messages à connotation protestataire ou revendicative. Pour une entreprise, le préjudice s'évaluera davantage en termes d'image, avec d'éventuelles incidences commerciales. Cependant, un très grand nombre de sites institutionnels abritent également des services en ligne qui se sont considérablement développés ces dernières années, et dont l'interruption causerait d'importantes perturbations dans la vie sociale et économique de la nation.

Beaucoup plus préoccupant est le risque d'attaques de systèmes à vocation opérationnelle. On pense notamment à ceux qui permettent la distribution de l'eau et de l'électricité, les télécommunications, la circulation des trains, des métros, des avions, les transactions interbancaires, les processus de fabrication industriels. Normalement, le cloisonnement entre ce qui est accessible depuis l'extérieur, via internet, et les réseaux internes que les administrations et les entreprises utilisent pour leurs activités opérationnelles, rend ceux-ci moins vulnérables aux attaques extérieures. Mais, dans les faits, très rares sont les systèmes informatiques totalement isolés de l'extérieur. Les interconnexions se sont multipliées pour répondre au besoin de communication entre ces systèmes, parfois aussi pour contrôler ou gérer des opérations à distance ou encore pour effectuer de la télémaintenance. Elles sont autant de vulnérabilités supplémentaires.

Jusqu'à aujourd'hui, on ne connaît pas d'exemple d'une infrastructure critique qui aurait été arrêtée par une attaque informatique. Mais, pour prévenir ce risque, il faut prendre des mesures de sécurité très strictes et rester très vigilant sur l'évolution de la menace. À titre d'exemple, EDF maintient un isolement quasi absolu des systèmes régissant la production et la distribution d'électricité, les rares passerelles existant entre ce réseau opérationnel et le reste de l'entreprise faisant l'objet de mesures de protection et de surveillance extrêmement poussées. De même, les mesures de contrôle interne sont très rigoureuses, de manière à prévenir le risque d'un acte malveillant provenant de l'intérieur même de l'entreprise. Enfin, EDF possède un plan de continuité qui permet, en cas de panne d'un système informatique, de basculer très rapidement sur un système redondant. On le voit, les opérateurs de réseaux essentiels à la vie économique et sociale de la Nation se doivent d'envisager une panoplie complète de mesures de sécurité face aux atteintes potentielles à leurs systèmes d'information. L'exigence d'étanchéité et de protection est encore plus forte pour tous les systèmes à vocation militaire, désormais essentiels en matière d'information, de communication et de mise en œuvre des armements.

Enfin, une menace de nature différente pèse sur les détenteurs d'informations sensibles de nature politique, militaire, économique, scientifique ou technologique, que ce soit au sein de l'appareil d'État, des grandes institutions de recherche ou des entreprises, y compris petites ou moyennes. Ils constituent un troisième type de cibles potentielles pour des attaques informatiques. On se situe ici dans le champ des activités d'espionnage ou d'ingérence, au travers de méthodes nouvelles visant à cibler les ordinateurs et les systèmes mobiles ou périphériques de personnes identifiées en fonction de leur niveau de responsabilité et de leurs contacts. Le recours aux technologies d'intrusion peut intervenir en complément ou à la place d'autres modes de captation de données informatiques, tels que le vol d'ordinateurs portables des personnes cibles ou leur « fouille » informatique, par exemple aux passages de frontières. L'objectif est d'acquérir des informations d'intérêt politique, militaire, économique, scientifique, technologique ou industriel.

Qui dirige les attaques informatiques ?

À l'évidence, les attaques informatiques actuelles ne peuvent être imputées à de simples « amateurs » isolés, procédant par jeu ou par défi et désireux de tester ou de démontrer leur niveau de performance technique. Avec l'essor de l'Internet, s'est développée une nouvelle catégorie de pirates agissant en groupes et essentiellement motivés par l'appât du gain. Ces groupes mettent au point des outils qu'ils peuvent exploiter directement ou offrir sur le marché à des clients tels que des organisations criminelles ou mafieuses, des officines d'espionnage économique, des entreprises ou des services de renseignement.

Les États eux-mêmes ont bien entendu développé leurs propres moyens de « guerre informatique ». Si nombre de services de renseignement entretiennent une compétence offensive dans le domaine informatique, ne serait-ce qu'en matière d'écoute passive des flux d'information, leur implication dans des attaques n'a jamais été avérée. Toutefois, le « cyberespace » devient aujourd'hui très ouvertement considéré par les États comme une nouvelle dimension du champ de bataille.

L'exemple le plus frappant est celui de la Chine, qui a fait de la lutte informatique une partie intégrante de sa stratégie de sécurité, y voyant le moyen de compenser l'infériorité de ses capacités conventionnelles. Bien qu'aucune information officielle ne filtre à ce sujet, la Chine semble avoir concentré au sein de l'Armée populaire de libération la totalité de ses capacités étatiques, tant défensives qu'offensives. On ne peut exclure que le gouvernement chinois s'appuie également sur les nombreux groupes de pirates informatiques nationaux, et sur lesquels il dispose d'importants moyens de pression, en raison du contrôle étroit exercé sur l'Internet. Avec la Chine, et en partie vis-à-vis de celle-ci, les États-Unis sont l'autre pays à disposer d'une doctrine militaire de lutte informatique, de commandements dédiés et de moyens spécifiques à cet effet. La France ne fait que tirer les conséquences de cette évolution en annonçant, dans son nouveau *Livre blanc*, qu'elle dotera à son tour les armées d'une doctrine et de capacités de lutte informatique offensive destinées à neutraliser les centres d'opération adverses.

L'utilisation de l'arme informatique par des groupes terroristes soit directement, soit indirectement par l'intermédiaire de pirates informatiques qu'ils rémunéreraient, est un risque qui a été fréquemment évoqué. Si les groupes terroristes utilisent largement Internet à des fins de propagande et comme moyen de communication, aucune attaque terroriste d'envergure par voie informatique, par exemple contre des infrastructures sensibles, n'a pour l'instant été répertoriée. Cependant, les organisations terroristes ont acquis une maîtrise significative des outils informatiques et de l'Internet qui pourrait, le cas échéant, les amener à tenter de telles opérations. À titre d'exemple, la branche armée du Jihad islamique palestinien a récemment déclaré avoir mis en place une unité de « cyberguerre » qui revendique des attaques contre des sites militaires et des sites de journaux israéliens. Par ailleurs, les groupes de pirates restent susceptibles de monnayer leurs services auprès de ces organisations.

Une menace qui ira inévitablement en s'accentuant

Les événements survenus en Estonie ou les attaques dites « chinoises » opérées contre plusieurs États occidentaux ne sont que de premières manifestations d'un phénomène appelé à s'accentuer, et ce pour au moins trois raisons.

Premièrement, il est banal de souligner que les systèmes d'information et l'Internet prennent une place chaque jour grandissante dans tous les domaines de la vie et du fonctionnement de nos sociétés, devenant de ce fait une cible potentielle. Il est, en effet, particulièrement tentant pour un agresseur, qu'il s'agisse d'un groupe non étatique ou d'un État, d'utiliser l'arme informatique pour perturber la vie courante, générer des troubles, accéder à des informations sensibles du point de vue politique, économique et militaire, et amoindrir nos capacités d'action.

Deuxièmement, ce mode opératoire est relativement accessible et « rentable ». Il s'appuie sur des technologies dont la maîtrise n'est pas réservée à un nombre limité de

spécialistes ou à des organisations étatiques. L'ouverture et l'interconnexion croissantes des réseaux, de même que la généralisation de produits standards, dont les vulnérabilités sont en permanence scrutées par les communautés de pirates informatiques, en facilitent l'usage. Il s'avère relativement peu coûteux et s'affranchit très facilement des distances et des frontières.

Enfin, l'attaque informatique est particulièrement difficile à identifier. Elle procède par rebonds, utilisant une succession d'adresses relais et permet de cacher ou de déguiser son identité. Le transit par un grand nombre de pays ou l'utilisation d'ordinateurs situés dans des sites publics comme les cybercafés entravent les possibilités d'enquête, et s'il est possible de localiser le serveur, les législations locales permettent rarement de remonter jusqu'à l'initiateur de l'attaque. Enfin, le lien entre les pirates informatiques et leurs commanditaires reste le plus souvent impossible à établir avec certitude.

Face à cette menace, la France est encore insuffisamment préparée et organisée

La France a atteint un haut degré dans la diffusion et l'usage des systèmes d'information, mais elle n'a sans doute pas accordé suffisamment d'importance à la sécurité de ces systèmes. Une politique d'ensemble de la sécurité des systèmes d'information a été définie en 1986. Elle a été revue en 1996 avec l'attribution au Secrétariat général de la Défense nationale (SGDN), à travers sa direction centrale de la Sécurité des systèmes d'information (DCSSI), d'une responsabilité particulière dans le domaine de l'identification et de la surveillance des risques.

Mais, les limites de ce dispositif ont été clairement identifiées depuis plusieurs années déjà. En mars 2004, le Premier ministre Jean-Pierre Raffarin s'en inquiétait et lançait un plan de renforcement de la sécurité des systèmes d'information [2]. L'année suivante, il confiait à Pierre Lasbordes, député de l'Essonne, un rapport publié en janvier 2006, dans lequel était dressé un constat sans complaisance des faiblesses de notre organisation et de nos moyens, notamment au regard de nos partenaires européens les plus proches.

Des efforts encore modestes

Certes, au cours des années récentes, les pouvoirs publics ne sont pas restés inactifs. Leurs efforts ont principalement porté sur trois domaines. Tout d'abord, le renforcement des capacités de veille et de réaction. Un Centre opérationnel de la sécurité des systèmes d'information (COSSI) a été créé en 2005 au sein de la DCSSI. Il assure une veille permanente sur la menace et les vulnérabilités, sur les attaques conduites dans le monde et sur les incidents affectant notamment les systèmes d'information gouvernementaux. Un dispositif de réaction, en cas d'attaques de grande ampleur visant l'État ou des opérateurs d'infrastructures d'importance vitale, est également prévu dans le cadre du plan Vigipirate et d'un plan spécifique, le plan Piranet, décliné au niveau de chaque administration.

La DCSSI a également développé des activités de conseil, de formation et d'information. Conformément aux recommandations du rapport Lasbordes, un portail internet gouvernemental consacré à la sécurité informatique a été ouvert au mois de février 2008 [3]. La DCSSI réalise des inspections au sein des ministères et organise des exercices interministériels en matière de sécurité des systèmes d'information.

Un troisième axe d'effort a permis de réels progrès sur la sécurisation des moyens de communication gouvernementaux. Le plus notable est la mise en place de l'Intranet sécurisé interministériel ISIS fin 2007. Il s'agit du premier réseau interministériel permettant le partage d'informations classifiées au niveau confidentiel-défense. Par ailleurs, un effort important est réalisé pour développer et acquérir des produits de haut niveau de sécurité destinés aux services gouvernementaux, notamment pour le chiffrement des communications téléphoniques et des échanges de données chiffrées sur Internet.

Des lacunes persistantes

En dépit de ces efforts récents, d'importantes lacunes subsistent. Le rapport d'information du Sénat en a identifié trois principales. Premièrement, notre organisation souffre de la dispersion et de l'excessive autonomie des différents acteurs en charge de la sécurité des systèmes d'information. Si la DCSSI est chargée d'impulser la politique de sécurité des systèmes d'information au sein l'État, plusieurs ministères disposent de compétences et

....

(2) L'exposé des motifs du plan interministériel dressait l'inventaire des difficultés persistantes en la matière : « *compétences et capacités opérationnelles trop réduites et isolées, manque de sensibilité des décideurs aux enjeux, insuffisance de produits de sécurité dûment qualifiés* [...] *prolifération d'interconnexions de réseaux mal sécurisés, réglementation nationale difficilement applicable, dimension européenne mal coordonnée* ».

(3) http://www.securite.informatique.gouv.fr

de moyens techniques spécifiques. C'est le cas du ministère de la Défense, avec l'expertise technique de la délégation générale pour l'Armement, le rôle des services de renseignement (direction générale de la Sécurité extérieure - DGSE ; direction de la Protection et de la Sécurité de la défense -DPSD) et les moyens propres des armées. Le ministère de l'Intérieur intervient également à travers la direction centrale du Renseignement intérieur (DCRI) ou certains services spécialisés de la police judiciaire, de même que, dans un domaine très différent, le ministère de l'Économie et des Finances, compétent pour le soutien à l'innovation et le développement de l'administration électronique. La coordination de ces différents acteurs et l'utilisation optimale de leurs moyens méritent incontestablement d'être améliorées.

Par ailleurs, chaque département ministériel dispose d'une totale autonomie dans la réalisation de ses réseaux, sans être tenu de se conformer aux recommandations de la DCSSI, par exemple pour l'usage de produits informatiques sécurisés. Au sein de chaque ministère, le haut fonctionnaire de défense est en charge de la sécurité des systèmes d'information. Mais bien souvent, son poids vis-à-vis des services informatiques est insuffisant pour faire prendre en compte les impératifs – et nécessairement les contraintes – liés à la protection des réseaux. Il existe par conséquent une très grande disparité dans la manière dont les ministères gèrent la sécurité de leurs systèmes.

La deuxième lacune, très frappante, est l'insuffisance des moyens. Bien que constituant, au niveau interministériel, le service pivot pour la sécurité des systèmes d'information, la DCSSI ne compte que cent dix agents, un effectif pratiquement inchangé depuis plusieurs années. Or, la DCSSI se voit confier des attributions extrêmement vastes : apporter son conseil à l'ensemble de l'administration par des missions de formation, d'inspection et de conseil ; évaluer et vérifier la sécurité des réseaux et des systèmes d'information des services publics ; agréer tous les matériels de chiffrement qui protègent des données classifiées ; orienter le développement de produits sécurisés ; gérer un service de veille, d'alerte et de réaction aux intrusions dans les systèmes d'information de l'État ; préparer et mettre en œuvre les mesures de sécurité des systèmes d'information prévues par les plans Vigipirate et Piranet... Il est absolument évident que l'effectif actuel de la DCSSI, ne peut pas lui permettre d'assurer pleinement toutes ces missions, ni le rôle de sensibilisation qui devrait être le sien, non seulement pour l'administration, mais, au-delà, vers les entreprises et l'ensemble du secteur privé.

Autre conséquence de la faiblesse des moyens, la France ne possède pas, à la différence de l'Allemagne, une capacité centralisée de surveillance et de détection des flux de données transitant entre les administrations et l'Internet. Cette lacune ne nous permet pas de détecter par nous-mêmes des attaques informatiques.

Enfin, la troisième faiblesse, qui sort du champ de l'administration, concerne nos entreprises, qui, à quelques exceptions près, semblent encore trop peu préparées à la menace informatique, notamment les PME. Elles paraissent donc particulièrement vulnérables.

Des partenaires mieux organisés et équipés

La France paraît particulièrement en retard par rapport à ses deux principaux partenaires européens, le Royaume-Uni et l'Allemagne. Le service britannique homologue de la DCSSI française, le *Communications and electronic security group* (CESG), qui relève de l'agence en charge du renseignement technique, le *Communication government head quarter (*CGHQ), compte environ 450 agents. Quant à l'équivalent allemand, le *Bundesamt für Sicherheit in des Informationstechnik* (BSI), rattaché au ministère de l'Intérieur, il bénéficie d'une augmentation régulière de ses effectifs, qui s'élevaient à 340 agents en 2001, et atteignent actuellement 500 agents.

Ces deux pays ont arrêté des orientations stratégiques en matière de sécurité de l'information (stratégie nationale de 2003 au Royaume-Uni, plan national pour la protection des infrastructures d'information de 2005 en Allemagne). Leur organisation met l'accent, beaucoup plus clairement qu'en France, sur le partenariat avec le secteur privé. Au Royaume-Uni, une instance spécifique, le *National infrastructure security coordination center*, sert de cadre à la coopération entre acteurs publics et privés. Elle traite de la sécurité des réseaux et des systèmes informatisés de contrôles industriels. Un centre de veille et d'alerte lui est rattaché. En Allemagne, le BSI entretient des liens étroits avec les opérateurs d'infrastructures critiques et les entreprises sensibles. Il faut aussi souligner qu'à la suite de la réunification et du transfert de la capitale à Berlin, l'Allemagne s'est dotée de systèmes de communication gouvernementaux extrêmement fiables et hautement sécurisés. Ces systèmes ont facilité le déploiement d'outils automatiques de surveillance des réseaux informatiques gouvernementaux, et leur offrent ainsi une capacité de détection dont la France est encore privée.

Hors d'Europe, les États-Unis possèdent bien entendu des moyens sans commune mesure avec ceux de nos voisins, et *a fortiori* ceux de la France. L'Information assurance directorate, qui constitue au sein de la *National security agency* (NSA) le service homologue de notre

DCSSI, compte environ 3 000 agents. La *Presidential National Security directive 54* approuvée le 8 janvier 2008 par le président Bush formalise une série de mesures visant à accentuer la protection des systèmes d'information gouvernementaux contre les attaques informatiques. Parmi celles-ci, figurent la montée en puissance du centre gouvernemental de veille et d'alerte, l'extension à tous les réseaux de l'administration et des agences fédérales du dispositif de détection opérationnel depuis plusieurs années au Département de la défense, ou encore la réduction de 2 000 à 50 du nombre de points d'accès des réseaux de l'administration à l'Internet, en vue de faciliter le déploiement de dispositifs de sécurité et de surveillance. Les politiques menées par nos partenaires témoignent d'une prise en compte accentuée de la menace et d'une claire volonté d'y répondre, par une organisation et des moyens adaptés.

Une coopération européenne limitée

Les attaques informatiques s'affranchissent des frontières et peuvent être dirigées simultanément contre plusieurs États. La surveillance des réseaux et la réaction aux attaques justifient donc une coopération internationale. Plusieurs enceintes multilatérales en ont pris conscience, mais pour l'heure, les actions entreprises à l'échelon international ne sont pas en mesure de compenser la modestie de nos moyens nationaux. Une coopération opérationnelle a été formalisée entre les structures gouvernementales compétentes de plusieurs États européens au sein de l'*European Government Computer Security Incident Response Team* (EGC). Il s'agit de partager l'information sur la menace et les vulnérabilités, de mettre en commun l'expertise technique et de coordonner les réactions en cas d'incident.

L'Union européenne a pour sa part énoncé, dans plusieurs documents de la Commission, des orientations générales qui ne se sont pas encore traduites par des avancées concrètes. Une agence spécialisée, l'*European Network and Information Security Agency* (ENISA), a été créée en 2004 à Heraklion, en Crète. Ses premières années de fonctionnement ont fait l'objet, l'an passé, d'une évaluation assez critique dans le cadre d'un audit demandé par la Commission. À l'évidence, l'Union européenne, dans les toutes prochaines années, se devra d'apporter des réponses efficaces, tant en matière de coopération opérationnelle que de réglementation, par exemple pour imposer aux opérateurs des mesures de protection des réseaux.

On observera qu'après les événements d'Estonie, l'OTAN a fait de la cyberdéfense l'une de ses priorités. Elle entend notamment renforcer sa capacité à coordonner l'assistance aux alliés subissant une attaque informatique et s'est dotée d'un centre d'expertise situé à Tallin. Si le développement de la coopération internationale est nécessaire, et même indispensable, il ne dispensera pas la France d'entreprendre résolument la mise à niveau de son organisation et de ses moyens.

Une impulsion politique forte, assortie de moyens humains et techniques beaucoup plus conséquents

En érigeant la protection de nos systèmes informatiques sensibles au rang de composante à part entière de notre politique de défense et de sécurité, le nouveau *Livre blanc* marque une inflexion notable. Il importe désormais d'en tirer toutes les conséquences au travers d'une politique de sécurité des systèmes d'information plus active et plus efficace.

Une priorité reconnue par *Le Livre blanc* sur la défense et la sécurité nationale

Dans les quinze années à venir, les attaques informatiques provenant d'acteurs non étatiques vont se multiplier, les attaques dissimulées, commanditées par des États, seront hautement probables, alors que des actions massives menées ouvertement par des États devront être considérées comme une hypothèse plausible. C'est en ces termes que *Le Livre blanc* évalue très clairement la menace et l'intègre dans notre stratégie nationale de défense et de sécurité.

La première réponse que propose *Le Livre blanc* porte sur l'organisation des pouvoirs publics. Une Agence interministérielle de la sécurité de systèmes d'information sera constituée à partir de l'actuelle DCSSI. Dotée d'une certaine autonomie, bien que placée sous la tutelle du futur Secrétariat général de la Défense et de la Sécurité nationale (SGDSN), elle reprendra les compétences de la DCSSI avec des ambitions plus larges, notamment en matière de concentration de l'expertise technique et de conseil aux opérateurs d'importance vitale. S'agissant des moyens techniques, la nouvelle agence disposera d'une véritable capacité de détection et de surveillance, c'est-à-dire d'outils informatiques branchés sur les passerelles reliant les administrations et l'Internet, ainsi que de techniciens capables d'interpréter les flux anormaux.

Enfin, au-delà des capacités défensives, qui se limitent à la protection des systèmes, *Le Livre blanc* prévoit le renforcement des capacités offensives visant à identifier l'attaquant, à connaître son mode opératoire, à le neutraliser, voire à lui appliquer des mesures de rétorsion. Les moyens dont disposent à cet effet les services de renseignement seront accentués, et une capacité de lutte offensive spécifiquement militaire sera développée, compte tenu de la probabilité de voir utiliser l'arme informatique dans les conflits armés.

Un effort à accentuer de manière résolue

Les perspectives ouvertes par *Le Livre blanc* sont bien entendu extrêmement positives, puisqu'elles devraient se traduire par des progrès substantiels en termes d'organisation et de moyens. Seront-elles pour autant à la hauteur des enjeux ?

Pour qu'il en soit ainsi, il est absolument indispensable que la mise en œuvre de ces orientations se traduise par une action résolue, sous-tendue par une forte volonté politique.

La question des moyens sera primordiale. *Le Livre blanc* reste à cet égard beaucoup trop évasif, se limitant à prévoir que la future agence ministérielle reprendrait les effectifs et les moyens de la DCSSI « *tout en les renforçant sensiblement* ». Le rapport du Sénat souhaite, pour sa part, un véritable changement d'échelle visant à moyen terme l'équivalence avec les Britanniques et les Allemands. Nous proposons, dans l'immédiat, un plan pluriannuel de renforcement des effectifs qui pourrait permettre à cette agence, d'ici trois à quatre ans, d'atteindre environ trois cents personnes contre une centaine aujourd'hui. C'est, à nos yeux, à cette condition que l'agence sera en mesure de réaliser ce que la DCSSI ne peut actuellement accomplir, faute de moyens : développer la labellisation des produits sécurisés, renforcer les capacités de formation, de conseil, d'audit, d'inspection ; mener une politique de communication active, absolument indispensable pour sensibiliser les responsables des administrations et des entreprises, comme tous les utilisateurs.

Mais des moyens supplémentaires seraient mal employés s'ils n'étaient mis au service d'une organisation plus cohérente et plus efficace. À cet effet, il faudra impérativement renforcer la coordination interministérielle à l'échelon du Premier ministre, afin de mettre en synergie les politiques et les capacités des différents acteurs. On peut penser, par exemple, à la coordination qui devra exister entre l'agence interministérielle, chargée du volet défensif, et les services de renseignement, notamment la DGSE, détentrice d'importants moyens techniques et de personnels spécialisés.

Il faudra également permettre à l'Agence interministérielle de jouer pleinement son rôle. Il ne s'agit pas de l'ériger en tutelle informatique de tous les ministères, mais elle devra néanmoins exercer un certain rôle directif. Il faudra, par exemple, qu'elle puisse imposer une réduction du nombre de passerelles entre les ministères et l'Internet, comme le font actuellement les États-Unis, et à l'image de ce qu'a bien réussi le réseau français de l'enseignement supérieur et de la recherche, RENATER, qui relie mille établissements, centres ou unités de recherche dispersés sur le territoire national à l'Internet, à travers trois passerelles parfaitement contrôlées. L'Agence devra aussi pouvoir rendre obligatoires certains types de produits sécurisés pour les réseaux les plus sensibles.

Enfin, un troisième axe d'effort concerne le partenariat entre les acteurs publics et les entreprises, aujourd'hui très insuffisant. Le renforcement des moyens de la future agence devra permettre de répondre aux attentes des entreprises en ce domaine. Elles souhaitent un interlocuteur unique capable de les conseiller, des catalogues plus étoffés de produits labellisés, des échanges d'information et des contacts beaucoup plus fréquents.

Par ailleurs, dans certains domaines, l'État et certaines entreprises sensibles ont des besoins analogues. Pourquoi ne mettraient-ils pas en commun leurs ressources pour faire développer par des entreprises françaises, les produits de sécurité très spécifiques qui leur sont nécessaires ? Cela soutiendrait notre industrie de la sécurité informatique et renforcerait la sécurité de nos systèmes, en évitant de nous fournir à l'étranger, le plus souvent aux États-Unis aujourd'hui, mais peut-être demain en Chine.

Conclusion

Bien que leurs conséquences se soient avérées relativement limitées, les événements survenus en Europe ces derniers mois ont clairement montré la réalité de la menace liée aux attaques informatiques. L'existence de groupes de pirates informatiques qui monnayent leurs savoir-faire, la diffusion de technologies toujours plus sophistiquées exploitant les vulnérabilités des systèmes d'information et la constitution de capacités offensives par les États laissent à penser que les actions de ce type se poursuivront et s'amplifieront, car elles offrent un moyen discret et relativement peu coûteux de pénaliser ou de fragiliser un pays. L'une des caractéristiques de cette menace est son évolution très

rapide, puisqu'elle s'adapte en permanence aux derniers développements de la technologie. Dès lors, il devient urgent pour la France de rattraper dans ce domaine un retard identifié depuis plusieurs années.

C'est pourquoi il importe que les orientations définies par *Le Livre blanc* sur la défense et la sécurité nationale soient suivies de progrès rapides et concrets. Il s'agit d'assurer la mise en œuvre effective, par l'ensemble des acteurs publics, d'une politique de sécurité adaptée à l'évolution de la menace, mais également d'accroître les moyens humains et techniques des structures spécialisées, et, en tout premier lieu, ceux de la nouvelle Agence interministérielle. C'est à ces conditions que notre dispositif public pourra jouer tout son rôle en matière de sensibilisation, de formation, de protection, de surveillance et de réponse aux menaces, au service de l'État tout d'abord, mais aussi plus largement de l'ensemble des organismes publics ou privés dont la protection intéresse notre défense et notre sécurité.

Roger ROMANI

De la vulnérabilité à la crise des systèmes d'information

Stanislas de MAUPEOU

Les systèmes d'information sont devenus les centres nerveux de nos sociétés. Pourtant, leur dépendance stratégique vis-à-vis des réseaux informatiques est souvent sous-estimée. La perception du risque d'attaque informatique est encore imparfaite et le passage d'une vulnérabilité technique à une crise sociétale reste un scénario improbable. L'objet de cet article est précisément de décrire ce passage du fait technique à la crise, crise qui constitue un danger pour la survie des organisations.

From Vulnerability to Crisis

Information systems have become the central nervous system of our societies, but this vital dependence is often underestimated. The perception of the risk of attack on information is still imperfect. The transformation of technical vulnerability into a social crisis may remain an improbable, maybe even an impossible, scenario. But the danger of a social crisis starting from technical origins represents a threat to the survival of organisations.

Stanislas de Maupeou

Responsable du Centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques (CERTA : www.certa.ssi.gouv.fr), Stanislas de Maupeou est un acteur et un observateur des enjeux de la sécurité de l'information. Dans le cadre du traitement des attaques informatiques, il est amené à apprécier le risque, à préconiser des actions de prévention et à recommander des mesures de réaction.

Ce matin, lorsque vous êtes arrivé à votre bureau, votre ordinateur n'a pas démarré correctement, ni celui de votre collègue, ni ceux de toute l'entreprise d'ailleurs... Simple problème informatique, pensez-vous, sans conséquence heureusement, ce n'est qu'un problème technique mineur à régler. Oui mais... La chaîne de production connaît aussi des dysfonctionnements, des rumeurs se répandent, les informaticiens sont injoignables, vos prestataires s'inquiètent car des informations incohérentes leur parviennent, une agence de notation financière n'a pas eu vos chiffres pour son indice... Votre cours de bourse a un peu bougé aujourd'hui, des clients n'ont pas été livrés à temps, une partie de la population s'inquiète et des journalistes vous sollicitent pour comprendre une situation qui est en train de vous échapper.

Avez-vous déjà réellement connu une VRAIE crise liée à l'informatique ? Mesurez-vous réellement ce qu'est un risque en informatique ? La perception du risque informatique est encore imparfaite parce que les attaques sont le plus souvent complexes à expliquer et que, jusqu'à présent, il n'y a pas eu, en France, de crise majeure liée à l'informatique.

L'information est vitale. La vie, le développement et la survie de toute organisation en dépendent. L'information est un actif et les vulnérabilités de sa gestion constituent une menace. L'information est entrée dans le champ de crise des sociétés.

Le paradoxe est le suivant : alors que les experts observent tous les jours des attaques informatiques, les décideurs et les utilisateurs ne perçoivent pas que la crise est souvent toute proche ! Pas seulement une crise informatique à proprement parler, mais bien une crise pour la société (perte de données, perte d'argent, atteinte à l'image, responsabilité de l'organisation, panique, déstabilisation et désinformation) via l'informatique. Il ne s'agira plus alors d'une affaire d'informaticiens mais d'une gestion politique de la crise exigeant une prise de décision politique.

L'objet de cet article est précisément de décrire ce glissement ténu de la vulnérabilité, qui est une donnée technique, à la crise, qui est un événement de société : passage souvent mal maîtrisé et représentant un danger pour la survie des organisations. Les décideurs ne peuvent plus ignorer leur dépendance stratégique vis-à-vis des réseaux dans un monde totalement interconnecté au sens des réseaux informatiques.

Un système d'information comprend l'ensemble des utilisateurs et des moyens (aujourd'hui principalement informatiques) permettant de faire vivre une information dans une organisation. Nous nous limiterons ici aux moyens informatiques (les logiciels, les protocoles, les ordinateurs). Mais il est clair que les utilisateurs sont des acteurs clefs pour la sécurité d'un tel système !

Qu'est ce qu'une vulnérabilité ?

Aujourd'hui, nous pouvons tous constater, à nos dépens, que l'informatique n'est pas aussi simple et fiable qu'un bouton électrique, qu'un téléphone, qu'un téléviseur, etc. L'informatique est devenue indispensable à nos organisations (qui pourrait prétendre s'en passer pendant quelques jours, voire quelques heures ?) et pourtant nos systèmes sont très largement vulnérables aux attaques. C'est pourquoi il est nécessaire de les corriger régulièrement. Accepteriez-vous de corriger (même par une manipulation simple) votre téléphone, votre machine à laver plusieurs fois par mois comme c'est le cas pour les logiciels ? Les faits parlent d'eux-mêmes : en 2007, la société Microsoft a diffusé 69 bulletins de sécurité traitant 100 vulnérabilités spécifiques (sources Microsoft). La société *Symantec* recense plus de 2000 vulnérabilités durant les six derniers mois de l'année 2007 (*Symantec Global Internet Security Threat Report*, avril 2007). Le Certa a diffusé en 2007 près de 600 avis de sécurité correspondant à des mises à jour de logiciels.

Quel est le lien entre vulnérabilité et attaque ?

Une vulnérabilité donne potentiellement la faculté à un attaquant de réaliser tout un ensemble d'actions allant du vol d'informations à la prise de contrôle à distance de la machine vulnérable, lui permettant ainsi de faire absolument ce qu'il veut sur cette dernière (vol d'informations, modification des informations, attaque d'autres machines...). C'est pourquoi il est fondamental, pour la survie des systèmes informatiques, d'appliquer les correctifs de sécurité proposés, en règle générale, gratuitement par les éditeurs. Dans la construction d'une attaque, la première étape consiste à rechercher les machines vulnérables. L'immense majorité des attaques est due à des logiciels qui n'ont pas été corrigés.

Certaines vulnérabilités ne sont pas corrigées par les éditeurs, soit parce que cela représente un coût élevé, soit parce que la correction est longue à concevoir, soit encore parce que l'éditeur cherche ainsi à inciter l'utilisateur à changer de version.

Les responsables de la sécurité informatique et les administrateurs de réseaux sont chargés de veiller au maintien du niveau de sécurité d'un système et ils peuvent de façon cohérente s'appuyer sur un centre d'expertise (comme par exemple le CERTA pour l'administration : www.certa.ssi.gouv.fr).

Quels sont les impacts de la crise ?

On peut définir une crise comme une situation où les conditions dans lesquelles s'exerce une activité sont remises en cause, ou comme un ensemble de phénomènes se manifestant de façon brutale et intense, mais pendant une période limitée et laissant présager un changement généralement décisif dans l'évolution d'un événement. Toute crise a des impacts importants sur l'activité même de l'organisme touché. Cette définition très générale s'applique tout particulièrement à l'informatique pour les raisons suivantes :

- les réseaux sont interconnectés, donc personne n'est a priori spontanément protégé ;
- les réseaux informatiques sont conçus pour diffuser vite et largement l'information, donc ils propagent dans les mêmes conditions les attaques ;
- la cinétique des attaques informatiques est plus proche de celle d'un accident de voiture que de celle d'une pandémie.

Du fait même de la dépendance de nos organisations aux réseaux informatiques, une attaque pourrait provoquer de façon brutale et intense des dysfonctionnements majeurs dans les domaines de l'énergie, du transport, du commerce, etc. Ainsi, il est possible d'aller d'une imperceptible vulnérabilité de sécurité d'un logiciel à une crise ayant des impacts majeurs sur la société.

De la vulnérabilité à la crise ?

Les systèmes d'information sont au cœur du fonctionnement de notre société et de la vie des entreprises. Ils en constituent le système nerveux dans le sens où ils sont au centre des prises de décisions, et où ils permettent les échanges permanents entre les individus ou entre les organisations. Nous utilisons sans même nous en rendre compte la puissance et la fluidité des réseaux informatiques. Cependant, comme pour notre propre système nerveux, une défaillance du système d'information peut avoir des conséquences considérables pour les organisations : perte de la mémoire, diffusion dégradée de l'information vers des sites de production, incapacité momentanée de transmettre une information, modification ou lecture d'une information, etc. Tous ces symptômes sont connus mais le risque est souvent mal apprécié ou sous-estimé : comme pour notre organisme, nous avons tendance à penser que les accidents sont pour les autres et que notre hygiène de vie nous met à l'abri, jusqu'au moment où cela nous arrive !

En dépit de tous les scénarios annoncés, le lecteur pourrait s'interroger sur une démarche quelque peu paranoïaque de l'auteur en constatant que mis à part quelques virus populaires, aucune des catastrophes annoncées jusqu'à présent ne s'est encore réalisée ! Mais faudra-t-il une catastrophe pour que l'on passe de la prise de conscience à l'acte ?

Lorsqu'une vulnérabilité est découverte sur une application, il est difficile d'en mesurer l'impact. En effet, celui-ci dépend de nombreux facteurs objectifs comme par exemple :

- l'attaque nécessite-t-elle l'action de l'utilisateur (cliquer sur une pièce jointe) ou bien se propage-t-elle automatiquement sur les réseaux ?
- l'attaque est-elle discrète (installation d'un enregistreur de frappes de clavier qui captera ainsi toutes les actions de l'utilisateur) ou bien s'agit-il « simplement » d'une attaque qui détruit des données ?
- l'attaque concerne-t-elle un logiciel grand public ?
- existe-t-il un moyen efficace et simple de s'en protéger ?

En fonction des réponses, il est possible d'apprécier le risque selon que la vulnérabilité provoque une crise ou reste cantonnée à un aspect technique. Toutefois, afin de pouvoir prévenir ce risque, il faut bien évidemment être capable de détecter la vulnérabilité, d'en analyser le profil technique, de la tester, de valider le contournement. Et enfin, de diffuser une information fiable et rationnelle vers les décideurs, les directions des systèmes d'information, les entreprises et le grand public.

Ces compétences existent dans des centres de supervision et d'alerte comme le Centre opérationnel de la sécurité des systèmes d'information (COSSI) de la direction centrale de la Sécurité des systèmes d'information

(DCSSI) qui fonctionne de façon permanente (24h/24 et 7 jours sur 7), depuis mai 2005. Cependant, de tels centres de supervision opérationnelle de la sécurité existent en nombre très insuffisant en France. Ils constituent pourtant une façon efficace de résoudre un incident informatique, d'en mesurer l'impact, de proposer des mesures de protection et de préparer, sinon d'anticiper, les prémices d'une crise sociétale.

Lorsque la crise précipitera des personnes dans les rues, désinformera ou déstabilisera la population, la vulnérabilité technique sera oubliée et seules compteront les conséquences sur le fonctionnement du système nerveux !

Conclusion

La maîtrise de l'information a toujours été un enjeu, et cela bien avant l'ère de l'informatique. Cependant, l'informatique en réseau offre de nouvelles capacités d'attaque. Attaques qui n'ont plus aucune limite géographique et disposent d'un effet de levier considérable par l'interconnexion de millions de machines.

Notre société mondialement interconnectée impose un changement de regard :

- substituer à une culture du problème informatique une culture de management du risque ;
- passer d'une organisation qui répare les pannes à une supervision qui détecte/évalue/protège ;
- intégrer les cyber-crises dans les dispositifs classiques de gestion de crise.

Il ne s'agit pas d'attiser les peurs mais d'inciter les décideurs à prendre conscience de leur dépendance de fait vis-à-vis des réseaux informatiques. La sécurité informatique n'est pas d'abord une affaire de spécialistes au prétexte qu'elle est complexe, c'est une question d'appréciation et de gestion du risque dans le fonctionnement même de nos organisations. Le passage d'une vulnérabilité technique à une crise sera probablement très rapide avec des effets erratiques et imprévisibles. Il s'agira alors de coordonner le temps de l'analyse technique, le temps des procédures judiciaires et des enquêtes, la mesure de l'impact des décisions politiques sur le fonctionnement des sociétés et le temps des médias.

Les attaques informatiques sont classées dans le *Livre blanc* sur la défense et la sécurité nationale parmi les menaces les plus élevées sur notre société. La création d'une agence de la sécurité des systèmes d'information, rattachée au futur Secrétariat général de la Défense et de la Sécurité nationale (SGDSN) a été décidée afin de mieux répondre à ces enjeux. L'agence disposera, à cet effet, de moyens sensiblement renforcés.

Stanislas de MAUPEOU

Cybercrime : jurisprudence de la Cour de cassation

Yves CHARPENEL

La Chambre criminelle de la Cour de cassation, fidèle à son rôle régulateur du droit, a régulièrement l'occasion de rendre des décisions dans le domaine de la cybercriminalité, et ses tendances les plus récentes font apparaître que cinq grandes catégories d'infractions sont plus particulièrement concernées. L'approche de la chambre criminelle dans ce domaine est double : elle veille à assurer la réalité de l'aggravation pénale liée à la cybercriminalité, et elle contrôle strictement l'utilisation des techniques particulières d'enquêtes qu'implique cette forme de criminalité.

Cybercrime: Jurisprudence of the Court of Cassation

The Criminal Section of the Court of Cassation, although carrying out its usual role in the justice system, is regularly called upon to render decisions in the area of cybercrime. The most recent trends in court cases reveal five general categories of typical cybercrimes. The court also has a double responsibility: to assure the severity of penal sanctions for cybercrime and to oversee the use of investigative techniques necessary to the pursuit of this new type of criminality.

Yves Charpenel

Lauréat de la faculté de droit de Paris X et de l'École nationale de la magistrature, rapporteur de la commission de l'informatique du ministère de la Justice, procureur général à Reims et à Fort-de-France, directeur des Affaires criminelles et des Grâces, il est actuellement avocat général à la Chambre criminelle de la Cour de cassation. Il est également expert pour l'ONU et le Conseil de l'Europe en droit et procédure pénale. Il a publié, en 2006, *Les rendez-vous de la politique pénale* aux éditions Armand Colin et, en 2008, *Notre justice pénale* aux éditions Timée.

Juridiction la plus élevée au sein de l'ordre judiciaire français, la Cour de cassation a vocation, depuis sa création en 1790, à veiller à la bonne application des lois. Dans le domaine pénal, c'est la Chambre criminelle de la Cour de cassation qui est chargée de cette mission difficile et, chaque année, l'examen de 9 000 pourvois donne l'occasion à la quarantaine de conseillers et à la dizaine d'avocats généraux qui la composent de passer en revue l'ensemble des dispositions des lois de fond comme de procédure qui forment le champ de la justice pénale. Comme rien de ce qui est juridique ne lui est étranger, il était inévitable que la Chambre criminelle ait à s'intéresser à la mise en œuvre des dispositions légales relatives à la cybercriminalité.

On sait que le rôle de la Cour suprême n'est pas de rejuger le fond des dossiers déjà passés par le tamis des juridictions pénales de premier degré et d'appel, mais de vérifier que la loi a bien été appliquée aux faits qui ont justifié le litige. L'éclairage qu'elle va donner sur la cybercriminalité n'est donc non pas celui du législateur ou de l'acteur de politiques publiques, mais bien celui du juge de l'application de la loi. Elle est, en effet, plus particulièrement chargée de donner aux juges du fond et, au travers de leurs décisions, aux justiciables, qu'ils soient victimes ou auteurs de la cybercriminalité, des règles d'interprétation de la loi destinées à rendre plus sûres les frontières que la loi a voulu à un moment donné fixer entre le licite et l'illicite.

Elle s'efforce ainsi de répondre à l'impérieuse nécessité d'une sécurité juridique raisonnable dans un domaine aussi mouvant, dans les pratiques comme dans les règles du jeu. En effet, le règlement d'un litige particulier est souvent l'occasion, pour la Chambre criminelle, de servir de boussole au juge comme au justiciable pour le traitement d'affaires comparables.

Dans un domaine où la fluidité et le renouvellement des techniques imposent une grande réactivité, les modes et les rythmes de traitement de la Chambre criminelle permettent, en outre, actuellement, de constater que la jurisprudence de la Cour de cassation offre un suivi assez fidèle des évolutions du phénomène de la cybercriminalité. Ainsi les quatre mois, en moyenne, qu'elle passe pour régler les conflits qui lui sont soumis restent compatibles avec la double exigence de son rôle de régulation juridique, suffisamment rapide pour répondre utilement aux questions qui sous-tendent l'existence des procès, et suffisamment longue pour permettre un recul nécessaire par rapport à l'actualité, et mieux distinguer le contingent de l'essentiel.

Naturellement, le découpage analytique traditionnel de la répartition des compétences au sein des quatre sections de la Chambre criminelle (procédure, assises, intérêts civils et affaires financières) n'a pas vocation à intégrer spécifiquement les difficultés juridiques liées à la cybercriminalité, et les différents sujets abordés peuvent être indistinctement traités par toutes ces formations spécialisées. L'utilisation des technologies numériques par des criminels connaît peu de frontières ou de limites, et cette vocation fâcheuse à l'universalité (de territoire comme de domaine d'activité) se retrouve dans le bref panorama des décisions rendues dans ce domaine par la Chambre criminelle. On y trouve, sans surprise, aussi bien des affaires qui montrent le lien entre crime organisé et cybercriminalité que des procédures relevant de la délinquance individuelle. Toutes, cependant, ont en commun de mettre en évidence des atteintes aux biens et aux personnes qui fondent précisément la nécessité d'une lutte persévérante contre toutes les formes de la cybercriminalité ; lutte à laquelle participe la jurisprudence émergente de la Chambre criminelle, à sa façon et à sa place, qui vise la sécurisation des règles, condition nécessaire (à défaut d'être toujours suffisante) d'une action de terrain efficace.

Que la loi soit obscure, ou qu'elle soit simplement mal comprise, c'est à la Chambre criminelle de faciliter, par ses décisions répétées et cohérentes, une connaissance plus acérée des réalités criminelles et des conditions opérationnelles des dispositifs juridiques mis en place pour les combattre. L'examen des décisions rendues depuis ces trois dernières années par la Chambre criminelle sur l'utilisation de nouvelles technologies révèle que la majorité des infractions pouvant être reliées à la cybercriminalité, et dont les difficultés d'application ont justifié un recours devant la Cour suprême, sont relatives à cinq grandes catégories d'infractions.

Différents types infractions

Les infractions au droit de la presse

L'utilisation intensive de l'Internet pour toutes les formes de communication génère logiquement une vaste gamme d'infractions que la loi française a articulée autour d'une dizaine d'incriminations, rappelées dans plusieurs circulaires et présentées pédagogiquement dans un guide méthodologique à destination des procureurs dès 2002.

La Chambre criminelle répète inlassablement, au fil des cas qui lui sont déférés chaque année, quelques principes

élémentaires qui conditionnent l'efficacité du dispositif. L'interprétation stricte de la loi pénale s'applique ainsi au monde de l'Internet, comme le souligne un arrêt du 3 février 2004 qui refuse l'application du texte sur la diffusion de message violent ou pornographique à un mineur quand le message est adressé par erreur à un majeur. De même, un arrêt du 30 mai 2007 applique aux poursuites en diffamation aggravées par la diffusion sur Internet les mêmes exigences dans l'articulation des passages incriminés que pour les infractions commises par voie de presse plus traditionnelle.

D'une manière générale, la jurisprudence s'attache à vérifier que les rigueurs procédurales appliquées aux infractions traditionnelles sont applicables aussi aux cyber-infractions. C'est le sens, par exemple, d'un arrêt du 19 septembre 2006 qui fixe le point de départ de la courte prescription de presse à la date à laquelle un message litigieux a été mis pour la première fois à la disposition des utilisateurs.

La pédopornographie

La répétition des affaires mettant en lumière la diffusion, sur Internet, d'images pédopornographiques a entraîné une succession de décisions de la Chambre criminelle. Citons, parmi les plus significatives, celle du 29 mars 2006 où la Chambre criminelle a rappelé qu'il suffisait de constater l'existence, sur l'ordinateur du prévenu, d'un dispositif d'accès libre à l'Internet (ici un logiciel *peer to peer* classique) pour caractériser l'infraction de diffusion d'images pornographiques de mineur au moyen d'un réseau de télécommunication.

Rappelons également, cette fois dans le sens d'une exigence de rigueur et de loyauté dans le procédé d'investigation, deux décisions ayant censuré des enquêtes qui avaient permis de « traquer », sur Internet, des pédo-internautes, par des méthodes pouvant être considérées comme une provocation. La première décision, en date du 11 mai 2006, invalidait une procédure où le policier s'était fait passer sur Internet pour un mineur en quête de rencontre homosexuelle ; et la seconde, du 7 février 2007, annulait une procédure née d'un renseignement transmis aux autorités françaises par le FBI qui avait identifié un amateur d'images pédophiles en créant de toutes pièces un vrai « faux » site pédo-pornographique.

Le piratage

S'agissant des conséquences civiles du cyber-piratage, un arrêt du 8 mars 2005 avait rappelé que l'existence d'une infraction de captation frauduleuse de programmes télédiffusés, réservés à un public d'abonnés (piratage de TPS), suffisait à légitimer une demande de réparation intégrale du préjudice économique.

Sur le plan pénal, l'administrateur d'un forum privé ayant diffusé sur Internet des logiciels permettant le téléchargement illicite de logiciels de jeux avait été identifié grâce à l'utilisation, par les services de police, d'un fichier informatique des adresses IP des internautes utilisateurs. Un arrêt du 4 avril 2007 a validé le procédé d'enquête dans la mesure où il garantissait, après avis de la Commission nationale de l'informatique et des libertés (CNIL), l'équilibre entre les droits des personnes figurant dans le fichier et ceux des personnes lésées par le piratage.

L'escroquerie

Nouvelle terre d'élection de la tromperie, l'Internet a désormais été intégré aux éléments de caractérisation des manœuvres frauduleuses de l'escroquerie. C'est le sens, par exemple, d'un arrêt du 5 septembre 2007 qui s'intéressait à une escroquerie faisant largement appel au site *eBay* en jouant sur les adresses IP au moment des enchères en ligne. La Chambre criminelle a écarté le moyen des mis en cause qui soutenaient que l'impossibilité pour l'enquête de retracer l'intégralité des opérations informatiques nécessaires aux enchères et aux virements subséquents interdisait de considérer l'infraction comme établie. La cour a ainsi consacré pour les cyber-escroqueries la jurisprudence traditionnelle du faisceau d'indices qui suffit à emporter la conviction du juge.

La contrefaçon

Dans un arrêt du 30 mai 2006, la Chambre criminelle a eu l'occasion de marquer les limites et la spécificité de ce qui est pénalement répréhensible en matière de copie de film téléchargée sur internet ou copiée à partir d'un cédérom, en cassant une décision qui avait relaxé un « téléchargeur » en raison du caractère privé de ces copies, sans avoir démontré le caractère licite de la copie d'origine favorable. Il y a donc infraction pénale quel que soit l'usage de la copie effectuée dès lors qu'elle a été faite sans autorisation des titulaires légitimes des droits.

On le voit, l'intervention de la Chambre criminelle, dans ce domaine, ne se résume pas à l'examen des seules lois qui visent spécifiquement la cybercriminalité et notamment celles relatives à l'Internet, mais aussi les infractions plus classiques qui ont été commises, ou aggravées par l'usage des moyens numériques.

Deux approches complémentaires

L'examen de cette jurisprudence récente révèle deux approches complémentaires de la Chambre criminelle.

La première s'attache à éclairer l'application des lois de fond, elle s'intéresse aux « cyber-infractions », celles qui donnent une nouvelle dimension aux infractions traditionnelles en utilisant l'Internet pour en faciliter la diffusion et se protéger des enquêtes. Dans la logique même de la convention de Budapest [1], notre droit pénal s'est considérablement enrichi pour tenir compte de l'utilisation de l'Internet par les criminels. Le fil conducteur de la Chambre criminelle est ici de veiller à assurer, dans la réalité des condamnations, le facteur d'aggravation que les lois contre la cybercriminalité ont expressément prévu.

La seconde vise à définir les contours juridiques des moyens d'investigations mobilisés contre la cybercriminalité : cyber-enquêteurs contre cybercriminels. La logique de la jurisprudence est, cette fois, la banalisation des cyber-modes d'enquêtes. Elle doit, en effet, faire en sorte que l'utilisation de l'Internet, pour lutter contre la criminalité, respecte le cadre strict des principes qui gouvernent les règles de procédure habituelles.

Au fil de ses décisions, la Chambre criminelle démontre que l'utilisation de cyber-moyens ou la nécessité de combattre les cybercrimes ne changent pas la nature de l'application de la loi pénale, qui se doit de maintenir le délicat équilibre entre l'efficacité de la répression et la défense des libertés individuelles. Elle démontre, par là même, que les méthodes éprouvées depuis deux siècles du contrôle rigoureux de la loi pénale ont su rester pertinentes en abordant les aspects les plus modernes et les plus techniques que l'Internet offre aussi bien au criminel qu'à celui qui le combat.

La complexité et la spécificité de droit pénal de l'Internet passé au filtre de la Chambre criminelle n'ont décidément pas fragilisé l'édifice mis en place sous l'ombre portée de la Cour européenne des droits de l'homme pour prévenir les dérives du « cybermonde ». Elles n'ont pas davantage affaibli le potentiel répressif, soit par un excès de précautions, soit, au contraire, par l'utilisation aventureuse de potentiels techniques. En l'état de ses développements les plus récents, elle offre manifestement à l'institution judiciaire pénale les moyens d'une riposte juridiquement assurée aux usagers malfaisants de l'Internet.

Yves CHARPENEL

....

(1) Adoptée par le Conseil de l'Europe le 23 novembre 2001, la convention incite les États à adopter des mesures pénales précises contre le crime dans le cyber-espace.

Cybercriminalité : l'importance du facteur humain

Daniel MARTIN

© Corbis

La cybercriminalité touche tous les domaines et ne cesse d'augmenter dans tous les secteurs d'activité. Elle vise à la fois les individus, mais aussi les entreprises et les structures gouvernementales qui peuvent se révéler à la fois des cibles, mais aussi des attaquants. Si, à première vue, la cybercriminalité peut paraître essentiellement d'origine technique, il n'en reste pas moins que le facteur humain joue un rôle central dans le passage à l'acte tout comme dans l'organisation des ripostes.

Cybercrime: The Importance of the Human Factor

Cybercrime now involves all kinds of activities. It aims at individuals, but also business enterprises and government agencies – all of which can be either targets or attackers. If at first glance cybercrime seems to be essentially of technical origin, the human factor plays a significant role. After all, humans initiate and respond to cybercrime.

Daniel Martin

Commissaire divisionnaire honoraire, créateur et ancien chef du Département des systèmes d'information de la DST, ancien chef du service de sécurité de l'OCDE et conseiller du directeur exécutif, rapporteur extérieur à la Cour des Comptes, membre du comité des experts du Haut comité français de défense civile (HCFDC), auditeur de l'INHES, éditorialiste à la revue de sécurité *La Lettre SENTINEL*, enseignant dans plusieurs facultés et grandes écoles (ENA, HEC, ESIEE...), président de l'Institut international des hautes études de la Cybercriminalité. Il est également l'auteur de plusieurs ouvrages, notamment aux éditions PUF, *La criminalité informatique*, (Prix AKROPOLIS 1998) et *Cybercrime : menaces, vulnérabilités, ripostes* (2001).

La cybercriminalité est un concept générique qui n'a pas de définition précise internationalement reconnue de tous. On considère généralement que deux grandes catégories d'infractions constituent l'univers de la cybercriminalité : celles où l'ordinateur est l'instrument de la perpétration de l'acte et celles où l'ordinateur est l'objet même de l'infraction ; ou encore, exprimé autrement, ce terme regroupe d'un côté la criminalité spécifiquement liée à l'informatique, de l'autre, les infractions commises à l'aide des nouvelles technologies informatiques.

La cybercriminalité n'est pas récente. Dès qu'un nouveau moyen technique apparaît sur le marché, on constate immédiatement des utilisations déviantes. Les premières générations d'ordinateurs centraux des années 1970 étaient réservées aux programmeurs ou aux comptables doués qui détournaient les « queues de zéro » (les centimes sur les comptes en banque) à leur profit ou encore qui utilisaient, à l'insu de leur hiérarchie, du temps machine à des fins inavouables. L'apparition des réseaux a permis d'ouvrir les possibilités, d'abord à l'intérieur de toute l'entreprise, puis à l'extérieur. Mais la véritable révolution résulte de la conjonction entre le micro-ordinateur personnel et l'avènement d'Internet. On est ainsi passé d'un monde quasi fermé où presque tout était contrôlable à un monde ouvert sans réelle possibilité de maîtrise.

Le constat

La mondialisation des marchés et l'internationalisation des échanges, tout comme la disparition des notions de temps et d'espace due à l'utilisation massive des technologies de l'information et de la communication, associées à la quasi-garantie de conserver l'anonymat sur les réseaux, ont permis l'émergence d'une nouvelle forme de criminalité. On travaille à la vitesse électronique - une transaction peut faire le tour du monde en quelques secondes - et les frontières physiques et matérielles n'existent plus pour les internautes. Autant d'atouts pour les criminels qui trouvent face à eux des services étatiques, police et justice, empêtrés dans les principes de compétence territoriale, de patrimoine national et de souveraineté.

Si on ajoute la standardisation des outils (Windows de Microsoft est installé sur près de 90 % des ordinateurs dans le monde), ainsi que la multiplication des utilisateurs (un milliard de PC en service aujourd'hui, 2 milliards d'ici 2014 avec plus de 270 millions d'ordinateurs vendus en 2007), on ne peut que constater l'extrême vulnérabilité de notre société globale de l'information. Dès qu'une faille apparaît dans un logiciel, et que cette faille est largement diffusée sur le Net, tous les utilisateurs de celui-ci deviennent immédiatement vulnérables et constituent une cible de choix pour tous les pirates potentiels. Tout est disponible sur tout, immédiatement, tout le temps et depuis n'importe où. Les criminels ont compris rapidement l'intérêt de cette nouvelle donne.

Pour compléter le tableau, il faut garder à l'esprit que, depuis la chute du mur de Berlin et la disparition de l'Union soviétique, nos anciens ennemis sont devenus des partenaires et nos alliés des concurrents féroces dans un monde de compétition acharnée où tous les coups sont permis. Les nouvelles technologies de l'information et de la communication (NTIC) participent grandement à ces nouveaux rapports de force. Nous sommes résolument entrés dans l'ère de l'information.

La cybercriminalité, une valeur en hausse

La société de l'information n'est pas sûre. Il suffit de lire la presse pour constater tous les jours que des forfaits sont commis un peu partout dans le monde. Mais il est bien difficile de mesurer l'impact réel de cette criminalité. En effet, les victimes ne se rendent pas toujours compte des attaques subies et lorsqu'elles détectent de tels faits, bien souvent, pour ne pas déclencher une défiance bien compréhensible de leurs clients, elles préfèrent taire leur mésaventure. Les experts s'accordent pour indiquer que le chiffre connu représente à peine dix pour cent de la réalité.

Les statistiques disponibles émanent essentiellement d'études menées dans le monde anglo-saxon. Selon *l'Internet Crime Complaint Center américain*, le coût de la cybercriminalité en 2007 pour les entreprises américaines serait de 240 millions de dollars, en très forte hausse, car multiplié par trois en un an. Pour le *Computer Security Institute* (CSI) qui travaille en étroite collaboration avec le *Federal Bureau of Investigations* (FBI), dans son rapport annuel 2007, la fraude financière constitue le poste de pertes le plus important, suivi par les pertes dues aux virus, vers et spywares, puis les pénétrations de systèmes par l'extérieur de l'entreprise et les vols de données confidentielles. Loin derrière, on trouve les attaques par déni de service, le « phishing », les « bots » ou encore les défacements de sites web.

En réalité, selon certains experts, le cybercrime rapporterait plus que le trafic de drogue au niveau mondial. Tout en présentant beaucoup moins de risques ! Il faut

dire ici que les sommes en jeu sur le Net sont colossales : si le site bien connu d'enchères et de ventes eBay était un pays, il figurerait au 6e rang mondial. De quoi attirer les plus vives convoitises.

L'infosphère, un monde très vulnérable

Les matériels utilisés dans nos sociétés de l'information comportent des failles, tout comme les logiciels et les réseaux qui servent à communiquer et où circulent les données. Ces produits sont le résultat de travaux intellectuels humains qui présentent des failles volontaires ou inconscientes. Par exemple, par commodité, les équipes d'ingénieurs des *operating systems* laissent traîner, dans les versions publiques, des portes dérobées (*back doors*) leur permettant d'intervenir rapidement si nécessaire sur les logiciels. Par ailleurs, périodiquement, les concepteurs de logiciels nous informent de failles qui se révèlent à l'usage et pour lesquelles il faut mettre à jour les versions utilisées sous peine de se voir pirater. Ces failles sont d'autant plus dangereuses que l'information circule très vite sur l'Internet et que les vulnérabilités dévoilées sont exploitées en temps réel par ceux qui passent leur temps à renifler les réseaux et à échanger ces données sensibles.

Des failles sont exploitables à tous les niveaux de nos sociétés de l'information. Au niveau des individus d'abord. Les conséquences touchent tout le monde et pas seulement les utilisateurs d'ordinateurs. Rappelons-nous les avatars subis par les clients de la SNCF en 2004 lorsqu'un blocage total des guichets dans toute la France a provoqué de longues et interminables files d'attente dans les gares ou encore, plus près de nous, quand les réservations de billets en ligne, à partir des bornes en gare, ont été fortement perturbées en pleines vacances de la Toussaint en 2007 et qu'Air France était en grève. Mais, plus grave, les données personnelles qui figurent dans les centaines de fichiers où chacun est répertorié ne sont pas étanches, ni à l'abri de pénétrations. Fin 2006, les fichiers de l'université de Californie de Los Angeles (UCLA) ont été piratés à partir d'une faille applicative. La base informatique contenait les informations personnelles de plus de 800 000 étudiants et enseignants. Selon le *Privacy Rights Clearinghouse* (PRC), ce sont les informations de plus de 100 millions d'individus qui auraient été volées ou égarées rien que pour l'année 2006. Ces données personnelles servent de support à des opérations et fraudes financières liées à l'usurpation d'identité.

Ces failles touchent également les services gouvernementaux qui régissent notre vie en société. Souvenons-nous, l'an dernier, des difficultés rencontrées par les contribuables qui voulaient déclarer leurs revenus en ligne et qui ne parvenaient pas à obtenir le fameux certificat obligatoire pour s'identifier et authentifier leur déclaration. Avec le développement de l'e-administration et l'arrivée du portail unique, la situation sera encore plus sensible. L'exemple récent des attaques contre les sites gouvernementaux de la Lituanie, qui succèdent à ceux de l'Estonie, démontre que le déni de service distribué (DDoS) à mobile politique existe bien et peut conduire à la paralysie d'un pays. Dans le cas de l'Estonie, fin avril et début mai 2007, les sites web du Président, du Parlement, du Premier ministre et de la quasi-totalité des ministères ont été paralysés par une vague d'attaques qui s'est rapidement étendue aux fournisseurs d'accès Internet, à la presse, aux banques en ligne, aux universités. Ces attaques étaient lancées à partir d'un réseau de zombies qui représentait plus d'un million d'ordinateurs répartis sur l'ensemble de la planète. L'ampleur de l'agression a privé un pays entier de l'usage normal des technologies de l'information.

Les entreprises, lieux de production de richesses, constituent, elles aussi, bien évidemment, des cibles recherchées.

Chacun de ces groupes énumérés constitue à la fois une cible mais aussi peut se révéler également un attaquant pour les autres (*cf.* schéma page suivante). Les services étatiques sont attaquables et attaqués par d'autres services étatiques, par des entreprises ou organisations, par des individus isolés ou en groupe. Les individus sont la cible des entreprises, surtout en matière commerciale, mais aussi éventuellement de services gouvernementaux, ce qui pose le problème de la protection des données personnelles et du respect de la vie privée. Ils sont aussi à la merci des individus qui tentent d'usurper leur identité à des fins financières. Les entreprises enfin sont l'objectif où se croisent tous les tirs. Espionnage industriel, vols de données confidentielles, pénétration dans les comptabilités, viol des réponses à appels d'offres, détournement de fichiers et de fonds, contrefaçon, corruption de personnel, etc.)

Un paradoxe préoccupant

Un sondage récent dévoile le pourcentage des entreprises, toutes catégories confondues, qui ne peuvent pas fonctionner sans recours à l'informatique : 40 % ne peuvent se passer d'informatique plus de quatre heures, 10 % plus d'un jour, 20 % plus de trois jours, 30 % plus d'une semaine. C'est reconnaître notre énorme dépendance face aux nouvelles technologies.

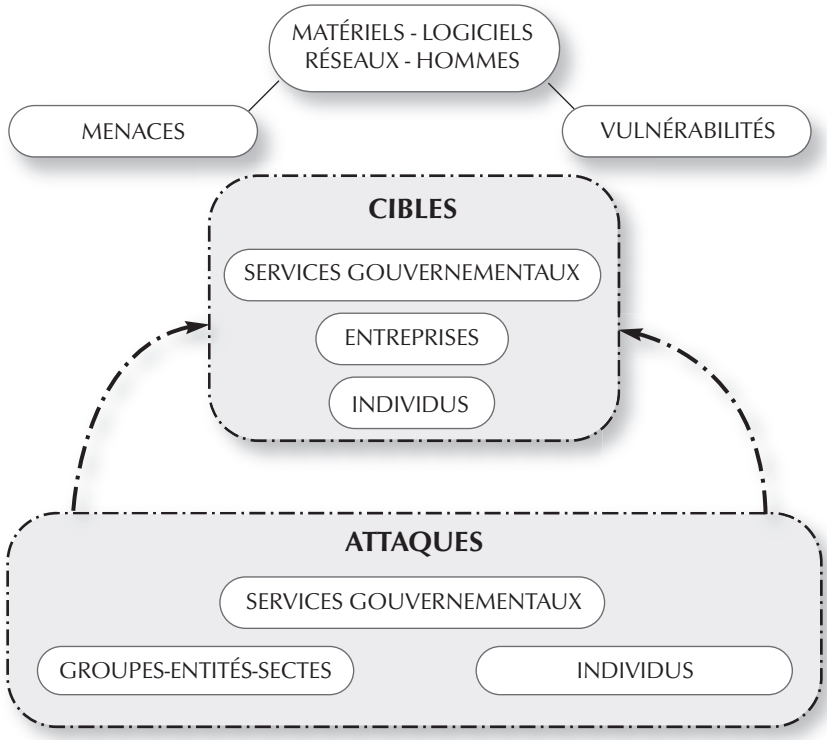


Schéma de principe des attaques et des cibles dans l'infosphère

Or, il ressort que, dans plus de 70 % des cas, la protection de l'information est largement négligée, voire ignorée, que les plans de sécurité et de reprise ou de continuité d'activités brillent par leur absence et que les personnels ne sont ni sensibilisés ni formés. On ne peut donc pas s'étonner si plus de 60 % des PME et PMI touchées par un sinistre informatique important disparaissent dans les trois années qui suivent. Comme pour l'accident, la plupart des chefs d'entreprise pensent que çà n'arrive qu'aux autres. Les paramètres suivants démontrent bien le contraire, car personne n'est à l'abri d'une panne ou d'une pénétration de ses systèmes d'information.

- toute entreprise gère sur ses ordinateurs des fichiers automatisés contenant des informations sensibles ou stratégiques ;
- tout système informatique et ses réseaux comportent une ou plusieurs failles qui permettent de contourner le système de sécurité ;
- toute personne ayant accès au système d'information a vocation à découvrir les faiblesses des dispositifs en place ;
- la probabilité d'utilisation malveillante est inversement proportionnelle aux risques encourus.

Un monde en ... ING ou en ... WARE

Empruntés à la langue anglaise, la plupart des mots nommant les difficultés rencontrées dans l'infosphère se terminent en ing ou ware. Hacking, carding, skimming, phishing, cracking, spamming, spoofing, scamming, snarfing, bluejacking, podslurping, whaling, poisoning, social engineering, mais aussi malwares, spywares et autres formules apparaissent au fur et à mesure que l'imagination humaine décline les opportunités présentées par les nouveaux outils mis sur le marché. Après les ordinateurs et les réseaux, on attaque aujourd'hui les mobiles et les téléphones, la voix sur IP, les smartphones. On se glisse dans les images et les pièces jointes des courriels pour introduire des logiciels espions dans les ordinateurs branchés sur le Net. Rien ni personne n'est à l'abri, surtout que le tout numérique conduit à une convergence entre les données, le son et l'image ainsi qu'à une forme d'uniformisation des outils conditionnant les échanges. Le tout se développant à très grande vitesse.

Le rapport publié dernièrement par F-Secure sur la sécurité montre qu'il y a eu, pour la seule année 2007, autant de virus que durant les vingt dernières années réunies. Concrètement, le nombre total des codes malicieux a augmenté de 100 % en une année pour arriver à un demi-million ! Le même éditeur de sécurité indique, dans

son bilan du premier semestre 2008, que le nombre de virus et autres malwares est en très forte hausse. 900 000 programmes malveillants ont été détectés sur les seuls six premiers mois de l'année. Les techniques employées sont de plus en plus sophistiquées. Aux tentatives de phishing bêtes et méchantes des débuts, qui s'adressaient, en anglais, à des clients français de banques françaises, ou encore dans un français approximatif, pour faire dévoiler aux clients leurs données confidentielles en vue de vider leur compte en banque, ont succédé des attaques beaucoup plus pertinentes et très ciblées, par exemple sur des dirigeants ou individus à haut revenu. Il s'agit du « whaling ».

Après avoir obtenu par social engineering le profil de la victime, le pirate envoie un courriel personnalisé qui incite à l'ouverture d'une pièce jointe pour obtenir plus d'informations. Dès le clic sur le lien, un code malveillant est téléchargé dans le but de découvrir et d'accéder aux informations confidentielles contenues dans l'ordinateur désormais infecté : données bancaires, informations clients par exemple. Depuis le début de l'année, selon les spécialistes de sécurité d'*iDefense*, une des divisions de *VeriSign*, au moins 15 000 personnes auraient été piégées. Elles ont pour certaines perdu jusqu'à 100 000 $. Les cybercriminels ciblent maintenant leurs victimes : elles travaillaient toutes dans des entreprises figurant dans le classement Fortune 500, dans des banques ou cabinets d'avocats. Ces attaques par envoi de courriel représentaient en 2007 plus de trois milliards de dollars.

Pas besoin d'être un spécialiste ou un bon technicien pour effectuer des opérations criminelles sur le Net : des logiciels et données sont disponibles directement, moyennant finance. Le laboratoire de sécurité de G DATA étudie les modèles économiques mis en place par les cybercriminels à travers le monde et nous révèle les tarifs pratiqués : 2 à 25 $ les informations sur les cartes de crédit (prix variables en fonction des données disponibles : code, nom, date expiration). 15 $ pour l'infection de 1 000 systèmes. 25 à 50 $ pour la fourniture d'un million d'adresses e-mail. De 25 à 100 $ par attaque de déni de service (DDoS) avec les dix premières minutes offertes, puis 20 $ l'heure et 100 $ la journée. Les prix peuvent monter de 5 000 à 50 000 $ pour la fourniture d'une faille de sécurité inconnue. Il s'agit bien d'une activité fort lucrative. Les apprentis pirates moins fortunés iront sur les sites d'enchères spécialisés comme WabiSabiLabi où les prix des codes malveillants s'échangent pour 500 euros.

Autre forme de délinquance qu'on ne peut pas ne pas aborder, car nous en sommes tous victimes : le spamming ou envoi de courriels indésirables (les pourriels). On considère que plus de 97 % des messages échangés en France sont des spams. Ces messages utilisent maintenant massivement des images. Plus de 15 milliards de spams image inondent Internet chaque jour. Ce qui prend de plus en plus de place sur la bande passante, encombre les serveurs de messagerie et représente une charge de plus en plus significative pour les services informatiques et le personnel des entreprises. La Commission des Communautés européennes indique que, pour l'année 2006, le coût du pourriel a été estimé à 39 milliards d'euros au niveau mondial. En Europe, le coût a été estimé à 3,5 milliards d'euros pour l'Allemagne, 1,9 milliard pour le Royaume-Uni et 1,4 milliard pour la France.

Mais le vol d'identité numérique ou phishing est le leader des menaces s'étant développées ces dernières années. Une des menaces les plus dangereuses car elle s'adresse directement à notre portefeuille. Tout est bon pour recueillir à notre insu les données, notamment le couple « login-mot de passe » qui permet d'accéder aux comptes en banque et de les vider.

Le facteur humain

Derrière toutes les manifestations de vulnérabilité et d'exploitation des failles, se conjugue systématiquement le facteur humain. Le risque humain reste la faille ultime. Une majorité d'actes de malveillance provient de l'intérieur de l'entreprise. La preuve en est que l'installation de caméras de surveillance au sein d'une entreprise peut avoir pour effet de réduire de plus de 90 % le vol. Il reste que pour les délits informatiques, on considère que plus de 70 % des problèmes sont liés directement au personnel interne ou à la sous-traitance et que, pour le reste, une complicité active ou passive est généralement constatée. On est donc loin du pirate isolé qui, par génie, réussit à pénétrer les ordinateurs et les fichiers les plus secrets. La réalité est bien moins romanesque. Le portait type du pirate des années 1970-1980 a pratiquement définitivement disparu. Le jeune adolescent boutonneux et blanc-bec, qui reste prostré dans sa chambre, en passant la nuit devant son ordinateur, et qui ne rêve que d'exploits en pénétrant les sites les plus prestigieux, a laissé place à des artistes beaucoup plus intéressés et avides d'argent.

Les motivations

Avant tout, c'est l'appât du gain qui est le ressort principal. Très rapidement, les pirates ont compris que leurs connaissances étaient monnayables. Déjà, à la fin des années 1980, les membres du *Chaos Computer Club* de Hambourg avaient proposé leurs services au KGB soviétique

pour pénétrer des sites occidentaux et en extraire les informations les plus secrètes. Les services soviétiques de l'époque ont ouvert la ligne budgétaire de rémunération des sources la plus importante depuis la dernière guerre mondiale, pour couvrir une opération très fructueuse pour l'URSS. C'est avouer tout ce que l'informatique apportait comme progrès au renseignement !

L'idéologie, qui constitue un pilier important du comportement humain, est également très présente dans les motivations des pirates. On aurait pu penser que l'effondrement du communisme et la fin de l'empire soviétique allaient sonner le glas des idéologies motivantes. Il n'en est rien, bien au contraire. L'émergence des sectes et des groupuscules associatifs extrémistes (éco-terrorisme, anti-avortement, anti-vivisection par exemple) a relancé avec énergie les pires turpitudes. Attaques de saturation, prosélytisme de la haine, du racisme et du terrorisme remplissent l'Internet et constituent des exemples à suivre, ainsi qu'une vitrine de diffusion à l'échelle mondiale.

Le sexe reste également, malgré la libéralisation des mœurs, un argument de choix pour contraindre un agent récalcitrant à exécuter une tâche ou un acte qu'il n'a pas envie de faire. Le chantage à la photo truquée numériquement marche encore très bien. Rares sont ceux qui ne sont pas ébranlés lorsqu'on leur présente une photo un peu spéciale prise avec un partenaire mineur, au bon moment. Ils n'ont pas envie de voir ce genre de photo transmise à leur conjoint, chef d'entreprise ou à un journal de grande diffusion. Il ne faut pas chercher plus loin certaines trahisons ou retournements. On peut obtenir ainsi facilement beaucoup d'informations : mots de passe, login, accès à des profils dans l'entreprise, copie de documents, détails techniques, etc.

Mais la reine des motivations reste secrète. On tombe dedans sans s'en rendre compte le plus souvent. Elle fait appel au plus profond de nous, à notre ego. Aviver les jalousies, flatter les orgueils, réveiller la cupidité, engendrer la vengeance, autant de moyens de faire basculer quelqu'un du côté souhaité. Quel pirate n'a pas rêvé d'être le meilleur ? De le faire savoir à la communauté, de gagner beaucoup d'argent sans peine, de satisfaire sa curiosité, de se venger d'un concurrent, d'impressionner ses amis et ses petites amies ? C'est de cette manière que les spécialistes du social engineering font « cracher le morceau » ou « tirent les vers du nez » des personnels non sensibilisés manquant de vigilance.

Dans les services de renseignement, on résume la situation avec une formule lapidaire. Il s'agit de « A.I.S.E. » ou encore de la règle des 3 C. A pour argent, I pour idéologie, S comme sexe et E pour ego. Plus trivialement, on considère que l'adhésion provient de trois sphères : la sphère du raisonnement ou du cerveau (le premier C), la sphère de l'émotion ou du cœur (le deuxième C) et enfin la sphère de l'affectivité physique ou du C... (le dernier C).

Les profils

Pour Isabelle Tisserand, coordinatrice du Cercle européen de la sécurité des systèmes d'information : « *La déviance du cybercriminel défie une autorité symbolique en transgressant les normes d'utilisation d'un système qu'il a ou non compris et intégré (le mécanisme citoyen est inactif). Dans son passage à l'acte, l'auteur satisfait ses pulsions mais répond également à celles encouragées par la structure même de l'Internet. Sur le réseau planétaire, il a en effet tout loisir de combler des pulsions de plaisir, de performance et de pouvoir. Les suprêmes plaisirs du cybercriminel résident - selon les structures psychiques - dans le fait de ne pas être identifié, de ne pas être attrapé (appétence pour les bénéfices de l'anonymat, recherche des limites de l'autorité, évaluation de sa pertinence) ou, à l'inverse, de sortir de l'anonymat de la relation homme-machine pour se faire déifier par les médias et pour ses exploits (délire de toute puissance, satisfactions égotiques)* [1] ».

Traditionnellement, on tente de classer les pirates en catégories, en fonction de leur niveau et/ou de leur degré de dangerosité. En bas de l'échelle, on distingue les simples curieux qui veulent voir comment ça marche. Puis, ceux qui vont chercher sur Internet, via des forums spécialisés, des programmes disponibles et prêts à l'emploi. On trouve aujourd'hui un kit de phishing universel pour environ 1 000 $ clés en main. Ce kit utilise une technique dite « *Man in the Middle* », qui permet au pirate de se positionner entre le client et sa banque pour récupérer toutes informations utiles (codes, mots de passe, etc.). Ces pirates sont généralement méprisés par les vrais techniciens car, en effet, ce qui les intéresse n'est qu'un rapport effort/plaisir favorable.

Dans l'élite des pirates, au sommet de la hiérarchie, on distingue les « chapeaux blancs » ou *White Hats* qui respectent une certaine éthique et qui sont proches des milieux de la sécurité ou des administrateurs réseaux. Ils

(1) « Comprendre les cybercriminels, une démarche analytique et comportementale préalable à toute action », 11 avril 2008, http://www.lecercle.biz/

peuvent venir en aide aux cyber-policiers ou à l'autorité en général. Puis les « chapeaux noirs » ou *Black Hats*, les véritables cybercriminels qui créent les virus, vers ou autres maliciels et qui ne respectent rien. Au milieu, on peut parler des « chapeaux gris » ou *Grey Hats* qui sont un peu entre les deux.

Mais le danger le plus grand est représenté par ce qu'on appelle les crackers qui ne pensent qu'à tirer un bénéfice financier de leurs compétences. Ils sont les cibles des mafias, des cartels de la drogue, du crime organisé, mais aussi des services gouvernementaux qui doivent s'impliquer directement dans la guerre de l'information. Si, dans un premier temps, le FBI procédait à l'arrestation des pirates lors de leur congrès annuel, le célèbre DefCon de Las Vegas ; aujourd'hui, il tente de recruter les meilleurs pour qu'ils deviennent les « *nouveaux guerriers de l'Amérique* ».

De nos jours, selon le rapport *Virtual Criminology* de McAfee, les groupes criminels traditionnels ont de plus en plus besoin de transférer des fonds en grosse quantité sans posséder les connaissances techniques nécessaires. Alors, ils font appel aux jeunes en visant tout particulièrement les universitaires, les clubs informatiques et les forums de discussion. Ils exploitent bien évidemment les réseaux sociaux du Web 2.0. Certains groupes criminels vont jusqu'à payer les études des futurs informaticiens afin de former un réservoir potentiel de travailleurs compétents dans lequel ils n'auront plus qu'à puiser le moment venu (on est tout à fait dans la logique du film *La Firme* de Sydney Pollack dans lequel un jeune avocat est recruté par un groupe mafieux sans s'en rendre compte).

Les victimes

Mais la cybercriminalité ne saurait avoir autant de succès sans la participation, souvent inconsciente, des victimes. Les utilisateurs pèchent par excès de confiance et emploient des technologies sans vraiment avoir pris toutes les précautions nécessaires. Il faut dire que les produits disponibles sur le marché sont très tentants ! Les postes nomades sont commodes et permettent de se connecter depuis n'importe quel point du monde, les clés USB sont formidables de facilité d'emploi, le Wi-Fi apporte un confort exceptionnel, les bornes d'accès dans les gares et aéroports sont merveilleuses. Le problème, c'est que toutes ces technologies présentent chacune des failles si elles ne sont pas parfaitement bien maîtrisées. On se croit à l'abri lorsqu'on utilise un anti-virus, un pare-feux, un anti-spams, un anti-spywares, mais la réalité est telle que ces produits sont rarement mis à jour comme il le faudrait et paramétrés correctement. Des logiciels achetés sur le net à des prix cassés ne peuvent que renfermer de futurs soucis et pourquoi pas des programmes malveillants de type « keylogger » qui récupèrent les frappes de clavier et dévoilent les données sensibles une fois l'appareil relié au réseau. Ils contaminent éventuellement toute l'entreprise et représentent le maillon faible. Il n'y a pas de miracle. Conclusion : ces vulnérabilités ouvrent des brèches au sein des réseaux des entreprises. Login et mots de passe sont si facilement cassables avec les produits disponibles sur le Net qu'on ne peut qu'espérer qu'ils soient correctement composés et modifiés périodiquement.

Si on ajoute que des informations personnelles, souvent complètes, voire sensibles sont volontairement fournies aux divers réseaux sociaux, de type *Viaduc* ou *Facebook*, et exploitables par qui veut bien les consulter, alors on comprend mieux le souci des responsables de la sécurité des informations qui se plaignent de ne pas avoir les budgets utiles pour former et sensibiliser les utilisateurs à ces nouvelles formes de menaces. Dans le monde matériel, le préfet de Police de Paris a lancé il y a quelques années une campagne d'information intitulée : « *Ne soyez pas cambriolables !* ». Cette formule convient également parfaitement bien au monde virtuel. Il s'agit de ne pas faciliter la tâche des pirates par notre propre comportement.

Des ripostes organisées

La niveau international

Sans prise de conscience et harmonisation des cadres légaux applicables au niveau international, la riposte est vouée à l'échec. On pourrait croire que le monde virtuel est comme celui de *Madmax*, sans foi ni loi. C'est une erreur, car en matière de réglementations et de réactions internationales, c'est plutôt le trop plein ! Toutes les organisations en parlent, tout le monde s'en occupe, mais pour quel bilan ?

Le Conseil de l'Europe a été le premier à produire une Convention de lutte contre la cybercriminalité. Ce texte, signé par 30 pays à Budapest en 2001 (dont le Canada, le Japon, l'Afrique du Sud et les États-Unis) n'a pour l'instant été ratifié que par 13 des 27 pays européens et reste non signé par des pays pourtant essentiels comme la Chine, la Russie ou encore l'Inde. Il est entré en vigueur en France en 2006. La Convention présente des avantages substantiels en matière de lutte contre les cybercriminels. Elle liste les infractions retenues (confidentialité, intégrité et disponibilité des données et systèmes, falsification, fraude, atteintes à la propriété intellectuelle, contenus

illicites) et règle des questions clés (conservation rapide des données stockées, divulgation rapide des données de trafic, injonction de produire, perquisitions et saisies de données, collecte en temps réel, interception des données de contenu). Elle renforce la coopération et l'entraide entre les services de police et de justice. Malheureusement, tous les pays n'adhèrent pas et son application reste donc limitée aux pays qui coopéraient déjà entre eux.

L'Union européenne a créé l'*European Network and Information Security Agency* (ENISA) installée en Grèce. Cinquante personnes pour un budget annuel de huit millions d'euros. Qui en a entendu parler ? Quelles propositions traduites dans les faits ?

Les travaux de l'Organisation de coopération et de développement économiques (OCDE) paraissent plus sérieux. L'OCDE s'est intéressée, depuis longtemps, au phénomène des nouvelles technologies de l'information et de la communication. Sans doute parce que cette organisation regroupe les trente pays les plus riches du monde. Son mode de fonctionnement est propice également à l'élaboration de produits concrets. En effet, la règle de l'unanimité entre ses membres fait que quand un texte est adopté, il peut s'appliquer d'emblée. C'est ainsi que les lignes directrices sur la sécurité de l'information, celles sur le développement du commerce électronique, le respect de la vie privée, le cryptage, la corruption et le blanchiment font référence. Son texte intitulé « Vers une culture de sécurité », à travers une approche réaliste, reconnaît que la sécurité est un phénomène mondial qui ne peut pas se soustraire des différences culturelles existantes.

Le G8 est une organisation particulière, quasi informelle et qui ne dispose d'aucun budget particulier, mais qui est indispensable pour donner les orientations, favoriser le développement des échanges, évaluer la menace, favoriser la prévention, organiser la communication pour une meilleure efficacité (création d'équipes formées dans chaque pays et opérationnelles 24/24 et 7 jours sur 7).

L'Organisation du Traité de l'Atlantique Nord (OTAN) n'est pas en reste. Sept pays membres de l'OTAN viennent de décider la création officielle d'un centre d'excellence pour la cyberdéfense à Tallin pour faire suite aux attaques informatiques subies par l'Estonie. Ce centre aidera l'OTAN à prévenir et à contrer avec succès les menaces dans le domaine informatique.

L'organisation *International Multilateral Partnership Against Cyber-Terrorism* (IMPACT) a été créée par le congrès international sur les technologies informatiques (WCIT) pour lutter contre toutes les formes de cyber-menaces en réunissant les représentants des secteurs privés et publics. IMPACT a pour vocation de devenir un centre d'aide et d'assistance international destiné à apporter un soutien aux pays, organisations ou grandes entreprises susceptibles de faire l'objet d'attaques informatiques.

L'Organisation internationale de police criminelle (OIPC INTERPOL) n'est pas en reste non plus, tout comme EUROPOL, pour travailler sur ces domaines. La liste n'est pas exhaustive. On pourrait rajouter l'Organisation mondiale de la propriété intellectuelle (OMPI) ou encore l'Organisation mondiale du commerce (OMC). Que d'énergie perdue, que de moyens redondants ! Toutes ces organisations réparties un peu partout dans le monde œuvrent sur les mêmes sujets sans pourtant communiquer d'une manière efficace, laissant la part belle aux cyber-délinquants.

Le niveau national

Le secteur public

La France dispose depuis longtemps d'un arsenal juridique puissant et adapté pour faire face à la criminalité informatique. Dès 1978, la création de la Commission nationale de l'informatique et des libertés (CNIL) a pris en compte les dangers que peuvent faire courir les NTIC aux libertés individuelles. Dès le début des années 1980, la loi Godfrain a tenu compte des nouvelles infractions susceptibles d'être commises grâce et par ces NTIC. Aujourd'hui, le Code pénal a intégré toutes ces données. De multiples lois sont venues renforcer l'aspect juridique : loi sur la sécurité quotidienne (LSQ), loi sur la sécurité intérieure (LSI), loi sur la confiance dans l'économie numérique (LCEN), loi d'orientation pour la sécurité intérieure (LOPSI), etc.

Une organisation administrative musclée vient compléter ces dispositifs législatifs. Le Secrétariat général pour la Défense nationale (SGDN) abrite la direction centrale de la Sécurité des systèmes d'information (DCSSI) qui a en charge la protection nationale des systèmes et des infrastructures critiques sensibles. En son sein, le Centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques (CERTA) émet des avis et alertes relatives aux attaques informatiques. Pour quels résultats ? En dehors des initiés, qui a entendu parler de ces structures, qui consulte les avis d'alerte émis par le CERTA ? Un manque certain de communication caractérise le système actuel qui perd ainsi une grande partie de son utilité.

Police et gendarmerie disposent de structures spécialisées pour lutter contre le crime informatique. La direction centrale de la Police judiciaire (DCPJ) possède un office

spécialisé : L'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC). La gendarmerie dispose d'un centre spécial au Fort de Rosny-sous-Bois, l'Institut de recherche criminelle (IRCGN). La préfecture de police, une Brigade d'enquêtes aux fraudes aux technologies de l'information (BEFTI). On peut ajouter toutes les structures qui travaillent sur les mêmes problématiques dans les autres ministères (Défense, Economie, Finances et Industrie, à travers les douanes et le Groupe d'action financière (GAFI), Justice) et les commissions interministérielles qui planchent aussi sur le sujet.

Quelle débauche, là aussi, de moyens techniques et humains ! Il est grand temps de réfléchir à une juste mutualisation tant des ressources humaines que techniques, mais aussi à une rationalisation des méthodes et des outils utilisés.

Les personnels sont en nombre insuffisant, certes, mais on pourrait au moins réfléchir à une autre organisation qui mettrait en valeur le potentiel humain. Le *turn-over* est trop important au niveau des troupes spécialisées. On est souvent en présence du syndrome « du stagiaire en transit », car il est très difficile de stabiliser les postes. De plus, les formations et le niveau des rémunérations des fonctionnaires de ce secteur sont trop faibles. Si on ajoute que les échanges « public-privé » sont médiocres, on mesure le chemin à parcourir pour combler le retard face à des organisations criminelles pointues.

Cependant, un espoir réel semble émerger. Lors de la présentation du *Livre blanc* sur la Défense, le chef de l'État vient de clairement indiquer que les menaces informatiques devaient être considérées au même titre que les menaces terroristes, nucléaires et biologiques. Une agence de la sécurité des systèmes d'information va être créée pour répondre notamment à la détection et à la surveillance d'éventuelles attaques. Une nouvelle stratégie qualifiée d'offensive et défensive consistera à riposter en cas d'attaques pour neutraliser les systèmes d'information et de commandement des adversaires. Cette agence devra également informer le grand public via le portail gouvernemental www.securite-informatique.gouv.fr. Même si la marge de progression reste importante, ce premier pas est essentiel.

Le secteur privé

Le niveau de protection est très variable entre les grosses entreprises et les PME-PMI. Les entreprises sont un peu les otages des commerçants de la sécurité. On ne peut que constater la frilosité des investissements de sécurité et de protection, notamment avec pour cause la difficulté d'évaluer les dégâts potentiels dus à un sinistre informatique et donc d'établir un retour sur investissement. Des organisations comme le Club de la sécurité de l'information français (CLUSIF) ou encore le Club informatique des grandes entreprises françaises (CIGREF) donnent des indications précieuses pour les entreprises.

Pour faire face aux nouveaux risques, une entreprise doit être capable de mettre en œuvre des protections de base : identifier ses informations vitales, bien connaître ses responsabilités et engagements et mettre toutes les garanties de son côté. En un mot, être conscient de la situation à tous les niveaux. Un travail de veille est donc absolument nécessaire : veille commerciale (connaissance du secteur), scientifique (suivi des brevets), technologique (innovations), concurrentielle (procédés des entreprises du secteur), stratégique (politique des concurrents), juridique (connaissance des textes), gouvernementale (intentions politiques), etc.

Des questions clés doivent être clairement posées : bien identifier ses correspondants (personnes physiques et morales), authentifier toutes les parties en cause tout au long de la chaîne de traitement, garantir, en toutes circonstances, la confidentialité des données échangées.

Des réponses existent sur le marché pour limiter les risques et les rendre acceptables : recours à la biométrie, au cryptage des données, authentification des serveurs, traçabilité des transactions et aussi, souvent et plus simplement, la réalisation d'un audit peut conduire à réorganiser les structures internes de l'entreprise pour tenir compte des menaces existantes.

Le niveau des citoyens-consommateurs

Au niveau individuel, un manque certain de sensibilisation et de formation constitue une faille énorme et une opportunité certaine pour les délinquants. Les individus sont entre les mains des vendeurs de logiciels et des commerçants de l'informatique. Une fois devant leur machine, les clients sont livrés à eux-mêmes. L'informatique est encore trop hermétique. Acheter des produits de sécurité n'est pas suffisant pour se prémunir des attaques. Une meilleure communication vis-à-vis du public est nécessaire. L'effort doit provenir à la fois du secteur public bien-sûr, mais aussi du privé et des organisations de consommateurs. Toute la publicité doit également être faite autour des condamnations des cybercriminels. Les médias ont un rôle important à jouer dans ce domaine.

Conclusion

Pour faire face, il faut revenir aux principes fondamentaux et à de véritables commandements à respecter scrupuleusement :

- faire simple : ne pas mettre en place des procédures incompréhensibles non maîtrisées ;
- diversifier les défenses : mettre un maximum d'obstacles possibles et une procédure d'alerte dès qu'un élément est violé ;
- point de passage obligé : contraindre les transactions à passer sous le contrôle systématique d'un véritable filtre ;
- défense à tous les niveaux, en particulier établir une charte d'utilisation des outils et vérifier que le personnel y adhère et respecte les consignes, ne pas hésiter à prendre des sanctions en cas de manquement grave, le faire savoir ;
- déterminer le maillon le plus faible ;
- maîtriser l'octroi des privilèges, car le danger vient du manque de connaissance globale des possibilités de chacun ;
- surveiller les pannes, elles représentent un moment propice aux vulnérabilités ;
- avoir une approche globale et non pas point par point sans véritable cohérence ;
- bien choisir ses partenaires, la sous-traitance peut constituer une faille comme les fournisseurs ou la maintenance.

Enfin, on veillera systématiquement à mutualiser les moyens (matériels et humains), à harmoniser les méthodes et les outils en faisant travailler ensemble secteur privé et secteur public, sans omettre les associations de consommateurs. Il faudrait sensibiliser et former sans discontinuer, accepter de s'évaluer en permanence, appliquer les meilleures pratiques, améliorer les échanges et la connaissance, en un mot, communiquer et faire savoir.

Le sujet de la cybercriminalité est planétaire. L'examen de la situation tend à démontrer que les criminels ont encore de beaux jours devant eux car la coopération internationale et l'harmonisation judiciaire, qui seules pourraient mettre un frein sérieux à la prolifération de la cybercriminalité, sont encore loin d'un niveau opérationnel efficace. Malgré les efforts de certains, notamment ceux des services publics, les initiatives semblent trop dispersées et insuffisantes. Les entreprises ne consacrent pas non plus assez de moyens à la prévention dans ces domaines techniques qui rebutent les financiers. Elles ne semblent pas encore avoir pris conscience de la sécurité à accorder à l'information.

Il reste à espérer que la récente création de la direction centrale du Renseignement intérieur (DCRI) apportera un souffle nouveau à la sensibilisation des entreprises qui constituent le véritable patrimoine de notre pays. De la même manière, le fait que le *Livre blanc sur* la défense souligne, enfin, qu'à côté des risques nucléaires, radiologiques, bactériologiques et chimiques, le risque informatique, qui a pénétré toutes les couches de nos sociétés, en particulier nos infrastructures critiques, constitue une priorité. C'est une indication forte qui montre le bon chemin. Mais ces louables principes ne pourront conduire au succès que si nous sommes tous directement concernés et si nous savons utiliser les moyens mis à notre disposition.

Lutter contre la cybercriminalité, c'est l'affaire de tous et pas seulement des spécialistes. Le facteur humain est déterminant comme souvent, pour ne pas dire toujours. Trois mots seulement sont à retenir pour faire face : intelligence, anticipation et vigilance. Car comme le disait Napoléon : « si se faire battre est excusable, se faire surprendre est impardonnable ».

Daniel MARTIN

Webologie

http://

www.f-secure.fr
www.ssi.gouv.fr/dcssi
www.gocsi.com
www.wikipedia.fr
www.verisign.fr
www.symantec.fr
www.wslabi.com
www.defcon.org
www.fr.mcafee.com
www.enisa.europa.eu
www.europa.eu/index
www.oecd.org
www.interpol.int
www.wipo.int
www.cnil.fr
www.sgdn.gouv.fr
www.melani.admin.ch
www.blackhat.com
www.nato.int
www.prefecture-police-paris.interieur.gouv.fr
www.clusif.asso.fr
www.cigref.typepad.fr
www.wto.org

Cybercriminalité : la recherche de profits

Myriam QUÉMÉNER

© Corbis

La délinquance économico-financière sur Internet prend désormais une importance croissante et constitue un fléau auquel les États doivent faire face de façon pertinente. La motivation principale des pirates est la recherche de profits, et la cybercriminalité, délinquance transnationale par excellence, est devenue une activité délictueuse des plus lucratives, qui permet de blanchir plus facilement l'argent issu de la criminalité classique. Il s'agit de cerner cette population de cyberdélinquants et leurs divers modes opératoires.

Cybercrime: The Profit Motive

The financial and economic delinquency of the internet have taken on a growing importance that has become a scourge that governments must deal with as effectively as possible. The principal motivation of hackers and cybercrime has become profit – the ultimate transnational delinquency which has become one of the most lucrative types of scams. It allows the easy laundering of money made by traditional criminal activities. It has become essential to better understand the various modes of operation of this kind of crime.

Myriam Quéméner

Magistrat depuis 1986, substitut général au service criminel de la Cour d'Appel de Versailles après avoir été précédemment sous-directrice à la direction des Affaires criminelles et des Grâces. Elle participe comme expert à des séminaires internationaux organisés par les ministères et le Conseil de l'Europe sur la cybercriminalité. Elle a écrit plusieurs articles sur la cybercriminalité et publié avec Joël Ferry, en 2007, *Cybercriminalité, défi mondial et réponses* aux éditions Economica.

La cybercriminalité n'a rien de virtuel et tend aujourd'hui vers le crime organisé en parvenant à manipuler des sommes d'argent colossales. L'objectif des actions malveillantes est essentiellement lucratif, et la cybercriminalité est, désormais, structurée et essentiellement guidée par la recherche de profits importants en prenant peu de risques. Une enquête auprès de 2000 sociétés a révélé que la cybercriminalité coûte, en moyenne, 24 000 dollars par an à une entreprise américaine, soit 67 milliards de dollars à l'échelle des États-Unis. Le coût de la fraude, 2,7 millions d'euros en moyenne, reste élevé et, dans 41 % des cas, il s'accompagne d'autres dommages comme l'atteinte à l'image de l'entreprise.

Organisation des cyberdélinquants

La cybercriminalité est devenue l'affaire de professionnels et non plus le fait d'agissements d'étudiants en informatique ou d'amateurs. La recherche d'argent est le moteur essentiel de ces individus dont les activités sont désormais bien délimitées.

Les « hackers » ou pirates informatiques représentent l'ensemble des cybercriminels et sont, comme au niveau de la criminalité organisée, répartis en catégories spécialisées. Depuis quelques années, les hackers ont même leur rendez-vous européen [1], à savoir une conférence de haut niveau où se réunissent les meilleurs d'entre eux pour s'informer et échanger sur les techniques les plus innovantes.

Le « cracker » ou « chapeau noir », souvent confondu avec le hacker, pénètre les systèmes informatiques avec l'intention de nuire, et, en général, il essaye de tirer profit de ses méfaits, par exemple, porter préjudice à un concurrent, en acquérant des données confidentielles. Ils fonctionnent généralement comme des réseaux mafieux, pour leur propre compte ou le compte d'autrui. Souvent très performants techniquement, ils peuvent égaler les compétences des hackers et leur but est de maximiser cette connaissance à leur profit.

Certains jeunes commencent leur carrière dès l'adolescence. Dénommés « script kiddles », ils manipulent les ordinateurs sans mesurer les conséquences de leurs actes et constituent la main-d'œuvre de base. Âgés de 15 à 20 ans, les « kids » circulent sur les forums, achètent des listes de spams qu'ils revendent ensuite, et parviennent à se faire un peu d'argent en négociant des éléments utilisés pour commettre des fraudes. On trouve, par exemple, ce type de jeunes en Ukraine. Ils sont la vraie « main-d'œuvre » en la matière. Ce trafic leur génère des revenus mensuels modestes et ils se font parfois « arnaquer » eux-mêmes.

Les « codeurs » ont une expérience supérieure à cinq ans dans le monde des hackers. Âgés de 20 à 25 ans, ils ont un rôle de programmeurs professionnels et sont parfois autodidactes. Ils vendent généralement des outils prêts à l'emploi comme des « bots » faits sur mesure, ou des chevaux de Troie.

Les « drops », sensiblement plus âgés que les kids, jouent un rôle incontournable dans la cybercriminalité et transforment l'argent « virtuel » en vrai argent. Ils offrent aux criminels l'opportunité de transférer l'argent volé sur leurs propres comptes en banque. Une fois l'opération effectuée, ils gardent un pourcentage, généralement de l'ordre de 50 % des montants transférés. La condition essentielle pour devenir un drop, mis à part le fait d'avoir un compte en banque, est de résider dans un pays ne réprimant pas les délits numériques comme, par exemple, l'Indonésie, la Malaisie et la Bolivie. Cette organisation démontre que les délinquants profitent des « cyberparadis » et pose le problème de la nécessité de créer une législation mondiale de lutte contre la cybercriminalité.

Une « mule » est une personne utilisée pour transporter des objets illicites telles des armes ou- de la drogue, et ce, parfois à son insu. Sur Internet, les mules sont recrutées par e-mail pour « transporter de l'argent » contre rémunération, l'objectif du fraudeur pouvant être le vol, le détournement d'argent, le blanchiment d'argent, etc. Pour la recruter, le pirate abuse un internaute qui se rend ainsi complice d'une fraude, de vol, de détournement ou de blanchiment d'argent passible de poursuites. Les cyberdélinquants envoient, par exemple, des e-mails proposant de devenir le collaborateur d'une prétendue société financière internationale. Parfois, un pseudo-contrat de travail est joint pour rendre l'offre plus crédible. Il est indiqué à l'internaute qu'il recevra des fonds sur son compte bancaire et qu'il devra les transférer vers un autre compte. En tant qu'intermédiaire, il percevra une commission pouvant aller jusqu'à 3 000 euros par mois via *Western Union*. Le cyber-escroc utilise donc un autre compte pour faire transiter cet argent d'origine frauduleuse et le transfère dans un autre pays. Les mules sont ainsi utilisées pour brouiller les pistes d'analyse d'une fraude et rendre beaucoup plus difficile, voire impossible la

(1) *Cf.* « black Hat Europe 2008, le rendez-vous européen des hackers », revue *Mag Securs*, avril-juin 2008.

récupération des fonds. Le risque pour la personne servant de mule est d'être mise en examen pour complicité de fraude et poursuivie pénalement.

Certaines mafias ont également investi ce domaine, ce qui permet d'affirmer que la cybercriminalité est une délinquance commise en bande organisée. Cerner l'ampleur de l'implication des mafias n'est pas chose aisée, même si de fortes présomptions existent et des certitudes concernant l'action des mafias [2], par exemple en Roumanie, qui sont spécialisées dans le domaine du « carding ». Le piratage des systèmes bancaires est très souvent le fait d'organisations criminelles organisées, souvent d'Europe de l'Est.

En effet, de nombreux groupes criminels ont très vite compris que l'anonymat et la liberté que procure Internet permet assez facilement des opérations de blanchiment d'argent et, à cet égard, le domaine des jeux en ligne est un terrain très lucratif.

L'utilisation facile de « e-gold » en a fait un moyen de paiement universel. E-gold possède aussi trois caractéristiques essentielles pour les cybercriminels, à savoir l'anonymat car il est possible d'ouvrir un compte e-gold en moins d'une minute ; l'absence de vérification ; et enfin aucune obligation de donner une adresse e-mail valide. D'autres devises électroniques sont aussi largement utilisées dans les échanges entre criminels Web, mais e-gold est la référence en matière de transactions entre les cyberdélinquants. Il s'agit des transferts offerts par *Money Gram* ou encore *Western Union* qui sont irréversibles, quasiment anonymes et traversant les frontières presque instantanément puisque, même si, en théorie, une pièce d'identité est exigée pour recevoir l'argent liquide, en pratique, les bureaux dans certains pays ne font pas de vérifications.

Il existe des sites sur lesquels il est possible d'acheter des objets avec une carte volée, appelés sites « cartable ». Ces sites sont des magasins « on-line » qui n'exigent pas que l'adresse de facturation et de livraison soit la même. Ainsi, les criminels achètent des marchandises on-line, les font livrer aux drops qui les leur retournent, et, ensuite, la marchandise est vendue sur des sites aux enchères en ligne.

Voilà un scénario typique pour de l'extorsion en ligne : une compagnie qui fait de la vente sur Internet reçoit un e-mail menaçant. Elle doit payer 10 000 dollars sinon son site Internet serait estropié. La compagnie ignore le mail et, quelques jours après, son serveur bloque, ce qui entraîne des pertes d'argent considérables. Ensuite, arrive un deuxième mail, cette fois-ci demandant 40 000 dollars. En cas de non-paiement, la compagnie risque encore des pertes. En revanche, si elle paie, on lui offre généreusement une protection pendant un an. Après avoir fait le calcul, la compagnie paie.

La criminalité en ligne agit de façon plus mobile que jamais. Ainsi, le « phishing », qui semblait trouver sa source pour 60 % dans des organisations russes piratant des sites européens au cours du premier semestre 2007, s'est tourné vers la Chine pour installer ses activités en ligne au cours du second semestre. Les pays peu protégés ou mal équipés sont les premiers visés. Le Pérou fournit ainsi 9 % des attaques en ligne contre les vingt-cinq pays les mieux équipés en haut débit, alors que 80 % de ses internautes utilisent des cybercafés. Le marché de la piraterie informatique existe désormais. Par exemple, pour faire envoyer 20 millions d'e-mails indésirables, le tarif est de 314 euros et la location d'un serveur permettant d'envoyer 74 millions de spams chaque mois coûte 396 euros [3].

On assiste aujourd'hui à la banalisation des outils de piratage qui sont désormais accessibles à presque tous les pays. Ce commerce est considéré comme plus rentable que celui du trafic des stupéfiants et souvent moins risqué. Des sites vendent d'ailleurs des kits de piratage pour la somme de 10 dollars et de phishing pour 5 dollars par exemple [4]. Ils facilitent la mise en ligne de sites Internet frauduleux, calqués sur des sites véritables tout en gérant l'envoi massif de courriels incitant les internautes à se connecter aux fausses pages afin de récupérer le plus de données. Les experts en cybercriminalité de l'*Internet Security System* d'IBM [5] ont ainsi découvert qu'il était possible de louer les services d'un réseau d'ordinateurs infectés par un programme malveillant dénommé Botnet, constitué de 150 000 PC, pour la somme de 350 $ par semaine. Il apparaît que les tarifs dépendent souvent de la taille de ce réseau et il faut compter un minimum de 100 euros pour quelques heures. Ainsi, des cybercriminels

....

(2) *Cf.* Guillaume Lovet, « L'argent sale sur le net : les modèles économiques des cybercriminels », *Revue de la Défense Nationale et Sécurité Collective*, mai 2008.

(3) *Cf.* Gerric Poncet, « les tarifs de la cybercriminalité », en date du 2 juillet 2008, site : www.lepoint.fr

(4) Voir la revue Mag Securs, n° 18, p. 33, interview de Guillaume Lovet.

(5) *Cf.* le blog de la *X-Force Intelligence*.

peuvent le louer pour mener une opération de spams. Leur but est de saturer les serveurs de messagerie des grandes entreprises sous l'importance du trafic. Par exemple, pour un tarif variant de 2 à 25 $, le pirate peut fournir des informations de carte de crédit, le prix étant fonction des informations disponibles tels le code, la date d'expiration, le nom du propriétaire...).

Actuellement, des boîtes à outils informatiques vendues sur le marché noir de la criminalité diffusent deux nouvelles tendances, à savoir la modification furtive des navigateurs et la transformation discrète des pages Internet par phishing. D'autres moyens de piratage circulent sur la Toile et permettent de constater que tout se vend sur Internet comme les numéros de carte de crédit facturés environ entre 0,5 et 5 dollars pièce ou les coordonnées bancaires entre 30 et 400 dollars.

Depuis deux ans environ, une véritable économie souterraine consistant à faire commerce des failles de sécurité et de kits de « malwares » (logiciels malveillants) s'est développée en raison de son caractère lucratif. Il existe même des bourses aux échanges, véritable marché noir où non seulement les failles de sécurité, mais également les informations collectées, tels les numéros de sécurité sociale ou de passeport, les adresses électroniques et physiques peuvent se monnayer au cours du jour. Il s'agit d'activités qui démontrent à l'évidence la créativité des cyberdélinquants qui adaptent sans cesse leurs modes opératoires, qui se diversifient et évoluent constamment.

Typologies des cyberfraudes

Le « carding » est le piratage de cartes bancaires par diverses techniques matérielles, logicielles ou subversives aux fins d'obtenir et de revendre les données de cartes bancaires, de s'en servir pour effectuer des achats frauduleux, au préjudice du porteur légal. Le carding se décline en trois étapes, à savoir le « coding », qui n'est autre que le piratage des données, le « vending » ou revente des numéros de cartes bancaires et des informations sur le titulaire, enfin, le « cashing » qui regroupe les échanges financiers délictueux comme les escroqueries et le blanchiment d'argent. Une fois ces informations récupérées, il s'agit de les monnayer discrètement. Pour ce faire, de nombreuses sociétés de ventes commerciales virtuelles voient le jour afin de générer de faux achats mais de véritables transactions.

Le « skimming » est une criminalité essentiellement d'Europe de l'Est, en particulier de Bulgarie et de Roumanie. Il s'agit du piratage de distributeur automatique de billets (DAB), à l'aide notamment de faux claviers et de micros-caméras. Le nombre de ces attaques ne cesse de croître ; ainsi 520 distributeurs ont été piratés en 2006, contre 200 en 2005 et 80 en 2004. À l'heure actuelle, les banques réagissent, et ce type d'affaire devrait progressivement diminuer.

Le « spamming » [6] désigne l'envoi massif et automatique de messages électroniques non sollicités, généralement adressés à des fins publicitaires, voire frauduleuses. À l'heure actuelle, leur part est évaluée à plus de 80 % du trafic e-mail total [7] et 16 milliards de spams seraient envoyés chaque jour en Europe. Les spams peuvent être de simples publicités, mais aussi des messages émis par des virus et les propageant, des incitations à visiter des sites frauduleux qui capturent des informations confidentielles.

Des formes dérivées de spamming se sont développées ces dernières années, surnommées « arnaque à la nigériane » ou fraude 4-1-9 [8], qui ont pour objectif d'abuser de la crédulité des internautes en utilisant les messageries électroniques pour leur soutirer de l'argent. Cette tromperie repose sur un envoi de mails visant à faire croire à la victime que l'expéditeur possède une importante somme d'argent comme des fonds à placer à l'étranger suite à un changement de contexte politique et fait part de son besoin d'utiliser un compte existant pour transférer cet argent. Pour crédibiliser le scénario, les fraudeurs mettent en place de faux sites bancaires qui usurpent l'identité d'établissements internationaux. Ces derniers visent à faire croire aux victimes que l'argent promis existe réellement.

Les réseaux sociaux constituent le nouveau moyen de diffusion des « scams » nigérians « 419 ». Ce phénomène a été observé pour la première fois par les chercheurs des laboratoires *BitDefender* sur le site Internet de réseaux professionnels *LinkedIn*, mais d'autres sites de réseau sociaux peuvent également en être la cible. L'email de scam est envoyé sous la forme d'une invitation qui est un

(6) Ou « pourriel », terme choisi en référence à un célèbre sketch des Monty Python, troupe comique britannique, parodiant une publicité radiophonique pour le Spam, une sorte de jambon épicé, pendant laquelle la marque Spam était répétée à de multiples reprises.

(7) Source : direction du Développement des médias.

(8) Fraude dénommée 4-1-9 en référence à l'article du Code pénal nigérian interdisant cette pratique.

moyen par lequel un utilisateur demande à être ajouté au réseau social d'un autre utilisateur. Cette requête est appuyée par une page de profil construite qui semble authentifier la demande de mise en relation du fraudeur. Ces messages ne pouvant être envoyés que par les titulaires de comptes du réseau social en contournant complètement les filtres antispams.

Cette nouvelle forme du procédé de scam 419 est plus dangereuse que les précédentes, car les probabilités de se faire piéger pour les utilisateurs du réseau sont beaucoup plus importantes puisqu'ils utilisent cet outil pour développer leurs affaires ou leur carrière, et ont donc tendance à lui accorder une confiance implicite. Le réseau social ne vérifie en aucune façon l'identité des personnes s'inscrivant sur le site, ce qui peut parfois donner lieu à des dérapages comme, par exemple, lors d'un incident récent où des sites pornographiques ont ajouté des pages utilisateurs « sur mesure » sur le réseau social de manière à améliorer leur référencement sur les moteurs de recherche. L'envoi de spams nombreux peut donner lieu à des poursuites sur la base de la loi Godfrain.

Le phishing [9] et le « pharming » [10] sont deux techniques permettant de faire croire aux victimes qu'elles se trouvent sur un site Web sécurisé, leur banque par exemple, alors qu'elles sont en fait sur un site Web factice où leurs informations bancaires vont leur être dérobées. La première utilise le spam pour attirer leur victime sur un faux site. La seconde consiste à rediriger les victimes vers le faux site Web alors qu'elles ont bien tapé une adresse Web correcte dans leur navigateur.

Si les banques anglo-saxonnes ont été les premières cibles des cyber-escrocs, désormais tous les établissements bancaires européens sont visés, et 90 % des attaques par phishing concernent des établissements financiers. Ces cyber-escrocs peuvent récupérer jusqu'à 400 fois la mise initiale [11]. Plus ou moins discrète en ciblant l'humain, elle est actuellement en forte progression, mais pour le moment très peu d'informations concrètes, de cas d'attaques sont disponibles, car les entreprises sont particulièrement réservées sur ce sujet, n'osant évoquer qu'elles puissent en avoir été victimes. C'est une technique de fraude qui vise aussi bien les particuliers que les entreprises et le secteur bancaire. Les forums de phishing représentent un marché pour les acheteurs et vendeurs d'informations financières volées. Les acheteurs peuvent être aussi bien des individus que des organisations criminelles.

Pour 100 000 mails, envoyés, les pirates récoltent environ vingt comptes bancaires à soldes différents. Par la suite, ils peuvent, soit vendre l'information pour une valeur entre 100 $ et 500 $ par compte, payable par e-gold, soit transformer l'argent virtuel en vrai argent via les drops. Évidemment, la deuxième solution rapporte plus, mais elle comporte plus de risques aussi - il s'agit de trouver un drop à qui on fait confiance.

Ce sont des manifestations de la criminalité organisée, et ces techniques, qui peuvent être qualifiées juridiquement d'escroqueries en bande organisée [12], sont souvent traitées par les juridictions interrégionales spécialisées (JIRS). Elles peuvent également être sanctionnées sur le fondement de l'infraction de collecte frauduleuse de données nominatives en application de l'article 226-18 du code pénal [13]. Car, au final, le pirate se procure des données personnelles et les traite de manière frauduleuse informatiquement.

Des escrocs utilisent également le téléphone portable pour tenter de récupérer les identifiants bancaires de leurs victimes. Par exemple, un SMS envoyé sur le téléphone mobile des victimes confirme leur inscription à un site payant de rencontre sur Internet alors qu'elles n'ont rien demandé. Pour ne pas payer, le SMS leur demande d'annuler l'inscription en se connectant à un site Internet qui est, en fait, un site pirate qui va installer un cheval de Troie à leur insu et voler des informations personnelles, comme les identifiants bancaires.

Désormais, on assiste aussi à l'exploitation des réseaux sociaux comme *Facebook* ou *Linked-In* par des cyber-criminels. Ces réseaux, qui concentrent une quantité phénoménale d'informations personnelles, permettent de rassembler suffisamment d'éléments pour se substituer à l'identité des utilisateurs. Le détournement de l'identité d'un individu, la récupération d'éléments à caractère personnel vont ensuite leur servir pour se faire passer pour un autre afin de commettre des délits, des achats avec des moyens de paiement usurpés.

....

(9) Contraction des mots anglais *phreaking*, fraude informatique et *fishing* (pêche) se traduisant parfois en « hameçonnage, filoutage ».

(10) Le terme pharming provient de la contraction des mots anglais *farming* et *phone phreaking*, qui pourrait se traduire par « piratage de lignes téléphoniques ».

(11) *Cf.* Guillaume Lovet, *op. cit.*

(12) Article 312-2 du Code pénal.

(13) Cette infraction est punie de cinq ans d'emprisonnement, et de 300 000 euros d'amende.

Ce « business parallèle » est difficilement mesurable, mais il ne cesse de se développer depuis plusieurs années, ce qui démontre l'existence d'un « marché ». Ce type d'arnaque joue sur la curiosité, la naïveté ou l'appât du gain des internautes. Le client est informé qu'il ne faut jamais laisser ses coordonnées sur le réseau. Il est le principal artisan de sa sécurité. Par ailleurs, les procédés évoluent et sont de plus en plus rusés, des cyberdélinquants font, en effet, du prosélytisme en matière de sécurité. Ainsi, de récents courriels frauduleux, très convaincants, mettent en garde les clients de banques contre le filoutage, rappelant que les banques ne demanderont jamais de détails sur un compte par courriel, et les invitant à signaler tout message suspect. Mis en confiance par ces avertissements, le client va être tenté de cliquer pour signaler le site et c'est alors que la victime va être redirigée vers un site frauduleux.

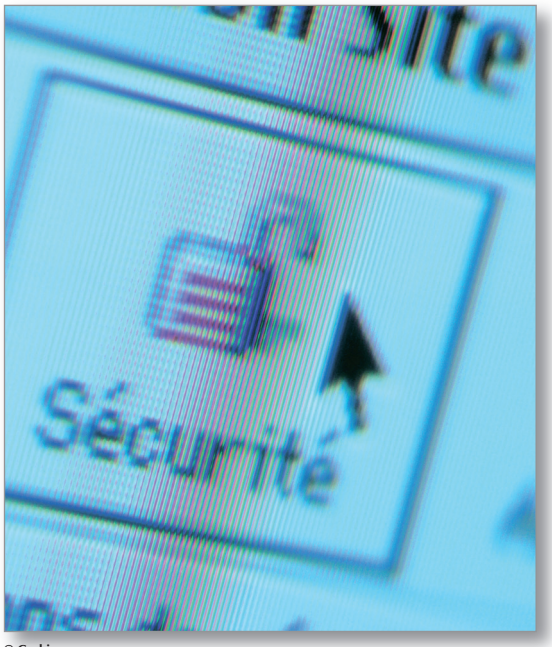
En conclusion, on comprend aisément que la lutte contre la cybercriminalité implique une mobilisation sans faille de l'ensemble des acteurs et un renforcement de la coopération internationale. Les données circulent à la vitesse de la lumière et sont difficiles à pister. La cybercriminalité pose de nombreux défis et dans le « cybermonde » qui évolue sans cesse, les services de police et de justice luttant contre la cybercriminalité doivent mettre en place des stratégies d'anticipation des menaces et de répression au risque de mettre en péril les internautes et de freiner le développement de la société du numérique.

Myriam QUÉMÉNER

Sécurité des systèmes critiques et cybercriminalité :

vers une sécurité globale ?

Walter SCHÖN



© Corbis

Cet article se propose de mettre en perspective, pour les systèmes informatiques dits « critiques », les problématiques de résistance à la cybercriminalité, et de faculté à éviter des comportements catastrophiques suite à des événements d'autre origine, pouvant être des défaillances internes des composants matériels, des perturbations de l'environnement, voire des fautes humaines involontaires dans la conception ou l'exploitation du système. De manière assez fâcheuse, la langue française désigne les deux problématiques par le même mot « sécurité », traduisant, de fait, les deux mots anglais *security* et *safety*. La sécurité de systèmes informatiques modernes communicants, comme on peut en trouver, par exemple, dans les systèmes de signalisation ferroviaire récents, rend d'ailleurs incontournable la maîtrise conjointe de la *safety*, (parfois appelée sécurité innocuité) et de la *security* (parfois appelée sécurité confidentialité) pour atteindre une « sécurité globale ».

The Security of Critical Systems and Cybercrime: Toward Overall Security?

It is necessary to consider our ability to avoid catastrophic behavior that threatens critical information systems following events such as internal flaws in material components, environmental disturbances or even involuntary human error in the conception and operation of systems. Unfortunately, in French the same word, securité, is used to cover two different problematics – what in English is expressed in two different words: security and safety. The interconnected modern information systems, such as rail traffic signals, point out the need to deal in an overall way with both security and safety.

Walter Schön

Ancien élève de l'École normale supérieure, agrégé de physique et docteur d'État en physique de la matière condensée. Il a été, entre 1989 et 1998, responsable adjoint des Départements d'études systèmes et sûreté de fonctionnement d'Alstom Transport et Matra Transport, où il a participé à la constitution des dossiers de sécurité de systèmes embarqués critiques appliqués au transport ferroviaire. Depuis 1998, il est professeur dans le Département génie informatique de l'université de technologie de Compiègne où il enseigne le génie du logiciel, en particulier le logiciel critique pour les transports, ainsi que la cryptographie avancée dans les enseignements de sécurité informatique.

Cet article aborde la problématique des systèmes informatiques dits « critiques », dont un dysfonctionnement, quelle qu'en soit l'origine, peut avoir des conséquences graves en termes de dommages aux personnes, aux biens et à l'environnement. La problématique de la cyber-délinquance, de la cybercriminalité, voire du cyber-terrorisme ne peut, en effet, plus se limiter aux intrusions passives ou actives à des informations utilisées par la suite pour mener des actions de terrorisme « classique » (par exemple). À l'ère où nos avions, trains, voitures, centrales de production d'énergie sont contrôlés et commandés par des systèmes informatiques qui communiquent de plus en plus, il faut impérativement avoir réfléchi à la problématique de l'intrusion malveillante dans ces systèmes à des fins criminelles ou terroristes. Il doit, par conséquent, être plus difficile de provoquer une catastrophe technologique par des moyens informatiques que par des moyens « classiques ». Cet article se propose de montrer que les techniques de couverture des dysfonctionnements « accidentels », classiquement mises en œuvre pour les systèmes critiques, ne sont pas si éloignées de celles permettant la couverture des dysfonctionnements dus à la malveillance humaine. La possibilité de ces dernières peut amener simplement à mener certaines techniques avec une rigueur accrue (la cyber-malveillance étant donc dans ce cas également couverte). Dans certains cas, une extension est nécessaire car la technique ne couvre, à la base, que les événements « accidentels ».

Des fautes, des erreurs et des défaillances incluant l'intention de nuire

Selon une terminologie maintenant normalisée, les comportements indésirables pouvant affecter les systèmes industriels (y compris les systèmes informatiques) sont désignés par le vocable défaillance, que le dictionnaire définit comme l'arrêt du fonctionnement normal, et les normes internationales applicables au domaine comme la cessation de l'aptitude à effectuer une fonction requise. Il convient donc de souligner, à ce stade, que l'étude des défaillances commence, par conséquent, par définir où finit le normal et où commence l'anormal, ou, ce qui revient au même, quelles sont les fonctions requises et celles qui ne le sont pas. L'approche classique du problème implique donc de partitionner les états du système en deux classes mutuellement exclusives où le fonctionnement du système est décrété normal (respectivement anormal), quitte à définir au besoin plusieurs partitions (et donc plusieurs points de vue pour la notion de défaillance d'un même système).

La science, pour l'ingénieur qui traite de manière générale des défaillances (et naturellement des moyens et méthodes à mettre en œuvre pour les maîtriser), est appelée sûreté de fonctionnement [Villemeur, 1988]. Elle regroupe les quatre disciplines que sont la Fiabilité (mesurée par une probabilité pour un système de fonctionner sans défaillance sur une durée donnée), la Disponibilité (mesurée par la probabilité instantanée pour un système d'être non défaillant), la Maintenabilité (mesurée par une probabilité de parvenir à réparer un système défaillant sur une durée donnée), et la Sécurité, le sigle FDMS étant synonyme de sûreté de fonctionnement. La sécurité peut se définir de manière, pour l'instant, non formalisée comme l'aptitude pour un système d'éviter de provoquer des événements dits catastrophiques (en termes de dommages aux personnes ou aux biens). Elle regroupe, de fait, deux notions différentes que sont la robustesse (vis-à-vis de possibles conséquences catastrophiques) en présence :

- d'événements internes ou externes au système qui ne sont pas des actions humaines avec intention de nuire pour la première ;
- d'événements internes ou externes au système qui sont la conséquence d'actions humaines avec intention de nuire (la cybercriminalité étant la déclinaison pour les systèmes informatiques) pour la seconde.

La terminologie anglaise, plus précise dans ce cas, distingue ces deux notions par deux termes différents, à savoir *safety* pour la première (parfois traduit en français par sécurité innocuité) et *security* pour la seconde [1] (traduit cette fois par sécurité confidentialité, la confidentialité étant l'une des problématiques essentielles de la *security*, au moins en ce qui concerne les systèmes informatiques).

D'une manière générale donc, si l'on tient à être précis, le terme sûreté (tout court) est à éviter car source de confusion du fait d'une signification différente suivant les domaines dans lequel il est employé. On sait maintenant que la sûreté de fonctionnement inclut les aspects FDMS, le mot sûreté ayant une signification bien différente suivant que l'on parle de sûreté du territoire ou des espaces ouverts au public, ou bien de la sûreté nucléaire.

Pour les systèmes informatiques, l'approche qui fait maintenant référence [Laprie, 1995] distingue sous le terme d'entraves à la sûreté de fonctionnement, les trois

....

(1) La FDMS étant la traduction de RAMSS : *Reliability Availability Maintainability Safety & Security.*

niveaux que sont les fautes, les erreurs et les défaillances. À l'origine de la défaillance se trouve donc l'erreur (état erroné du système, par exemple un bit erroné dans un mot mémoire) qui est elle-même la conséquence d'une faute (par exemple un dysfonctionnement interne du circuit intégré support physique de cette mémoire, ce qui à l'échelle du composant est une défaillance). La théorie de la sûreté de fonctionnement des systèmes informatiques se développe donc autour de ces chaînes causales : fautes => erreurs => défaillances (parfois hautement ramifiées du fait du phénomène appelé propagation des erreurs). L'importance de la distinction entre faute et erreur est liée au fait qu'une faute peut rester latente ou dormante (par exemple une faute dans un mot mémoire correspondant à une instruction de programme le reste tant que l'instruction n'est pas exécutée), et ne se traduire par une erreur qu'une fois qu'elle est activée. La typologie des causes de défaillance des systèmes informatiques s'obtient donc d'une manière assez claire à partir d'une classification des fautes qui en sont l'origine première suivant cinq critères :

- la cause : physique ou humaine ;
- la nature : accidentelle, intentionnelle avec intention de nuire, intentionnelle sans intention de nuire ;
- la phase de création de la faute : en développement, en opération ;
- la situation par rapport au système : interne ou externe ;
- la persistance temporelle : permanente ou transitoire.

Sur les quarante-huit différents types théoriques de fautes auxquels conduirait cette classification, huit seulement apparaissent pertinents, répartis en trois grandes catégories :

Les fautes physiques accidentelles
- internes en développement (défauts de fabrication) ;
- internes en opération (défaillances de composant du support matériel) ;
- externe en opération (perturbations de l'environnement, par exemple rayonnements).

Les fautes humaines accidentelles ou intentionnelles sans intention de nuire
- internes en développement (traditionnellement appelées « bogues ») ;
- externes en opération (fautes de l'opérateur exploitant souvent appelées « erreurs humaines »).

Les fautes humaines avec intention de nuire
- internes en développement (fautes internes introduites intentionnellement par le développeur, en général pour constituer une faiblesse exploitée ultérieurement en vie opérationnelle, type porte dérobée ou bombe logique) ;
- internes en opération (à cette rubrique on classe les virus et vers qui doivent prendre place en interne bien que l'origine de la contamination soit nécessairement externe) ;
- externes en opération (à cette rubrique, on classe les intrusions de tous autres types profitant des ouvertures du système sur l'extérieur).

La sécurité innocuité va donc être l'aptitude du système à éviter les événements catastrophiques consécutivement aux fautes des deux premières catégories (y compris les fautes humaines accidentelles, le développement d'un système *safe* implique des méthodes permettant de maîtriser les « bogues » et une analyse des risques d'erreur humaine en opération). La sécurité confidentialité va, quant à elle, être l'aptitude à éviter de provoquer des événements catastrophiques consécutivement aux fautes de la troisième catégorie.

L'introduction sans cesse croissante de systèmes informatisés dans des domaines où la préoccupation de *safety* est essentielle (tels le transport, y compris automobile), que l'on appellera désormais systèmes critiques dans la suite de cet article, et surtout, le fait qu'un nombre croissant de ces systèmes utilise des communications ouvertes (par transmission radio) implique de prendre également en compte la *security* pour parvenir à une maîtrise de la « sécurité globale ». Ainsi, les transports aériens ou ferroviaires, qui sont entrés par l'introduction de systèmes de contrôle-commande numériques communicants dans l'ère de la *cyber-safety* doivent aussi prendre en compte la *cyber-security* pour éviter – car étant d'ailleurs la cible privilégiée des terroristes – qu'ils ne deviennent celle des cyber-terroristes [2].

Techniques de couverture des fautes autres que celles liées à la malveillance humaine

Dans cette section, on reprend la classification des fautes établie dans la section précédente, et on décrit les

(2) Il doit ainsi être, par exemple, plus difficile de provoquer une catastrophe ferroviaire par intrusion malveillante dans les communications sol / bord des systèmes de signalisation modernes, que par des méthodes de terrorisme « à l'ancienne » impliquant l'intrusion physique sur les lieux, donc plus risquées du point de vue du terroriste.

principales techniques mises en œuvre pour faire en sorte que les fautes autres que celles liées à la malveillance humaine ne conduisent à des défaillances catastrophiques. On passe ainsi en revue les principales techniques de sécurité innocuité avant de voir, dans la section suivante, dans quelles mesures celles-ci couvrent également, ou peuvent être étendues pour couvrir également, les tentatives de malveillance humaine.

Fautes physiques accidentelles internes en développement

Les fautes physiques accidentelles internes en développement (défauts de fabrication) sont, en tout premier lieu, couvertes par la maîtrise de la qualité en fabrication. Ce domaine est un sujet à part entière qui n'est pas celui de cet article. Notons toutefois en complément qu'une telle faute qui aurait franchi cette barrière peut rester dormante jusqu'à son activation en opération (où elle provoque une erreur). Certaines techniques développées ci-après, conçues pour couvrir d'autres types de fautes le font en détectant les erreurs induites (et par conséquent peuvent également couvrir certains défauts de fabrication).

Fautes physiques accidentelles internes ou externes en opération

La couverture des fautes physiques accidentelles internes ou externes en opération est l'un des sujets majeurs de la sécurité innocuité, à savoir les moyens à mettre en œuvre pour prévenir tout comportement pouvant causer des dommages de gravité importante d'un système correctement conçu et fabriqué, mais subissant en opération des défaillances internes de ses composants électroniques, ou des perturbations du fonctionnement de ses composants par l'environnement. Toutes les techniques de couverture de ces fautes reposent sur la notion de redondance.

Redondance matérielle

La plus connue de ces techniques est la redondance matérielle qui consiste à mettre en place plusieurs unités effectuant les mêmes traitements, la sécurité reposant sur l'accord sur les résultats (unanimité ou vote majoritaire). C'est ainsi que sont conçus les systèmes informatiques embarqués qui effectuent les commandes de vol des avions actuels ou des engins spatiaux. L'hypothèse sous-jacente est, dans ce cas, l'indépendance des fautes accidentelles pouvant affecter les unités redondantes, tout mode commun (causes communes pouvant en affecter plusieurs, voire toutes) mettant à mal l'efficacité de la redondance. Ce point doit être soigneusement réfléchi (en particulier, pour ce qui concerne le partage d'alimentation, de données d'entrées ou de sorties communes, voire de conditions d'environnement semblables) afin d'atteindre effectivement le niveau de sécurité théorique. Cela amène, par exemple, pour certaines architectures embarquées dans les domaines du transport, à redonder les bus d'entrée et de sortie ou à disséminer les unités redondantes sur différentes parties du véhicule (diversification géographique).

Lorsque les unités redondantes sont de même technologie, on parle de redondance homogène. Dans le cas où la diversification technologique a été volontairement recherchée, on parle de redondance hétérogène. L'idée sous-jacente est, dans ce cas, de couvrir également de possibles fautes humaines internes en développement ayant pu affecter les briques technologiques utilisées (à savoir essentiellement les processeurs). On sait ainsi que les premières versions des processeurs Pentium souffraient de fautes de conception qui affectaient certaines opérations, qui pouvaient donc être détectées par diversification technologique (la même faute affectant un processeur de fournisseur différent étant extrêmement improbable).

Notons donc au passage que, conçue à la base pour couvrir les fautes de conception accidentelles ou sans intention de nuire, la technique peut couvrir une faute malveillante lors de la conception du processeur, théoriquement envisageable bien que difficilement réalisable en pratique et d'un usage moins aisé que l'insertion de code malveillant dans un logiciel applicatif, qui est, en revanche, l'une des problématiques majeures de la cybercriminalité. La couverture des fautes de conception des logiciels donne parfois lieu à une technique comparable à savoir la redondance de développement (plusieurs versions du logiciel étant développées sur la base des mêmes spécifications par des équipes indépendantes).

Outre son coût élevé qui la rend rarement mise en pratique, la technique a l'inconvénient de laisser ouverte la question de possibles modes communs (les solutions de conception retenues par les équipes indépendantes pouvant s'avérer voisines pour de simples raisons culturelles), et de ne pas couvrir les fautes de la spécification initiale. Pour ces raisons, bien que couvrant théoriquement la cybercriminalité en provenance d'éléments infiltrés dans les équipes de développement (à condition, bien sûr, que les recrutements au sein de ces équipes soient également suffisamment indépendants), cette technique ne nous semble pas à recommander.

Redondance informationnelle

Une autre technique consiste à redonder non pas l'unité de traitement, support physique compris, mais l'information manipulée par l'unité de traitement, afin de permettre un contrôle en ligne et en temps réel de la vraisemblance de l'information manipulée et des opérations effectuées. On entre ici dans le domaine des codes détecteurs et correcteurs d'erreurs, technique majeure de la sûreté de fonctionnement des systèmes informatiques. D'un principe très simple, consistant à traiter, outre l'information principale, une information en partie redondante permettant le contrôle, sa mise en œuvre peut couvrir un très vaste champ, qui va du bit de parité (technique de base utilisée dès les premiers échanges de données informatiques par modem) couvrant une faute simple sur un message, à des techniques de codage beaucoup plus élaborées permettant de détecter avec un niveau de probabilité très élevé toute altération d'une donnée, voire de permettre de la corriger.

Sans entrer dans le détail, citons les principales techniques de codage utilisées pour les systèmes informatiques critiques. Ainsi, les codes les plus récurrents pour vérifier, par exemple, l'intégrité d'une donnée à l'arrivée d'un message sur un réseau, sont les codes type CRC (codes à redondance cyclique basés sur des opérations polynomiales) qui suivant le polynôme employé permettent, avec un taux de confiance plus ou moins élevé, de garantir que la donnée n'a pas été modifiée accidentellement. Certains codes, type codes de Hamming, permettent même de corriger des fautes accidentelles (en ramenant la donnée détectée, erronée car hors code, à la donnée la plus proche dans le code, ce qui implique d'ailleurs des hypothèses sous-jacentes sur le nombre de fautes ayant pu affecter le message). Enfin, certaines techniques, dont le monoprocesseur codé [Forin, 1989 ; 1996], mis en œuvre avec succès dans le ferroviaire [3] utilisent un code arithmétique pour contrôler la vraisemblance des opérations.

Pour prendre une image simple mais assez représentative, le processeur codé procède comme l'écolier vérifiant la vraisemblance de sa multiplication par l'ancestrale technique de la « preuve par 9 ». Outre les opérandes, une information en partie redondante (le modulo 9 des opérandes) permet de vérifier que l'opération est « vraisemblable ». Certes, le processeur utilise un modulo plus efficace que 9 (nombre choisi pour l'algorithme écolier pour de simples raisons de faisabilité pratique des calculs à la main) : à savoir un grand entier dit « clé du code » sur 32 ou 48 bits qui rend l'erreur non détectée très improbable (probabilité de l'ordre de 1/A), mais l'idée sous-jacente est bien la même. Le processeur codé manipule des données codées constituées de deux parties : la partie dite fonctionnelle qui contient la valeur de la variable, et une partie dite code qui contient une information en partie redondante, permettant de vérifier la vraisemblance des opérations. Ces opérations doivent par conséquent être adaptées : les opérations arithmétiques sont remplacées par les Opérations élémentaires (OPELs), manipulant les deux parties des données codées, en effectuant l'opération arithmétique dans la partie fonctionnelle, et une opération permettant de conserver la cohérence du codage dans la partie code. La mise en pratique nécessite toutefois quelques compléments, afin de garantir que toutes les erreurs vraisemblables d'un processeur soient détectées (c'est d'ailleurs l'une des faiblesses de la preuve par 9 de ne pas détecter certaines erreurs naturelles des calculs à la main).

Or, prendre une variable pour une autre est une simple erreur d'adresse qui n'est détectée qu'au prix de l'ajout dans le champ code d'une signature statique permettant d'identifier les variables. Cette signature est conçue pour être « prédéterminable » hors ligne (plusieurs exécutions d'une même instruction vont pouvoir conduire à des valeurs différentes des variables, mais les signatures seront toujours les mêmes). Les signatures attendues peuvent donc être embarquées dans des PROMs et toute confusion entre opérandes pourra ainsi être détectée (avec une probabilité très élevée car les signatures peuvent prendre toutes les valeurs entre 0 et la clé du code A, les « collisions de signature » sont donc très improbables).

De même, afin de couvrir tout problème de « fraîcheur », des données (ces applications embarquées temps réel étant toujours exécutées de manière cyclique), le champ code porte également une date. À noter que la prédétermination des signatures des variables (nécessairement fonction des opérations qui ont permis de les calculer, et des signatures des variables opérandes de ces opérations, les variables de base ayant des signatures tirées au hasard) est effectué par un outil appelé Outil de prédétermination des signatures qui utilise le code source (et agit donc selon un processus parallèle et analogue à celui de la

(3) Utilisent en particulier cette technique, les systèmes de signalisation dits TVM sur TGV, le système SACEM [Hennebert, 1994] sur la ligne A du RER Parisien ainsi que le système d'automatisation de l'exploitation des trains de la ligne 14 du métro de Paris [Lecompte, Beaurent, 1996].

compilation). Toute faute, quelle qu'en soit l'origine (y compris « bogue » dans le compilateur), ayant affecté le processus de compilation est donc détectée, sauf cas très improbable de faute affectant de manière parallèle et analogue le processus de prédétermination des signatures.

Fautes humaines accidentelles internes en développement

Les fautes humaines accidentelles internes en développement ou « bogues » sont couvertes par les méthodologies de développement adaptées au niveau de criticité de l'application envisagée. Ainsi, pour prendre l'exemple du ferroviaire, la norme de référence (EN 50 128 [4]) définit comme obligatoire, hautement recommandé ou recommandé l'usage de certaines techniques de développement, pouvant aller jusqu'au développement totalement formel avec le système de preuves associé, selon le niveau d'intégrité de la sécurité (*Safety Integrity Level* : SIL) envisagé, niveau pouvant aller de 0 (aucune exigence particulière de sécurité) à 4 (logiciel pouvant entraîner des conséquences catastrophiques sur les personnes et les biens). C'est pour couvrir ce type de fautes que sont prévues les activités de Vérification et Validation qui peuvent être très variées (tests, simulation exhaustive de modèles, preuves...). Pour les systèmes critiques, il est de toute première importance que ces activités soient réalisées par une équipe totalement indépendante de l'équipe de développement (ce qui n'empêche toutefois pas cette dernière d'effectuer ses propres tests). Nous y reviendrons.

Fautes humaines accidentelles externes en opération

Les fautes humaines accidentelles externes en opération sont le domaine privilégié des études d'interface homme / système technologique et touchent là aux aspects ergonomie et psychologie cognitive. Ces aspects, de toute première importance pour les systèmes critiques, dont la plupart des incidents ou accidents majeurs de fonctionnement sont liés à ce que l'on appelle communément « l'erreur humaine », ne sont pas le cadre de cet article qui se propose de montrer que certaines techniques de robustesse aux fautes accidentelles, couvrent de fait ou peuvent être étendues pour couvrir les malveillances humaines.

Techniques de couverture des fautes liées à la malveillance humaine

Ayant, dans ce qui précède, évoqué les principales techniques de couverture des fautes accidentelles, quelle qu'en soit l'origine (physique ou humaine donc), on décrira, dans ce qui suit, comment ces techniques ou une extension de ces techniques permettent de couvrir certaines fautes humaines avec intention de nuire, problématique de la cyber-délinquance, cybercriminalité ou cyber-terrorisme.

Fautes malveillantes internes en développement

Le problème des fautes malveillantes internes en développement est de toute première importance, probablement sous-estimée à ce jour. Un fragment de code malveillant embarqué dans une application critique par l'un de ses développeurs malintentionnés, quelles que soient ses motivations (agissant comme « taupe » pour le compte d'une organisation terroriste, d'une puissance étrangère, ou simplement mécontent de son augmentation de salaire), représente, en effet, une vulnérabilité importante pour les systèmes critiques dont la couverture n'est guère évidente. De plus, après avoir été embarquées en secret par les individus malveillants infiltrés dans les équipes de développement, ces « bombes logiques », comme on les appelle, peuvent rester dormantes, dans l'attente d'un signal secret pouvant être envoyé ultérieurement (pour tout système communicant avec l'extérieur d'une manière ou d'une autre, pour lequel la bombe logique est une porte dérobée secrète).

Pour l'anecdote, on rappellera que bien avant d'occuper les fonctions de ministre de l'Économie, des Finances et de l'Industrie [5], Thierry Breton avait décrit, dans un thriller technologique à succès [6] [1984], les mécanismes par lesquels une telle bombe logique pouvait être utilisée comme une arme redoutable en période de guerre froide, en permettant de commander la défaillance des systèmes informatiques d'un ennemi grâce à un signal secret dissimulé dans des données que ces systèmes consultaient régulièrement sur le réseau (en l'espèce il s'agissait de

(4) EN 50 128, Railway Applications – Software for railway control and protection systems. CENELEC.
(5) De 2005 à 2007 dans les gouvernements de Jean-Pierre Raffarin, puis Dominique de Villepin.
(6) *Softwar, la guerre douce*, titre qui est évidemment un jeu sur le mot anglais « Software » qui désigne le logiciel.

valeurs de données météorologiques bien précises sur des îles bien précises).

Parmi toutes les techniques de robustesse aux fautes décrites plus haut, très peu permettent de couvrir ce type de cyber-malveillance interne aux équipes de développement. La redondance de développement le permet en partie (sous réserve de l'indépendance suffisante des équipes et de leur recrutement permettant avec une confiance raisonnable d'exclure leur infiltration malveillante par des éléments coordonnés), mais on en a déjà signalé le coût et la difficulté de mise en œuvre. Dans les faits, la couverture la plus efficace est liée aux activités de vérification et validation qui, sous réserve d'une couverture exhaustive de toutes les branches du code (critère souvent utilisé pour les tests dits « boîte blanche »), vont donc passer par les fragments de code de la bombe logique et en détecter les fonctionnalités malveillantes. On voit ici clairement la nécessité absolue de faire réaliser les activités de vérification et validation par une équipe indépendante de l'équipe de développement, indépendante en termes de recrutement, pour exclure toute action coordonnée de l'une introduisant la bombe logique et de l'autre (complicité par non-détection volontaire), indépendante également dans le processus d'élaboration des cahiers de tests et dans les documents ayant permis cette élaboration [7].

Fautes malveillantes internes en opération

Les fautes internes humaines malveillantes en opération (virus, vers, chevaux de Troie, etc.) concernent pour l'instant peu, fort heureusement, les systèmes critiques, car moins ouverts sur l'extérieur que ne le sont les ordinateurs personnels (pratiquement tous reliés à Internet à l'heure actuelle) et du fait que les opérations de maintenance (type mises à jour logicielles, installations...) y sont encadrées par des procédures rigoureuses mises en œuvre par du personnel qualifié. La propagation d'un virus ou d'un ver, sur des réseaux de machines personnelles, est le plus souvent le fait d'applications de provenance douteuse (téléchargées ou reçues par mail), que l'utilisateur exécute, voire installe (quand il en a les droits) par simple curiosité ou pour leur aspect plaisant, ou encore pour leur côté ludique.

Une telle vulnérabilité, qui a pour conséquence la florissante industrie des antivirus sur les machines personnelles, n'existe heureusement pas pour les systèmes critiques qui n'ont à exécuter que les applications pour lesquelles ils ont été conçus et dont la maintenance est soigneusement organisée. Ce dernier point apparaît d'ailleurs sous cet éclairage comme crucial car la cyber-délinquance par personne malveillante infiltrée dans le personnel de maintenance, est donc, après la cyber-délinquance en développement, évoquée dans la sous-section précédente, une deuxième voie d'entrée aux actions malveillantes concernant les systèmes critiques. Ce point est également probablement un point sensible à l'époque où nos automobiles se voient appliquer régulièrement des « patchs » logiciels concernant une partie ou une autre de l'informatique embarquée. Ce type de maintenance doit demeurer réalisable par le seul personnel habilité faute de quoi on risque de voir se répandre des automobiles aux performances « bricolées » (ce qui existe visiblement déjà de manière assez marginale) et également d'ouvrir la porte aux virus embarqués sur automobiles... dont on imagine la gravité.

Fautes malveillantes externes en opération

Les fautes malveillantes externes en opération (intrusion de tous types exploitant les communications du système avec l'extérieur) constituent l'essentiel de la problématique de la cyber-délinquance/criminalité ou terrorisme. C'est le cœur des activités des pirates ou « hackers » de tous types dont les motivations sont d'ailleurs très diverses, allant du simple jeu ou défi (pour accéder à des données protégées ou pour modifier un site web), jusqu'à de véritables actions criminelles ou terroristes organisées, en passant par des actions frauduleuses de diverses natures (détournements de moyens de paiement, téléchargements illégaux, etc.).

Moins ouverts sur l'extérieur, les systèmes critiques sont, à ce jour, moins concernés par ces phénomènes, mais la situation est en pleine évolution. En effet, de plus en plus de systèmes de ce type, en particulier pour le contrôle-commande des systèmes de transport, utilisent des communications numériques (en particulier entre bord et sol ou entre plusieurs mobiles, dans le cas du transport). Ces communications se font de plus en plus par liaison radio en exploitant des réseaux type téléphonie mobile (ou une déclinaison particulière dédiée comme le GSM-R pour les applications de signalisation ferroviaire normalisée européenne ERTMS), ou des protocoles normalisés (il est probable de voir sous peu des applications au domaine du transport basées sur des communications WiFi). Il est donc clair que c'est dans ces communications

(7) On touche là, probablement, une limite car les deux équipes finissent toujours par partager certains documents, dont les spécifications fonctionnelles qui ne sont pas faites en double sauf « redondance de développement » dont on a déjà signalé les inconvénients.

que se situe potentiellement le point faible, objet de possibles attaques de cyber-délinquants. Le développement de tels systèmes communicants (il est symptomatique à cet égard que les systèmes modernes de contrôle des trains en applications urbaines soient appelés « CBTC », *Communication Based Train Control*) ne fera qu'accentuer cette tendance qu'il convient de traiter avec le plus grand sérieux. Ces cyber-attaques sur systèmes de transport ne sont d'ailleurs déjà plus de la science-fiction comme en témoigne l'incident sérieux survenu en janvier 2008, dans la ville de Lodz, en Pologne, où un jeune Polonais de quatorze ans est parvenu à faire dérailler un tramway [8] en s'introduisant frauduleusement dans une communication bord-sol par infrarouges ayant pour fonction de télé-commander les aiguilles depuis la cabine de conduite du train. Certes, le garçon avait eu la possibilité, préalablement, de s'introduire frauduleusement dans le dépôt du tramway pour y dérober des objets et documents lui ayant facilité la tâche. La première faille de *security* fut donc, comme le plus souvent, un accès trop facile aux locaux ou aux personnes responsables de ces locaux. La technique utilisée par la suite laisse toutefois perplexe sur le niveau de robustesse aux intrusions du système en question. À partir des informations qu'il avait collectées, le jeune pirate réussit à construire un dispositif permettant la commande des aiguillages, à partir d'une simple télé-commande de téléviseur ! L'accident, fait d'un jeune inconscient qui fit tout de même douze blessés, fait réfléchir aux possibles conséquences d'une attaque par une organisation terroriste bien outillée et renseignée, qui parviendrait à diffuser de fausses informations de position aux systèmes modernes de contrôle-commande ferroviaires. La catastrophe ferroviaire, œuvre d'un cyber-terroriste et non pas d'un terroriste « classique » expert en explosifs !

Rassurons toutefois le lecteur, le cas a été envisagé, et traité, pour tous les systèmes modernes récents dont font partie ceux conformes à la spécification ERTMS pour l'aspect grandes lignes, et les systèmes type CBTC pour l'urbain. Examinons, toutefois, dans quelle mesure les techniques de protection exposées dans la section précédente couvrent ou ne couvrent pas ce cas. Les techniques de protection d'un message par code type CRC, Hamming... efficaces contre les fautes accidentelles sont totalement inopérantes contre les fautes malveillantes : admettant même que l'individu malveillant ignore le polynôme modulo utilisé pour un CRC par exemple, celui-ci n'a pas été conçu pour être une clé secrète d'un crypto système symétrique. Toute attaque, même simple (en force brute), aurait de bonnes chances d'aboutir. Il en est de même pour un message protégé par une technique de type processeur codé avec signature : d'une part, la taille de la signature sur 32 ou 48 bits est maintenant modeste par rapport à la taille recommandée actuellement pour les clés (128 voire 256 bits), mais surtout, cette signature est, comme on l'a souligné, statique pour une variable donnée, et ne change donc pas d'un cycle à un autre (le contenu fonctionnel de la donnée ayant pu par contre changer). L'extraction de la signature d'une donnée et sa réinjection dans une donnée malveillante constituent une faute qui n'a pas été retenue (on s'en doute) comme faute naturelle d'un microprocesseur... Elle est, en revanche, à la portée d'un cyber-délinquant un peu au fait de cette technique.

À ce stade, une conclusion s'impose : la protection contre la modification malveillante d'une information échangée est, depuis l'origine du problème (probablement aussi ancienne que l'écriture), le domaine de la cryptographie. C'est donc bien sûr là que se situe la bonne manière de traiter le problème et pas par des techniques qui n'ont envisagé que l'accidentel, quoique, comme on va le voir, il y a des parentés.

Le lecteur doit tout d'abord savoir, s'il l'ignorait, que les protections cryptographiques classiques contre l'intrusion sur un réseau WiFi (type clés wep) ne résistent pas aux attaques d'un cyber-délinquant expérimenté. Cela va bien pour le réseau domestique (des « couches » supplémentaires permettent de garantir la confidentialité des échanges avec les sites dits « sécurisés ») qui a peu de chance d'intéresser une organisation terroriste, mais pas pour un système de communication sol/train par exemple. En revanche, il existe, dans l'arsenal cryptographique, une version de la protection des modifications de messages adaptée aux modifications malveillantes, c'est le domaine des Codes d'authentification de messages (Message Authentification Codes, MAC), qui utilisent pour la plupart des fonctions de hachage combinées à une clé secrète partagée par l'émetteur et le destinataire : on parle alors de *Keyed-Hash Message Authentification Code* (HMAC) ou code d'authentification de messages à fonction de hachage avec clé, standardisé par le National Institute of Standards and Technology [9]. Une fonction de hachage génère une empreinte de taille fixe (256 à 512 bits pour les algorithmes actuellement en usage type SHA) d'un message de taille éventuellement variable, de telle sorte qu'il

(8) Dépêche AFP du 9 janvier 2008.

(9) *Federal Information Processing Standards Publication 198 (FIPS 198), The Keyed-Hash Message Authentication Code (HMAC),* http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf

est non seulement très improbable qu'une modification accidentelle d'un message en génère un qui ait la même empreinte, mais que, de plus, trouver (volontairement) un message ayant cette même empreinte est un problème difficile (irréalisable, dans des délais raisonnables, dans l'état actuel des connaissances scientifiques et des technologies informatiques). Les fonctions de hachage actuelles sont même résistantes aux collisions (il est difficile de trouver deux messages de même empreinte) pour des raisons de robustesse dans d'autres applications (dont la signature électronique mentionnée plus loin). La fonction de hachage peut donc être vue comme un code détecteur d'erreurs de haut de gamme, mais ne permet pas de couvrir les substitutions malveillantes de message par un attaquant, car il lui suffit de substituer également l'empreinte d'origine par l'empreinte du message substitué (l'algorithme de calcul des empreintes est bien évidemment public). Il faut donc utiliser la fonction de hachage conjointement avec une clé secrète, afin de réaliser une empreinte qu'il soit impossible de falsifier sans connaître cette clé. Le code d'authentification ainsi obtenu garantit donc l'intégrité du message ainsi que son origine de manière très similaire à la signature électronique qui pourrait d'ailleurs également être utilisée dans ce contexte (la différence étant que les algorithmes de signature électronique emploient des crypto systèmes asymétriques ou à clé publique afin que tout le monde puisse vérifier l'authenticité du message). Les messages d'authentification sont donc un moyen efficace de protection contre les intrusions dans des systèmes qui doivent échanger des messages sur des médias ouverts, dont les communications radio, mais peuvent, en définitive, être vus comme une extension des codes détecteurs d'erreurs qui couvrent les modifications accidentelles de messages, aux cas de modifications à caractère malveillant.

Conclusion

Les systèmes dits « critiques » (qui peuvent présenter des dangers pour l'homme ou l'environnement) doivent être conçus pour éviter que ces dangers ne se manifestent suite à des événements que, faute de terme plus adapté, on peut appeler « accidentels », sachant que cette notion recouvre des phénomènes physiques internes ou externes (que le langage courant appelle respectivement « pannes » et « perturbations »), ainsi que des phénomènes humains sans intention de nuire en conception ou en exploitation (que le langage courant appelle respectivement « bogue » et « erreur humaine »). Tout développement de système critique intègre des moyens de couverture de ce qu'un langage plus rigoureux appelle « fautes autres qu'humaines avec intention de nuire ». La plupart de ces techniques de couverture, qui permet d'obtenir le niveau de safety ou « sécurité innocuité », a été passée en revue au début de cet article. Mais à l'heure actuelle, un système critique se doit d'intégrer également la problématique de robustesse aux agressions humaines avec intention de nuire, en particulier pour les systèmes de plus en plus nombreux amenés à communiquer en exploitant des liaisons radio.

La seconde partie de cet article a permis de passer en revue les différents types d'agression envisageables et de voir dans quelle mesure elles étaient couvertes par les techniques conçues pour la sécurité innocuité. On a vu, à cette occasion, le degré de parenté qu'il existait entre les deux problématiques (la couverture de la malveillance amenant souvent à une mise en œuvre, avec une rigueur accrue ou avec quelques aménagements, des techniques conçues pour la sécurité innocuité). La prise en compte simultanée des deux problématiques de sécurité innocuité et sécurité confidentialité dans un concept commun de sécurité globale est donc certainement l'avenir pour les systèmes critiques.

Walter SCHÖN

Bibliographie

FORIN (P.), 1989, "Vital coded microprocessor principles and application for various transit systems", *in IFAC - Control, Computers, Communications in Transportation*, p. 137-142.

FORIN (P.), 1996, « Une nouvelle génération du processeur sécuritaire codé », *Revue Générale des Chemins de fer*, 6 : 38-41, Juin.

HENNEBERT (C.), 1994, « Transports ferroviaires : Le SACEM et ses dérivés », *in ARAGO 15, Informatique tolérante aux fautes*, Paris, Masson, p. 141-149.

LAPRIE (J.-C.) (dir.), 1995, *Guide de la sûreté de fonctionnement*, Laboratoire d'ingénierie de la sûreté de fonctionnement, Toulouse, Cépaduès, 369 p.

LECOMPTE (P.), BEAURENT (P.-J.), 1996, « Le système d'automatisation de l'exploitation des trains (SAET) de METEOR », *Revue Générale des Chemins de fer*, 6 :31-34, Juin.

VILLEMEUR (A.), 1998, *Sûreté de fonctionnement des systèmes industriels : fiabilité - acteurs humains informatisation*, Paris, Eyrolles.

Normes et cybercriminalité

Jean-Marc PICARD

Les États-Unis, au lendemain de la catastrophe du 11 septembre, ont lancé un vaste programme sur la normalisation en matière de sécurité et de protection du citoyen. Ce programme, repris au niveau mondial, européen et français, s'inscrit dans un vaste mouvement de production de standards et de normes en matière de protection des systèmes d'information et de lutte contre la cybercriminalité. Les normes techniques possèdent un pouvoir réel contraignant parfois la loi et la réglementation. Cet article se propose de dresser un court aperçu de l'ensemble de ces normes internationales.

Norms and Cybercrime

After the attacks of September 11, the United States launched a vast program of civil protection. This program has been extended to the international level, in France as well as in Europe, and includes establishing norms in the protection of information systems and the fight against cybercrime. As is well known, these technical norms sometimes bump up against laws and regulations. It is, thus, important to consider the nautre of these international norms.

Jean-Marc Picard

Jean-Marc Picard, enseignant-chercheur à l'université de technologie de Compiègne (UTC), a été dix-huit ans dans l'industrie dont dix comme directeur marketing, qualité et sécurité d'un grand groupe d'ingénierie et de services informatique. Auditeur IHESI, il a été vice-président de l'Association nationale des auditeurs IHESI/INHES et vice-président du groupe d'impulsion stratégique sur la sécurité et la protection du citoyen à l'Afnor. Auditeur qualité international, ancien vice-président de l'Institut pour la maitrise des risques et la sûreté de fonctionnement (IMDR SDF), il est expert auprès de nombreuses industries et institutions. Il est actuellement conseiller de défense auprès du ministre de l'Intérieur, président du forum sur la sécurité à l'Afnor et président de la commission de normalisation sur la sécurité sociétale.

Dans nos précédents numéros, nous avons souvent évoqué le pouvoir de la normalisation internationale. Les normes techniques relatives aux produits, y compris les produits/services de la société de l'information, peuvent inférer ou contraindre les réglementations nationales. En effet, dans le cadre des accords de l'Organisation mondiale du commerce (OMC) et du traité européen, les réglementations techniques ne peuvent difficilement contredire une norme technique internationale, sauf pour des impératifs de sécurité nationale, mais de manière limitée. La venue de nouvelles normes conditionne donc en grande partie la lutte contre la cybercriminalité, dès lors que celles-ci traitent des moyens, techniques et systèmes de protection, voire de contre-mesures.

Le champ de la normalisation

Les normes sont des spécifications énonçant des règles ou des caractéristiques techniques de produits, services ou organisations. En matière de cybercriminalité, les normes traitent essentiellement de la protection des systèmes d'information et des caractéristiques techniques de matériel et logiciels. Elles concernent également la sécurité des transactions et échanges de données au niveau de leur intégrité, de leur confidentialité. Mais, les normes traitent aussi des spécifications de produits ou logiciels, ceux-ci étant parfois des armes ou des produits de sécurité : normes sur la carte à puce, sur la biométrie (reconnaissance par empreintes digitales, etc.).

Nous limiterons, dès lors, notre panorama aux normes relatives à quelques aspects de la protection des systèmes et matériel [1]. Il s'agit de normes défensives, les spécifications techniques à caractère offensif faisant l'objet actuellement de réflexions en amont. Ces dernières ont peu de chance de déboucher sur la production de normes pour des raisons évidentes de confidentialité, sauf à quelques exceptions [2]. Dans le domaine de la protection, certaines spécifications techniques ne peuvent faire l'objet de normes publiques, et seulement de spécifications techniques classifiées et soumises au secret défense. En définitive, comme pour l'ensemble de la conduite des affaires, la normalisation devient un outil privilégié de régulation et de formulation de règles, car sa qualité essentielle est d'être le plus souvent mondiale et commune au monde public et privé.

Comment concevoir qu'une grande banque comme BNP Paribas, par exemple, dont le système informatique est déployé dans le monde entier, n'ait pas un raisonnement global pour sa politique de sécurité de l'information ? De telles entreprises se doivent de disposer de règles internationales et acceptées par la communauté internationale. Le plus souvent, les normes s'imposent donc logiquement aux réglementations techniques nationales. [3]

Une normalisation omniprésente dans les TIC

Le monde des technologies de l'information et de la communication (TIC) est régi par un ensemble considérable de normes, qu'il s'agisse d'exigences techniques ou organisationnelles. Les composants technologiques, les logiciels, les langages, les méthodes de développement, les exigences d'interfaces font tous l'objet de normes. Les protocoles internet (HTTP, TCP IP), les protocoles d'échanges de données et tous les protocoles de sécurité (anti-intrusion, cryptographie) font l'objet de normes. Il en va de même pour la gestion de la sécurité. En fait, si les spécifications sont nombreuses à faire l'objet de normes, bon nombre de recommandations, plus ou moins officielles, et de bonnes pratiques sont, quant à elles, soumises non pas aux normes, mais aux documents consensuels qui s'imposent.

En d'autres termes, pour le profane, les normes sont aux TIC (matériel et logiciel) ce que sont les dossiers de permis de construire et plans détaillés de construction à un bâtiment. Plus le plan est précis (plus la norme est précise), moins le produit aura de spécificité. Et le problème majeur réside dans les spécificités hors normes. Celles-ci ne sont pas interdites, mais créent parfois des soucis, voire des failles de sécurité. Car un logiciel, par exemple,

(1) Nous n'évoquerons pas non plus ou peu le monde de la sûreté de fonctionnement logiciel (en gros la fiabilité du logiciel). Pourtant, la fiabilité et la robustesse du logiciel conditionnent sa sécurité ou sa résistance aux attaques. Conceptuellement, fiabilité interne et capacité à réagir aux attaques sont des concepts comparables et qui font appel à des techniques très proches. Se reporter à l'article de Walter Schön sur le sujet (dans ce même numéro).

(2) Les normes sur la cryptographie comprenant aussi des fonctions de brouillage sont parfois considérées comme des armes.

(3) Ce qui ne veut pas dire pour autant que les normes contredisent la réglementation systématiquement, ni qu'il ne puisse y avoir de cohabitation entre les deux. Le fait est que les normes influent de plus en plus les réglementations.

doit faire ce pourquoi il est spécifié, mais en principe rien d'autre. Ainsi, en matière de sécurité et de fiabilité, on craint tout autant une fonction (ou fonctionnalité) intempestive qu'une déficience de fonctionnalité. Or, le distinguo entre une fonction intempestive, c'est-à-dire une fonction qui se manifeste sans justification et une « nouvelle » fonction ou fonction hors norme est parfois subtil. De la sorte, un produit parfaitement conforme à une norme qui ne fait ni plus ni moins que la norme est parfois en apparence sécurisant, sous réserve qu'elle soit complète. Le problème d'un tel produit est que le constructeur a peu de place pour marquer sa créativité et son originalité, surtout si la norme précise en outre des fonctions attendues, des performances du produit. L'offre peut ainsi se limiter entre des produits parfaitement conformes aux normes, sécurisants, mais sans différence notoire, et des produits offrant des fonctions supplémentaires, attrayantes, mais générant parfois un doute sur la sécurité [4].

Quelques acteurs majeurs

Il existe schématiquement quatre principaux types d'acteurs initiateurs de travaux normatifs et parfois prescripteurs de normes :

- des organismes de normalisation internationaux, régionaux, et nationaux ;
- des organisations professionnelles à vocation technique ou scientifique ;
- des pouvoirs publics nationaux ;
- des organisations publiques internationales.

Les organismes de normalisation

Bien que présentés dans un numéro précédent, signalons les principaux acteurs. Il s'agit en premier de l'ISO, de la CEI (*International Electrotechnical Commission*) et de l'Union internationale des télécommunications (UIT) [5] pour la téléphonie. Ces trois organismes ont créé un comité technique commun, le JTC1 [6]. Ce comité technique est le premier d'une liste qui en compte environ 250. C'est un État dans l'État, tant son influence sur les marchés est forte. Il crée des standards sur tous les aspects des TIC. Certes, ISO a produit des standards informatiques, parfois en dehors du JTC1.

Au niveau européen, trois organismes se répartissent la tâche, mais produisent peu de normes propres. En effet, les grands standards sont le plus souvent produits à l'échelle mondiale. Ces organismes sont le CEN (*European Committee for Standardization*), pendant de l'ISO pour l'Europe, et respectivement le Cenelec pour la CEI et l'Institut européen de normalisation des télécommunications (ETSI) pour l'UIT. L'ETSI est un consortium d'industriels qui diffère des organismes précédents en réunissant un large ensemble de parties prenantes.

En France, Afnor et l'Union technique de l'électricité (UTE) se partagent la tâche avec un comité ETSI France. Signalons que ISO, CEN et Afnor travaillent souvent sur les normes de management et d'organisation générale des systèmes d'informations, alors que la filière associée CEI/IEC, CENELEC et ETSI traitent beaucoup plus des produits, interfaces techniques, fiabilité des systèmes et logiciels. Mais ce distinguo est à prendre avec prudence, étant donné qu'au niveau mondial, la production des travaux est souvent commune à tous ces organismes. Retenons au niveau national, l'organisme national américain ANSI, grand producteur de normes pour les Systèmes d'information (SI) et les TIC, le Britannique BSI et l'allemand DIN qui, avec Afnor, produisent l'essentiel des normes européennes.

Les organisations professionnelles

Les organisations professionnelles revêtent des formes diverses. En France, nous citerons l'UTE, regroupant les professionnels du secteur. Cette association de professionnels a le statut de bureau de normalisation, c'est-à-dire en quelque sorte, le sous-traitant exclusif d'Afnor pour le domaine de l'électrotechnique, englobant une grande partie du monde des TIC. On peut trouver le très actif club de la sécurité de l'information français (Clusif [7]), ou l'ECTA

....

(4) Pour plus de précisions nous convions le lecteur à lire l'article de Walter Schön dans le présent numéro.

(5) *Cf.* la présentation détaillée des organismes de normalisation dans les numéros 3 et 4 des *Cahiers de la sécurité*.

(6) Le JTC1 possède dix-huit sous-comités de normalisation actifs dont quatre semblent essentiels pour nos préoccupations :
- JTC 1/SC 17 : identification des cartes et des personnes ;
- JTC 1/SC 27 : techniques de sécurité des technologies de l'information ;
- JTC 1/SC 31 : techniques d'identification et de captage automatique des données ;
- JTC 1/SC 37 : biométrie.

(7) Ce fameux club regroupe plus de 300 entreprises et collectivités d'importance. Il est notamment le promoteur de la méthode MEHARI (MEthode Harmonisée d'Analyse de RIsques).

européenne [8] ou encore l'IEEE [9], association internationale de professionnels. Très structurée, cette association technique produit des standards qui sont souvent repris par le JTC1, et deviennent normes. Ainsi, par exemple, le WiFi n'est qu'un protocole de communication défini par la norme ISO 802.11 reprenant l'IEEE 802.11. Le WPA2 (*WiFi Protected Access*) qui est un protocole du WiFi définissant le type de cryptage entre, par exemple, votre portable et votre « box » vous reliant à internet via l'ADSL, a été implanté par la WiFi Alliance (les fabricants). Il existe une version du standard, l'IEEE 802.11i de 2004, qui sera repris sous forme de norme par l'ISO. Le standard MPEG [10] qui sert à compresser les images vidéo est en fait une norme issue du JTC1. D'une manière générale, le principe est simple. Un consortium d'industriels [11], ou une association professionnelle (EISA, JPEG, etc.), fait la promotion de son standard et en fait une norme ISO. Mieux qu'un brevet, sa solution devient la référence mondiale !

OASIS

Organization for the Advancement of Structured Information Standards est un consortium qui regroupe principalement les plus grandes compagnies mondiales. Il produit des standards qui ont valeur de « pré-norme » par l'ISO. Ces standards sont des extensions du standard XML qui permet de produire des pages internet plus élaborées que le standard HTML. Créé en 1993, OASIS regroupe 3 500 membres de plus de 100 pays accueillant parfois des membres « pauvres » comme Debian qui distribue une version du fameux LINUX.

Le cas du *World Wide Web Consortium*

« WWW », ces trois lettres que vous voyez sur la fenêtre de votre navigateur sont utilisées par le protocole « HTTP » qui vient du *World Wide Web Consortium* (W3C), organisme de production de standards qui ne sont pas des normes au sens ISO, mais qui peuvent le devenir dans un second temps. Cet organisme à but non lucratif, fondé en 1994, est un consortium développant des recommandations et standards comme HTML (page web), XHTML, XML ou encore URL (l'adresse d'un site internet). En d'autres termes, votre utilisation d'Internet se résume en grande partie à l'utilisation de programmes complètement standardisés par le W3C. Le W3C a été fondé au MIT (*Massachusetts Institute of Technology*) par un ancien chercheur de l'Organisation européenne pour la recherche nucléaire (CERN), avec le soutien de l'agence américaine de recherche avancée de projets de défense (DARPA) et la CEE. L'Institut national de recherche en informatique et en automatique (INRIA) y joue un rôle important.

N. B. : les standards du W3C ne donnent pas lieu à certification, ce qui peut expliquer que le manque de rigueur, dans l'application qui peut en découler, génère bugs et problèmes divers.

La transparence essentielle des travaux de ces organismes semble aujourd'hui assurée. Une spécification technique produite par ces organismes peut, en théorie, être autant une avancée en sécurité qu'une régression. La présence assidue, plus encore que l'adhésion de nombreuses parties prenantes aux groupes de travail, est un gage de sécurité. En effet, un standard ou une norme mal conçus peuvent générer des failles de sécurité pour le plus grand bonheur d'éditeurs de logiciels parfois peu scrupuleux. En d'autres termes, les failles de sécurité donnent aussi beaucoup de travail à certains.

Les pouvoirs publics

En France, plusieurs structures connues, émanant du ministère de l'Intérieur ou de la Défense, traitent de la surveillance et de la répression de la cybercriminalité. Mais la prescription ou la production de référentiels à caractère prénormatif, voire le contrôle technique de la conformité de produits à ces référentiels sont l'œuvre quasi exclusive de la direction centrale de la Sécurité des systèmes d'information (DCSSI). Cette direction émane du Secrétariat général de la Défense nationale (SGDN) rattaché au Premier ministre. Elle couvre un vaste ensemble de missions. Parmi celles-ci, la DCSSI assure la fonction d'autorité nationale de régulation pour la sécurité des systèmes d'information (SSI) en délivrant les agréments, cautions ou certificats pour les systèmes d'information

....

(8) *L'European Competitive Telecommunications Association*, fondée en 1998, représente l'industrie des télécommunications auprès des autorités gouvernementales et des autorités ou agences de régulation et tient un forum pour le développement des réseaux.

(9) L'IEEE (*Institute of Electrical and Electronics Engineers*) est une organisation considérable qui compte plus de 375 000 membres dans 160 pays. Organisée en 324 sections en 10 régions et regroupant 1 784 chapitres, l'IEEE gère environ 1 300 standards actifs et a publié près de 1,7 million de documents techniques !

(10) MPEG (*Moving Picture Experts Group*), est le groupe de travail SC 29/WG 11 du comité technique mixte JTC 1 de l'ISO et de la CEI pour les technologies de l'information.

(11) Il en existe de nombreux. En Europe, l'*European Telecommunications Network Operators Association* (ETNO) ou encore l'*European Institute for Research and Strategic Studies in Telecommunications* (EURESCOM).

de l'État, les procédés et les produits cryptologiques employés par l'administration et les services publics, et en contrôlant les centres d'évaluation de la sécurité des technologies de l'information (CESTI). Ces centres, avec la DCSSI, valident donc la conformité d'un équipement matériel et logiciel avec des exigences de sécurité émanant de normes ou référentiels comme les critères communs (CC) que nous verrons plus loin. Indépendamment, la DCSSI évalue les menaces, donne l'alerte, organise des formations et assure un pôle d'expertise et publie de nombreux référentiels [12] et guides s'apparentant à des documents prénormatifs. C'est le cas en matière de label de sécurité développé depuis peu par la DCSSI concernant les logiciels libres. La DCSSI émet des spécifications ou règles de protection pour les informations sensibles. Ces règles ne sont pas diffusées publiquement, ayant trait à la protection du secret défense.

Enfin, des organisations comme l'OTAN gèrent des spécifications secrètes s'apparentant à des normes. Nous frôlons ici le paradoxe dans la mesure où par définition une norme est publique. Mais une norme publique peut poser les règles quant à des mécanismes utilisant des principes, sinon des données secrètes. C'est le cas des systèmes de sécurité dont nous parlerons plus loin.

Les organisations publiques internationales

Si beaucoup d'organisations internationales traitent de la sécurité des systèmes d'information – il existe un institut européen sur le sujet [13] – l'OCDE tient un rôle de premier ordre. Elle a été à l'origine d'une grande part de la production de règles de sécurité et de spécifications pour les matériels et systèmes qui sont appelés les critères communs (*Common Criteria*). En outre, son conseil adopte des lignes directrices régissant la sécurité des systèmes et réseaux d'information.

Les principaux référentiels normatifs

Les normes peuvent être classées de plusieurs manières. Tout d'abord, il convient de distinguer les normes sur les matériels, sur les dispositifs de reconnaissance et sur les logiciels. Encore faudrait t-il en considérer les différentes composantes. S'il existe de nombreuses normes techniques de bas niveau, c'est-à-dire traitant de mécanismes physiques ou logiques de base, il existe des normes traitant à notre avis des domaines les plus sensibles :

- les premières concernent les produits (notamment de sécurité) ; il s'agit, par exemple, des lecteurs de carte à puce, Firewall, routeurs et certains types de serveurs ;
- les secondes traitent de la protection des systèmes d'information et de la politique de sécurité des systèmes d'information. Ce sont des normes d'organisation. Les normes dont nous parlons sont souvent complétées ou concurrencées par des spécifications ou bonnes pratique appelées référentiels. Il ne s'agit pas de normes officielles, mais de documents souvent reconnus comme des références incontestables.

Les normes et référentiels portant sur les produits (matériels ou logiciels)

Elles ont pour but généralement de préserver directement ou indirectement l'intégrité, la confidentialité et la disponibilité de l'information. Certaines de ces normes traitent de mécanisme de sécurité. C'est le cas des suivantes : la norme ISO/CEI 9 798 [14] traite de l'authentification, l'ISO/IEC 9 796 [15] du cryptage, l'ISO/CEI 11 770 [16] de la gestion des clefs, enfin l'ISO/CEI 18 014 [17] concerne la gestion du temps. L'ITU-T X.509 traite, quant à elle, des certificats, notamment pour les télédéclarations. D'autres normes, comme l'ISO/CEI 7 064:2003 traitant des mécanismes utilisant des caractères de contrôle, sont des exemples

....

(12) Comme la méthode EBIOS.

(13) Il s'agit de l'ENISA : *European Network and Information Security Agency*, qui développe notamment des travaux prénormatif sur la résilience des réseaux informatiques ou l'authentification en matière d'identification. L'Enisa est en étroite liaison avec la CEI/IEC.

(14) Six parties traitant des techniques de sécurité, et plus précisément des mécanismes d'authentification utilisant des algorithmes de chiffrement symétriques, utilisant un algorithme à clé publique, utilisant des techniques de signature numériques, utilisant une fonction cryptographique de vérification, utilisant des techniques à divulgation nulle, utilisant un transfert manuel de données.

(15) Elle spécifie des schémas de signature numérique utilisant des algorithmes pour sécuriser transactions ou cryptage et des mécanismes reposant sur sur une factorisation entière ou sur les logarithmes discrets.

(16) Cette norme traite de la gestion de clés et des mécanismes utilisant des techniques symétriques, asymétriques et des mécanismes reposant sur des secrets faibles.

(17) Celle-ci traite des services d'estampillage de temps, services d'horodatage : mécanismes produisant des jetons indépendants ou des jetons liés

de normes techniques parmi des milliers se rapportant à la sécurité des produits (matériel ou logiciel). En matière de biométrie, l'ISO n'est pas en reste avec une bonne trentaine de normes ou parties de normes issues de nombreux référentiels [18]. Également pas moins de cinquante normes majeures définissent les spécifications techniques pour les cartes d'identification personnelles [19]. Enfin ceux qui auraient peur d'exécuter des transactions financières sur Internet, par crainte de voir leur identité usurpée et de devenir victime de cybercriminalité, peuvent compter sur la norme ISO 21 188:2006 qui établit des pratiques et des politiques en matière de confidentialité sur Internet.

Un des premiers référentiels sur les critères permettant d'évaluer la sécurité des produits relevant des technologies de l'information a été le *Trusted Computer System Evaluation Criteria*, communément appelé TCSEC ou *Livre orange* (*Orange Book*) du département de Défense (DOD) américain. Ce document, un référentiel quasi normatif, s'avérait peu applicable pour les industriels, et traitait essentiellement de la capacité d'un appareil à être invulnérable à des attaques. Ce référentiel a servi à développer, en France, la méthode MEPS (méthode d'évaluation de produits de sécurité), pour le GIE [20] des cartes bancaires. L'utilisation de ces critères conduit notamment à développer, outre un certain nombre de tests, une véritable étude de sécurité. Dans ce cadre, les premières méthodes d'analyse de risque se développent en France. Il s'agit principalement de Marion et Melisa. Les méthodes sont une forme de bonnes pratiques, et deviennent souvent des « pré-normes », dès lors qu'elles sont adoptées par une large communauté.

Plus tard, les Anglais défieront leur propre référentiel avec le mémorandum CESG numéro 3 [21] développé à usage gouvernemental, et des propositions du ministère du Commerce et de l'Industrie réunies dans le *Livre vert* [22] pour les produits commerciaux. Le service de sécurité de l'information allemand a publié ses propres critères en 1989 [23], et à la même époque, des critères ont été développés en France sous le nom du *Livre bleu-blanc-rouge* sous la houlette du SCSSI, l'actuelle DCSSI. Nos trois pays associés alors aux Pays-Bas décidèrent, avec bon sens, d'harmoniser ces critères et créèrent, sous l'égide de la CEE en 1991, les critères d'évaluation de la sécurité des systèmes informatiques, les ITSEC. Les Canadiens, qui voulaient faire le lien entre les TSEC américains et les ITSEC européens, développeront leur propre démarche. Enfin, l'ISO, sous l'impulsion de l'OCDE en 1990, à travers le SC 27 du JTC1, lancera des travaux qui ont abouti à l'élaboration des critères communs (CC) d'évaluation de la sécurité des technologies de l'information, qui permettent de définir un cadre pour l'évaluation de produits ou de systèmes informatiques. Ces critères vont faire l'objet de la principale norme internationale [24]. Cette norme est extrêmement fournie et précise sur certains points. Il faut dire qu'avec près de 500 pages, c'est sans doute une des normes les plus imposantes. CC et ITSEC sont conçus pour être certifiés. En France, c'est un système qui sort du schéma classique, puisque la DCSSI (donc l'État) certifie en s'appuyant sur des laboratoires spécialisés [25] qui ont été préalablement accrédités par le Comité français d'accréditation (COFRAC) et agréés par lui. La certification ITSEC, comme CC repose sur l'attribution d'un niveau d'assurance (sécurité) de EAL1 à EAL7 pour l'ISO 15 408. Ce niveau est déterminé sur la base de l'examen d'une cible de sécurité comprenant l'environnement d'utilisation et de maintenance [26]. De plus, la démarche CC permet la certification de profils de sécurité, c'est-à-dire de standard en quelque sorte.

La démarche sécurité des critères communs peut être vulgarisée, notamment par le point de vue suivant. Auparavant, le propriétaire d'un système évaluait ses biens et voulait minimiser les risques. Il essayait d'identifier les dangers ou vulnérabilités qu'il comptait réduire par des contre-mesures soit en les supprimant soit en se munissant de barrière de sécurité. Les agresseurs, quant à eux, concevaient des menaces afin d'abuser des biens. Ce scénario, qui a fait ses preuves, ne s'en trouve pas moins obsolète. En effet, il ne tient pas compte du contexte de l'utilisation, des utilisateurs, des développeurs, de la maintenance, etc. Ainsi, les critères communs amènent une

••••

(18) Normes ISO 19784, 19785, 19794, 19795, 24708, 24709, 24713, 24714, 24722, 24741, etc.

(19) Normes ISO/IEC 8484, 4909, 7811-1:2002, 7812-1, 7813, 7816-3, 10373-1, NP 14443-1, 15457-1, NP 15693-1, 18013-2, 24727-1, NP 24749, etc.

(20) Groupement d'intérêt économique (GIE).

(21) *UK Systems Security Confidence Levels*, CESG Memorandum N° 3,*Communications-Electronics Security Group*, United Kingdom, January 1989.

(22) DTI *Commercial Computer Security Centre Evaluation Levels Manual*, V22, *Department of Trade and Industry*, United Kingdom, February 1989.

(23) *Criteria for the Evaluation of Trustworthiness of Information Technology* (IT) Systems, ISBN 3-88784-200-6, *German Information Security Agency* (*Bundesamt für Sicherheit in der Informationstechnik*), Federal Republic of Germany, January 1989.

(24) [ISO 15408] Technologies de l'information – Techniques de sécurité– Critères d'évaluation pour la sécurité TI revue en 2008.

(25) Les Cesti, presque tous privés, sont moins de dix.

(26) TOE pour *Taget Of Evaluation*.

philosophie nouvelle. Il s'agit de donner, via la certification, la certitude au propriétaire, qui a besoin d'avoir confiance en son système, que ce dernier (technique et humain) dispose de contre-mesures qui minimisent les risques à l'égard des biens de toute nature. Cette notion de contre-mesure sera largement exploitée dans les normes ISO 27 000 et dans les normes ISO 28 000 sur le transport (*cf. Cahier de la sécurité* n°4). Un des principes de cette norme postule que la sécurisation d'un système d'information suppose, entre autres, la mise en place d'une politique de sécurité des systèmes d'information. Ainsi, la norme ISO 13 335 [27] répondra à cette exigence, tout comme la série ISO 27 000.

Les normes et référentiels portant sur la sécurité des systèmes d'information

La norme la plus connue est sans conteste l'ISO 27 000, ou plutôt les normes de la série ISO 27 000. L'ISO 27 001, sorte d'ISO 9 001 de la sécurité des SI reprend les concepts de grandes normes de management (ISO 9001, ISO 14 001, ISO 28 001, etc.).

La BS 7 799 et l'ISO 17 999

Créée en 1995, à partir d'un guide de bonnes pratiques en 1991, la norme britannique BS 7 799, revue en 1998 et 2002, traite de la mise en œuvre d'un système de management de la sécurité (SMS) des SI ou ISMS en anglais. La BS 7 799 présentait dix mesures clés regroupant potentiellement cent mesures applicables. Depuis, cette norme, devenue ISO 17 999 pour sa première partie en 1999, puis évoluant vers l'ISO/IEC 27 000, repose sur l'identification et la maîtrise des risques comportant près de cent trente mesures de sécurité. Sa partie deux, publiée en 2002, va reprendre les concepts des ISO 9 000 et 14 000. La BS 7 799, avant d'être reprise au niveau mondial, va connaître des adaptations dans de nombreux pays sous la forme de normes locales.

L'ISO 27 000

L'SO 27 000, ou plutôt la série des normes ISO 27 000, est un ensemble complet de spécifications traitant de la sécurité des systèmes d'information. Cette série majeure de normes internationales s'inscrit aux côtés d'autres séries non moins célèbres que nous avons déjà évoquées dans de précédents numéros des *Cahiers de la sécurité*.

Il s'agit des ISO 9 000 sur le management de la qualité, mais pouvant traiter de la sécurité, des ISO 14 000 sur le management environnemental, mais aussi sur le risque industriel, de l'ISO 31 000 traitant du management du risque, de la récente 22 399 sur la continuité d'activité, de la série ISO 22 000 sur la sécurité alimentaire, de la série ISO 28 000 sur la sécurité/sûreté de la logistique et de la *supply chain*.

La norme ISO 27 001 est issue de la norme BS 7 799-publiée par le BSI, elle est complétée par plusieurs normes allant de la 27 002 à la 27 006 traitant de la mise en œuvre d'un SMSI comme de la gestion des risques (27 005). Cette très complète série ISO 27 000, à l'instar des ISO 28 000 (*Supply chain* et logistique), que nous avons évoquées dans un précédent numéro, développe les notions de menace (*threat*), de vulnérabilités et de scénarios d'incident. Cette dernière postule qu'un incident n'est pas le fruit forcément d'une vulnérabilité, comme présupposé dans les scénarios de risques. En ce sens, l'approche « heuristique » est largement exploitée. Cette norme traitera de sujets très divers comme la liste des personnes autorisées à recevoir des données, les restrictions d'accès aux locaux, etc.

La mise en œuvre d'un SMSI est l'occasion de formaliser une Politique de sécurité de l'information (PSI). Selon le Clusif, dans son rapport de 2007, 47 % des entreprises (44 % des mairies) s'appuient sur une « norme » pour formaliser leur PSI. Les normes ISO 2 700x [28] (ou ISO 17 799) arrivent en tête, en particulier dans les grandes entreprises (32 % d'entre elles utilisent l'ISO). Mais dans l'Hexagone, le guide PSSI de la direction centrale de la Sécurité des SI (DCSSI) concurrence l'ISO 27 000.

Norme ISO 13 335

« *Guidelines for the management of IT Security* » (directives pour la gestion de la sécurité des technologies d'information). Cette norme, qui existe depuis plus de dix ans, est plus précise que l'ISO 17 999. Citée par la 27 001, elle propose des analyses de risques que l'on retrouvera dans les méthodes EBIOS ou MEHARI.

(27) [ISO 13335] Technologies de l'information – Lignes directrices pour le management de sécurité IT – ISO/IEC, 2001.

(28) L'ISO 27001 est inspirée de la norme anglaise BS 7799-2 ; l'ISO 27002détaille les mesures de sécurité qui sont listées dans l'annexe de l'ISO 27001 ; l'ISO 27003 est un guide de mise en œuvre d'un SMSI qui sortira en 2009 ; l'ISO 27004 est un guide de mesurage du SMSI, qui explique comment mettre en œuvre des indicateurs pour un SMSI ; l'ISO 27005 est un guide de gestion de risques ; enfin, l'ISO 27006 concerne les organismes de certification.

La notion de PSI

Les normes évoquées précédemment induisent, voire exigent la mise en œuvre d'une politique de sécurité de l'information : PSI. Ce concept a été depuis longtemps promu par l'Organisation de coopération et de développement économiques (OCDE), dont le conseil avait adopté, en 2002 [29], une nouvelle version des « *lignes directrices régissant la sécurité des systèmes et réseaux d'information - vers une culture de la sécurité* » [30], afin de prendre en compte l'accroissement de l'interconnexion des réseaux et l'évolution des données en termes de type, volume, sensibilité, ainsi que les nouveaux enjeux liés, par exemple, aux projets gouvernementaux et de commerce électronique.

Les nouvelles lignes directrices de l'OCDE introduisent les notions de « culture de sécurité » et de processus de gestion des risques avec un mode opératoire proche des systèmes de management qualité. Elles décrivent les neuf principes :

1. sensibilisation ;
2. responsabilité ;
3. réaction ;
4. éthique ;
5. démocratie ;
6. évaluation des risques ;
7. conception et mise en œuvre de la sécurité ;
8. gestion de la sécurité ;
9. réévaluation.

Ces principes sont censés permettre de couvrir l'ensemble des sections de l'ISO/IEC 13 335, ainsi que l'ensemble des domaines de l'ISO/IEC 17 799 et ISO 27 001, et d'assurer la compatibilité avec l'ISO/IEC 15 408 (critères communs d'évaluation). La démarche permet de décliner les principes en règles de sécurité cohérentes et adaptées au contexte (graduation des moyens).

La norme ISO 20 000 et ITIL

La norme internationale ISO/IEC 20000-1 datant de 2005 définit les exigences que se doit d'appliquer un fournisseur de services gérés. C'est une norme « qualité », mais qui ne néglige pas pour autant la sécurité, promise sans doute à une grande popularité. Elle est fondée sur la norme britannique BS 15000-2, qu'elle annule et remplace. Destinée aux fournisseurs de services, notamment à Internet, cette norme a pour but d'assurer une qualité de service aux clients, elle comprend des aspects sur la sécurité, mais tient plus d'une extension des fameuses ISO 9 000 sur la qualité. Cette norme est l'antichambre d'un ensemble célèbre de bonnes pratiques édictées par l'Office public britannique du commerce appelées ITIL. ITIL est donc un ensemble de recommandations ou spécifications qui ne sont pas aujourd'hui des normes. Lancé à l'origine par le gouvernement britannique, ITIL traite essentiellement de la qualité des services informatiques fournis (y compris internes). ITIL a de plus en plus intégré de fortes et lourdes exigences en matière de sécurité informatique. À ce jour, ITIL V3.0 contient six livres essentiels de recommandations.

Le référentiel de gestion de services informatiques rendus sur la base d'une infrastructure informatique et de télécommunications, en suivant les recommandations ITIL, est connu sous le nom d'ITSM (*IT Service Management*) et constitue le fond de la norme ISO 20 000. Deux organismes certifient ITIL : l'ISEB (*Information Systems Examination Board*), en Grande-Bretagne, et l'EXIN, aux Pays-Bas. Ce contrôle de la conformité comme la majeure partie des certifications anglo-saxonnes n'est pas conforme au schéma réglementaire sur la certification en France, qui doit obéir à des règles strictes en matière d'accréditation. De la sorte, les Anglos-Saxons nous habituent une fois de plus à établir des contrôles de toute sorte par des organismes de statut très variables, mais le plus souvent privés. La certification ITIL, contrairement à la très « orthodoxe » ISO 20 000, porte sur le personnel et non sur l'entreprise ou l'organisation.

Les enjeux

Une multitude de produits informatiques font donc l'objet de normes garantissant un certain niveau de sécurité. Nous avons vu aussi que le management des systèmes pouvait obéir à des dispositions très sérieuses et normalisées garantissant un certain niveau de sécurité. Mais à ce jour, de nombreux problèmes restent sensibles. Sans tous les énumérer, quatre nous semblent importants à souligner.

La maîtrise de l'appareil normatif

Les normes, par définition, standardisent les solutions techniques. Une norme peut être foncièrement mauvaise !

(29) Reprenant une recommandation du Conseil et annexe (lignes directrices régissant la sécurité des systèmes d'information) du 26 novembre 1992, qui fut suivie en France par un Guide pour l'élaboration d'une politique de sécurité interne (PSI) à l'usage du responsable de la sécurité du système d'information, version 1.1, 15 septembre 1994, Service central de la sécurité des systèmes d'information (SCSSI).

(30) Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information – vers une culture de la sécurité, 29 juillet 2002.

Ainsi, le poids des autorités dans l'élaboration de spécifications de sécurité peut sembler rassurant. Mais la sécurité des réseaux dépasse depuis plusieurs années le cadre militaire. Aujourd'hui, le foisonnement d'organismes et de lobbies ne contribue pas forcément à la clarté des objectifs. Maîtriser l'appareil normatif devient impossible, et tous les pays ne s'y investissent pas également. De plus, le rajout de spécifications discrètes à la demande d'autorités, dans plusieurs pays, ruine la confiance que l'on peut avoir dans certains standards.

Sécurité du contrôle de conformité et de la certification

La certification repose sur des audits, évaluations, tests et contrôles. Le résultat de ces examens est hautement confidentiel. La protection et la connaissance des résultats constituent un réel problème. Par ailleurs, beaucoup d'organismes, par exemple les assurances, peuvent exiger logiquement d'un client des certifications comme garantie. Mais, il est toujours délicat pour une société de transmettre à une assurance ou tout autre partenaire étranger des informations pertinentes sur le niveau de sécurité des systèmes. Ce problème de la confidentialité n'est pas simple déjà dans le monde de la défense. Mais, pour ce qui nous concerne, nous ne sommes ni dans un cadre étatique ni national. Comment garantir l'intégrité et la compétence des experts par ailleurs ? Nous avons un retard considérable sur la qualité et l'homogénéité des expertises.

La sécurité des fournisseurs et intervenants

Les normes ne traitent pas pour l'instant du problème de la sécurité des fournisseurs, des personnes et des intervenants. La sécurité des fournisseurs, c'est aussi la sécurité des certificats de sécurité. Et compte tenu du cadre très réglementé du droit du travail et de la spécificité des droits nationaux, il semble difficile d'imaginer des référentiels dans le domaine. Pour autant, le TC 223 ISO sur la sécurité sociétale pourrait à terme s'intéresser à cette problématique. Enfin, en matière de clefs et de cryptographie, beaucoup d'algorithmes sont basés sur l'utilisation massive de grands nombres premiers. Sans rentrer dans les détails mathématiques, la production de nombres premiers suppose de recourir à des professionnels. Comment garantir que ces professionnels, qui fournissent des nombres premiers, donnent réellement des nombres premiers rares et authentiques. Ainsi, un certain nombre de points sensibles ne sont pas encore traités. D'une manière générale, aucune norme ne traite réellement de la sécurité des fournisseurs, à l'exception de la collection ISO 28 000 dans le domaine du fret mais pas des TIC !

La sécurité du développement

Il n'y a pas de sécurité sans fiabilité, sans sûreté de fonctionnement. Or, la fiabilité du logiciel est un problème délicat, car les systèmes deviennent de plus en plus lourds, gros et complexes. De plus, les systèmes, comme les automobiles, partagent de nombreux composants identiques. Si l'un d'eux défaille, c'est un problème potentiel à grande échelle qui peut se poser. Le développement de logiciels libres, dont les sources sont publiques, va sans doute contribuer globalement à une plus grande sécurité. En revanche, les normes traitent abondamment de la qualité des processus de développement et des produits logiciels. Elles sont trop nombreuses pour pouvoir les aborder ici.

Comme pour la sécurité routière, norme et règlement ne font pas tout. Certes, ce n'est pas parce qu'il y a un accident qu'il faut supprimer le code de la route, mais le complexifier peut avoir des effets pervers. Il en va de même pour la sécurité des TIC. Normes et réglementation ne valent d'abord que par ce que l'on en applique. Et dans ce domaine, le contrôle technique et l'audit sont des activités sur lesquelles nous avons d'immenses progrès à accomplir.

Jean-Marc PICARD

Combattre le cybercrime

Un point de vue du ministre de la Justice de l'État de Washington

Rob McKENNA

Dans le monde entier, des entités privées et publiques ont été mises au défi de développer rapidement de nouvelles techniques afin de faire face au « cybercrime ». Le ministère de la Justice de l'État de Washington est reconnu comme un leader national pour ses efforts dans la lutte contre la criminalité « high-tech ». L'État de Washington a été l'un des premiers à adopter une loi interdisant explicitement les activités de logiciels espions (« spyware ») et à imposer des peines sévères à ceux qui l'enfreindraient. Le succès de cette entreprise dépend d'une législation bien ficelée, de ressources adéquates, de partenariats, d'un soutien aux forces de police, et de l'information dispensée aux consommateurs et aux entreprises.

Fighting Cybercrime
A Perspective from the Washington State Attorney General

Throughout the world, public and private entities have been challenged to quickly develop new techniques to address cybercrime. The Washington State Attorney General's Office is known as a national leader in efforts to fight high-tech crimes. Washington was one of the first states to adopt a law explicitly prohibiting spyware activities and imposing serious penalties on violators. Success depends on well-crafted legislation, adequate resources, partnerships, support for law enforcement, and consumer and business education.

Rob McKenna

Rob Mc Kenna a été élu 17e ministre de la Justice de l'État de Washington et a pris ses fonctions en 2005. Il a commencé sa carrière de juriste en 1988 chez Perkins Coie, l'un des cinquante meilleurs cabinets d'avocats des États-Unis. Il a obtenu son diplôme d'avocat à l'université de Chicago (*University of Chicago Law School*), est titulaire de deux licences en économie et études internationales. Il est membre du *Aspen-Rodel Fellowships in Public Leadership*, association conçue dans le but de réunir les meilleurs dirigeants qui commencent à se distinguer dans le pays, pour discuter des grandes questions de la gouvernance démocratique et d'un service public efficace.

Tandis qu'Internet a révolutionné la manière de communiquer et de conduire ses affaires pour bon nombre de personnes, il a aussi favorisé une augmentation gigantesque de la criminalité exploitant cette technologie. Dans le monde entier, les entités publiques et privées ont été mises au défi de développer rapidement de nouvelles techniques pour faire face au cybercrime, qui va de la fraude financière à la diffusion de logiciels malveillants et destructeurs (*destructive malware*), en passant par l'exploitation des enfants, le harcèlement et le vol de secrets commerciaux.

L'augmentation du cybercrime

75 % des adultes et 90 % des enfants, estime-t-on, utilisent Internet [1] aux États-Unis. Avec un tel nombre de familles, d'entités gouvernementales et d'entreprises en ligne, l'essor correspondant du cybercrime représente une sérieuse menace pour la sécurité publique, l'économie et la sécurité nationale.

L'impact réel du cybercrime aux États-Unis demeure inconnu, car les incidents ne sont pas toujours signalés ou détectés. Les études disponibles révèlent une augmentation substantielle de l'activité illégale, qui comporte :

- Les spams : la société Postini a repéré plus de 60 milliards de spams entre septembre 2006 et mars 2007. La société a relevé une augmentation de 65 % de spams depuis janvier 2002 [2] ;

- Les ordinateurs infectés par des bots (robogiciels) : la Symantec a relevé 63 912 ordinateurs infectés chaque jour pendant cinq mois en 2005, soit une augmentation de 11 % par rapport à la précédente période étudiée [3] ;

- Les attaques d'un cheval de Troie : 2 millions sur les 4 millions d'ordinateurs nettoyés par un outil de suppression de logiciels malveillants de Microsoft, entre janvier et juin 2006, étaient infectés par au moins un cheval de Troie déguisé. Durant le même laps de temps, 43 000 nouvelles variantes de logiciels malveillants ont été découvertes. Le secteur des services financiers a été victime de presque 40 % de toutes les attaques de chevaux de Troie l'année dernière, selon Counterpane [4].

- Espions clavier enregistreurs de frappe (*Keyloggers*) : Le Groupe de travail contre les faux courriels ou pages web (*Anti-Phishing Working Group* - APWG), une association d'entreprises informatiques, a rapporté que le nombre de sites hébergeant des enregistreurs de frappe criminels (*keylogging crimeware*) s'élevait à 3 362 en janvier 2008. [5]

- Faux courriels ou pages web : APWG a détecté 299 307 URLs uniques durant l'année 2007, et a noté que les États-Unis restent le premier pays hébergeant des sites d'hameçonnage avec 37 % du total de ce genre de sites. Plus de 55 % des attaques d'hameçonnage sont des contrefaçons de sites internet d'entreprises hébergées aux États-Unis, selon un rapport d'IBM. [6]

- Les virus : 38 % des individus interrogés par « *Consumer Report* » ont fait État d'une infection de leur ordinateur par un virus durant ces deux dernières années, et 34 % ont signalé une infection par un logiciel espion durant les six derniers mois. Les infections par virus ont incité 1, 8 million de foyers à remplacer leurs ordinateurs personnels ces deux dernières années, et 850 000 les ont remplacés ces six derniers mois en raison d'infections par des logiciels espions. [7]

Les entreprises, autant que les usagers, sont victimes de cette criminalité :

- le Centre de plaintes pour crimes sur Internet (*Internet Crime Complaint Center*) a totalisé plus de 90 000 plaintes auprès des services de police en 2007, qui s'élèvent à des pertes de près de 239,09 millions de dollars [8];

- les consommateurs américains ont perdu une somme estimée à 7,2 milliards de dollars en raison de virus, logiciels espions et hameçonnage en 2006 [9];

....

(1) *Pew Internet and American Life Project*, février 2008, www.pewinternet.org

(2) «Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats», GAO-07-705, U.S. *Government Accountability Office*, juin 2007, www.gao.gov

(3) *Idem*.

(4) *Idem*.

(5) «Phishing Activity Trends -January 2008», *Antiphishing Working Group*, www.antiphishing.org

(6) *Op. cit.*, www.gao.gov

(7) «2007 State of the Net report», Consumers Reports, http://www.consumerreports.org

(8) «2007 Internet Crime Report», *Internet Crime Complaint Center*, www.ic3.gov, La création de ce centre est le résultat du partenariat entre le *Federal Bureau of Investigation* (FBI), l'association à but non lucratif *National White Collar Crime Center* et le *Bureau of Justice Assistance*.

(9) «2007 State of the Net report», *Consumers Reports*, http://www.consumerreports.org

- les organisations américaines ont perdu une somme estimée à 67,2 milliards de dollars en raison de la criminalité informatique en 2005 [10];

- une enquête auprès d'entreprises américaines a montré que les pertes moyennes annuelles dues au cybercrime ont plus que doublé, passant de 168 000 dollars en 2006 à 424 000 dollars en 2007 [11].

La mise en réseau des ordinateurs a aussi ouvert la voie à des types de criminalité qui menacent la sécurité publique, comme le harcèlement et l'exploitation des enfants.

- une enquête récente [12] a montré qu'un enfant sur sept ayant entre 10 et 17 ans a reçu une sollicitation sexuelle en ligne ; un sur trois s'est trouvé involontairement exposé à des photos de personnes nues ou d'activités sexuelles ; et un sur onze a été menacé ou harcelé ;

- d'autres recherches ont montré que 7 % des jeunes adolescents utilisateurs du Net disent avoir eu peur ou s'être sentis mal à l'aise à la suite d'un contact en ligne avec un inconnu [13];

- des responsables gouvernementaux ont annoncé en juillet 2007 que MySpace.com a recensé, sur son site internet en réseau très en vogue, plus de 29 000 délinquants sexuels fichés par les services de police.

Patrouiller dans le cyberspace

De nombreux organismes aux États-Unis ont pour mission de détecter, enquêter et poursuivre en justice le cybercrime. Les acteurs clefs à l'échelon du gouvernement fédéral sont le ministère de la Justice, de la Sécurité intérieure, de la Défense, et la Commission Fédérale du Commerce. Les polices, à l'échelon local et à celui des États, jouent aussi un rôle important en matière de protection de la population.

En tant que premiers magistrats de la hiérarchie judiciaire de chacun des États fédérés, les ministres de la Justice exercent une fonction de conseillers auprès des organes législatifs et exécutifs, et jouent aussi le rôle de procureur général au service de tous les citoyens. Bien que variant d'une juridiction à l'autre en raison des dispositions constitutionnelles et statutaires de chaque État, leurs pouvoirs habituels consistent à faire appliquer les lois de leur État fédéré ; agir en tant que défenseurs des intérêts publics dans des domaines tels que la protection de l'enfance, la protection des consommateurs, la régulation antitrust et des services publics ; proposer des lois ; et porter la responsabilité de représenter le gouvernement de l'État lors des procès.

Le ministère de la Justice de l'État de Washington est reconnu comme un leader national en matière d'efforts pour combattre les crimes high-tech. En 2000, l'État de Washington est devenu le deuxième État fédéré en matière d'innovation dans ce domaine. Le ministère de la Justice de l'État a développé une unité entièrement spécialisée dans la protection des consommateurs victimes de criminalité high-tech [14]. Il propose aussi une législation permettant d'épauler la police et les juges d'instruction dans leur travail, fournit une formation aux résidents de l'État de Washington afin de les prémunir contre le cybercrime, et construit des partenariats efficaces avec différents organismes qui travaillent à combattre cette menace.

Peu de temps après avoir gagné mon élection au poste de ministre de la Justice en 2005, j'ai recherché un appui supplémentaire auprès des assemblées législatives de notre État afin de faire face à l'augmentation vertigineuse de la fraude high-tech et des affaires de vols d'identités dans notre État. Les deux chambres ont approuvé une rallonge budgétaire de 1,6 million de dollars pour notre Bureau de protection du consommateur, dont une partie a pu financer deux nouveaux experts juridiques, un expert en analyses d'ordinateurs, ainsi qu'un laboratoire informatique de pointe où des outils sophistiqués sont utilisés pour détecter les hackers, les pourvoyeurs de logiciels espions et d'autres types de fraudes sur Internet.

....

(10) «2005 Computer Crime Survey», FBI.

(11) «2007 Computer Crime and Security Survey», *Computer Security Institute*, www.gocsi.com

(12) «Online Victimization: A Report on the Nation's Youth», 2006, *National Center for Missing and Exploited Children* (Centre National pour les Enfants exploités ou Disparus), www.missingkids.com

(13) «Teens and Online Stranger Contact», octobre 2007, *Pew Internet and American Life Project*, www.pewinternet.org

(14) Le combat du ministre de la Justice de l'État de Washington (*Washington Attorney General*) contre le cybercrime se déroule essentiellement dans le domaine du droit civil, dans lequel les sanctions comprennent des amendes pour les contrevenants et des dispositions injonctives qui rendent obligatoires des changements dans les pratiques commerciales. Si les ministres de la Justice de certains États fédérés ont autorité pour engager des poursuites judiciaires pour des affaires criminelles qui peuvent entraîner l'emprisonnement, la législation de l'État de Washington limite l'autorité du ministère pour enquêter et poursuivre de telles affaires en justice criminelle. Le ministère n'ouvre pas d'enquêtes criminelles sans une requête de la part du procureur d'un comté ou du Gouverneur.

Éliminer les « spyware »

Le spyware [15] est manifestement devenu la plus importante menace en ligne pour les consommateurs et le monde des affaires depuis l'existence d'Internet. L'État de Washington a été l'un des premiers à adopter une loi interdisant explicitement les activités de spyware et prévoyant de lourdes sanctions à l'encontre de ceux qui l'enfreindraient.

La Loi de l'État de Washington sur les Logiciels Espions des Ordinateurs (*Washington Computer Spyware Act* [16]) a pris effet en juillet 2005, et donne au ministère de la Justice un puissant instrument pour décourager et poursuivre en justice les pourvoyeurs de spyware. Le ministère de la Justice a obtenu des jugements favorables aux consommateurs dans la totalité des six poursuites en justice déjà intentées.

Treize États fédérés ont maintenant adopté une législation qui combat spécifiquement le spyware. La nécessité d'un tel dispositif est rendue évidente si on se reporte aux statistiques stupéfiantes, y compris les rapports qui estiment que le spyware et d'autres logiciels indésirables sont installés sur 80 % des ordinateurs des usagers [17]. Une étude réalisée par des fournisseurs de logiciels a trouvé une moyenne de vingt-cinq logiciels espions, logiciels publicitaires (« adwares ») et autres programmes potentiellement indésirables par ordinateur personnel [18]. Microsoft a relevé que 50 % de ses demandes d'assistance informatique de la part de ses utilisateurs confrontés à des pannes d'ordinateurs provenaient de spywares.

Tandis que s'accroissent les inquiétudes sur la sécurité informatique, la confiance du consommateur dans le commerce et les transactions financières en ligne est susceptible d'être ébranlée. La seule manière de préserver la fiabilité du marché Internet est, du point de vue du ministère de la Justice, d'aborder les procès high-tech comme n'importe quels autres et d'exercer ses pouvoirs de police au moment opportun.

Dans leur combat contre le spyware, les États rencontrent un problème majeur, à savoir la confusion très répandue et la controverse sur les définitions du spyware par opposition à l'adware. Certains pensent qu'un logiciel qui ramasse la moindre information sur l'usage d'un ordinateur par son utilisateur devrait être appelé spyware. D'autres considèrent qu'un logiciel intégré affichant de la publicité ciblée est un spyware. D'autres encore pensent que la définition devrait être limitée au logiciel qui vole des informations personnelles.

La loi de l'État de Washington sur les spyware définit celui-ci par les effets du logiciel sur l'ordinateur d'un utilisateur, ainsi que par la méthode selon laquelle il a été installé. La loi interdit de recueillir des informations personnelles identifiables par le biais de l'espionnage qui surveille la frappe sur le clavier (enregistreurs de frappe) ; de collecter l'historique de la navigation d'un usager sur le Net ; de prendre le contrôle d'un ordinateur personnel pour envoyer des courriels non autorisés ou des virus ; de créer de fausses charges financières ; d'orchestrer des attaques groupées sur d'autres ordinateurs ; d'ouvrir des « pop-ups [19]» ; de modifier les paramètres de sécurité ; et d'interférer avec la capacité de l'utilisateur à identifier et enlever le spyware.

La loi de l'État de Washington sur les spyware ne se limite pas à proscrire les programmes qui répondent à la définition la plus étroite de ce dernier, mais punit aussi ceux qui font des présentations faussées pour inciter les utilisateurs à installer un logiciel, y compris les présentations trompeuses quant à l'efficacité de la protection assurée par un logiciel de sécurité sur un ordinateur personnel.

Le ministère de la Justice – ou tout possesseur d'un site web ou d'une marque de fabrique qui est victime de piratage par spyware – peut intenter une poursuite en justice en invoquant notre loi. Microsoft l'a fait avec beaucoup de succès. Les accusés peuvent être condamnés jusqu'à 100 000 dollars d'amende pour infraction ou à hauteur de l'évaluation des dommages subis, et un tribunal peut même relever le seuil des dommages à hauteur d'un maximum de 2 millions de dollars. Une infraction à la loi sur les spyware est aussi une infraction à la loi de l'État de Washington sur la protection du consommateur [20], au terme de laquelle les contrevenants peuvent être condamnés à une amende pouvant s'élever jusqu'à 2 000 dollars par infraction.

....

(15) Globalement, le spyware est un logiciel trompeur installé dans un ordinateur, souvent à l'insu de l'usager ou sans son consentement en connaissance de cause. Un tel logiciel peut collecter et transmettre des informations personnelles, modifier d'importantes configurations de confidentialité et de sécurité, et même prendre totalement le contrôle de l'ordinateur de l'usager.

(16) *Revised Code of Washington* (RCW) 19.270, www.leg.wa.gov

(17) Enquêtes réalisées en 2004 par l'Institut d'études de marchés IDC et le *National Cyber Security Alliance*.

(18) *Earthlink and Webroot Software's SpyAudit*, rapport rendu public en février 2005.

(19) Fenêtre intruse ou fenêtre surgissante de publicités agressives dans une fenêtre secondaire qui s'affiche sans avoir été sollicitée par l'utilisateur devant la fenêtre de navigation principale lorsqu'on navigue sur Internet.

(20) RCW 19.86, www.leg.wa.gov

Le ministère de la Justice a intenté six procès fondés sur notre loi contre les Spyware. Ces poursuites judiciaires ont eu pour objet une variété d'itérations de spywares, et ont toutes entraîné des décisions comprenant des dommages et intérêts, des injonctions à cessation immédiates des activités incriminées, et le dédommagement des consommateurs lésés. Les exemples sont les suivants :

- En janvier 2006, nous avons intenté notre premier procès contre *Secure Computer*, installé à New York, un supposé vendeur de produits anti-spyware, qui faisait de la publicité par le biais de « pop-ups » (fenêtre intruse ou fenêtre surgissante) qui déformaient le risque, pour l'utilisateur, d'une infection par spyware. Le pop-up, qui ressemblait à une alerte officielle de sécurité de Microsoft, encourageait l'utilisateur à mettre en place un scan gratuit de l'ordinateur. Le scan montrait toujours la présence d'un spyware, même s'il n'y en avait aucun. Les pop-ups ne pouvaient pas être fermés en cliquant sur les points de fermeture habituels. Une issue au procès fut finalement trouvée avec tous les accusés par un dédommagement d'un million de dollars aux consommateurs.

- En août 2006, le ministère de la Justice de l'État de Washington a poursuivi *Digital Enterprises d/b/a/Movieland.com*, accusé d'offrir des abonnements avec essais gratuits à des films pour adultes, pour ensuite facturer les particuliers en leur envoyant d'incessants pop-ups sous forme de vidéos, leur réclamant un paiement après l'expiration de la période d'essai. Les destinataires se trouvaient dans l'incapacité de fermer ou réduire les pop-ups. L'État de Washington allégua que *Movieland* avait installé le spyware à l'origine de la présentation répétitive de la vidéo, et de sa réinstallation automatique, même lorsque l'usager tentait de la désinstaller. L'affaire s'est réglée par une injonction obligeant les accusés à cesser de faire de la publicité par le biais de cette méthode, le paiement d'indemnités et le dédommagement des consommateurs.

- En octobre 2006, nous avons poursuivi *High Falls Media* et *ROC Telecommunications* pour leur logiciel « Spyware Slayer » qui incitait, de manière frauduleuse, les utilisateurs à l'installer en prétendant faussement que leurs ordinateurs étaient prétendument déjà infectés. L'affaire s'est réglée par une injonction limitant à l'avenir ces pratiques publicitaires, et le paiement d'indemnités ainsi que le dédommagement des consommateurs.

- En novembre 2006, nous avons poursuivi un particulier de New York à propos de son logiciel « QuickShield » qui incitait les usagers à l'installer en faisant de fausses évaluations de leurs vulnérabilités en matière de sécurité. L'affaire s'est réglée encore une fois par une injonction de cessation, le paiement d'indemnités et le dédommagement des consommateurs.

- En février 2007, l'État de Washington a poursuivi *Securelink Networks* et LLC, installés en Californie, et plusieurs autres accusés, pour l'utilisation de messages « Net Send » et des scans gratuits trompeurs pour vendre leurs produits (Registry Sweeper Pro, Registry Rinse, Registry Doc, Registry Cleaner 32 et Registry Cleaner Pro). Les messages induisaient les utilisateurs en erreur en leur faisant croire que leurs ordinateurs étaient infectés, et qu'il leur fallait acheter les produits en question afin de les nettoyer. Le tribunal accepta les requêtes de l'État de Washington qui réclamait un jugement immédiat, ordonnant aux accusés de rembourser des centaines de consommateurs de l'État de Washington.

- En mars 2008, nous avons poursuivi un particulier, à Scottsdale en Arizona, pour avoir contraint les usagers à acheter un logiciel bloquant les pop-ups de leur ordinateur en les bombardant préalablement de publicités pour le Viagra, et d'autres de nature pornographique. Notre plainte alléguait que les usagers qui téléchargeaient les produits vantés par la publicité, qui comprenaient Messenger Blocker, WinAntiVirus Pro 2007, System Doctor et WinAntiSpyware, subissaient un préjudice supplémentaire quand le logiciel provoqua l'envoi massif et furtif de messages, à partir de leurs propres ordinateurs, vers d'autres ordinateurs personnels, à un rythme d'un toutes les deux secondes. L'affaire s'est réglée en mai 2008 par une injonction de cessation et le dédommagement des usagers lésés.

À l'échelon fédéral, l'accès non autorisé à un ordinateur est illégal, aux termes de la loi *Computer Fraud and Abuse Act* [21]. Les législateurs fédéraux ont tenté en vain, à partir de 2004 et plus récemment en 2007, de voter une loi pénalisant plus sévèrement les créateurs de spyware en augmentant les peines de prison. La loi établissant la Commission au commerce fédéral (*Federal Trade Commission Act* – FTCA) fournit des dispositions facilitant les poursuites contre les fournisseurs de spyware. Bien que le FTCA ne soit pas aussi précis que le *Computer Spyware Act* de l'État de Washington dans la définition des pratiques frauduleuses, il s'est avéré assez efficace dans de nombreuses poursuites judiciaires fédérales.

(21) 18 U.S.C. § 1030, http://www.gpoaccess.gov/USCODE/index.html

Réduire les spams

À vrai dire, le ministère de la Justice de l'État de Washington a combattu le crime high-tech depuis plus de dix ans, et a fait date en octobre 1998 en lançant la première poursuite en justice d'un État fédéré contre un pourvoyeur d'e-mails non sollicités (« spammer »).

La loi de l'État de Washington contre les courriers électroniques commerciaux indésirables (*Unsolicited Commercial Act*) [22], entrée en vigueur un peu plus tôt cette année-là, a été une des premières dans le pays à réglementer l'envoi de spams. Elle interdit l'envoi de courriels commerciaux indésirables et contenant des informations mensongères, qui utiliseraient le nom de domaine d'un tiers sans autorisation, ou déformeraient le point d'origine du message. La loi impose des pénalités qui peuvent aller jusqu'à 500 dollars par courriel.

Notre poursuite judiciaire accusait un résident de l'Oregon, Jason Heckel, d'avoir envoyé des spams à des millions d'utilisateurs d'Internet pour vendre sa brochure en ligne, intitulée « Comment tirer un avantage d'Internet ». La Cour suprême de l'État de Washington a confirmé, en 2001, la constitutionnalité de notre loi de l'État contre les spams. La Cour suprême fédérale a refusé de réexaminer l'affaire, rendant impossible tout appel de la part de Heckel.

Les assemblées ont amendé la loi anti-spam de notre État en 2005, pour interdire spécifiquement les faux e-mails ou fausses pages web dans lesquels l'identité falsifiée des voleurs induit les consommateurs en erreur. Ces e-mails, qui semblent provenir d'une entreprise, d'une banque ou d'un site de vente aux enchères en ligne, extorquent des informations personnelles. La loi rend illégal le fait qu'une personne travestisse son identité dans le but de solliciter ces informations en ligne.

Le Congrès fédéral a voté la loi *Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act* [23] en 2003, interdisant les e-mails faux ou trompeurs et exigeant que les auteurs de la publicité laissent aux destinataires la possibilité de refuser des sollicitations ultérieures.

Le ministère de la Justice de l'État de Washington a entrepris sa première poursuite en justice en invoquant cette loi peu de temps après son entrée en vigueur en 2004. Le procès intenté, instruit à l'*U.S. District Court*, alléguait que AvTech Direct, une entreprise de marketing californienne maintenant disparue, et MD&I, une société de vente d'ordinateurs installée en Californie, utilisaient des annonces trompeuses et faisaient croire que les messages provenaient d'autres sources.

Stopper la publicité mensongère sur Internet

Le ministère de la Justice de l'État de Washington a porté devant les tribunaux plus d'une douzaine d'affaires impliquant la publicité sur Internet depuis 2005. Au-delà de notre législation sur les spyware et les spams, la loi de l'État de Washington « *Unfair Business Practices-Consumer Protection Act* » [24] nous donne un large pouvoir de réglementation. La législation interdit les pratiques déloyales ou trompeuses en matière commerciale et autorise le ministère à réclamer des amendes pouvant aller jusqu'à 2 000 dollars par infraction.

Très récemment, nous avons pris des mesures répressives à l'encontre de publicitaires affiliés à Internet qui utilisaient des pop-ups Net Send ou Windows Messenger pour commercialiser des logiciels de façon trompeuse. Windows Messenger Service, à ne pas confondre avec le programme de messages instantanés Windows Live Messenger, est essentiellement conçu pour être utilisé sur un réseau et autorise ses administrateurs à envoyer des notices aux usagers. Notre enquête a découvert qu'un nombre croissant d'individus inondait les consommateurs de messages Net Send et de publicités par pop-ups traditionnels qui ressemblaient fréquemment à des systèmes d'alerte. Leur intention était de faire peur aux usagers pour qu'ils achètent un produit supposé protéger leur ordinateur contre les pop-ups, virus et spywares. De nombreux usagers se sont retrouvés en train de payer pour un programme qui n'était quasiment d'aucune utilité ou qui rendait leur ordinateur encore plus vulnérable aux malware. Nos poursuites en justice ont eu pour résultat l'arrêt définitif de nombre de ces opérations et l'obtention de remboursements aux usagers.

Nous avons aussi récemment intenté des poursuites contre des sociétés en ligne qui faisaient la promotion de produits onéreux « gratuits », comme des télévisions à

(22) RCW 19.190, www.leg.wa.gov
(23) U.S.C. §§ 7701-7713 and 18 U.S.C. § 1037, http://www.gpoaccess.gov/USCODE/index.html
(24) RCW 19.86, www.leg.wa.gov

haute définition, des caméras digitales et des ordinateurs portables. Les consommateurs devaient finalement payer une somme plus élevée que le prix réel afin de les recevoir. Plus encore, nous avons allégué que ces entreprises étaient en fait à la recherche d'informations personnelles concernant les usagers, afin de pouvoir les vendre. Ces poursuites en justice ont eu pour résultat des injonctions interdisant les pratiques de ces sociétés et prévoyant des réparations pour les consommateurs. Nos poursuites en justice ont aussi concerné des pratiques de facturations trompeuses et le non-respect de commandes de marchandises, entre autres affaires.

Promouvoir la sécurité des données

La sécurité des données et la protection des informations personnelles sont devenues des défis juridiques et commerciaux majeurs, tant pour les entités publiques que privées. On estime que les entreprises dépensent chacune une moyenne de 5 millions de dollars pour se remettre d'un incident concernant le non-respect de la sécurité de leurs données. Bien entendu, ces violations ont des effets très néfastes sur la confiance des consommateurs. Par conséquent, le public réclame plus de protections. La sécurité financière est d'une importance primordiale, et il est de notre responsabilité de protéger le public contre les pratiques commerciales qui mettent en danger leur sécurité.

L'État de Washington s'est joint à presque la moitié des États fédérés qui légifèrent sur la violation de la sécurité en ligne pour exiger de la part des entreprises, ainsi que des organes gouvernementaux à l'échelon local et fédéral, qu'ils divulguent les violations de leurs systèmes de sécurité non cryptés contenant des informations personnelles de leurs clients. Aucun organisme répressif n'est spécifiquement désigné pour appliquer notre loi punissant le viol des données personnelles [25], mais le ministre de la Justice peut assumer ce rôle par défaut.

Le but de notre législation est d'assurer que, si un viol de données survient, les usagers en soient rapidement notifiés, afin de leur permettre de s'assurer de la protection de leurs informations personnelles. Notre législation exige que la divulgation d'un non-respect de la confidentialité des données soit faite « *sans retard déraisonnable, compatible avec les besoins légitimes pour appliquer la loi* ». Cela comprend une notification écrite et électronique ou, dans certains cas, la publication d'avertissements dans les médias. La législation encourage les administrations et les entreprises à assumer la responsabilité des données des usagers et à leur permettre d'agir rapidement pour assurer l'intégrité de leurs informations personnelles.

Une autre loi de l'État de Washington [26] exige des entreprises et des administrations publiques qu'elles détruisent les informations personnelles de manière responsable. Les contrevenants engagent leur responsabilité civile si un particulier subit un préjudice à la suite d'une infraction. Le ministère de la Justice s'est donné pour mission de se concentrer sur un travail de prise de conscience afin que les entreprises et les administrations puissent développer des systèmes capables de protéger les informations capitales qui leur sont confiées par leur clientèle et par les usagers.

Protéger les enfants sur le Net

En tant que premier responsable du système judiciaire de l'État de Washington, j'ai la possibilité exceptionnelle de travailler avec les services de police, les procureurs, les législateurs et les groupes d'intérêt pour améliorer la sécurité publique. Dans le cadre de la campagne menée par nos services en faveur de la sécurité sur Internet (*SafetyNet)*, nos équipes se sont rendues sur le terrain dans l'État de Washington afin de faire partager ce que nous avons appris des experts sur les dangers d'Internet et pour parler des manières dont les enfants peuvent éviter ces dangers. Nous avons visité des écoles, rencontré les services de police et parlé avec des associations de parents d'élèves pour diffuser le message sur la sécurité.

En 2006, le ministère de la Justice s'est associé au Centre national pour les enfants disparus et exploités (*National Center for Missing & Exploited Children*), afin de proposer des séminaires de formation pour préparer 400 éducateurs et officiers de police à enseigner la sécurité sur Internet en utilisant un programme créé par une organisation appelée *NetSmartz*. En 2006, je me suis associé au *National Center for Missing & Exploited Children* avec des leaders de l'ensemble de l'État pour encourager 10 000 parents et responsables de mineurs à s'informer sur les questions de sécurité sur Internet et sur les procédés de prévention à travers *The Connected Family Online Classroom*, développée par la compagnie de télécommunications *Qwest*.

(25) RCW 19.255.010 and RCW 42.56.590, www.leg.wa.gov
(26) RCW 19.215.010, www.leg.wa.gov

En 2007, j'ai formé l'Équipe Spéciale (*Task Force*) pour la sécurité des jeunes sur Internet, afin de renforcer la sensibilisation à la sécurité sur le Net dans l'État de Washington. Cette large coalition englobe les forces de police, les groupes d'intérêts de défense de l'enfant, les experts universitaires, les représentants du gouvernement à l'échelon local et de l'État, les entreprises de technologie et les associations, ainsi que les citoyens concernés. Les membres sont divisés en trois sous-comités, chacun se concentrant sur un problème particulier lié à la sécurité des jeunes sur Internet. Cette équipe spéciale révise, entre autres activités, la législation en cours dans des domaines apparentés tels que la pornographie impliquant des enfants et les communications illégales avec des mineurs.

En janvier 2008, les ministres de la Justice de tout le pays ont signé un accord avec *MySpace*, créant une équipe spéciale [27] afin de développer une technologie permettant de vérifier l'âge et l'identité des utilisateurs des sites de réseaux sociaux. *MySpace* et les ministres de la Justice se sont entendus sur une déclaration commune de principes fondamentaux dans laquelle nous mettons l'accent sur notre objectif commun de protéger les enfants des dangers de sites à teneur inappropriée et de contacts indésirables de la part d'adultes. Grâce à cet accord, *MySpace* a réalisé de gros progrès en matière de sécurité, comprenant le passage en revue d'images et vidéos afin d'y repérer un éventuel contenu nocif, et d'autres dispositions techniques destinées à protéger de nouveaux utilisateurs de moins de 18 ans contre tout contact en ligne indésirable avec un adulte. L'entreprise *MySpace* élimine aussi les profils électroniques créés par des délinquants sexuels fichés par la police.

MySpace travaille à établir les profils des utilisateurs de 16 et 17 ans en les gardant confidentiels, et prévoit de mettre en place un « verrouillage de l'âge », par lequel les utilisateurs qui indiquent qu'ils ont moins de 18 ans ne pourront pas modifier l'âge déclaré. L'accord exige aussi que la société dresse un registre des adresses électroniques fournies par les parents qui désirent restreindre l'accès de leur enfant au site. La société a créé des matériaux pédagogiques pour les parents, établi un service en ligne 24 heures sur 24 pour répondre aux enquêtes de la police, et formé plus de 3 500 policiers.

Nous sommes parvenus à un accord similaire avec *Facebook* en mai dernier et cette société a, elle aussi, rejoint l'équipe spéciale. Ce dernier rendra des comptes aux ministères de la Justice tous les trois mois et publiera un rapport officiel avec des conclusions et recommandations fin 2008.

Les défis qui demeurent

En dépit d'immenses progrès réalisés dans la surveillance du cyberespace, les entités publiques et privées demeurent confrontées à des défis. Dans un rapport adressé au Congrès en juin 2007, le *U.S. Government Accountability Office* décrivait plusieurs obstacles à la mise en œuvre de mesures contre le cybercrime, comme le manque de comptes-rendus précis des délits aux services de police ; la difficulté à obtenir et garder des enquêteurs, des procureurs et des experts en analyses d'ordinateurs ; les difficultés à rester au fait des technologies en cours et des techniques criminelles ; et le fait de travailler dans un environnement sans frontières.

À la différence des délits traditionnels, ceux qui sont perpétrés par le biais des réseaux informatiques peuvent être commis de loin, effectués automatiquement et sont en mesure d'attaquer un très grand nombre de victimes simultanément. Les auteurs peuvent rester plus facilement anonymes. Les enquêtes sont plus compliquées en raison de la nécessité de traiter avec de multiples juridictions, chacune ayant sa propre législation et ses procédures légales.

En dépit d'initiatives fréquentes et significatives destinées à informer les particuliers de leurs droits et des aides dont ils peuvent bénéficier, des études [28] laissent penser que 17 % d'Américains n'ont toujours pas de logiciels antivirus installés sur leur ordinateur et qu'environ un tiers n'utilise pas de logiciel pour bloquer ou enlever un spyware. Les chercheurs ont aussi découvert que la moitié des Américains possédant des connexions internet sans fil à domicile n'ont pas pris les précautions de base, telles que l'encodage. On estime à environ 3,7 millions le nombre de foyers américains possédant des raccordements avec des transmissions à large bande, et qui ne possèdent toujours pas de mur pare-feu.

Certaines études suggèrent que, sauf s'ils sont confrontés à un gros problème, les Américains ont tendance à ne pas se soucier de leurs informations personnelles, ni à prendre des dispositions pour limiter leur quantité susceptible d'être trouvée en ligne [29].

(27) L'équipe spéciale est dirigée par le Berkman Center for Internet and Society at Harvard University, http://cyber.law.harvard.edu/

(28) *Consumers Reports*, 2007, State of the Net report, www.consumerreports.org and McAfee-National Cyber Safety Alliance Online Safety Study, octobre 2007, www.staysafeonline.org

(29) «Privacy Implications of Fast, Mobile Internet Access», Pew Internet and American Life Project, février 2008, www.pewinternet.org

L'importance des partenariats

Les partenariats constituent un élément clef pour combattre le cybercrime avec succès. Très tôt, les changements rapides dans la nature de la criminalité et de la technologie ont entraîné des partenariats presque involontaires entre citoyens, entreprises, gouvernement et police, alors que tous se débattaient pour trouver des moyens efficaces pour faire face à ces nouvelles menaces. Par exemple, dans le passé, un service chargé de faire respecter la loi et s'occupant d'instruire un procès n'aurait pu compter que sur la coopération amicale de fournisseurs de services internet acceptant de divulguer les informations nécessaires pour engager des poursuites judiciaires dans une affaire de cybercrime. Même la police disposant de ressources suffisantes pour ouvrir la voie sur ce nouveau front de la lutte anticriminelle trouvait qu'il était difficile de maîtriser le vaste univers en perpétuelle évolution de la criminalité sur Internet.

Heureusement, nous sommes aujourd'hui bien mieux armés pour lutter contre la délinquance high-tech. Il existe maintenant des mécanismes permettant d'assurer la coordination entre la police, les fournisseurs de services et d'autres. Par exemple, nos services ont travaillé en coopération avec Microsoft et AOL afin de rassembler l'information nécessaire pour engager des poursuites judiciaires contre des pourvoyeurs de spywares et de spams.

De plus, alors que les citoyens recherchent une plus grande protection contre la délinquance en ligne, le rôle du gouvernement évolue pour faire face à ces questions. L'Association nationale des ministres de la Justice (*National Association of Attorneys General*) anime une conférence annuelle sur le cybercrime pour fournir une formation en matière d'enquêtes, de législation, de procès et de campagnes d'éducation publique. Grâce à un effort de coopération, mis en place en 2003, entre notre association, le Centre national de la justice et l'État de droit de l'université du Mississippi (*National Center for Justice and The Rule of Law*), plus de 415 procureurs rattachés à des ministères de la Justice ont suivi une formation spéciale sur la criminalité électronique. J'ai personnellement dirigé deux séminaires sur la technologie pour des ministres de la justice et leurs équipes lors de nos réunions nationales.

Afin de réduire le nombre de victimes de ces comportements criminels, il est également crucial de renforcer la sensibilisation du public à l'importance de la protection des informations. Le ministère de la Justice de l'État de Washington s'est associé avec l'*American Association of Retired People* (AARP), Microsoft et la Commission fédérale du commerce, en 2006, pour présenter une Campagne de Cyber-sécurité, afin d'éduquer le public sur les dangers du Net, comme les faux courriers électroniques ou pages web, les virus et les spyware. La sécurité sur Internet fait aussi partie de notre programme d'éducation à la prévention contre le vol d'identité.

Les services de police s'équipent de nouvelles armes pour mener des enquêtes high-tech, car les traces et preuves d'actes criminels sont de plus en plus stockées sur des ordinateurs, des téléphones portables, des caméras numériques, dans des courriers électroniques, des messages et imageries électroniques. Les entreprises intensifient la sécurisation des données. Plus important encore, tous les acteurs reconnaissent maintenant que les partenariats ne sont pas seulement utiles, mais nécessaires et cruciaux afin de combattre et prévenir ce type de criminalité.

Conclusion

Le combat contre le cybercrime implique notre participation à tous – gouvernement, secteur privé, ainsi que le public. Le ministère de la Justice de l'État de Washington travaille intensément pour fournir un *leadership* à l'échelon de l'État, soutenir les services de police, éduquer les consommateurs, aider les entreprises et protéger les enfants. Les partenariats constituent la clef pour une réussite à long terme.

Rob McKENNA

1968 aux origines de la sociologie de la police

Jean-Louis LOUBET DEL BAYLE

En ces temps de commémoration des événements de mai 1968, on voudrait évoquer ici une conséquence au premier abord assez paradoxale de ces événements, à savoir la façon dont ceux-ci ont ouvert la voie, en France, et plus largement, en Europe, au développement des recherches sur les institutions policières en contribuant ainsi à l'essor de cette discipline que l'on peut appeler aujourd'hui la *sociologie de la police* (en usant ici du terme police dans son sens fonctionnel et en l'appliquant à toutes les institutions assurant des fonctions policières).

En effet, la dénonciation par les mouvements contestataires de l'époque de l'orientation « répressive » des institutions politiques et sociales établies a conduit à accorder une attention particulière à ce qui est alors apparu comme l'un des instruments privilégiés de cette « répression » : la police. Commence ainsi à se manifester un mouvement d'intérêt pour la connaissance des institutions policières et de leurs pratiques, qui s'articule donc sur de fortes motivations idéologiques, en s'accompagnant d'une prégnante orientation normative, celle-ci se traduisant par une attitude très critique, surtout soucieuse de débusquer et de dénoncer dans la police le « bras armé » de l'ordre social établi. Cela dit, et quelle que soit l'ambiguïté de ces motivations initiales, s'est ainsi amorcée une évolution qui va faire émerger les institutions policières et leurs pratiques comme des objets légitimes de la réflexion intellectuelle et scientifique.

Avant 1968 : un quasi-désert bibliographique

Jusque là, en France tout particulièrement, la réflexion sur la police était très peu développée et un observateur pouvait noter, non sans raison, au tout début des années 1970 : « *Dans notre pays latin, bourré d'inhibitions et d'interdits, les sujets tabous ne manquent pas. La police est de ceux-là. Une forme de pudeur rend muets les hommes politiques, de l'opposition comme de la majorité, au moment de répondre aux questions concernant la place de cette institution dans le pays* » [1]. Le comportement des milieux intellectuels n'était guère différent. Ainsi, en 1970, la première édition de l'*Encyclopoedia Universalis* ne comportait pas d'article « police », alors qu'on trouvait dans son équivalent anglais, l'*Encyclopaedia Britannica*, un article de vingt pages sur le sujet. De même, dans l'index-matière de la *Revue Française de Science Politique* pour les années 1951-71 ne figurait pas d'entrée « police » et, en 1970 toujours, rendant compte en cinq lignes du livre de David H. Bayley, *The police and political development in India*, la chronique bibliographique de cette même revue s'étonnait « *qu'une si importante étude soit consacrée à un tel sujet* » !

En France, les ressources bibliographiques en matière de connaissances sur les phénomènes policiers étaient donc à cette époque des plus limitées [2]. Elles ont, en effet, longtemps été rares et essentiellement constituées, à côté de quelques ouvrages de journalistes [3] et de polémistes, par des écrits de policiers. Soit des livres de mémoires et de souvenirs, au contenu souvent très anecdotique, soit, de façon plus technique, des thèses de droit rédigées par des commissaires de police, comportant assez fréquemment des perspectives réformatrices, notamment pour remédier à l'éclatement des services de police qui a caractérisé l'organisation policière française jusqu'en 1941. À cela, il faut ajouter un certain nombre d'ouvrages sur l'histoire de la police, concernant surtout l'histoire de la police de Paris après le XVII^{e} siècle.

Après la Seconde Guerre mondiale, la situation jusqu'aux années 1970 ne s'était guère modifiée. La littérature sur la police est alors toujours une littérature de commissaires de police, que leur formation, leurs intérêts et leurs goûts personnels incitaient parfois à une réflexion plus générale

(1) J. Sarrazin, *La police en miettes*, Paris, Calman-Lévy, 1974, p. 207.
(2) Cf. Jean Bastier, *Introduction à une historiographie des institutions policières françaises,* Toulouse, Publications du CERP, 1989, 84 p.
(3) Comme celui d'André Ulmann, *Le quatrième pouvoir, police*, Paris, Aubier,1935, 285 p.

sur leur métier. Ainsi avec les ouvrages historiques des commissaires Henri Buisson [4], Jacques Delarue [5] ou Willy-Paul Romain [6]. À cela, il faut ajouter les travaux de policiers engagés dans des activités d'enseignement dans les Instituts de criminologie, comme le commissaire Fernand Cathala à l'Institut d'études criminelles de Toulouse ou le commissaire Marcel Le Clère à l'Institut de criminologie de Paris. Celui-ci publiera, dans la collection *Que-sais je ?*, deux ouvrages, l'un, en 1947, sur *L'histoire de la police*, l'autre, plus fonctionnel, en 1972, intitulé *La police*. Par ailleurs, dans un article de l'*Encyclopédie Larousse*, il se prononçait, en 1971, pour l'apparition d'une «policologie» [7], consistant dans l'étude de « *l'ensemble des règles pragmatiques, technologiques et déontologiques régissant l'organisation et les interventions de la police* », avec la perspective « *d'atténuer la position inconfortable occupée par la police dans toute société évoluée* » et le souci d'éviter aux citoyens les risques qui peuvent naître des « *nécessités facilement invoquées de l'ordre, jointes à la possibilité d'une coercition immédiate* ». C'est donc une approche qui mettait l'accent sur l'intérêt du développement des connaissances, mais en l'accompagnant d'une perspective normative, à la fois réformiste et légitimatrice, de l'action policière, comme en témoigne par exemple aussi le titre de l'un des ouvrages du commissaire Cathala, *Cette police si décriée* [8].

Cette perspective réformiste, on la retrouvait chez un autre commissaire de police, secrétaire général du Syndicat des commissaires de 1955 à 1968, Jean Susini, qui, lui aussi, s'est fait parallèlement l'avocat d'un développement de la recherche scientifique sur les questions policières. Il fut à l'origine de la création, au début de 1968, d'un *Bureau de criminologie et des sciences humaines* au sein de la direction de la Formation de la Police nationale, qui ne survivra pas aux événements de mai. Bien qu'orienté principalement vers la recherche criminologique, ce Bureau n'excluait pas d'utiliser les « sciences humaines » pour étudier « les problèmes latents dans les diverses branches de la police » [9]. Au début des années 1970, la même préoccupation conduira Jean Susini à traverser l'Atlantique et à devenir pendant quelques années professeur associé à l'École de criminologie de l'université de Montréal. Cette expérience nord-américaine le mit en contact avec le courant de recherches qui avait commencé à se développer aux États-Unis dans les années 1960, dont il va s'attacher à faire connaître les travaux à travers les « chroniques de police » trimestrielles qu'il publie dans la *Revue de Science Criminelle et de Droit Pénal Comparé*, en plaidant à la fois pour le développement de ce type de recherches en France et pour la prise en compte de ce genre de travaux dans la réflexion sur l'évolution des institutions et des pratiques policières françaises [10].

Cette approche – lorsqu'elle n'était pas anecdotique - était donc une approche qui restait fortement marquée par des perspectives professionnelles, comme c'est encore une approche à partir d'un point de vue professionnel, celui d'un représentant de l'institution judiciaire, que l'on trouvait dans les livres successifs publiés par le magistrat Serge Fuster sous le pseudonyme de Casamayor [11]. Par ailleurs, les perspectives de ces travaux restaient très juridiques avec des orientations, comme on l'a vu, plus ou moins légitimatrices et réformistes, les perspectives de Jean Susini étant les plus novatrices du fait de son ouverture nord-américaine.

Le changement des années 1970

C'est cette situation qui va se transformer après 1968. Comme on l'a déjà indiqué, pour des motifs scientifiquement ambigus, va naître un courant de recherches sur les institutions policières, qui, peu à peu, plus ou moins épuré de sa dimension idéologique, va évoluer, chez un certain nombre de chercheurs, d'une réflexion militante vers une réflexion scientifique. C'est vrai pour la France, mais ce phénomène a aussi été observable en Grande-Bretagne ou en Allemagne et, dans ces pays, nombre de travaux publiés dans le dernier quart du XX^{e} siècle sont nés d'une curiosité initiale qui n'était pas exempte d'*a prori* idéologiques et normatifs. De ce fait, dans les années

••••

(4) *La police : son histoire*, Paris, Nouvelles Editions Latines, 1958, 318 p.

(5) *Histoire de la Gestapo,* Paris, Fayard, 1962, 472 p.

(6) *Le Dossier de la police : en bourgeois et en tenue*, Paris, Librairie Académique Perrin, 1966, 438 p.

(7) Article « Policologie », *Encyclopédie Larousse*, Paris, Larousse, 1971, p. 9625.

(8) Saverdun, Editions du Champ de Mars, 1971. Il a aussi publié chez le même éditeur : *La police au fil des jours* (1981), *La police face à la criminalité* (1984), *Délinquance et enquêtes financières* (1987).

(9) J. Susini : « La Direction de la formation et le Bureau de Criminologie et de Sciences humaines de la Police Nationale », *Revue de Science Criminelle et de Droit Pénal Comparé*, 1968, III, p. 679 et s.

(10) Les plus importantes de ces chroniques ont été rassemblées à l'initiative du CERP dans l'ouvrage *La police, pour une approche nouvelle*, Toulouse, Presses de l'IEP de Toulouse, 1982, 262 p.

(11) *Le bras séculier : justice et police*, Paris, Seuil, 1960, 310 p. ; *La police*, Paris, Seuil, 1973, 199 p.

1970, la police, et donc aussi la réflexion intellectuelle sur les phénomènes policiers, vont se trouver au centre de vives discussions de nature idéologique et politique[12]. D'autant plus qu'à partir de 1974-75 vont commencer à émerger en France les problèmes posés par la croissance des phénomènes de délinquance et d'insécurité, qui se traduiront, par exemple, par la publication du *Rapport Peyrefitte* sur la violence en 1977 [13] et, jusqu'en 1981, par des controverses sur la réalité du « sentiment d'insécurité », tenu par certains comme l'alibi idéologique d'une dérive autoritaire du pouvoir politique de l'époque.

Dans ce contexte, le premier travail de recherche universitaire important conduit par un non-policier est alors la thèse de droit public soutenue en 1972 par Jean-Jacques Gleizal, *La police nationale : droit et pratique policière en France*. En partant d'une approche juridico-administrative, celui-ci y étudiait le processus de modernisation des institutions policières françaises qui a abouti à la constitution de la Police nationale, telle qu'elle se présentait à la fin des années 1960, après la réforme centralisatrice de 1941, complétée, en 1966, par l'intégration dans la Police nationale de la préfecture de police de Paris. En termes socio-politiques, il interprétait cette évolution centralisatrice comme le processus de construction d'un « État policier », pour faire face à « *l'intensification de la lutte des classes* », résultant de l'émergence d'un « *capitalisme monopolistique d'État* » [14].

Devenu professeur à la faculté de droit de Grenoble, Jean-Jacques Gleizal, qui se définissait comme un « juriste-politologue », y créera un *Centre d'études et de recherches sur la formation et l'administration*, dans le cadre duquel, tout en continuant lui-même à travailler sur ces questions, il fait effectuer un certain nombre de recherches concernant les problèmes policiers, avec des points de vue proches des orientations du groupe « Critique du droit ». C'est aussi en partie dans l'orbite de ce groupe que se développeront à Lyon, tout à la fin des années 1970, les recherches du politologue Claude Journès, spécialiste notamment de l'étude de la Grande Bretagne, dans le cadre d'un C*entre d'épistémologie juridique et politique*.

Parallèlement, un jeune enseignant de droit public, Bernard Asso, qui avait été membre du cabinet du ministre de l'Intérieur Raymond Marcellin au début des années 1970, avait créé, en 1974, à la faculté de droit de Nice, au sein d'un Centre d'études administratives, un *Centre d'études du droit de la police*, dont les activités étaient en relation avec la préparation des étudiants aux concours d'entrée dans la Police nationale. Ce centre organisera en 1977 un colloque sur « la sécurité dans les villes », réunissant des intervenants policiers et universitaires, dont il sera rendu compte dans *la Revue de la Police nationale*. Ses animateurs publieront en 1979 un ouvrage de présentation des *Missions et structures de la Police nationale* [15].

En 1976, se crée enfin, à notre initiative, à l'Université des Sciences sociales de Toulouse, dans le cadre de l'Institut d'études politiques, le *Centre d'études et de recherches sur la police (*CERP). Influencé par certaines des thèses de Jean Susini, ce centre entendait, dès sa création, se singulariser par trois spécificités : la volonté d'abord de substituer à une approche à dominante juridique, une approche sociologique et politologique des institutions policières et de leur fonctionnement ; le souci ensuite d'étudier ces problèmes dans une perspective aussi objective que possible, en tentant de se libérer, autant que faire se peut, des controverses idéologiques ou partisanes suscitées par ces questions ; la préoccupation enfin de distinguer la démarche scientifique à mettre en oeuvre pour la connaissance des réalités policières de la réflexion normative [16].

Ainsi, à la fin des années 1970, le développement de la recherche sur les institutions et les pratiques policières s'est organisé en France autour de trois ou quatre pôles institutionnels, qui présentaient la particularité d'être tous implantés dans des universités non parisiennes, à Grenoble et Lyon, à Nice et à Toulouse. Cela étant, le développement de ces recherches reste alors freiné par la centralisation du système policier français et par les réticences que manifestent les institutions policières, en tant que telles, pour s'ouvrir aux investigations des chercheurs, alors que pourtant s'exprime au niveau individuel une volonté des policiers de faire mieux connaître les caractéristiques et les difficultés de leur métier.

....

(12) On peut rappeler ici que, dans cette perspective, le cas de la première édition (1970) de l'*Encyclopaedia Universalis*, déjà citée, était doublement significatif : du désintérêt pour l'objet, hérité du passé, – pas d'article « police » – mais aussi de son idéologisation, reflétant, cette fois, le contexte du moment, car elle comportait une entrée « police », mais avec un renvoi au mot « répression ».

(13) *Réponses à la violence*, 1977, Paris, Presses Pocket, 228 p.

(14) Grenoble, Presses Universitaires de Grenoble, 1974, 352 p.

(15) P. Arrighi et B. Asso, Paris, Editions de la Revue Moderne, 1979, 296 p.

(16) Sur les circonstances de la création de ce centre, on pourra se reporter à notre article « Eléments d'ego-histoire », *Revue Internationale de Criminologie et de Police technique et scientifique*, 2004, n° 4.

De ce fait, les recherches de terrain supposant un minimum de coopération des institutions policières ne sont alors possibles que lorsque des responsables policiers prennent à titre individuel l'initiative de faciliter le travail des chercheurs, comme ce sera le cas pour la thèse sur les pratiques policières en matière de flagrant délit préparée par René Lévy dans le cadre du *Service d'études pénales et criminologiques du ministère de la Justice*, dirigé par Philippe Robert, qui deviendra plus tard, en 1984, le CESDIP (*Centre d'études sociologiques sur le droit et les institutions pénales*). En fait, les quelques travaux réalisés durant la fin des années 1970 sont des travaux isolés qui ne nécessitent pas d'autorisations institutionnelles, comme la thèse d'Irène Dootjes-Dussuyer sur *Les images de la police dans l'opinion publique* (Grenoble II, 1979), celle de Marie-Hélène Cubaynes, sur *La police et la presse : des institutions et des hommes* (Toulouse I, 1980) [17], celle d'Henri Souchon sur *Le pouvoir discrétionnaire des organes de police* [18], les recherches bibliographiques de Marcel Le Clère [19]et de Jean-Claude Salomon [20], ou le colloque historique sur *L'État et sa police* [21] organisé en 1977 à l'initiative de l'Institut d'histoire administrative.

À l'issue de cette période, la légitimité scientifique de ce type de recherche demeure encore très fragile et le milieu universitaire, encore imprégné des thèses idéologiques dominantes à la fin des années 1960, reste fortement réticent. Si notre article sur « La police dans le système politique » est accepté par la *Revue Française de Science politique* en 1981, le sociologue du travail Dominique Monjardet choisit encore, en 1983, de publier le petit ouvrage monographique qu'il consacre aux policiers sous le pseudonyme de Pierre Demonque [22].

Les développements des années 1980

Dans cette histoire amorcée en 1968, 1982 représente une date importante. Après l'alternance politique de 1981, à l'initiative de la direction de la Formation de la Police nationale et de son directeur Jean-Marc Erbès, s'organise un programme de réforme de la formation des policiers qui entend faire une place aux enseignements que la recherche sociologique peut apporter pour la connaissance des réalités policières. Pour ce faire est alors créé, sous l'égide de la direction de la Formation, avec la collaboration du ministère de la Recherche, un Comité scientifique composé de chercheurs et de policiers [23]. Celui-ci était investi d'une double mission : d'une part, définir les orientations des recherches à susciter et à encourager, d'autre part, organiser des appels d'offre pour gérer des crédits accordés par le ministère de la Recherche afin de favoriser le développement de ce type de recherches.

Cette initiative est importante dans la mesure où elle consacre la légitimité de ces recherches, aussi bien aux yeux de la Police nationale qu'à ceux d'un certain nombre de responsables de la recherche scientifique. En témoignera le numéro spécial qui, à l'instigation de Dominique Monjardet, sera consacré en 1985 à ces questions par la revue *Sociologie du travail*, qui s'ouvrira sur un article de Jean-Claude Monet [24] exprimant le point de vue de l'institution policière sur cet appel aux sciences sociales. La légitimation policière a aussi une conséquence de grande importance pour les chercheurs, à savoir l'ouverture de la Police nationale à leurs investigations et l'accès à des terrains de recherche restés jusque-là inaccessibles. Par ailleurs, dans le même temps, concrétisant cette évolution, est confiée à un organisme de recherche extérieur, la société *Interface*, la réalisation d'une grande étude sociographique interne sur les personnels de la Police nationale, comportant notamment l'analyse de prés de 9 000 réponses à une enquête par questionnaire [25].

Ces mesures incitatives vont atteindre leurs objectifs. Elles contribuent d'abord à soutenir et à dynamiser les activités des pôles institutionnels qui s'étaient constitués antérieurement à Grenoble, Lyon, Nice et Toulouse. Jean-Jacques Gleizal publie ainsi, en 1985, *Le désordre*

••••

(17) *La police et la presse : des institutions et des hommes,* Publications du CERP, 2 tomes, 1981.

(18) *Admonester, du pouvoir discrétionnaire des organes de police*. Éditions du CNRS, 1981, 201 p.

(19) *Bibliographie critique de la police*, Paris, Yzer, 1981, 351 p.

(20) *Bibliographie historique des institutions policières françaises*, Toulouse, Publications du CERP, 1986, 78 p.

(21) L'État et sa police, Genève, Droz, 1979, 216 p.

(22) *Les policiers*, Paris, La Découverte, 1983. 130 p.

(23) Celui-ci était notamment composé de : André Bruston, Georges Carrot, Laurence Coutrot, Jean-Marc Erbès, Jean-Jacques Gleizal, Claude Guillot, Claude Journès, Jean-Louis Loubet del Bayle, Gérard Métoudi, Jean-Claude Monet, Dominique Monjardet, Claude Noreck, André Sibille, Jean Susini, Bernard Tarrin. Animé par André Sibille, ce comité sera présidé par le politologue Claude Emeri de 1984 à 1986.

(24) Qui publiera, en 1993, *Police et sociétés en Europe*, Paris, La documentation Française, 338 p.

(25) *Les policiers, leur métier, leur formation*, Paris, La documentation Française, 1983, 182 p.

policier [26], Claude Journès édite l'ouvrage *Une science politique de la police* [27], et tous deux mettent en en chantier, avec Jacqueline Gatti-Domenach, le livre qui sera publié en 1994 sur *La police, le cas des démocraties occidentales* [28]. À Toulouse, l'activité du CERP se traduira notamment par la publication sous notre direction de deux ouvrages, *Guide des recherches sur la police* (1985) et *Police et société* (1988), aux Presses de l'IEP de Toulouse, par les études conduites en collaboration avec Serge Albouy sur « Les rapports police-public dans la formation des gardiens de la paix » [29], par la thèse de Georges Portelli sur *Le portrait socio-culturel des commissaires de police*, et par un séminaire sur « Police et politique » qui nourrira un peu plus tard la rédaction de notre ouvrage *La police, approche socio-politique* [30]. Ces mesures amènent certains chercheurs proches du CESDIP à s'orienter dans cette voie, comme René Lévy en matière de police judiciaire [31] ou Frédéric Ocqueteau sur les questions de sécurité privée [32]. Le CESDIP organise aussi un séminaire périodique pour réunir les chercheurs français travaillant en ce domaine, auxquels se joindront bientôt des chercheurs étrangers rassemblés dans le cadre du *Groupe européen de recherche sur les normativités* (GERN) que crée, avec le soutien du CNRS, Philippe Robert en 1985.

Commencent, par ailleurs, à se nouer des relations entre chercheurs français et certains chercheurs du *Centre international de criminologie comparée* de l'université de Montréal et de l'*Association internationale des criminologues de langue française*, comme Denis Szabo [33] ou Jean Paul Brodeur. Elles incitent aussi de nouveaux chercheurs à s'intéresser à ce type d'objet dans le cadre des contrats de recherche gérés par le Comité scientifique de la Police nationale. Ainsi des politologues : par exemple à l'Université de Paris I, autour de Philippe Braud [34], ou à l'Institut d'études politiques de Paris autour de Pierre Favre [35]. Il en est de même chez les sociologues [36], et c'est dans ce cadre que Dominique Monjardet engage les recherches de terrain dont il dressera plus tard le bilan dans son ouvrage *Ce que fait la police* [37]. De même, cette période voit s'achever le travail monumental de Georges Carrot, *Histoire du maintien de l'ordre en France de la Révolution Française à 1968* [38], tandis que Michel Bergès, Jean-Marc Berlière et Marie Vogel entreprennent leurs recherches sur l'histoire policière de la III[e] République, qui déboucheront au début de la décennie suivante [39].

Le mouvement que l'on vient de décrire a surtout concerné les recherches sur la Police nationale. Il a néanmoins touché aussi l'autre institution policière française qu'est la Gendarmerie nationale, mais avec une chronologie un peu différente. En effet, la gendarmerie a été l'objet d'une recherche, autorisée par elle et financée par le ministère de la Recherche, de façon relativement précoce, dès la fin des années 1970, avec l'enquête de Hubert Lafont et Philippe Meyer, qui sera publiée sous le titre *Le nouvel ordre gendarmique* [40]. Mais, cette étude, ayant reçu

....

(26) Paris, Presses Universitaires de France, 202 p.

(27) Lyon, Presses Universitaires de Lyon, 1988, 218 p.

(28) Paris, Presses Universitaires de France, 1994, 390 p.

(29) Toulouse, Publications du CERP, 1988, 192 p.

(30) Paris, Montchrestien, 1992, 158 p. En 1995, l'activité du CERP se traduira par la création de la collection « *Sécurité et société* » aux Éditions l'Harmattan, dont le catalogue comporte à ce jour plus d'une vingtaine de titres, et par l'organisation de formations universitaires de troisième cycle (master), à finalité professionnelle ou de recherche.

(31) *Du suspect au coupable : le travail de police judiciaire*, Paris, Meridiens-Klinksiek, 1987, 184 p.

(32) Dont il fera la synthèse dans *Les défis de la sécurité privée*, Paris, L'Harmattan, 1997, 184 p.

(33) Fondateur de l'École de Criminologie de l'université de Montréal et organisateur, en 1972, d'un colloque international sur la police, qui sera à l'origine de l'ouvrage *Police, culture et société,* préfacé par lui et postfacé par J. Susini (D. Szabo ed., Montréal, Presses de l'Université de Montréal, 1977, 262 p)

(34) Avec des travaux dont on trouve l'écho dans *La violence politique dans les démocraties européennes occidentales*, (P. Braud, ed., Paris, L'Harmattan, 1993, 414 p.), et le début des recherches de Patrick Bruneteaux (*cf. Maintenir l'ordre,* Paris, Presses de la FNSP, 1995, 420p.) et d'Alain Pinel (*Une police de Vichy : les GMR* (Paris, L'Harmattan, Collection « Sécurité et société », 2004, 400 p.)

(35) Avec notamment des travaux sur le phénomène des manifestations et sur leur contrôle. *Cf.* P. Favre, ed., *La manifestation*, Paris, FNSP, 1990, 397 p.

(36) Ainsi, Dominique Lhuillier, *La police au quotidien*, Paris, L'Harmattan, 1987, 232 p. ; Marc Jeanjean, *Un ethnologue chez les policiers*, Paris, Métaillé, 1990, 300 p.

(37) Paris, La Découverte, 1996, 316 p. *Cf.* aussi *La police au quotidien. Eléments de sociologie du travail policier,* multigraphié, Paris, GST-CNRS, université Paris VII, 1984, 222 p.

(38) Publié par le CERP. Toulouse, Presses de l'IEP de Toulouse, 1984, 2 tomes, 890 p.

(39) M. Bergès, *Corporatismes et construction de l'État : le champ policier (1852-1940)*, Thèse, Toulouse, CERP, 1994; *Le Syndicalisme policier (1880-1940)*, Paris, L'Harmattan, 1995 - Berlière J.M, *L'institution policière en France sous la III[e] République, 1875-1914*, Lille, Atelier national de reproduction des thèses, 3 vol.,1991; *Le préfet Lépine*, Denoël, Paris, 1993, 280 p. - M. Vogel, *Les polices urbaines sous la III[e] République*, Thèse, Grenoble, 1993.

(40) Paris, Seuil, 1980, 216 p.

un accueil réservé de l'institution, restera sans lendemain immédiat. Il faudra attendre la fin des années 1980, après les remous provoqués par la crise résultant de la fronde épistolaire de l'été 1989, pour voir la gendarmerie s'ouvrir aux recherches de François Dieu, chercheur au Centre d'études de recherches sur la police de Toulouse [41].

Telles sont les grandes lignes de l'évolution française de la réflexion intellectuelle et scientifique sur les questions et les institutions policières qui s'est amorcée dans le prolongement des évènements de mai 1968 et dont l'une des conséquences institutionnelles sera, en 1989, en élargissant le champ des investigations à toutes les questions de sécurité intérieure, la création de l'*Institut des hautes études de la sécurité intérieure* (IHESI), devenu depuis l'*Institut national des hautes études de sécurité* (INHES).

Obstacles et réticences

Ce rappel historique présente un intérêt non seulement pour la connaissance du passé, mais aussi en raison des leçons que l'on peut en tirer pour le présent. Notamment du fait des remarques et des interrogations qu'il peut susciter du point de vue de la psychologie et de la sociologie de la connaissance, pour mettre en évidence les obstacles intellectuels que le développement de la sociologie de la police a pu, et peut encore, rencontrer.

Une première observation concerne la *marginalité* des initiatives qui ont marqué cette histoire en France. Marginalité dans le temps, avec une apparition tardive par rapport aux pays anglo-saxons et à l'évolution nord-américaine, qui a précédé d'une à deux décennies l'évolution française [42]. Marginalité dans l'espace, avec un développement qui s'est fait initialement dans des pôles de recherche « périphériques », non parisiens, ce qui ne saurait être sans signification quand on sait l'hyper-centralisation parisienne de la vie intellectuelle et universitaire française. La conclusion à en tirer est sans doute que ce type de recherches et de réflexion n'a pu naître que dans des lieux et à des moments situés, pour des raisons diverses, un peu à l'écart des conformismes et des modes de pensée et de réflexion installés. Ce poids des conformismes idéologiques ou intellectuels restant d'ailleurs une des difficultés récurrentes auxquelles continue à se heurter ce type de recherches, chez les chercheurs eux-mêmes comme dans leur environnement, notamment du fait d'une médiatisation de ces questions, dans laquelle l'intérêt traditionnel de la presse pour les faits divers se mêle à des considérations qui peuvent être plus idéologiques et plus politiques selon l'actualité ou la sensibilité du moment.

Cela dit, cette marginalité est d'autant plus *paradoxale* qu'il n'est pas besoin d'une réflexion approfondie pour constater à quel point ces questions se trouvent pourtant au coeur de l'organisation des sociétés, et c'est le côté positif des événements de mai 1968 et des années 1970 de l'avoir mis en évidence. Dès lors, on ne peut que s'étonner que sociologues comme politologues aient mis si longtemps à s'en apercevoir. On ne peut, sur ce point, que partager les interrogations du chercheur américain David H Bayley lorsqu'il constate à propos des politologues : « *Le désintérêt des politologues à l'égard de la police est particulièrement curieux. Le maintien de l'ordre est la quintessence de la fonction gouvernementale. Non seulement la légitimité du pouvoir est pour une large part dépendante de sa capacité à maintenir l'ordre, mais l'ordre constitue le critère permettant de dire si un pouvoir politique existe ou non. Conceptuellement comme fonctionnellement, pouvoir politique et ordre sont liés. Bien que les politologues aient reconnu l'utilité d'étudier les fonctions de gouvernement, ils ont négligé l'étude de ses responsabilités fondamentales. Ceci se manifeste dans le fait qu'il y a de très nombreuses études sur les parlements, le pouvoir judiciaire, les armées, les gouvernements, les partis politiques, l'administration en général, mais très peu sur la police. Pourtant la police détermine les limites de la liberté dans une société organisée et constitue un trait essentiel pour caractériser un régime politique*» [43]. Cela dit, cette relation avec l'essence du politique est aussi sans doute, tout aussi paradoxalement, une source de difficultés pour aborder sereinement cet objet, d'autant plus qu'en même temps on constate une tendance des différents acteurs concernés – policiers, politiques, médias – à en escamoter la réalité ou à la réduire à des interprétations superficiellement partisanes [44].

(41) F. Dieu, *Gendarmerie et modernité,* Paris, Montchrestien, 1993, 495 p. Premier d'une série de plusieurs ouvrages, dont : *Gendarmerie. Secrets d'un corps* (Bruxelles, Complexe, 2000) ou *Sociologie de la Gendarmerie* (Paris, L'Harmattan, 2008). Il est aujourd'hui directeur du Centre d'études et de recherches sur la police de l'université de Toulouse I.

(42) Cela dit, on doit constater que la littérature internationale reste très largement à dominante anglo-saxonne, avec une tendance de la sociologie de la police internationale à privilégier, en conséquence, les points de vue intellectuels anglo-saxons. On a pu dire que les chercheurs français en la matière se comptent en unités ou, au mieux, en dizaines, alors qu'ils se comptent pas centaines en Grande-Bretagne et par milliers aux États-Unis.

(43) *Patterns of policing*, New Brunswick NJ, Rutgers University Press, 1985. p. 5

(44) *Cf.* J.L Loubet del Bayle, *Police et politique. Une approche sociologique*, Paris, L'Harmattan, 2006, 320 p.

Si, en ce qui concerne l'attention portée à ces réalités, les choses ont un peu évolué pour certains sociologues et politologues, on peut néanmoins penser que du chemin reste à faire si l'on envisage la reconnaissance de la *légitimité scientifique* de ces recherches, aussi bien en sociologie qu'en science politique. En science politique, il suffit, par exemple, d'ouvrir les nombreux manuels de science politique du marché universitaire pour constater qu'ils ignorent à peu près tous cette dimension de la réalité politique, alors que, pourtant, beaucoup de ces ouvrages se réfèrent à l'approche weberienne du politique, en faisant référence à la « monopolisation de la violence légitime », tout en ignorant les institutions qui en sont, dans l'ordre interne, la manifestation [45]. De même, les réticences idéologiques, séquelles persistantes du contexte des années 1970, n'ont pas complètement disparu [46], et certains politologues semblent d'autant plus en rester à des préjugés datant de cette époque que leurs travaux s'inspirent assez souvent de références intellectuelles issues de cette période, en illustrant les récents et sévères propos de Marcel Gauchet sur le champ intellectuel français, lorsqu'il décrit celui-ci comme encore encombré par « *les suppôts diversement talentueux et les suiveurs plus ou moins originaux du lacanisme, du derridisme, du foucaldisme ou du bourdivisme* » [47].

Un objet scientifique problématique

Cela dit, au-delà des préjugés idéologiques, David H. Bayley [48] met cependant l'accent sur quelques raisons objectives qui peuvent expliquer la relative cécité intellectuelle que l'on a pu constater pendant longtemps en la matière, en France comme dans d'autres pays. Tout d'abord, la police n'apparaît pas, à première vue, comme un acteur décisif dans la genèse des grands événements historiques, son rôle semblant se limiter à la quotidienneté d'activités routinières, ayant plus de rapport avec le destin prosaïque des individus ordinaires qu'avec le sort des nations et des États. De ce fait, l'exercice des fonctions policières est aussi perçu comme peu prestigieux, surtout caractérisé par la fréquentation des bas-fonds de la société, ce prestige étant d'autant plus faible que les policiers, et même les chefs de police, ont été pendant longtemps peu recrutés dans les classes supérieures de la société. Enfin, l'usage de la violence à des fins internes, dans des conflits civils, et avec une orientation par nature assez souvent conservatrice, est génératrice de réticences qui sont d'autant plus accentuées que l'activité de la police a parfois un caractère quelque peu sordide et ne s'accompagne pas de l'imagerie héroïque qui entoure l'histoire militaire. Ces difficultés inhérentes à l'objet et à sa représentation, sont, en outre, renforcées en France par les conséquences indirectes du sous-développement de la recherche criminologique, qui n'a pas réussi à y acquérir de réel statut universitaire du fait de la tendance séculaire des facultés de droit à confondre étude du fait criminel et étude du droit pénal [49].

À cela on peut ajouter les difficultés concrètes que représente une tradition de secret, à laquelle se heurtent d'ailleurs souvent, de manière générale, les recherches de science administrative, mais qui est ici considérablement aggravée dans la mesure où le secret peut apparaître comme une nécessité fonctionnelle, indispensable pour permettre à la police d'assurer avec efficacité les missions qui sont les siennes. Ce souci, sinon cette obsession, du secret, a d'ailleurs été relevé par tous les chercheurs qui se sont intéressés à la « culture policière » ou ont tenté de décrire « la personnalité de travail » des policiers. Aussi, après avoir souligné que la police a encore moins d'historiens et surtout de sociologues que l'armée, est-ce sur cet obstacle que certains mettent l'accent lorsqu'ils constatent que la police est un objet qui se dérobe à

••••

(45) Sur ce point *cf.* F. Dieu, « Un objet (longtemps) négligé de la recherche scientifique : les institutions de coercition » in E. Darras et O. Philippe (ed), *La science politique une et multiple*, Paris, L'Harmattan, 2004.

(46) Elles restent notamment sensibles dans des domaines dont les réactions sont souvent, par nature, décalées dans le temps par rapport à l'évolution intellectuelle, comme celui de la gestion des recrutements et des carrières universitaires ou celui de l'organisation administrative de la recherche. Ainsi, alors qu'il a acquis progressivement une réputation reconnue, nationalement et internationalement, dans un domaine où la recherche française est très peu présente, le Centre d'études et de recherches sur la police de l'université de Toulouse I a vu périodiquement son existence administrative contestée, tant par les autorités universitaires locales que nationales.

(47) « Bilan d'une génération », *Le Débat*, mars-avril 2008, p. 107.

(48) *Patterns of policing, op. cit.*, p. 6 et *sqq*.

(49) *Cf.* sur cette situation le constat récent de la mission Bauer (Bauer Alain et *al.*, « Déceler, étudier, former : une voie nouvelle pour la recherche stratégique. Rapprocher et mobiliser les institutions publiques chargées de penser la sécurité », *Cahiers de la sécurité*, supplément au n°4, avril-juin 2008, 165 p.). Concernant les conséquences négatives qu'a eues sur l'histoire universitaire française la tendance historique des Facultés de droit à confondre criminalité et droit pénal, économie et droit économique, politique et droit constitutionnel, *cf* J.L Loubet del Bayle, « La science politique et les facultés de droit, approche socio-institutionnelle », *in* E. Darras, O. Philippe (ed), *La science politique une et multiple, op. cit.*

l'observation : « *Une police est plus disposée à recueillir des renseignements sur les autres groupes qu'à en donner sur elle-même* » [50].

De plus, la police est une institution qui tend à susciter spontanément des attitudes et des *jugements contrastés*, souvent fortement influencés par des réactions affectives ou des préjugés idéologiques ou partisans, plus ou moins en relation avec le contexte social, médiatique ou politique du moment. C'est ainsi que la médiatisation des questions de police a tendance à encourager leur instrumentalisation par les acteurs politiques, avec, notamment, assez souvent, une utilisation de ce vecteur par l'opposition pour déstabiliser le pouvoir en place, en mettant, par exemple, en avant le thème de « l'insécurité » et de « l'inefficacité » de la police lorsque l'opposition est de « droite », ou celui des « bavures » et des dérives « liberticides » lorsque l'opposition est de « gauche ». Sur ces points, le contexte des années 1970 évoqué précédemment constitue une illustration assez probante de ces observations, à quoi s'ajoutent parfois les ambiguïtés que peut créer la tentation chez certains chercheurs de jouer les « conseillers du Prince ». De ce fait, il n'est pas rare que les écrits sur la police se caractérisent, plus ou moins ouvertement et plus ou moins explicitement, par des orientations critiques ou apologétiques, en mêlant approche scientifique et points de vue normatifs [51].

Aussi n'est-il pas facile au chercheur d'adopter en ce domaine l'attitude de *neutralité* qui doit être la sienne, en évitant, selon la recommandation d'Auguste Comte, de considérer l'objet de ses investigations comme un objet de critique ou d'admiration. D'autre part, à supposer qu'il parvienne à cette objectivité, il lui est encore plus difficile de faire admettre et reconnaître cette neutralité, qui risque d'être toujours vue avec suspicion au gré de préjugés contradictoires. Pour les uns - c'est souvent la réaction des institutions policières elles-mêmes - la curiosité du chercheur sera suspecte de cacher des intentions malveillantes, sinon subversives, tandis que, pour d'autres – c'est plutôt la réaction universitaire - l'intérêt scientifique porté à la police ne pourra être que l'alibi de la complicité d' « intellectuels organiques » avec le pouvoir établi et avec ses aspects les plus autoritaires et les plus répressifs. Le chercheur se heurte ainsi souvent à une censure - et parfois une autocensure - idéologique à laquelle il peut lui être difficile d'échapper. On peut ajouter que celle-ci est d'autant plus susceptible de pénaliser le développement de la recherche que, ces mêmes raisons semblent aussi conduire certains chercheurs à éprouver des difficultés pour mettre en œuvre le processus cumulatif de connaissances, qui est pourtant la condition nécessaire de tout progrès scientifique, quel qu'en soit l'objet. Il suffit de constater les lacunes des références et des bibliographies de certains ouvrages pour se convaincre de l'existence de ce problème, et pour regretter que cette sorte de maladie infantile de la discipline tarde, en France, à se résorber.

Enfin, parmi les causes possibles des réticences à étudier l'objet policier, il en est une plus profonde et plus inconsciente qu'évoque notamment Olivier Philippe dans son travail sur *La représentation de la police dans le cinéma français* [52], lorsqu'il remarque que, d'une certaine façon, la mise en oeuvre de la fonction policière traduit un échec de la communauté à assurer l'intégration de ses membres et est donc, de ce fait, révélatrice de ce qui « fonctionne mal » dans une société, en attirant l'attention sur des zones d'ombre que l'inconscient social est plus disposé à dissimuler qu'à mettre en évidence. *A contrario*, cette observation permet de rendre compte du traitement différent accordé à l'institution militaire qui, elle, apparaît, à l'inverse, comme le symbole et la manifestation de l'unité de la société, toute entière mobilisée pour défendre collectivement son identité contre les menaces extérieures, en l'exaltant et en la glorifiant.

Dans ce sens, on peut d'ailleurs observer qu'un peu partout le développement de la réflexion intellectuelle sur la police et les pratiques policières à partir des années 1950, a été plus ou moins lié à des situations de *crise*, dans lesquelles s'est trouvée plus ou moins impliquée la police. Tel a été le cas aux États-Unis, avec les émeutes urbaines et le développement du mouvement des droits civiques dans les années 1950-1960. De même, en Grande Bretagne, les problèmes de maintien de l'ordre liés aux troubles interethniques, au terrorisme irlandais et à l'aggravation d'un certain nombre de conflits sociaux n'ont pas été étrangers à l'attention qui s'est portée sur les questions de police. Quant à la France, c'est aussi une situation de crise de l'institution policière qui, comme on

(50) J.W. Lapierre, *Analyse des systèmes politiques*, Paris, PUF, 1973, p. 18.

(51) Cette remarque ne condamne évidemment pas toute réflexion normative sur ces sujets. Elle tend seulement à souligner que les deux types de réflexion doivent être distingués et ne pas se perturber, en évitant notamment que les choix normatifs ne viennent altérer la perception et l'analyse objective de la réalité, en notant d'ailleurs qu'une authentique réflexion normative suppose une connaissance informée des phénomènes auxquels elle s'applique.

(52) Paris, L'Harmattan, Collection « Sécurité et société », 1999, 480 p.

l'a vu, dans les années 1970, a préparé l'évolution des années 1980. Avec, d'abord, les interrogations sur la nature et la légitimité des institutions policières, qui se sont développées dans le climat plus ou moins « libertaire » des événements de mai 68 et, ensuite, avec les difficultés grandissantes que ces institutions ont rencontrées pour faire face à la montée de la petite et moyenne délinquance et les interrogations sur « l'insécurité » qui ont marqué la seconde moitié des années 1970, dans un contexte d'affrontements idéologiques et partisans.

Plus généralement, ceci montre que, d'une certaine manière, le développement des recherches sur les institutions et les pratiques policières ne relève pas seulement de l'histoire de la connaissance, mais qu'il est aussi révélateur des problèmes que connaissent ces institutions pour s'adapter à un environnement dont elles reflètent les profondes transformations. S'il est vrai, comme l'a noté Denis Szabo, que la police peut être considérée comme un véritable « *sismographe social* » [53], particulièrement sensible aux mouvements et aux changements qui affectent l'évolution des sociétés, des plus superficiels aux plus profonds, il est évident qu'à travers les mutations qui caractérisent aujourd'hui les institutions policières et leurs pratiques, et les questions qu'elles suscitent, ce sont des phénomènes beaucoup plus généraux qui sont perceptibles, qu'il s'agisse de l'évolution des formes de contrôle social, des tendances anomiques que peut comporter le développement de l'individualisme dans les sociétés contemporaines, ou, plus fondamentalement encore, des interrogations qui peuvent se manifester sur la nature du lien social, sur ses conséquences et sur ses justifications.

Dans l'évolution que l'on a décrite, 1968 a bien été une date importante, illustrant les connexions qui peuvent s'établir, parfois d'une manière paradoxale, entre l'histoire sociale et l'histoire intellectuelle. Cela dit, en matière de sociologie de la police, l'héritage de 1968 peut être considéré comme ambivalent. Il a contribué à déclencher un mouvement de curiosité et de réflexion sur des réalités dont l'on avait jusque-là tendance à ignorer l'importance sociale, en insérant ainsi la recherche française dans le courant du développement international de la réflexion scientifique sur ces questions. En même temps, ce mouvement, encore aujourd'hui, a parfois du mal à se libérer du contexte dans lequel il est né, qui pèse encore doublement sur son état actuel. D'une part, du côté des chercheurs, en raison de son parasitage par des considérations liées aux préjugés idéologiques ou aux passions politiques partisanes, dont il n'arrive pas toujours à s'abstraire, dans un domaine où ces pressions restent fortes, du fait notamment, comme on l'a vu, de la tendance persistante chez les acteurs politiques à une instrumentalisation de ces questions, comme aussi du fait de leur médiatisation. D'autre part, en raison des réticences et des préventions que ce parasitage peut induire du côté des institutions policières et de leurs agents comme du côté des responsables politiques ou administratifs, en les incitant à considérer trop facilement qu'ils n'ont rien à apprendre des connaissances que la sociologie de la police peut leur apporter ou en limitant leur intérêt pour celles-ci à la récupération de quelques formules simplificatrices.

Jean-Louis LOUBET DEL BAYLE
Centre d'études et de recherches sur la police (CERP)
Université des Sciences sociales de Toulouse

(53) *Police, culture et société, op. cit.*, p. 7.

Du dualisme policier à la dualité policière

Réflexions sur les mutations du système policier français

François DIEU

Cet article envisage la situation actuelle et le devenir du dualisme police-gendarmerie à l'aune des mutations du système policier français. Cette construction empirique, qui n'est pas sans présenter certains avantages pour la puissance publique, connaît un processus de recomposition sous la pression de trois principaux phénomènes : la crise de la militarité de la gendarmerie, le mouvement de rapprochement entre la police et la gendarmerie, la montée en puissance de nouveaux acteurs policiers, notamment la re-création des polices municipales.

L'ambition d'une démocratie pluraliste, comme la France, est de déployer un arsenal normatif et symbolique pour que les deux termes — police et société — ne soient pas antagonistes. Il importe que la police ne soit pas contre la société, qu'elle soit, au contraire, une institution au service de la société dans l'accomplissement d'une mission de régulation sociale pour laquelle elle dispose de la faculté de recourir à la contrainte physique légitime. La police, comme toute composante de l'appareil administratif, ne dispose pas de légitimité propre, ne pouvant évoluer en dehors d'une prise en compte des règles et caractéristiques, mais aussi des aspirations et demandes du corps social. Cette inscription sociétale de la police présente de nombreuses facettes en perpétuelle construction, qui sont autant d'objets de préoccupations sociales et de réformes institutionnelles.

Le système policier français est caractérisé traditionnellement par deux éléments : le centralisme et le dualisme. Produit de la centralisation politique et administrative engagée dès l'Ancien régime, la police française est une police d'État, c'est-à-dire relevant de l'autorité exclusive du pouvoir central, avec comme priorité le maintien de l'ordre public. Quant au caractère dualiste, il procède de l'existence non d'une police unique, mais de deux forces présentant des différences manifestes, si ce n'est par rapport au cadre juridique de leur action, au moins par leur statut et leur histoire, ainsi que par leur mode d'organisation et de fonctionnement : la Police nationale (force civile) et la gendarmerie (force militaire).

Le dualisme policier apparaît non comme le résultat tangible de la volonté de construire un système reposant sur deux composantes, mais comme le produit avant tout des circonstances historiques. Le système policier n'a fait, en somme, que reproduire — avec l'évolution séparée de ces deux institutions, l'une rurale, l'autre urbaine — la profonde dualité de la société française, au plan de la géographie physique et humaine, qui ne devait partiellement s'estomper qu'au XX^{e} siècle. La rencontre, le brassage, sous la pression de l'exode rural et de la société de consommation, de la civilisation rurale (paysanne) et du monde urbain (industriel) devait d'ailleurs conditionner la mise en relation, en concurrence des deux institutions policières qui jusque-là s'étaient développées isolément, chacune dans son propre espace d'intervention sociale, selon des modalités particulières, mais à partir d'une logique commune d'insertion territoriale et de centralisation progressive. Par-delà ses justifications (*a posteriori*) idéologiques (empêcher l'émergence d'un pouvoir policier et contribuer à l'indépendance des magistrats), la bipolarité du système policier français résulte de la conjonction des

manœuvres opportunistes du pouvoir politique soucieux de s'assurer le soutien de l'appareil policier et de la concurrence auxquelles se livrent les deux institutions policières désireuses de conserver leur implantation territoriale et fonctionnelle. La pérennité de cette construction institutionnelle participe aussi de l'immobilisme et de la frilosité réformatrice, justifiés, il est vrai, par l'absence de dysfonctionnements majeurs révélés et d'un capital confiance élevé, plus particulièrement, pour une gendarmerie immanquablement menacée dans son existence même par les velléités de constitution d'un appareil policier unitaire.

Certains phénomènes, se manifestant de manière plus ou moins explicite, donnent à penser que ce système dualiste fasse l'objet de remises en cause et d'altérations, sous la pression de trois principaux phénomènes : la crise de la militarité de la gendarmerie, le mouvement de rapprochement entre la police et la gendarmerie, la montée en puissance de nouveaux acteurs policiers, notamment la re-création des polices municipales. Ces mutations sont de nature à transformer le dualisme policier, caractérisé par le partage du monopole policier entre la police et la gendarmerie, en un pluralisme policier dans lequel la dualité police-gendarmerie tend, de surcroît, à être de moins en moins marquée.

La crise de la militarité de la gendarmerie

Si, depuis l'ordonnance du 25 janvier 1536, la gendarmerie s'est vue confier, au fil des époques, des missions de police à caractère civil, les différents textes déterminant depuis son organisation et son service ont réaffirmé constamment son appartenance aux forces armées. La gendarmerie est demeurée une force militaire par le statut de ses personnels, leur formation, leur mode de vie et leurs valeurs, par ses équipements (comme en matière d'uniformes et d'armements), son cérémonial et sa symbolique, par le soutien que lui apportent les autres forces armées (comme le génie pour la construction des casernes et, dans leur domaine respectif, le service de santé et le service des essences), et par certaines missions, notamment la police militaire et la prévôté, la protection des points sensibles, voire la participation directe à la défense militaire.

La principale justification de cette militarité réside dans la possibilité de disposer d'une force capable d'exécuter des missions de sécurité dans un contexte dégradé. En effet, dans les situations de crise, par ses moyens militaires, la gendarmerie est de nature à participer, conjointement ou simultanément, à des opérations de police menées contre des éléments subversifs et à des combats terrestres engagés contre des formations ennemies, en assurant une continuité entre les actions policière et militaire dans le cas où la frontière entre ces deux types d'action serait difficile à fixer. Afin de renforcer la légitimité de son existence et de son implantation institutionnelle, la gendarmerie s'est, en quelque sorte, engouffrée dans ce créneau doctrinal de la continuité, du « *continuum* » Défense nationale-sécurité intérieure, dont la nécessité a été réaffirmée par le *Livre blanc* sur la défense (1994) à la faveur de la stigmatisation de menaces transfrontalières (terrorisme et criminalité organisée). Son implication dans les opérations de maintien de la paix et de police internationale conduites, en particulier dans l'ex-Yougoslavie, a pu apparaître comme une autre justification de la préservation d'une force de police à statut militaire susceptible de rendre opérationnel un principe de continuité, qui peut s'analyser comme le prolongement de doctrines plus anciennes comme celles de la guerre révolutionnaire qui, sur fond de guerre froide et de décolonisation, ont souligné la nécessité de forger des parades à la stratégie « indirecte » des organisations subversives. Sur un autre plan, l'état militaire de la gendarmerie représente aussi le moyen de faire réaliser, à peu de frais (en comparaison de la Police nationale, voire des polices municipales), en recourant à des personnels rendus disponibles (en termes de temps de travail et d'astreintes) par leur statut, des missions de police civile sur un espace immense (95 % du territoire national), sous la forme d'unités de taille extrêmement réduite, la discipline militaire pouvant pallier la perte d'énergie et de contrôle induite par ce saupoudrage des effectifs sur le terrain.

Par-delà les éléments objectifs incitant à ranger la gendarmerie dans le champ de la défense, l'identité militaire revêt une dimension culturelle, symbolique, voire affective et charnelle. Ainsi, lorsqu'on interroge l' « *homo gendarmicus* », ce dernier, quel que soit son grade, son ancienneté ou son unité, est généralement porté à afficher un attachement sans réserve à l'idée, au statut, à la condition, aux valeurs militaires, sans toujours être en mesure d'en donner une définition précise et d'en cerner les caractéristiques et les effets. Il est vrai que, contrairement aux autres forces armées, la gendarmerie n'entretient qu'un rapport relativement distant, indirect et limité, avec le combat guerrier, même dans ses formes les plus actuelles, les plus technologiques, les moins martiales. Le quotidien du gendarme ne réside pas dans la préparation et la conduite d'un combat contre des éléments ennemis, en recourant pour ce faire à la puissance

de feu d'un avion de chasse, d'une batterie de missiles embarqués ou d'un char de combat. Il s'agit surtout, pour lui, de faire respecter l'ordre et de produire de la sécurité, en patrouillant dans les lotissements, en interpellant des cambrioleurs, en faisant face à des agriculteurs en colère ou en infligeant des amendes pour excès de vitesse. Aussi, par certains côtés, l'identité militaire de la gendarmerie apparaît comme une construction culturelle aussi imposante qu'inconsistante, aussi prégnante que dogmatique, une sorte de coquille plus ou moins vide malgré les références à l'idée d'armée (de la sécurité intérieure) et à une historiographie vantant les épisodes guerriers émaillant ses huit siècles au service de l'ordre. En effet, la modicité de sa participation effective à la défense comme l'évocation magnifiée de son rôle lors des campagnes napoléoniennes paraissent des arguments relativement modestes pour revendiquer et asseoir une militarité, et ce d'autant plus que cette dernière connaît un processus global d'obscurcissement et d'altération.

La gendarmerie n'est guère parvenue, contrairement aux autres composantes de la « famille militaire », à édifier et à faire reconnaître sa propre identité militaire, tant il est vrai qu'au-delà d'un creuset organisationnel et culturel commun, les aviateurs, les marins, mais aussi les médecins militaires ou les personnels du service des essences ont su construire et imposer une manière particulière de concevoir et de vivre leur identité militaire par rapport, notamment, à leurs camarades de l'infanterie ou de l'artillerie. Si l'identité militaire semble une réalité à géométrie variable, ses prolongements gendarmiques paraissent condamnés, quant à eux, à une marginalité synonyme d'ambiguïté et de précarité. De fait, toute altération de cette identité militaire, sous la pression notamment de facteurs socioculturels, affectera tendanciellement de manière plus conséquente la gendarmerie, compte tenu de sa relation contingente au combat militaire et de son inscription manifeste dans le champ policier.

Aussi la militarité de la gendarmerie se trouve-t-elle directement remise en cause par les difficultés de conciliation d'une certaine spécificité socioculturelle attachée aux métiers des armes avec les aspirations de la société de consommation et des loisirs désormais ouvertement partagées par les gendarmes. L'enquête de terrain révèle, on l'a vu, une tendance à l'altération de la « morale professionnelle » du gendarme. Cette mutation culturelle est de nature à poser la question de l'appartenance du gendarme à la condition militaire et donc, à terme, de la persistance du statut militaire de la gendarmerie. Cette rupture sociale à la sphère militaire pourrait alors conduire les gouvernants sur la voie d'une démilitarisation de la gendarmerie. Une telle évolution serait d'ailleurs facilitée par la relative passivité dont semble faire preuve le champ de la défense vis-à-vis du sort réservé à la gendarmerie, pour ne pas dire la logique de refoulement de ce corps par des armées en proie, il est vrai, à une crise profonde, morale et organisationnelle, liée au processus de professionnalisation et à la réduction drastique de leur format.

Cette logique de refoulement s'était manifestée au début du XX^{e} siècle en matière de maintien de l'ordre, l'armée de ligne, il est vrai, entièrement mobilisée dans une stratégie de la revanche, s'accommodant parfaitement de la disparition de son implication dans des tâches si impopulaires de « cognes », dans ce que Stendhal, dans *Lucien Lewen* [1836], fustige comme des « *guerres de Maréchaussée* [...], *de tronçon de choux, contre de malheureux ouvriers mourant de faim* ». À l'origine de la constitution d'une troisième force en charge des attroupements et manifestations se trouve, en effet, le postulat selon lequel le maintien de l'ordre requiert l'engagement de forces mobiles disponibles en permanence, pouvant être en mesure de rétablir efficacement l'ordre sans pour autant transformer les rues en champs de bataille. Après de nombreuses années d'hésitations et d'expériences tragiques, cette idée s'est traduite par la mise en place de deux forces spécialisées présentant nombre de points communs malgré leur différence de statut, l'une militaire (gendarmique) : la gendarmerie mobile (1921), l'autre civile (policière) : les compagnies républicaines de sécurité (1944). Après avoir ainsi contribué, sur un plan fonctionnel, à l'abandon des tâches ordinaires de police des foules, ce processus de refoulement semble donc se poursuivre, sur un plan cette fois organique, avec comme « victime » désignée une gendarmerie considérée, il est vrai, comme « périphérique » à raison de son activité fondamentalement policière.

Par certains côtés, il peut s'agir aussi de la conséquence logique de son processus d'autonomisation au sein de l'édifice de défense, et singulièrement par rapport à l'armée de terre (consacrée par les décrets du 6 et 13 janvier 1950), sur fond de rancœurs, de jalousies et d'accusations plus ou moins anciennes. Pour ne retenir que quatre griefs couramment adressés à la gendarmerie : ne pas être une force combattante (avec l'image du gendarme à cheval repoussant les « poilus » vers les tranchées durant la Grande Guerre) ; grever les ressources de la défense (les crédits destinés à l'acquisition de blindés ou d'avions de chasse pouvant être « détournés » pour financer les dépenses d'entretien des brigades, voire pour déployer davantage de cinémomètres) ; cultiver un sentiment de supériorité vis-à-vis des « biffins » et « matelots » (la gendarmerie est ainsi accusée de tirer argument du choix des élèves les mieux classés au sortir de Saint-Çyr de rejoindre généra-

lement ses rangs pour se considérer comme une élite proposant prestiges et perspectives de carrière) ; « faire pénétrer le ver dans le fruit » (les gendarmes, par leurs manifestations ouvertes et médiatisées d'indiscipline de l'été 1989, de décembre 2001 et de l'automne 2007, sont considérés comme pouvant nuire à la cohésion et à la spécificité des armées, en y introduisant, par exemple, des logiques de contestation et de syndicalisme).

Le rapprochement police-gendarmerie

Même si, lors de la campagne présidentielle de 2002, les deux principaux candidats, Jacques Chirac et Lionel Jospin avaient pris position en faveur de cette réforme, la modification du rattachement ministériel de la gendarmerie, à l'annonce de la composition du gouvernement Raffarin, a malgré tout fait l'effet d'un électrochoc. Il est vrai que la question qui est posée dépasse le domaine purement politique et institutionnel : il ne s'agit pas seulement de savoir qui commande la gendarmerie, le ministre de la Défense ou son collègue de l'Intérieur. La question du rattachement ministériel de la gendarmerie est généralement corrélée avec celle de son statut et, au-delà, avec celle de la préservation du dualisme policier. Ils sont nombreux, en effet, dans les rangs de l'institution, à redouter que cette réforme soit le préalable, le point de départ d'une démilitarisation déguisée ou non de la gendarmerie qui signifierait, à terme, sa disparition par fusion dans un corps unique de police à statut civil, sonnant le glas, de fait, du dualisme policier et de ses avantages en termes de préservation de l'indépendance du pouvoir politique et des magistrats. Avec comme spectre la disparition de la gendarmerie belge entamée au début des années 1990, ce scénario-catastrophe emprunte les trois étapes suivantes : rattachement au ministère de l'Intérieur, démilitarisation, intégration dans la Police nationale.

Pour ce qui est de la nature exacte du rattachement de la gendarmerie au ministère de l'Intérieur (décret du 15 mai 2002), il a été opéré une distinction entre les domaines organique et fonctionnel (opérationnel) : le rattachement concernerait seulement l'emploi de ses formations dans le cadre des missions de sécurité intérieure, c'est-à-dire de maintien de l'ordre et de sécurité publique, ce qui ne remettrait pas en cause l'administration et la gestion par le ministère de la Défense de ses personnels (militaires) et de ses moyens. Aussi n'est mentionnée en aucune manière une autorité quelconque du ministre de l'Intérieur sur la direction générale de la Gendarmerie, à la différence des autres directions générales et directions qui lui étaient antérieurement rattachées (notamment la direction générale de la Police nationale). L'exercice des missions de défense et de police judiciaire demeure sous la responsabilité, respectivement, du ministre de la Défense et son collègue de la Justice. Dans l'état actuel des choses, il appartient donc au ministère de la Défense de prendre en charge l'ensemble du personnel et des moyens de la gendarmerie, alors qu'il n'est responsable que d'une partie extrêmement limitée de son emploi (les missions de défense militaire de la gendarmerie ne représentent guère plus de 2 % de son activité missionnelle). S'agissant de la dichotomie organique/fonctionnel établie par cette norme juridique, dans la pratique, à moins de s'en tenir à une vision purement formelle, il ne paraît exister de séparation nette entre ces deux domaines, l'exécution des missions ayant manifestement des répercussions sur l'administration et la gestion des personnels et des moyens et réciproquement. Quoi qu'il en soit, cette nouvelle donne politico-administrative serait de nature à générer, à plus ou moins brève échéance, des rapprochements statutaires inévitables avec la Police nationale (notamment en matière de temps de travail et de régime de disponibilité), tout en favorisant, dans les départements, l'emprise croissante de l'autorité préfectorale, pour ne pas dire la mise sous les ordres des préfets des formations de gendarmerie.

Bien que cette subordination à l'autorité civile soit demeurée, au moins depuis la Révolution, un des principes fondamentaux de l'action de la gendarmerie, son domaine d'exercice a longtemps été limité, pour l'essentiel, au maintien de l'ordre, à la police des foules. Son extension à la sécurité publique, à la police du quotidien s'explique, pour l'essentiel, par la départementalisation de la sécurité engagée depuis le début des années 1990. Ce mouvement a singulièrement remis en cause, il est vrai, le postulat selon lequel la gendarmerie, force militaire faisant partie intégrante des armées, ne constitue pas un service déconcentré d'une administration civile de l'État échappant, de ce fait, à l'autorité du préfet. Le caractère pour ainsi dire virtuel de cette disposition a pu apparaître lors de l'adoption de la loi du 21 janvier 1995 d'orientation et de programmation relative à la sécurité (LOPS), qui renforce notablement les pouvoirs du préfet : « *le représentant de l'État* [...] *anime et coordonne la prévention de la délinquance et de l'insécurité* [...] *fixe les missions et veille à la coordination des actions, en matière de sécurité publique, des différents services et forces dont dispose l'État* » (art. 6). Si le travail parlementaire avait permis d'opérer une rédaction définitive susceptible de préserver l'identité militaire de la gendarmerie (ce que confirme la mention « *sans préjudice des textes relatifs à la gendarmerie* »), cet article reconnaît malgré tout, en matière

de police administrative, l'autorité fonctionnelle du préfet sur la gendarmerie, sans pour autant induire alors – comme c'est le cas s'agissant de la police – une autorité hiérarchique sur le commandant de groupement de gendarmerie départementale.

Par la suite, en application d'une préconisation du *Rapport Carraz-Hyest* [avril 1998], les préfets se sont vus reconnaître la possibilité de concourir à la notation (appréciation) des commandants de groupement (cette notation étant toutefois de second rang par rapport à celle de l'autorité militaire), à l'image de ce qui existe en matière de police judiciaire s'agissant des procureurs de la République (ces derniers attribuant annuellement une notation aux officiers de police judiciaire habilités dans leur ressort, parmi lesquels figurent, bien évidemment, les commandants de groupement). Enfin, la loi du 18 mars 2003 pour la sécurité intérieure (LSI) apparaît comme une nouvelle étape dans ce processus, en reconnaissant au préfet une mission de direction s'appliquant indistinctement sur les policiers et les gendarmes préposés aux tâches de sécurité publique et de police des foules : « *il dirige l'action des services de la police nationale et des unités de la gendarmerie nationale en matière d'ordre public et de police administrative. Les responsables locaux de ces services et unités lui rendent compte de l'exécution et des résultats des missions qui leur ont été fixées* ». Dans le même ordre d'idées, la nomination, entre 1995 et 2004, de préfets au poste de directeur général de la gendarmerie (la fonction étant exercée jusque-là par des magistrats) peut être interprétée comme une manifestation de cette mainmise graduelle du ministère de l'Intérieur sur la gendarmerie, préfigurant et rendant possible le rattachement ministériel opéré au lendemain de la réélection du Président Chirac, tout en donnant à cette dernière mesure (de régularisation ?) une valeur formelle, pour ne pas dire symbolique. Par ailleurs, diverses initiatives de rapprochement entre les deux institutions, sous les auspices du ministère de l'Intérieur, étaient intervenues ces dernières années, en particulier en matière de représentation à l'étranger (avec la création d'un réseau unique d'attachés de sécurité intérieure).

Cette incorporation progressive, presque insensible de la gendarmerie au ministère de l'Intérieur par le biais de l'autorité préfectorale, loin de se limiter à un processus purement machiavélique, apparaît comme une réponse aux appels à une plus grande rationalité lancés par les (rares) rapports de parlementaires et de spécialistes qui, au moins depuis la fin des années 1970, avaient mis en évidence les effets dysfonctionnels de la séparation ministérielle entre police et gendarmerie. En effet, cette situation est jugée responsable de la quasi-absence de coopération entre les deux composantes du système policier français, ce qui ne posait peut-être pas problème jusqu'au début du XX^{e} siècle au regard de la séparation tranchée entre les territoires urbains et ruraux, de la modicité des flux de population et du caractère encore largement statique (et contenu) de la délinquance. Cette scission dans le système policier, qui se traduit, par exemple, par une incompatibilité des moyens de transmission ou encore par une quasi-absence d'opérations communes, a pu apparaître problématique à l'aune de la montée en puissance, ces trente dernières années, de l'insécurité objective (délinquance) et ressentie (sentiment d'insécurité), de son omniprésence dans le quotidien des populations (notamment les plus précarisées) et de son inscription, nationalement et localement, dans le débat démocratique et sur l'agenda public. Conséquence directe de cette diffusion de l'insécurité et manifestation d'une certaine impuissance de l'État pour endiguer jusque-là sa progression, le rattachement de la gendarmerie au ministère de l'Intérieur a d'ailleurs été la première mesure significative prise par le gouvernement Raffarin au sortir d'une campagne présidentielle dominée par le thème de l'insécurité. Par la suite, sont intervenues la réforme du Conseil de sécurité intérieure (décret du 15 mai 2002), la mise en place des groupes d'intervention régionaux (circulaire du 22 mai 2002), ainsi que l'institution des conférences départementales de sécurité et la refonte des instances locales de prévention de la délinquance (décret du 17 juillet 2002), ces diverses mesures étant reprises dans la loi du 29 août 2002 d'orientation et de programmation relative à la sécurité intérieure (LOPSI).

Malgré diverses rumeurs laissant penser à la constitution d'un « grand ministère de la sécurité », réunissant sous une autorité politique et dans un budget unique police et gendarmerie, l'élection présidentielle de 2007 n'a pas modifié cette logique de double rattachement de la gendarmerie. Il est vrai que le passage de Michèle Alliot-Marie du ministère de la Défense à celui de l'Intérieur a pu faciliter cette continuité s'agissant du positionnement de la gendarmerie. Le décret du 31 mai 2007 précisant les attributions du ministre de l'Intérieur confirme et renforce cette subordination fonctionnelle de la gendarmerie au ministre de l'Intérieur, tout en amorçant une possible extension de cette dernière dans le domaine organique en lui reconnaissant certaines attributions organisationnelles et budgétaires : « *pour l'exercice de ses missions de sécurité intérieure, le ministre de l'Intérieur, de l'Outre-mer et des Collectivités territoriales est responsable de l'emploi des services de la Gendarmerie nationale* [...]. *À cette fin, il définit les missions de ces services et détermine les conditions d'accomplissement de ces missions et les modalités d'organisation qui en résultent. Conjointement avec le ministre de la Défense, il définit l'utilisation des moyens budgétaires attribués à la gendarmerie nationale*

et en assure le suivi » (art. 4). À l'évidence, il s'agit d'une deuxième étape significative dans le processus devant aboutir, dans une troisième et dernière étape, à un rattachement pur et simple de la gendarmerie au ministère de l'Intérieur.

À l'occasion d'un discours prononcé le 29 novembre 2007 à la Défense (Paris) en présence de 2 000 policiers et gendarmes, le Président Sarkozy, tout en affirmant qu' « *il n'y aura pas de fusion police-gendarmerie tant que je serai président* », a d'ailleurs annoncé le rattachement de la gendarmerie au ministère de l'Intérieur à compter du 1er janvier 2009, pour ce qui est de l'emploi, de l'organisation, des objectifs et des moyens d'investissement et de fonctionnement (les domaines de la santé, du paiement des soldes ou encore de l'immobilier devant demeurer dans le domaine de la défense). La constitution de ce « grand ministère de la sécurité », réunissant police et gendarmerie sous une même autorité politico-administrative pourra alors permettre, le cas échéant, de définir et mettre en œuvre une coopération entre les deux forces, au plan des structures de commandement, de gestion et de soutien, mais aussi et surtout des unités et acteurs de terrain, dans les domaines de la sécurité publique, du renseignement, de la police judiciaire et du maintien de l'ordre. Et d'observer que les autres États européens ayant conservé des forces de police à statut militaire, comme l'Italie (*Carabinieri*) et l'Espagne (*Guardia civil*), ont fait le choix, depuis plusieurs années, de ce rattachement à un ministère commun, sans pour autant d'ailleurs avoir engagé un processus manifeste de démilitarisation, ni obtenu de gains extrêmement significatifs en matière de coopération entre les diverses composantes du système policier, ce que révèle notamment, s'agissant de l'Italie, la gestion problématique des manifestations anti-mondialisation lors du sommet de Gênes (juillet 2001).

Si aucun projet politique n'a jusqu'à présent clairement préconisé la démilitarisation de la gendarmerie, voire son absorption par la police nationale, ce *statu quo* ne signifie pas que la dualité police-gendarmerie demeure perpétuellement la caractéristique essentielle du système policier français, tant il paraît exister de puissants facteurs de rapprochement entre ces deux organisations. Ainsi, alors que la Police nationale s'est engagée dans un processus de « militarisation » (avec l'adoption de règles de comportement et d'éléments symboliques empruntés à la sphère militaire, ce qui est perceptible notamment au niveau de la formation des personnels) inhérent à sa mobilisation dans la lutte contre la criminalité (identifié en Grande-Bretagne et aux États-Unis avec le développement d'unités de police paramilitaires spécialisées dans l'intervention et le maintien de l'ordre), la gendarmerie connaît, depuis au moins le début des années 1970, une tendance à la « policiarisation » en relation avec le développement de son activité de police judiciaire. En d'autres termes : une police qui se militarise et une gendarmerie qui se policiarise...

La diffusion dans l'ensemble du tissu administratif des fondements du management public constitue également un facteur prépondérant de rapprochement pour des organisations policières soumises aux mêmes règles en matière de gestion administrative, logistique et budgétaire. Ainsi gendarmerie et police font-elles l'objet d'une présentation pratiquement similaire au niveau des lois de finances (LOLF) en tant que « programme » relevant de la « mission interministérielle sécurité », tout en se voyant appliquer, depuis 2003, divers dispositifs relatifs au développement de la « culture du résultat » (notamment le plan d'action annuel et les primes pour résultats exceptionnels). La pression exercée sur la gendarmerie – en privilégiant, en matière d'action publique, la logique de rationalité sur celle de territorialité – afin de réduire la dispersion de ses effectifs dans un maillage extrêmement dense de brigades – est de nature à doter les deux organisations d'unités élémentaires présentant d'indéniables similarités. Ainsi, la mise en œuvre du système des communautés de brigades peut-elle s'analyser, outre le constat de l'impossibilité de procéder à des dissolutions de brigades, comme une tentative de la gendarmerie de dépasser une approche jusque-là cantonale de la sécurité publique, par une unité du commandement et une mutualisation de moyens au niveau de territoires plus cohérents. Elle n'en représente pas moins une étape importante dans la constitution d'unités territoriales de gendarmerie au format important (en termes d'effectifs et d'espaces d'intervention) et aux modalités d'organisation et de fonctionnement comparables à celles des commissariats de police implantés dans les villes moyennes.

Une logique de rapprochement paraît, de surcroît, à l'œuvre, depuis plusieurs années, entre brigades territoriales et commissariats de police opérant dans les zones périurbaines, ce qui a rendu possible d'ailleurs, entre 2003 et 2007, le plan de remplacement de brigades par des commissariats dans plus de deux cents communes (222) situées à la périphérie des principales agglomérations et d'une quarantaine (41) de commissariats par des brigades dans une centaine de villes moyennes (121). Pour autant, le principal facteur d'homogénéisation réside dans l'individu, dans la mesure où gendarmerie et police recrutent, socialisent, hiérarchisent et déploient des hommes et des femmes présentant de profondes similarités, notamment au plan de leurs motivations et aspirations. Dans cette perspective, les revendications partagées par les personnels des deux organisations à maintenir un « dualisme équitable »,

à l'heure de la « réforme des corps et carrières » (police) et du « plan d'adaptation des grades aux responsabilités exercées » (gendarmerie), participent de ces rapprochements entre composantes humaines qui, au même titre que l'érosion des spécificités organisationnelles et fonctionnelles, pratiquent chaque jour des coupes sombres dans une dualité dont les fondements sont minés par les effets globalisants et unificateurs d'un changement social protéiforme.

Les rapprochements et mutualisations opérés depuis 2002 entre police et gendarmerie (mise pour emploi de la gendarmerie sous la responsabilité du ministre de l'Intérieur, création des groupes d'intervention régionaux, adoption de matériels et d'armements communs, déploiement du système des attachés de sécurité intérieure, etc.) ne font donc que reconnaître, sur un plan organisationnel et pratique, ce mouvement, en quelque sorte, d'attirance réciproque dont l'ultime séquence ne peut être que la fusion des deux organisations dans un corps unique de police, le statut civil s'imposant alors sur une militarité seulement tolérée par l'idéologie libérale dans le champ de la régulation des conflits internes. Cet « accommodement » s'explique alors par le fait que l'armée constitue, de par sa relation originelle à la guerre et son positionnement fonctionnel externe, le type idéal de l'appareil violent par rapport à une police (civile) recourant forcément – car devant concilier légalité et légitimation – à une force contenue et modérée parce que s'exerçant à l'intérieur du système social. Ce schéma dichotomique est produit et imposé, pour l'essentiel, par l'idéologie policière anglo-saxonne, pour qui la gendarmerie est l'illustration exemplaire du caractère autoritaire et centralisé – militariste – du système policier français.

Cette assimilation des forces de police à statut militaire à la force militaire se retrouve notamment exprimée par la résolution 690 (relative à la déclaration sur la police de 1979) de l'assemblée parlementaire du Conseil de l'Europe. L'absence de reconnaissance du droit syndical a fourni alors un argument pour conclure hâtivement à une incompatibilité de principe entre statut militaire et service (civil) de police (démocratique). Le Code européen d'éthique de la police [2001] a toutefois apporté une nuance en considérant que les policiers doivent pouvoir bénéficier « *du droit de se syndiquer ou de participer à des instances représentatives* », cette seconde option correspondant aux instances de concertation dont disposent les gendarmes. Pour autant, si la syndicalisation représente une forme supplémentaire de contrôle de l'activité policière, dans un souci de transparence et d'intégration sociale, il paraît pour le moins abusif de disqualifier les forces de police à statut militaire, sur la base de ce seul argument dont l'effet en la matière ne peut être, en toute hypothèse, que contingent et accessoire. C'est aussi faire abstraction, d'une part, des limitations généralement apportées à ce droit syndical (avec notamment l'interdiction du droit de grève et de manifester en uniforme), d'autre part, des logiques corporatistes privilégiées par des organisations syndicales qui peuvent les conduire à défendre les intérêts catégoriels des policiers indépendamment de leur adéquation avec l'intérêt général. En toute hypothèse, l'extrême diversité des situations observables, historiquement, dans la multiplicité des États ne peut qu'inciter à la prudence lorsqu'il s'agit d'opérer des corrélations mêmes tendancielles entre, d'un côté, le nombre de forces de police (monisme, dualisme, pluralisme), leur statut (civil, militaire), leur rattachement ministériel (intérieur, police, défense), leur inscription territoriale (étatique-fédérale, locale, municipale), de l'autre, la nature du régime politique (démocratique, autoritaire, totalitaire).

Du dualisme au pluralisme policier

Le « dualisme » ne semble plus vraiment correspondre, depuis une quinzaine d'années, à la réalité du système policier français. À l'instar des autres composantes du tissu administratif, cette construction empirique n'a pas été épargnée par le mouvement de remise en cause de l'État nation, par le haut, sous la pression des logiques d'intégration communautaire, et par le bas, compte tenu de la promotion politique et sociale des pouvoirs locaux.

Ainsi, le développement des politiques européennes de sécurité, sans pour autant aboutir (en dépit de la constitution d'un office européen de police « Europol » et d'une force de police européenne « FPE ») à la création d'une police unique pour l'ensemble de l'Union européenne, n'en bouscule pas moins le système dualiste français, compte tenu, d'une part, de l'évolution de la fonction de régulation dévolue aux douanes (dans le sens d'une « policiarisation » de fait, perceptible au niveau de ses modes de contrôle, du renforcement des pouvoirs judiciaires de ses agents et de son implication dans la lutte contre les trafics de stupéfiants), d'autre part, de la primauté reconnue dans les instances de coopération européenne aux forces de police à statut civil, c'est-à-dire, pour la France, à la Police nationale (ce qui a amené les polices à statut militaire à se regrouper dans des réseaux de coopération multilatérale). Par certains côtés, la résurgence de l'implication des armées dans les tâches de police, à la faveur des mesures de sécurisation anti-terroristes

(plan Vigipirate) et des opérations internationales de maintien de la paix (comme au Kosovo), ainsi que le développement de services de sécurité dans certaines administrations et entreprises publiques (comme la police ferroviaire – SUGE : surveillance générale, pour la SNCF – et les ERIS, équipes régionales d'intervention et de sécurité pour l'administration pénitentiaire) contribuent aussi à imprimer dans le système policier une double logique d'hybridation et de balkanisation, en phase, il est vrai, avec la diffusion des problématiques sécuritaires dans la société française.

Malgré la prépondérance des deux organisations policières régaliennes, le système policier français ne se limite pas à la dichotomie police-gendarmerie, le développement du secteur de la sécurité marchande conduisant également à l'émergence d'un acteur, certes de nature privée, mais contribuant à l'effectivité de la fonction policière. Reconnu juridiquement, au moins depuis le début des années 1980 (en particulier depuis les dispositions de la loi du 12 juillet 1983 réglementant les activités privées de surveillance, de gardiennage et de transport de fonds), comme une composante à part entière de la réponse à l'insécurité, le secteur de la sécurité privée a connu depuis un développement sans précédent. L'annexe I de la LOPS de 1995 donne une valeur législative à cette participation : « *Les entreprises de gardiennage, de surveillance et de transport de fonds, d'une part, les agences privées de recherche, d'autre part, exercent des activités de sécurité de nature privée. Elles concourent ainsi à la sécurité générale* ». Ce secteur emploie aujourd'hui autant d'agents que la Police nationale (soit 5 000 entreprises et 140 000 salariés dont 85 % dans le secteur de la surveillance humaine) et représente, à lui seul, un chiffre d'affaire annuel de plus de 3 milliards d'euros (ce marché étant dominé par quelques grandes entreprises puisque 170 sociétés de plus de 100 salariés emploient 80 % des effectifs et réalisent 75 % du chiffre d'affaire).

Cette immixtion de la logique du marché se traduit, par définition, par la prise en considération, par les entreprises et prestataires de sécurité, uniquement des demandes solvables, c'est-à-dire susceptibles de donner lieu au paiement du prix déterminé — par la loi de l'offre et de la demande — pour le service. Aussi ce développement de la sécurité privée peut-il être appréhendé comme une forme plus ou moins pernicieuse — sous couvert de libéralisme policé et de critique entendue sur l'impuissance de l'État tentaculaire — de retour en force de la loi du plus fort, c'est-à-dire de celui qui, particulier ou entreprise, dispose des ressources lui permettant, indépendamment de toute action régalienne, de garantir la sécurité de sa personne et de ses biens. La privatisation de la sécurité ne se limite pas, loin s'en faut, au seul secteur du gardiennage. En réalité, ce phénomène concerne surtout un pan entier de la réponse à l'insécurité négligé par la puissance publique, pour ne pas dire abandonné au secteur privé, à savoir la prise en charge de la victime, relevant, outre le secteur associatif (s'agissant des associations d'aide aux victimes), des entreprises d'assurance, l'extension de leur intervention dans le domaine des négligences humaines impliquant une dilution de la responsabilité à la fois collective et individuelle au profit d'une solidarité automatique et marchande.

Les logiques de décentralisation administrative ont également conduit à remettre en cause le monopole de l'État central dans la conduite des politiques publiques de sécurité, avec l'émergence d'un mouvement de localisation de la sécurité. Au plan de l'organisation policière, ce mouvement s'est traduit par un retour en force des polices municipales (5 641 agents en 1984 ; 10 977 en 1994 ; 16 520 en 2004), provoquant, sur un plan plus particulier, une intensification des débats et controverses sur la légitimité et la légalité de leur résurgence (le mouvement d'étatisation de la police, amorcé au milieu du XIX^{e} siècle et presque achevé par la loi du 23 avril 1941, avait conduit à transférer à la police d'État la responsabilité de l'ordre public dans les villes). Polices subsidiaires apparaissant, pour certains, comme des vestiges du pouvoir local de police, ces polices municipales donnent lieu à nombre d'interrogations et de réserves. Absence d'unité et de marge de manœuvre, organisation embryonnaire et hétérogène, diversité des doctrines d'emploi et des missions, positionnement problématique dans (entre) le système policier et la fonction publique territoriale, pouvoirs juridiques ambigus et limités, faiblesse endémique de l'encadrement, effectifs difficilement dénombrables, accusations de politisation sont les principaux éléments (griefs) qui caractérisent aujourd'hui la situation pour le moins ambivalente des polices municipales, ce qui n'empêche pas le développement de ces forces qui transforment, de fait, par leur existence et leur action quotidienne, le dualisme policier français en un pluralisme susceptible, à la lumière des débats actuels sur la municipalisation de la sécurité, de connaître d'importantes évolutions.

Bien qu'elle se traduise par une présence d'agents publics au service de la collectivité, la (re)création des polices municipales ces vingt-cinq dernières années, qui s'explique par différents facteurs (la progression de la délinquance et du sentiment d'insécurité, la politisation des questions de sécurité dans les élections locales, l'accroissement des demandes de sécurité de proximité), n'est cependant pas de nature à dissiper les craintes de ceux qui considèrent que la sécurité, comme d'ailleurs la santé ou l'éducation,

est un domaine où l'inégalité de traitement doit être prohibée, en application des principes républicains, mais aussi parce qu'il en va de la cohésion même du système social. Par certains côtés, le développement des polices municipales, consacré par la loi du 15 avril 1999, semble se situer à contre-courant d'une histoire de l'institution policière qui, avec l'avènement du régime républicain, a vu dans l'étatisation par étapes de la police une garantie de neutralité et de professionnalisme. La pression conjuguée d'une tradition jacobine ne pouvant se satisfaire de la satellisation des forces de police, des logiques de professionnalisation et de l'action corporatiste des syndicats policiers devait aboutir, en effet, entre 1851 et 1941, à l'intégration des polices municipales dans un corps régalien et à la relégation du maire au profit de l'État et de son représentant. Par ailleurs, à moins d'une réforme d'ensemble des ressources financières des collectivités locales, les disparités manifestes entre les communes, au même titre d'ailleurs que les différences d'interprétation et de doctrine en ce domaine, qu'il s'agisse de constituer ou non une police municipale, voire même de lui attribuer ou non telle ou telle mission ou bien encore tel ou tel équipement, tel ou tel armement, ne peuvent conduire qu'à des inégalités importantes de traitement entre les citoyens.

Dans un autre domaine, toute montée en puissance des polices municipales, par l'accroissement de leurs effectifs et l'amélioration des équipements et de la formation, supposera, à un moment ou à un autre, une extension des pouvoirs (judiciaires) de leurs agents, de manière à leur permettre d'exercer leur travail de policier de manière rationnelle et efficace, ce qui conduira, en fait comme en droit, à reconnaître l'existence, à côté de la gendarmerie et de la police, d'une troisième force composée d'une myriade de polices municipales. Certains parlementaires ont même préconisé d'étendre les pouvoirs de police du maire, en plaçant sous son autorité (opérationnelle) les forces de police en charge des missions de sécurité publique. Ces projets de municipalisation ont donné lieu à deux propositions de loi (29 novembre 2000 et 20 janvier 2001) qui n'ont pas été suivies d'effets.

L'appel aux communes dans les politiques de localisation de la sécurité ne s'est cependant pas traduit par une promotion des polices municipales, pour au moins deux raisons : la forte hétérogénéité du tissu des polices municipales représente un obstacle de taille à toute reconnaissance de leur implication effective dans la production locale de sécurité ; le partenariat déséquilibré avec les polices d'État (au moyen notamment des conventions de coordination) n'a pas permis pour l'instant la définition d'un champ d'intervention identitaire pour les polices municipales.

Cette re-création désordonnée et inachevée des polices municipales, dans un contexte de policiarisation des organisations de régulation sociale, n'en a pas moins conduit à une reconfiguration du système policier français, dualiste jusqu'à ces dernières années. Dans le même temps, les logiques de rapprochement à la fois institutionnel et socioculturel entre la police et la gendarmerie tendent à obscurcir les lignes de démarcation entre les deux institutions, la dualité police-gendarmerie devenant, dans les faits, de moins en moins marquée, ce qui peut progressivement, presque insensiblement créer les conditions nécessaires à leur intégration dans un corps policier (civil) unique. Au terme de ce processus, le dualisme policier vertical pourrait bien devenir horizontal, avec le passage d'une bipolarité organisationnelle (police-gendarmerie) à un partage des attributions policières entre le centre et la périphérie (polices étatiques-polices locales) qui semble être, il est vrai, le modèle dominant dans les démocraties occidentales. Pour autant, convient-il de ne pas se hasarder à prédire tel ou tel scénario en ce domaine, tant cette refondation suppose une intervention des gouvernants, pour prendre acte de ces mutations et les inscrire dans une réorganisation structurelle, probablement à la faveur d'une nouvelle donne politique, susceptible de s'imposer aux conservatismes et corporatismes.

François DIEU

Professeur de sociologie
à l'université des sciences sociales de Toulouse,

Directeur du Centre d'études et de recherches
sur la police (CERP)

Comment améliorer la Prévention Situationnelle ?

Synthèse du rapport du groupe diagnostic de sécurité n° 7 de la 19e session nationale d'études de l'INHES

Constats et diagnostic

Éléments de définition

Approches conceptuelles

Concept d'origine nord-américaine, la prévention situationnelle complète aujourd'hui celui de prévention de la délinquance. Inscrivant, aux côtés de l'auteur et de la victime, le contexte comme troisième élément du délit, il a pour objectif d'agir sur la dynamique de passage à l'acte des délinquants. Il se focalise donc sur les circonstances qui l'accompagnent, en empêchant ou en retardant sa commission, en la rendant plus difficile et plus risquée pour l'agresseur, notamment en diminuant la vulnérabilité des cibles éventuelles.

Illustration

L'exemple le plus fréquemment évoqué pour traduire ce que représente la prévention situationnelle, dans son approche classique, est celui de la théorie du « *broken glass* » de G. Kelling et J.Q Wilson. Cet exemple new-yorkais de réduction de la délinquance s'illustre autour du concept de fenêtres brisées selon lequel la production d'un cycle de violence découlerait d'un enchaînement d'actes en relation avec certains signes de désordres.

En réponse à cette dynamique, les techniques de prévention situationnelle visent à durcir les cibles selon un schéma décrit par Ronald Clark. Les travaux de ce professeur à l'université de Newark, aux États-Unis, décrivent quatre axes d'intervention, recouvrant seize techniques :

- Augmenter l'effort des délinquants par la protection des cibles, le contrôle des accès, le découragement du délinquant ou encore le contrôle des « *facilitators* » (cartes de crédit, armes à feu, identifiants téléphoniques).
- Augmenter les risques pour le délinquant potentiel, par le contrôle des entrées et des sorties, la surveillance formelle (dont radars), la surveillance par des employés (dont vidéosurveillance) ou la surveillance naturelle (éclairage...) ;
- Réduire les gains, par l'élimination des cibles, l'identification des biens, la réduction de la tentation ou la suppression des bénéfices ;
- Empêcher la justification, par la facilitation du respect de la loi, le contrôle des « désinhibiteurs » (alcool, drogues...), la mise en place de règles, la capacité à donner mauvaise conscience.

Atouts et limites dans une approche classique

Éric Chalumeau, président de la société d'ingénierie de la sécurité Icade Suretis, souligne que l'atout majeur de la prévention situationnelle repose sur le fait d'avoir été forgée à partir de travaux de recherche empirique et évaluative. Il relève trois acquis et trois faiblesses de ce concept et de ses applications [1].

Les acquis

Le premier acquis concerne la théorie des opportunités qui établit une relation entre la distribution géographique de la délinquance sur un territoire et la densité des occasions et des cibles. Le deuxième aspect conceptualisé est la théorie de l'espace défendable introduit par l'architecte américain Oscar Newman, qui a montré que l'on pouvait concevoir des espaces ou la surveillance naturelle des lieux par les occupants pouvait être facilitée. Le troisième élément est la théorie du choix rationnel selon laquelle tout délinquant procède à une évaluation coût - avantage, ainsi qu'à une évaluation sommaire de sa cible.

....

(1) « Prévention sociale, prévention situationnelle, fondements complémentaires d'une politique de sécurité », *Les cahiers du DSU*, mars 1999.

Les limites

Elles concerneraient les limites du champ préventif, ce type de prévention fonctionnant sur des délinquants occasionnels, mais beaucoup moins sur des délinquants d'habitude, surtout ceux affiliés à la grande délinquance, très actifs et recherchant en permanence de nouvelles stratégies. En outre, centrée principalement sur une approche des lieux ou des espaces de commission de l'acte, la prévention situationnelle ne tiendrait pas suffisamment compte du caractère dynamique inhérent au passage à l'acte.

Elles portent également sur le risque d'accroissement des inégalités devant l'insécurité. D'un côté, apparaîtraient les « victimes organisées », qu'il s'agisse de villes, d'entreprises, de commerces ou de particuliers, en mesure de se doter des moyens, notamment techniques, pour se protéger. De l'autre, les victimes potentielles, moins protégées et donc plus exposées. Enfin, l'un des risques est le développement non maîtrisé du marché privé de la sécurité.

En conclusion, Éric Chalumeau met en relation la prévention sociale et la prévention situationnelle, considérant que ces approches doivent être complémentaires. Il rejoint en cela la tendance qui se dégage des recommandations issues du rapport de la table ronde sur la prévention de la criminalité au Québec.

Essai de définition

Dans l'approche relativement récente de la prévention situationnelle, telle qu'elle est appréhendée en France, le concept recouvre « *l'ensemble des mesures d'urbanisme, d'architecture ou techniques visant à prévenir la commission d'actes délictueux ou à les rendre moins profitables 2*». La conception française cherche également à faciliter l'intervention des services de sécurité et de secours.

Avant de déterminer quelles seraient les mesures permettant d'améliorer la prévention situationnelle et après s'être interrogé sur le champ qu'elle peut recouvrir, le groupe de diagnostic a souhaité, dans le cadre de ses premiers travaux, apporter une tentative de définition actualisée : « *Afin d'en réduire la probabilité ou la gravité, la prévention situationnelle désigne les interventions juridiques, humaines ou techniques, visant à se prémunir contre la commission d'actes délictueux en rendant moins vulnérables les cibles potentielles. Dans ses dispositions les plus achevées, elle doit permettre d'aboutir à une anticipation des menaces.* »

Diagnostic

Le système de prévention est encore à construire.

Des informations connues mais mal exploitées

Les informations relatives au niveau d'insécurité sont globalement connues mais éparses et mal exploitées. Les retours d'expériences sur les événements et la pertinence des mesures de prévention sont rarement organisés et souvent négligés.

Une expertise encore trop confidentielle

Les théories et les savoirs de la prévention situationnelle demeurent l'affaire de spécialistes et leur diffusion reste faible. Ainsi, ce sujet n'apparaît-il pas dans le cursus de formation initial des aménageurs et concepteurs (écoles d'architecture, écoles d'ingénieur du bâtiment et des travaux publics), qui sont pourtant en première ligne dans la création d'espaces publics et privés.

La mise en œuvre de la prévention situationnelle est perfectible

La prévention situationnelle n'a pas vocation à s'appliquer à toutes les formes de délinquance

Son champ d'application apparaît aujourd'hui très large, des incivilités au terrorisme. Or, les spécialistes s'accordent à dire qu'elle trouve ses limites aux deux bouts de la chaîne.

Le sentiment d'insécurité apparaît souvent plus lié à des phénomènes d'incivilité ou de pression sociale qu'à des actes réels de délinquances devenus souvent rares dans des lieux publics très surveillés. Un employé de la SNCF interrogé évoque ainsi des insultes ou des déclarations polies mais violentes émanant de clients de type hommes d'affaire, ayant un impact important sur la situation de travail des personnels. Dans ce domaine, la SNCF a pu constater les limites des mesures de protection (enfermement des guichets, vitres renforcées, hygiaphones surprotégés) et l'aspect positif créé par une réouverture des espaces, une remise en valeur du lien social avec les clients et une formation des agents au traitement de l'accueil et des conflits. Le lien social retrouve ici toute sa place à côté des mesures de protection strictes. François

(2) Annexe 1 de la Loi n°2002-1094 du 29 août 2002 d'orientation et de programmation pour la sécurité intérieure.

Wellhoff [3] considère également que la prévention situationnelle a du sens pour les quartiers banals mais que sa capacité de réponse reste limitée dans les quartiers difficiles hors d'un traitement social de fond.

De même, la prévention situationnelle semble bien fonctionner sur des délinquants occasionnels, mais ses effets sont moins convaincants sur des délinquants d'habitude ou décidés, surtout ceux affiliés à la grande délinquance, *a fortiori* au terrorisme, très actifs et en recherche permanente de nouvelles stratégies. Les acteurs mettent en valeur la capacité des délinquants à déployer des stratégies de contournement. La plupart citent l'utilisation classique de la capuche pour se prémunir de la vidéosurveillance. Ainsi, à Lyon, les acteurs locaux constatent que la présence de caméras ne semble pas revêtir un aspect dissuasif absolu. En effet, le délinquant potentiel, bien que se sachant filmé, peut passer à l'acte, soit que le rapport gain/sanction lui apparaisse favorable (cas d'un petit *deal* qui ne donnera pas forcément lieu à une interpellation ou à une poursuite par le Parquet), soit qu'il mette en œuvre des mesures de déception (dissimulation du visage par exemple).

La prévention situationnelle montre également ses limites en matière de grande délinquance. Ainsi, la montée des violences dans le domaine des transports de fonds a pu montrer les limites et les risques d'une recherche systématique de durcissement de la cible.

En matière de terrorisme, la limite touche au terroriste lui-même. Pour ce dernier, que l'on puisse l'intercepter ou non, que l'on puisse ou non l'identifier/l'arrêter/le punir après les faits lui est souvent indifférent et ne l'empêchera pas nécessairement de passer à l'acte. Sa cause revêt à ses yeux une importance telle que ces éléments n'ont que peu d'effets sur lui. Pour ce qui est des terroristes qui commettent des attentats-suicides, ce constat est encore plus flagrant. Ainsi, la théorie de l'acteur rationnel, qui est à la base de la prévention situationnelle, est souvent inapplicable dans le cas du terrorisme. L'exemple de Londres est éclairant. La capitale britannique dispose d'un des systèmes de caméras le plus poussé au monde. Il était donc à peu près impossible que les poseurs de bombes du 7 juillet ne sachent pas qu'ils étaient filmés, donc qu'ils ne sachent pas qu'ils seraient potentiellement identifiés et arrêtés. Pourtant, cela ne les a pas empêchés de s'exécuter. On peut malgré tout reconnaître que les caméras de surveillance de Londres ont permis l'identification, puis l'arrestation, des coupables et, par conséquent, d'éventuelles attaques de la part de ces derniers ont pu être prévenues. Elles contribuent ainsi au travail des enquêteurs sur le démantèlement des réseaux, réduisent le risque de réitération et témoignent de l'efficacité de l'action publique pourvu qu'elle soit assortie des moyens d'intervention adaptés.

L'effet « splash » ou « plumeau » constitue une réalité inévitable

Compte tenu du partage des responsabilités territoriales entre les différents acteurs de la sécurité, et malgré les efforts de coordination des actions et de partage des informations menés au niveau local, la mise en œuvre de la prévention situationnelle ne peut s'inscrire que dans un espace donné et par nature limité. Dans ces circonstances, et à l'exception des milieux totalement confinés et fermés (maison d'arrêt par exemple), le déplacement de la délinquance vers des lieux plus propices à son exercice semble inévitable.

Ce déplacement peut revêtir différentes formes : extraterritoriale (les délinquants quittent la zone), ou intraterritoriale (les délinquants changent de lieu dans la même zone). Peuvent s'ajouter à ces déplacements géographiques des modifications dans les modes opératoires. Ce phénomène, appelé effet « *splash* » (ou « effet plumeau »), traduit en fait l'adaptation des délinquants en réaction aux mesures mises en œuvre dans le cadre de la prévention situationnelle et en constitue un des principaux « effets secondaires ». Il peut également se manifester par les effets d'une réglementation : l'interdiction d'occuper les halls d'immeuble a induit un déplacement des trafics dans les étages et les caves.

On identifie ainsi l'une des faiblesses de la prévention situationnelle, au sens où cet effet "splash" est susceptible d'accroître les inégalités devant l'insécurité. En effet, « *on peut ainsi observer d'un côté "des victimes organisées", type grandes surfaces, entreprises, des villes et des particuliers qui ont les moyens de s'équiper, d'acquérir des équipements techniques lourds. De l'autre, des victimes potentielles ou des espaces qui ne seront pas surveillés. D'où, un certain nombre de problèmes sur les transferts et les déplacements des délinquants. Si vous durcissez une cible ici, que va-t-il se passer à côté ?* » [4].

(3) Membre du Conseil général des Ponts et Chaussées et président du groupe de travail national sur le thème de la prévention situationnelle dans le domaine de l'urbanisme.

(4) *Les cahiers du DSU,* mars 1999

À ce jour, il apparaît que ce phénomène de déplacement n'est en général pas compensé et canalisé par des mesures d'organisation (régionalisation et mutualisation en termes de partage de l'information dans le temps et dans l'espace) qui permettraient d'assurer un suivi précis et pertinent de la trajectoire des délinquants et le traitement successif de ses manifestations.

Des dispositifs qui peuvent s'avérer coûteux, voire inaccessibles

« *La sécurité n'a pas de prix, mais elle a un coût.* » Le célèbre aphorisme constitue un aspect non négligeable des limites identifiées dans la mise en œuvre de la prévention situationnelle. À ce titre, les éléments collectés à propos de l'outil vidéo confirment les inégalités et freins économiques existant aujourd'hui en France.

Les équipements de vidéosurveillance présentent des prix élevés, voire prohibitifs. Ainsi, le coût d'investissement rapporté à la caméra est en moyenne compris entre 50 000 et 70 000 € pour les dispositifs de voie publique en milieu urbain, précisément ceux qui se sont le plus insuffisamment développés. Une pré-étude de la préfecture de police de Paris, pour 1 000 caméras, aboutirait à un montant de 61 000 € par caméra.

Renforçant ce premier constat d'ordre économique, il s'avère que le financement des dispositifs de vidéosurveillance est aussi éclaté que peu organisé. Actuellement, la vidéosurveillance est surtout financée par l'exploitant qui l'installe. L'État n'accorde qu'exceptionnellement son concours financier et les mécanismes classiques ont montré leurs limites.

La normalisation présente également des limites

La collaboration entre spécialistes de l'architecture et de l'urbanisme et experts en criminalité est une nécessité. Le domaine de la construction offre donc plusieurs exemples de démarches de normalisation. Le décret du 3 août 2007 instaure des études de sûreté et de sécurité et l'ANRU encourage des protocoles de Gestion urbaines de proximité (GUP) dans le cadre de ses investissements. L'AFNOR élabore, quant à elle, un texte sur la prévention de la malveillance dans l'urbanisme, fixant diverses directives architecturales pour améliorer la sécurité, qui deviendrait applicable aux opérations de renouvellement urbain. Pour autant, les spécialistes soulignent les limites de ces démarches normatives en tant que réponse technique à des faits de délinquance, par nature évolutifs.

La délinquance évoluant dans le temps et dans l'espace, les réponses techniques quelles qu'elles soient nécessiteront une adaptation patrimoniale lourde, que les maîtres d'ouvrage public concernés auront vraisemblablement des difficultés à appliquer dans la durée. En outre, toute adaptation aux nouvelles règles de sécurité peut générer par la réalisation de nouveaux équipements un nouveau sentiment d'insécurité dû à l'image perçue, soulevant la question de l'acceptabilité. Enfin, la création de normes trouve ses limites dans l'acceptation par le public des solutions préconisées en termes de restrictions des libertés individuelles.

Une intégration encore inégale des utilisateurs

À quelques exceptions que nous avons pu constater dans certaines grandes villes (Lyon, Tourcoing ou Londres par exemple), il s'avère que l'on a souvent recours à des solutions toutes faites, plaquées et pas toujours adaptées aux conditions réelles de vie des espaces concernés et à l'évolution de leurs usages. Ce constat démontre que la démarche partenariale entre les acteurs chargés de l'analyse, de la conception, de l'équipement, de l'aménagement et de la collectivité et des occupants qui pratiqueront au quotidien les dispositions mises en œuvre est souvent négligée ou menée de manière trop superficielle. Or, cette démarche s'avère fondamentale dans la réussite des projets.

Préconisations

Mettre en œuvre une approche globale et développer les partenariats

En concevant des espaces au service d'usages privilégiés

La prévention situationnelle a pour objectif de rendre, dès leur conception, les espaces publics et privés moins « criminogènes ». Le décret du 3 août 2007, pris en application de la loi du 29 août 2002 d'orientation et de programmation pour la sécurité intérieure, impose une enquête de sécurité publique pour les opérations d'aménagement de plus de 100 000 m^2 dans les agglomérations de plus de 100 000 habitants, ainsi que pour la création d'établissement recevant du public de première catégorie. Ce texte a favorisé l'émergence d'une ingénierie de sécurité qu'il importe d'améliorer à chaque étape (conception, mise en œuvre, pilotage, contrôle).

Le groupe recommande de veiller à ce que les mesures de prévention ne nuisent pas à la vocation première du

lieu (loisir, convivialité,etc.), sous peine de défavoriser l'appropriation par les utilisateurs et le contrôle social des lieux.

En s'appuyant sur la complémentarité des politiques publiques

La sécurité nécessite aujourd'hui une approche globale. L'échec relatif des politiques publiques depuis le rapport Peyrefitte (1977) en matière de prévention de la délinquance résulte d'un découplage ou d'une absence de coordination entre les différentes approches. L'insertion de la prévention situationnelle dans une politique globale de prévention de la délinquance apparaît donc comme un axe à privilégier.

Le groupe recommande, à cet effet, de mieux coordonner les politiques selon les trois axes que sont la prévention sociale, la prévention éducative et la prévention situationnelle.

En renforçant le pilotage des dispositifs aux plans national et local

La prévention situationnelle doit être considérée comme une dimension des politiques nationale et locale de sécurité. Celles-ci reposent sur toute une architecture de partenariats et de dispositifs institutionnels qui donnent satisfaction, dès lors qu'existe une volonté humaine et managériale de les faire vivre. Or, nul ne conteste aujourd'hui que ces partenariats ne donnent pas toute leur mesure, bridés par un ensemble d'obstacles doctrinaires, juridiques, techniques et budgétaires qu'il convient de lever, à travers un pilotage renforcé, afin de permettre à la prévention situationnelle de monter véritablement en puissance. Il convient donc d'évoluer vers un décloisonnement des administrations impliquées tant au niveau national, régional que local. Correctement pilotée et coordonnée, la politique de prévention situationnelle ainsi mise en œuvre limiterait par ailleurs la stratification des dispositifs et la dispersion des aides financières.

Le groupe recommande :

- sans préjudice des attributions propres à chaque ministère, de confier au ministère de l'Intérieur, le pilotage, la coordination et l'évaluation des actions menées et de créer, à cet effet, une structure horizontale permanente regroupant des représentants de chaque ministère concerné qui aurait pour vocation d'animer et de mobiliser leurs ressources ;
- de renforcer les compétences des préfets dans leur mission de pilotage local au sein des dispositifs partenariaux existants et de veiller à l'évaluation annuelle des conventions passées entre l'État local et ses partenaires locaux.

En impliquant d'avantage les forces en charge de la sécurité de proximité

Les expériences menées au Canada et en Grande-Bretagne mettent en évidence l'implication, sinon le rôle moteur joué par les forces de sécurité dans la mise en œuvre de la prévention situationnelle. Cette présence active s'exerce principalement au travers du concept de police de proximité ou de police communautaire.

L'analyse de François Dieu, professeur des universités et chercheur, indique les pistes de nature à renforcer l'efficience de la prévention situationnelle dans ce cadre. Le représentant de l'ordre y apparaît comme un professionnel de la sécurité mais aussi comme un membre à part entière de la population du territoire sur lequel il évolue. Cette insertion dans le tissu local permet de développer une approche partenariale et favorise le caractère proactif et globalisé de l'action policière. Cette conception du mandat de police s'intègre parfaitement dans une définition de la prévention situationnelle qui, dans ses dispositions les plus achevées, devrait permettre d'aboutir à une anticipation des menaces. Le développement de cette idée, tel que l'envisage l'auteur, permet d'appréhender de manière claire comment peut s'inscrire l'action des services de police et des unités de gendarmerie dans le cadre de la prévention situationnelle et la plus value qui peut en résulter. D'autre part, il correspond également à la mise en œuvre de la prévention situationnelle, telle qu'elle a pu être observée au sein de la *Metropolitan police* de Londres.

De même, le recours à des référents identifiés au sein des services de police et unités de gendarmerie, dispositif déjà en place (milieu scolaire) ou en cours d'installation (prévention technique de la malveillance), participe directement à la prévention situationnelle et contribue à cette nécessaire relation de proximité.

Le groupe recommande d'inscrire la prévention situationnelle comme un mode d'action privilégié des forces de sécurité, favorisant l'action de proximité et la résolution globale des problèmes ainsi que les liens avec les partenaires des CLSPD. La mise en œuvre des Unités territoriales de quartier (UTeQ) depuis le printemps 2008, s'inscrit dans un cadre de cette nature.

En intégrant mieux les usagers aux dispositifs

La prise en compte des avis et doléances des résidants des quartiers où sont déployées les techniques de prévention situationnelle demeure largement négligée.

Or de nombreuses expériences ont montré que l'implication des bénéficiaires s'avère fondamentale dans la réussite des projets. Beaucoup d'efforts sont voués à l'échec par le manque de motivation ou de prise de conscience des usagers. *A contrario*, d'autres exemples, notamment britanniques et américains, montrent l'intérêt d'une mobilisation collective spéculant sur le sens civique et la responsabilité citoyenne des habitants d'un quartier, en termes de surveillance de l'espace public et de dissuasion des incivilités et des actes de délinquance.

Le groupe recommande de développer un système de contrôle social équilibré, intégrant mieux les usagers au dispositif et permettant de sortir du contrôle policier et de la victimisation croissants. Il préconise la mise en œuvre d'une politique de quartiers de vie établissant un équilibre entre les acteurs sociaux, éducatifs et économiques de proximité, qui contribuent au sentiment de sécurité, et les citoyens-acteurs de la sécurité, nécessairement complémentaire de l'approche distanciée et virtuelle de la vidéosurveillance.

Se doter des outils nécessaires

En élaborant une doctrine nationale de prévention situationnelle

Un guide de référence vient d'être publié en matière de règles d'urbanisme, en application de la loi de 2007 sur la prévention de la délinquance. Ce type de démarche doit être étendu, en particulier en matière de vidéo surveillance. L'absence de doctrine nationale aboutit, en effet, à des écarts majeurs dans l'action des commissions départementales de vidéosurveillance, parfois laxistes, parfois d'une extrême sévérité.

Le groupe recommande ainsi d'assurer une large diffusion du guide (en cours de rédaction) instaurant une doctrine nationale en matière de vidéosurveillance et d'évaluer son appropriation par les partenaires auxquels il est destiné.

En améliorant les outils juridiques de la prévention situationnelle

Le dispositif juridique, qui encadre actuellement l'emploi de la vidéosurveillance, est caractérisé par sa rigidité ; il ne permet pas de répondre aux situations d'urgence, ni d'exploiter les possibilités offertes par l'évolution technologique des équipements. Il doit être simplifié et clarifié.

Le groupe recommande d'améliorer les outils juridiques en substituant la notion de « périmètre vidéo surveillé » à celle de schéma d'implantation des caméras et en allégeant et dématérialisant le traitement des demandes d'autorisation d'implantation des caméras.

En mettant en place un nouveau mode de financement à la hauteur des enjeux

Il est indispensable de créer un mécanisme de financement « incitatif » pour les collectivités locales afin de dynamiser leurs investissements en matière de prévention situationnelle. Une commune développant ou acceptant un système de radars ou de vidéosurveillance comportant des amendes au titre de la circulation dans les couloirs de bus, du non-respect des feux et signaux « stop », doit pouvoir bénéficier d'un retour sur son investissement par l'attribution directe d'une part du montant des amendes de circulation perçues sur son territoire.

Le groupe recommande d'instaurer un nouveau mode de financement en rétrocédant aux collectivités locales qui investissent dans la prévention situationnelle une part du produit des amendes de stationnement et circulation ; cette préconisation suppose trois préalables : la dépénalisation des amendes, la mise en œuvre de la verbalisation assistée par ordinateur (VAO) et le rattachement de la direction du Projet interministériel contrôle automatisé (DPICA) au ministère de l'Intérieur.

En se dotant d'outils de contrôle de la réalisation et de l'efficience

L'amélioration de l'efficacité de l'ingénierie de sécurité relative à la mise en œuvre de la prévention situationnelle passe par une complémentarité des politiques de sécurité et la convergence des organisations dédiées. Force est cependant de constater qu'il n'existe que peu de dispositifs de contrôle de l'efficience de cette politique.

Le groupe recommande donc de mettre en œuvre, sous la direction d'une structure horizontale permanente regroupant des représentants de chaque ministère, une démarche de contrôle de gestion jusqu'au niveau de chaque centre de responsabilité local.

En ciblant l'effort de recherche et de développement sur quelques technologies spécifiques

Le marché des technologies de sécurité est en évolution permanente et chaque mois passé voit apparaître des moyens nouveaux et plus performants : vidéosurveillance

« intelligente », appareil permettant de voir des objets cachés sous les vêtements, appareils détecteurs d'explosifs plus fins, biométrie... En même temps d'autres champs continuent à devoir être explorés : nouveaux explosifs, menaces NRBC (nucléaire, radiologique, biologique et chimique), etc. Dès lors, la généralisation de tels projets reste soumise à des efforts budgétaires importants qui devront être confirmés dans le cadre de la révision générale des politiques publiques.

Dans ce contexte, le groupe recommande :

- de soutenir les actions de recherche-développement pour favoriser l'émergence de technologies adaptées à la doctrine ;
- de privilégier la veille sur l'évolution des menaces et les moyens techniques d'y répondre ;
- dans le domaine de la vidéo, de cibler l'effort de recherche-développement sur les technologies d'exploitation des images vidéo : exportation et traitement rapide, développement de la vidéo « intelligente »...

Optimiser la gestion de l'information

L'efficacité de la prévention situationnelle repose sur une gestion de l'information intégrant un recueil systématique et une analyse au niveau approprié.

Au niveau tactique : en développant les échanges d'informations

Les enquêtes menées sur le terrain, notamment à Londres, ont permis de confirmer que l'action de prévention nécessite d'être bien informé sur les victimes et les lieux, à la fois en termes de géographie et de voisinage. Il semble donc nécessaire de développer, au sein des différentes instances, une démarche structurée de planification des interventions préventives fondées sur cette connaissance locale et détaillée, en établissant un diagnostic de criminalité et de sécurité, avant de déterminer les interventions à réaliser, et de mettre en œuvre une stratégie d'intervention et d'évaluer l'impact des interventions déjà réalisées. La démarche pourrait utilement s'inspirer de la pratique retenue par la ville de Lyon ou du « Guide sur la sécurité dans les milieux de vie » largement reconnu au niveau international qui traite de la mise en œuvre à grande échelle sans recourir à des normes, et s'accompagne des outils de partage d'expérience et de développement d'outils d'aide à l'analyse et au diagnostic.

Pour sa part, le recueil d'informations d'origines diverses au niveau local et leur traitement (analyse tactique) doit permettre, dans l'absolu, de déceler les signaux permettant de mettre en place les mesures préventives et dissuasives visant à éviter la commission d'infractions. Plus précisément, dans la mesure où la vidéosurveillance est retenue au niveau local, elle constitue une source d'informations en images et en temps réel précieuse pour comprendre les évolutions et anticiper, dès lors qu'il s'agit d'un moyen complémentaire au partage du renseignement.

Le groupe préconise :

- de systématiser les protocoles d'échange d'informations au sein des instances locales ;
- d'accroître l'exploitation des images en capitalisant celles associées à des points critiques ; cette démarche pouvant contribuer à une meilleure répartition des forces de police ;
- de développer une infrastructure d'informations et de services partagés.

Au niveau stratégique : en passant de l'observation à l'évaluation

L'analyse stratégique doit évoluer d'une d'observation statistique vers un rôle élargi d'évaluation technique, de diffusion des bonnes pratiques, d'orientation dans un principe d'action interministérielle, et de prospective nécessaire au niveau politique. Pour sa part, l'analyse stratégique permet notamment, à partir des données recueillies au niveau du STIC et de Judex [5], l'étude des phénomènes de délinquance avec pour objectif de déboucher sur la mise en œuvre de préconisations en vue de la neutralisation de ces agissements.

Un effort d'analyse est réalisé par l'Observatoire national de la délinquance (OND), mais qui doit pouvoir évoluer vers une dimension prospective ou, tout au moins, de support à l'analyse de l'efficacité des différentes stratégies de prévention des crimes et délits. Le développement de cette capacité prospective requiert pour l'OND de développer des liens et de confronter ses analyses avec ses homologues des autres ministères. L'OND pourrait

(5) Le système de traitement des infractions constatées (STIC) et le système JUdiciaire de Documentation et d'EXploitation (JUDEX), respectivement mis en oeuvre par la Police nationale et la Gendarmerie nationale, sont des systèmes d'information et de rapprochement judiciaires. Un système commun aux deux forces, baptisé ARIANE, est appelé à leur succéder à compter de 2008.

également porter un projet de diffusion des meilleures pratiques en matière de prévention situationnelle, être le réservoir de la connaissance tactico-pratique au service des niveaux locaux.

Ces exigences de détection précoce, d'analyse assistée, voire automatisée d'évaluation et de support à une politique de communication doivent constituer les fondements d'une politique de gestion d'une connaissance approfondie des milieux de délinquance, d'une évaluation stratégique renouvelée au niveau de l'OND, qui doit pouvoir évoluer d'un rôle d'observatoire géostatistique à un rôle de Conseil stratégique en matière de sécurité. Cette évolution passe par une diversification des sources d'informations et une implication forte dans la nature des données à recueillir au niveau du terrain.

Le groupe recommande de développer au niveau de l'OND les capacités de prospective et de diffusion des meilleures pratiques.

Au niveau politique : en créant un *continuum*

Il conviendrait que le ministère de l'Intérieur puisse développer un système de prévention info centrée, intégrant au niveau local la mise en œuvre de l'approche de prévention situationnelle. Cette nouvelle doctrine témoignerait d'une vision stratégique de l'État en matière de prévention des crimes et délits, intégrée à l'ensemble des actions de prévention permettant d'établir le juste équilibre technologique, humain et culturel adapté aux différents contextes situationnels locaux et offrant des opportunités de progresser vers une sécurité globale, véritable prolongement de l'ingénierie de sécurité mise en place par les législateurs successifs. Il s'agirait de basculer de la prévention situationnelle à partir des faits à une instrumentation de la prévision grâce à l'information.

Le groupe recommande :

- de mettre en place, en s'appuyant sur les services déconcentrés de l'État et sous l'autorité des préfets, un dispositif de détection des signaux faibles ;

- de créer un conseil stratégique de prévention situationnelle chargé d'adapter la doctrine nationale et de la décliner à l'échelon infraterritorial en une analyse de niveau tactique.

Adapter les dispositifs aux situations rencontrées

En tenant compte des évolutions spatiales, temporelles et comportementales

À cet effet, le groupe préconise de définir, à l'image de Vigipirate, des mesures graduées de vigilance, de prévention et de protection, d'une part, d'intervention et de réaction d'autre part, en fonction de menaces allant des incivilités au terrorisme. Cette approche dynamique permettrait d'adapter la réponse en fonction de l'évaluation de la menace.

En faisant preuve de pragmatisme

La mise en place de dispositif de prévention situationnelle nécessite un diagnostic préalable précis. L'objectif est de rechercher les problématiques de sécurités actuelles et futures, et ainsi déterminer les actions à développer. L'efficacité des actions mises en œuvre dépendra du niveau d'identification et de segmentation des problématiques. Plusieurs types de difficultés pourront être identifiés : locales et installées, importées, par opportunité, déplacement des phénomènes sur le moyen et long terme.

À ce titre, le diagnostic et les préconisations seront réalisés à l'échelle du territoire étudié. Les mesures mises en place devront également prendre en compte et anticiper les impacts sur l'environnement immédiat afin d'anticiper les phénomènes de déplacement. Les actions à mettre en œuvre sont de plusieurs types et pourront influer divers domaines. Cela pourra, par exemple, toucher l'architecture, les aménagements, les modes de gestion, l'information, la prévention et la formation des acteurs.

Le groupe recommande de concevoir, utiliser et diffuser des outils simples d'aide au diagnostic, de suivi de l'efficacité et de réajustement des actions.

En organisant et identifiant les retours d'expérience

À cet effet, le groupe préconise de systématiser les retours d'expérience, sources de connaissance, d'apprentissage et de formation pour tous les acteurs de la prévention situationnelle. L'Observatoire national de la délinquance aurait toute légitimité pour jouer un rôle support en ce domaine.

Veiller à l'équilibre entre sécurité et liberté

L'équilibre des sociétés démocratiques repose autant sur la liberté que sur la sécurité conçues comme des droits fondamentaux, indissociables et complémentaires, qui peuvent être opposés et qu'il faudra toujours concilier. La prévention situationnelle participe de cette exigence globale d'équilibre en ce qu'elle est conçue comme un moyen d'assurer l'exercice de la liberté dans un espace public sécurisé. Mais son développement technique et conceptuel met en jeu les limites de l'intervention collective à l'égard des libertés individuelles et de la perception que peuvent en avoir les citoyens concernés par cette problématique.

Aussi pour préserver l'équilibre d'un État de droit et de libertés comme le nôtre, les perspectives globales d'amélioration de la prévention situationnelle doivent faire l'objet d'un double questionnement qui concerne, d'une part, les limites intrinsèques de développement du concept de prévention situationnelle et, d'autre part, les moyens institutionnels d'en contrôler l'évolution.

Parce que le développement de la prévention situationnelle comporte des limites intrinsèques

La prévention situationnelle met en œuvre des techniques qui permettent un contrôle inédit des espaces publics d'échange et de circulation. Ainsi, la vidéosurveillance peut permettre une surveillance globale des déplacements individuels ou collectifs. La prévention situationnelle est à ce titre potentiellement plus liberticide que tout autre moyen de sécurité. La loi est la seule limite réelle à l'utilisation de cette technique contre les libertés publiques. Il est dès lors évident que le corps social doit être vigilant à l'égard des conséquences prévisibles de ses propres demandes de sécurité.

La question qui se pose en termes de libertés publiques est donc de savoir si la limite acceptable du développement des moyens de contrôle se situe au point de rupture à partir duquel la sécurité est assurée mais la liberté a disparu, ou si l'équilibre entre sécurité et liberté doit au contraire être fixé de ce point de vue au seuil d'acceptabilité ressentie par les usagers de sécurité. Dans cette perspective, la question de la pertinence des moyens d'évaluation du ressentiment des usagers reste à définir. Quelles sont alors les limites d'acceptabilité des populations concernées en regard du sentiment paradoxal d'insécurité qu'un surcroît de dispositifs visibles de sécurité peut également produire ?

La prévention situationnelle est un moyen immédiat de combattre le sentiment d'insécurité, mais trop de sécurité visible crée un ressenti sécuritaire qui peut s'avérer contre-productif. On doit en effet mettre en parallèle l'insécurité ressentie ou sentiment d'insécurité et le sentiment de surveillance qui participe de manière paradoxale au sentiment d'insécurité selon la résonance de l'inconscient collectif, selon la culture propre de la population concernée, et selon son histoire. Aussi, la sécurisation des espaces publics de liberté ne doit-elle pas créer un sentiment de liberté surveillée.

En se dotant des moyens d'en contrôler l'évolution

Le groupe recommande le recours à une autorité nationale indépendante, existante ou à créer, dotée de moyens matériels et humains lui permettant d'assumer des missions de centralisation de l'information, d'assistance et de conseil aux collectivités, d'information du public, mais aussi de contrôle de l'utilisation privée des technologies et de proposition de normes légales.

Accompagner le développement par la formation et la communication

La généralisation de la prévention situationnelle nécessite des actions de formation et de communication afin d'en favoriser l'acceptabilité.

En développant la formation

La complexité des problèmes liés à la prévention de la criminalité nécessite une professionnalisation toujours plus poussée des acteurs concernés, ainsi qu'une culture largement partagée. C'est pourquoi des actions spécifiques doivent être menées à leur profit. Pour les fonctionnaires et militaires, elles peuvent être intégrées dès le stade de la formation initiale, puis à l'occasion de leur évolution professionnelle en fonction des postes occupés. Ces formations ne sauraient se limiter aux membres des forces de l'ordre, l'ensemble des acteurs associés au niveau local ayant intérêt à être sensibilisés à la prévention situationnelle. Des actions adaptées peuvent également être organisées vers des publics spécialisés en fonction des responsabilités et métiers exercés. À titre d'exemple, une information destinée aux élus de contact comme les maires peut être dispensée, principalement au moment du renouvellement des conseils municipaux.

L'institut national des hautes études de sécurité (INHES) qui dispose des compétences nécessaires au travers de sa division formation et du réseau de ses auditeurs ainsi que d'un maillage permettant de couvrir le territoire, est en mesure de jouer un rôle moteur dans ce domaine. Enfin, la recherche de partenariats avec le milieu universitaire doit être encouragée afin de créer des liens entre praticiens et chercheurs, dans le but d'éviter que l'écart ne se creuse entre la théorie et la pratique, et de développer l'appropriation des outils permettant d'entreprendre des démarches préventives mieux structurées.

À cet effet, le groupe recommande de développer des actions de formation initiale et continue à destination de tous les acteurs concernés, en utilisant les compétences de l'INHES et en renforçant les synergies avec le milieu universitaire.

En favorisant la communication et l'acceptabilité

De manière liminaire, et afin de faciliter l'acceptabilité des mesures de prévention situationnelle, le premier constat qui s'impose est qu'il convient de développer une culture partagée à la fois par les prestataires de l'offre de sécurité et ses bénéficiaires.

La définition des modalités de la participation citoyenne à la prévention situationnelle et l'information du public apparaissent, à cet égard, indispensables pour surmonter les limites sociologiques de l'acception de la prévention situationnelle. Accompagner la mise en œuvre des mesures par des actions de communication au profit des usagers, en présentant le dispositif retenu et, par exemple, en soulignant les résultats obtenus par ces mêmes dispositifs dans d'autres endroits, en bref, rassurer et convaincre du bien fondé des mesures prises participent des pistes à exploiter. Comme l'indique Véronique Levan, il est nécessaire que les actions entreprises, notamment en matière de dispositifs techniques prennent en compte la question relative aux « coûts sociaux » et donc la nécessaire association des résidents. Elle souligne que la question de l'éthique de l'approche situationnelle est plus que jamais à l'ordre du jour au moment même où la politique de sécurité connaît un essor considérable [6]. La prise en compte des dimensions sociale et humaine de la demande sécuritaire est donc un facteur à ne pas négliger.

À titre d'exemple, on peut citer la création du collège d'éthique et de la charte d'éthique de la vidéosurveillance dans les espaces publics de la ville de Lyon, qui ont manifestement contribué à l'acceptabilité de la vidéosurveillance. Leur mise en œuvre n'a donné lieu à aucune polémique et a indéniablement contribué au consensus par son caractère rassurant. Après avoir rappelé les textes auxquels elle se réfère et défini son champ d'application, la charte détermine, en quatre articles, les principes régissant les conditions d'installation des caméras, celles de fonctionnement du système de vidéosurveillance, les règles relatives au traitement des images enregistrées ainsi que les dispositions arrêtées pour faire respecter la charte. À cet effet, un collège d'éthique, créé par délibération du conseil municipal du 14 avril 2003, et placé sous la présidence d'un conseiller d'État, a pour mission de veiller au respect des obligations législatives et réglementaires, d'informer et de recevoir les doléances des citoyens et de formuler des recommandations au maire.

De même, il convient d'être vigilant sur le risque d'accroissement des inégalités devant l'insécurité. Comme cela a été souligné, parmi les faiblesses mises au passif de la prévention situationnelle, pourrait figurer le fossé qui risquerait de se créer entre ceux en mesure de se doter des moyens, notamment techniques, pour se protéger (villes, entreprises, commerces ou particuliers) et ceux qui deviendraient des victimes potentielles car moins protégées, et donc plus exposées. Le corollaire de cette situation pourrait être une fragmentation des territoires où, à côté d'espaces protégés par des moyens privés, le risque serait de voir apparaître des zones intermédiaires à la charge de l'État. Un autre effet induit est le risque lié au développement non maîtrisé du marché privé de la sécurité ou, comme aux États-Unis, on pourrait assister à l'essor d'un lobby pro-prévention situationnelle encourageant le marché privé de la sécurité de haute technologie.

Le groupe recommande de confier à la structure horizontale permanente déjà évoquée une mission d'évaluation garantissant le respect des principes d'égalité d'accès des citoyens à la sécurité, d'éthique et de déontologie.

Conclusion

Parce qu'il s'agit d'une notion d'appropriation récente dans le monde des professionnels de la sécurité, la prévention situationnelle en France soulève maintes questions, notamment celles de sa définition et de son champ d'application.

(6) LEVAN (V.), 2004, « Sécurisation des quartiers sensibles : l'inéluctable ascension de la prévention situationnelle », *Champ pénal* - volume I – http://champepena.revues.org, novembre.

Pour autant les voies d'amélioration ne sauraient méconnaître l'organisation des différents acteurs intéressés, en particulier dans la nécessaire consolidation des partenariats à tous les niveaux d'échelle territoriale.

En outre, le développement de la prévention situationnelle, qui mérite une approche globale et partagée, suppose également une méthode rigoureuse et outillée, fondée sur une doctrine clairement établie et affichée.

Par ailleurs, sa spécificité tenant à son caractère dynamique, la gestion de l'information à tous les niveaux et stades, comme l'adaptabilité des dispositifs susceptibles d'être mis en place présentent deux des voies essentielles d'amélioration.

En tout état de cause, et parce que la prévention situationnelle constitue une nouvelle approche des questions de sécurité, il importe de veiller en permanence au délicat équilibre entre sécurité et libertés, tout en veillant à accompagner son développement par une communication et des actions de formation adaptées.

Groupe diagnostic de sécurité n° 7 *
19e Session nationale d'études 2007-2008

....

* Composition du GDS n° 7 : Christophe Audic, Ali Badaoui, Jean-François Carrillo, Gérard Clerissi, François Fontaine, Danièle Fourdan, Gilles Glin, Didier Joubert, Bruno Maingon, Stéphane Monier, Maïa Rhoner, Jacqueline Ross, Gilles Rousset, Patricia Schillinger, Bernard Soulie, Claire Thieffry, Michel Thomas.

La Chine en transe ? La Chine en transit

Jean-Claude LÉVY

Cet article se veut un témoignage pour faire connaître aux lecteurs des *Cahiers de la sécurité* le contexte Chinois après les J.O. et le tremblement de terre qui aurait provoqué environ 70 000 victimes. Il nous a paru intéressant de mettre en perspective cette vision provenant du terrain et l'analyse de la politique de recherche chinoise parue dans le troisième numéro des Cahiers de la sécurité [1]. Les quatre grandes tendances exposées par Marie Pierre Van Hoeke se retrouvent en contrepoint dans ces impressions de voyage rédigées par un connaisseur du monde chinois : la priorité affichée pour atteindre une autonomie dans l'innovation qui permettrait à la Chine d'accéder au rang de grande puissance scientifique et industrielle mondiale à l'horizon 2020 ; la cohabitation entre une organisation « soviétique » et le libéralisme américain justifie aujourd'hui des écarts de salaire de un à dix ou même vingt ; un besoin de reconnaissance internationale aussi fort dans les domaines industriels et de la recherche qu'en matière de sport, et enfin, une frontière floue entre le militaire et le civil qui incite à la méfiance.

La tension perceptible en avril 2008 n'était toutefois pas seulement liée à la conjoncture. La dimension environnementale en est plus généralement constitutive et elle se déroule au cœur de choix chinois stratégiques structurels ; économie circulaire [2], transition démographique [3] réussie, transition démocratique ébauchée, « transition » technologique [4] inaboutie. Cette tension devrait perdurer. La Chine est en transit, sinon en transe. Ce moment est révélateur d'interrogations structurelles. La relative faiblesse technologique de la Chine est-elle susceptible de compromettre l'avènement d'une « société harmonieuse » [5] tant souhaitée par le Gouvernement chinois ? Les choix et changements en cours sont-ils maintenant suffisamment explicites pour que l'on puisse se demander si l'on doit en attendre des inflexions diplomatiques nouvelles ?

....

(1) *Cahiers de la sécurité* n° 3, « Risques environnementaux, sommes-nous prêts ? », janvier-mars 2008, p. 164.

(2) On entend par « économie circulaire », un système économique qui est apte à réintroduire dans le cycle de la production et de la consommation tous les déchets, sous-produits ou objets usés, qui redeviennent alors soit matières premières nouvelles, soit objets réutilisables sous forme ancienne réhabilitée, ou encore sont réinventés sous une nouvelle forme.

(3) Transition démographique : phase d'évolution de la population d'un pays durant laquelle la mortalité se « modernise » (diminue fortement), alors que la natalité reste « archaïque », c'est-à-dire abondante, avant qu'un réajustement n'intervienne, par abaissement de la natalité. La transition économique est le passage d'un mode de production à un autre, soit du féodalisme au capitalisme, soit du capitalisme au socialisme, selon les concepts marxistes. La première a donné lieu à une abondante littérature, qui se poursuit ; la seconde relève désormais de la fantasmagorie. Le concept implique une alternative à celui de révolution, même s'il est censé la préparer. (D'après Brunet R., Ferras R., Thery H., *Les mots de la géographie*, Reclus-La documentation Française, 1993). Les concepts « économie socialiste de marché » et « économie circulaire » ne relèvent cependant pas du fantasme : la Chine d'après Deng Xiaoping tente d'en réaliser la viabilité (N.D.L.R.).

(4) Il y a longtemps que les pays développés ont effectué de façon inégale, ce que nous appelons, par commodité de langage, leur « transition » technologique, c'est-à-dire la valorisation de la recherche fondamentale en direction des applications industrielles innovantes et produites en série. Les réformes engagées aujourd'hui en France, du point de vue de la recherche, viseraient simplement à combler des lacunes préjudiciables au développement des PME/PMI.

(5) Du point de vue sociologique, le concept d'harmonie répond à des nécessités consubstantielles de la société chinoise, signifiées par plus de deux mille ans d'injonctions philosophiques ou littéraires : formulées par les Classiques avant Lao Tseu, Confucius, Mo Tseu, et après eux, par la grande poésie chinoise Tang et Song et par les grands romans des périodes Ming et Qing (*Rêve dans le pavillon rouge, Voyage à l'Ouest*...), jusqu'à la littérature du XX^{e} siècle. Ce concept n'est ni dogmatique ni figé dans la mémoire, il reste ouvert à enrichissement : en effet la littérature chinoise du XX^{e} siècle l'enrichit, curieusement, en parallèle, sinon en correspondance avec les productions littéraires occidentales, grâce la conscience aiguë de « l'absurde » que traduit par exemple Lu Xun, dans *La véridique histoire d'Ah.Q.* (pas si loin de Kafka), et que perçoit magistralement Malraux, en 1925, dans *La tentation de l'Occident*).

Tremblement de terre ou séisme politique latent ?

Pour le Gouvernement chinois, devant une année 2008 particulièrement compliquée, il est d'abord urgent de répondre, dans l'action et le verbe, aux catastrophes, telles qu'elles sont et telles que la population chinoise les perçoit. Ce gouvernement a effectivement été pris de court par l'abondance des imprévus (froid glacial du printemps, accident ferroviaire, affaire tibétaine, tremblement de terre), faisant certainement preuve, concernant le Tibet, d'une certaine myopie culturelle à propos des capacités prédictives du système face aux situations inattendues. Mais, il serait erroné d'en conclure que ce Gouvernement gérerait le pays sans compétence et prévisions à court et à long terme. La gestion de la « catastrophe » fait bien évidemment partie de la stratégie gouvernementale chinoise, catastrophe tout particulièrement « naturelle », associée à nombre de facteurs culturels, puisqu'elle porte à long terme sur l'écologie du pays et le développement durable : il n'y a qu'à lire les documents des derniers congrès du Parti communiste chinois (PCC) et de l'Assemblée populaire nationale (APN) et regarder ce qui est expérimenté sur le terrain à des échelles non négligeables. La réactivité transparente manifestée devant la détresse du Sichuan montre une remarquable aptitude à gérer, dans l'urgence et en profondeur, une crise de conjoncture. Ce qui fait « séisme » politique en Chine, c'est la réforme de grande ampleur engagée depuis le début des années 2000, concernant la recherche d'un nouveau contrat social, actuellement formulé dans les termes de société harmonieuse.

La réussite presque excessive des injonctions de Deng Xiaoping (qui s'était tout de même donné cent ans pour arriver à ses fins !), avec une croissance de plus de 10 %, a fait de l'environnement la pierre de touche de mille difficultés de tous ordres et désordres. L'environnement est une question clé pour comprendre et agir : revalorisation des ressources, introduction de l'écologie dans la perspective de l'après-Kyoto, dans tout un panel de décisions nationales et locales. Et, dans l'ensemble, la nouvelle politique de réforme, nécessairement à dimension environnementale, exige une reformulation de la qualité et du taux de croissance (aujourd'hui plus de 10 %), reformulation à la baisse (moins de 8 %) qui menace inévitablement les avantages marchands et capitalistiques acquis durant ces dernières années, menaçant aussi les équilibres politiques tant aux échelles locales que centrales. Ceci n'est pas sans correspondance, toutes choses égales par ailleurs, avec la reformulation des politiques environnementales à l'échelle de l'Union européenne, directives, lois, règlements des États membres, dont témoigne en France l'accouchement (difficile) du « Grenelle » de l'environnement.

L'économie circulaire et la société harmonieuse

En bref, la Chine, « sous tension », est contrainte de ne plus épuiser son capital naturel. Elle ne saurait perdurer en « usine du monde » sans que cette tension généralisée se « recycle », grâce à des régulations mobilisant sa politique intérieure et ses relations internationales.

Du point de vue de la politique intérieure, l'économie circulaire, désormais inscrite dans les lois et règlements, propose de réduire la tension sur les ressources naturelles, par une révision des processus de production et des comportements consuméristes. C'est un programme intégré, dont tout le monde peut consulter les termes sur Internet, et dont les réalisations existent déjà, comme l'Agence française du développement (AFD) a pu le constater partiellement à Wuhan (Recherche sur les montages financiers à Wuhan, ou à Guiyang sur les transports urbains). Et, le récent accord de 2008, entre le ministère de l'Écologie, de l'Énergie, du Développement durable et de l'Aménagement du territoire (MEDDAT) et le ministère de la Construction (MOC) sur l'intégration du développement durable urbain confirme ce programme. Le MOC est d'ailleurs devenu récemment ministère de la Construction et de la Planification urbaine et rurale, c'est-à-dire en relation plus forte avec les ressources naturelles et les paysans.

L'économie circulaire pourrait bien être l'ébauche d'un troisième grand mouvement significatif de la Chine, à la recherche d'elle-même depuis la Révolution qui a pris fin en 1949, ce mouvement est actuellement au moins amorcé dans la loi et dans l'expérimentation. Après l'indépendance « socialiste » et maoïste, depuis sept ou huit ans, la réforme de Deng Xiaoping pour une « économie socialiste de marché » rencontre ses limites, à la mesure des ressources naturelles disponibles et des catastrophes annoncées : cela signifie alors un troisième mouvement de la Chine vers la formule désormais martelée « société harmonieuse ». Ce n'est pas une commodité de langage démagogique susceptible d'amuser des observateurs inattentifs, de surcroît vaguement goguenards. Cette formule répond à une tension généralisée à trois dimensions : tension écologique sur les ressources naturelles, tension sociale sur l'inflation et la cohérence des politiques territoriales, associée à la première, avec consécutivement tension sur le mode de production inapte, dans son fonctionnement actuel, à résoudre les tensions écologiques et sociales.

La Chine est ainsi sous tension de façon structurelle, c'est mesurable concernant les nuisances et les pollutions,

la relation croissance du PIB/consommation énergétique/ressources en eau/qualité de l'air/développement des transports : chaque point de PIB gagné entame le capital écologique. C'est pourquoi, après que Mao a installé l'indépendance nationale et le « socialisme » (avec beaucoup de « casse »), que Deng a ouvert le pays à l'économie de marché (avec des dégâts non réductibles aux catastrophes naturelles), on peut considérer que les réformes de Hu Jintao et de Wen Jiabao ne prétendent pas moins qu'à une troisième étape, fondamentalement nécessaire, vers « l'économie socialiste écologique de marché », dont les avantages escomptés ne sont pas seulement écologiques, ils sont aussi de nature culturelle, touchant aux grandes philosophies chinoises (Confucius, Lao Tseu, Tchouang Tseu, Mo Tseu, etc.). L'élan religieux populaire observé alors à Pékin pour les victimes ne relève pas de la propagande : 10 000 chrétiens pékinois sont venus prier dans une cathédrale de Pékin qui ne saurait en contenir que 600 ! La Chine, sinon de foi, a besoin d'une société harmonieuse, de sagesse en rapport avec le monde et la nature tels qu'ils sont. Sur le plan prédictif, il est alors étrange que le Gouvernement ait sous-estimé les facteurs religieux et culturels au Tibet (nous avons pu nous-mêmes constater, au cours de l'été 2007, qu'il les gérait bien mieux, directement ou indirectement, au Xinjiang).

Après la transition démographique réussie, *quid* de la « transition » technologique ?

Mais, le temps est compté, et le pays se heurte à un obstacle difficilement surmontable ; après une transition démographique réussie et une transition démocratique ébauchée, la « transition » technologique peine à répondre à la demande, notamment pour articuler les avancées sociales et technologiques.

En effet, les réponses planétaires à l'avènement du XXIe siècle, nécessairement écologiques depuis *Le Rapport Brundtland*, qui se sont traduites par les analyses scientifiques du « Global Change », par les accords du Kyoto, néanmoins diversement appliqués, font problème partout. Les solutions exigeraient des choix économiques (Organisation mondiale du commerce), technologiques et politiques, à des échelles qu'il serait immodeste d'analyser ici. Mais concernant la Chine, en regard de ce qui vient d'être écrit, les solutions envisagées par le Gouvernement, sinon la gouvernance qu'il entend promouvoir, se dessinent dans la promotion d'une économie circulaire et d'une société éventuellement harmonieuse.

Ambitions démesurées, dira-t-on ? Fuite en avant ? Nous ne le pensons pas : « l'usine du monde » fonctionne « à plein régime ». Cela fait peur dans le monde et autour d'elle. Afin d'exorciser ces craintes, de « radicales » solutions de café du commerce sont quelquefois préconisées ici, qui suggèrent quelque boycott au détriment de la Chine : les magasins occidentaux se videraient très rapidement et la Chine, en retour, se trouverait bien en peine sans les technologies occidentales pour assurer quelque besoin social, harmonieux ou non ! Ce serait en outre ignorer que la Chine porte déjà en elle-même quelque faiblesse susceptible de rassurer ses détracteurs éventuels : principalement ce sont les technologies avancées qui y font question (à quelques branches industrielles près, les nouvelles technologies de l'information et de la communication par exemple). Presque tout ce qui se vend de technologiquement sophistiqué est encore d'extraction occidentale. Cela dit, les échanges de toute nature, mondialisés, génèrent des interdépendances telles qu'il n'est point d'atout ou de faiblesse qui ne soit partagé d'une façon ou d'une autre, à tout le moins dans les pays développés et émergents. L'Occident a besoin de l'usine chinoise, la Chine a besoin de la technologie occidentale. En fait, l'affaiblissement de la Chine serait contre-productif, y compris pour ceux qui le désireraient.

Il est vraisemblablement suffisant de contenir les ambitions chinoises, dans la limite des réciprocités négociées et bien établies, sur une dialectique des avantages mutuels. C'est d'ailleurs pourquoi l'intelligence économique tend à prendre une dimension accrue dans les instructions que donnent les gouvernements occidentaux et les firmes industrielles à leurs ressortissants appelés à travailler en Chine.

La Chine ne nous achète certainement pas assez, ni dans son intérêt ni dans le nôtre. Une inquiétude abusive n'est pas de mise, la « transition » technologique de la Chine prendra du temps, bien qu'elle soit vivement inscrite dans les grands programmes scientifiques (*cf.* le site du ministère de la Science et de la Technologie) : le fossé entre recherche fondamentale et découverte pré-industrielle est encore profond. La puissance chinoise a ainsi une faiblesse non négligeable pour faire un troisième pas en direction de la société harmonieuse, un pas tendu en zone à risque, comme au sein d'une sorte de « séisme lent ».

Coopération internationale, multipolarité, philosophie de l'histoire

Les choix chinois qui viennent d'être évoqués relèvent-ils d'une improvisation chaotique continue ou véritablement

d'une reconfiguration structurelle ? Et quoi qu'il en soit, ces transformations devraient-elles appeler quelque « rupture » éventuelle dans la politique européenne, et notamment française, à l'égard de la Chine ? Rien n'est moins certain.

Du point de vue géopolitique, s'il y a effectivement « rupture », elle est d'abord, de très long terme, amorcée par le Général de Gaulle en 1964, qui annonçait déjà un monde multipolaire et une sortie de la guerre froide. Le terme peut toutefois encore convenir aujourd'hui avec, au sein de ce dernier, l'idée de « puissances relatives » récemment avancée par le président de la République lors de la conférence des ambassadeurs qui s'est tenue du 27 au 29 août 2008. Toujours de ce point de vue, c'est à propos de la nature de la mondialisation qu'il y a des effets de rupture, avec l'émergence massive des nouvelles technologies et de l'écologie.

Alors, concernant les politiques européennes et françaises à l'égard de la Chine, dans l'hypothèse où la technologie est une dimension cruciale du développement économique, écologique et social, à la fois dans les choix locaux et géopolitiques (*cf.* le « nucléaire »), peut-être convient-il à la fois d'être prudent et audacieux, pour infléchir ou non de quelque façon que ce soit les lignes de la diplomatie. Prudent, parce que les échanges technologiques génèrent des transformations lourdes de conséquences sur les appareils de production et de consommation. Audacieux, parce que ces échanges sont irréversibles (*cf.* la réussite japonaise des années 1960). Il est clair qu'un grand nombre d'États, dont les États-Unis (en position scientifique et technologique avancée), reculent en raison de solides contraintes intérieures, pour favoriser des échanges accrus, face à l'après-Kyoto, où se jouent les technologies de demain. L'Union européenne porte plus audacieusement les accords de Kyoto, hésitant toutefois en de nombreux points, en raison de sa diversité. La Chine, enfin, n'a d'autre choix que d'avancer vers des solutions directement concrètes et culturelles : l'environnement est son talon d'Achille.

Mais, trop examiner la conjoncture géopolitique sous l'angle d'un combat de chefs, face à face ou triangle, relèverait d'une vision naïvement bipolaire. La Chine est forte et faible du point de vue technologique. Certes, la société harmonieuse peut trouver dans les modifications consuméristes et comportementales un important gisement énergétique et de matières premières : les économies d'énergie réalisées à l'échelle de la consommation, où des pratiques raisonnables sont immenses (ce fut très bien analysé ici lors de la première crise pétrolière et les directives européennes agissent dans ce sens). Mais, c'est en relation avec des technologies avancées, propres, avec une ingénierie administrative et financière associée qu'il faut compter. La Chine est encore bien démunie de ces technologies-là, outre que les tensions internes, évoquées ci-dessus, en retardent parfois l'adoption. Elle regarde depuis longtemps vers le Japon et la Russie, et les effets du tremblement de terre accentuent ce regard (la présence de techniciens japonais – peut-être militaires - au Sichuan est un signe). Une perspective d'échange est ouverte, mais non franchie (sans angélisme donc) : « donnant-donnant » et « gagnant-gagnant » : ouverture à la Chine des technologies avancées, ouverture aux « occidentaux » d'un marché chinois encore difficile d'accès.

Les événements politiques qui ont accompagné l'affaire tibétaine, le refroidissement peut-être durable de la relation « stratégique » franco-chinoise, demandent certainement à être examinés en relation étroite avec le contexte intérieur chinois évoqué ci-dessus. L'Europe, et tout particulièrement la France, n'a peut-être pas intérêt à tenir la dragée trop haute à une Chine à la recherche d'elle-même grâce à un mode de production et de consommation conforme au développement durable. De notre point de vue, la Chine est réellement engagée dans une perspective écologique vitale non seulement pour elle-même, mais aussi pour le reste de la planète. L'économie circulaire à la chinoise, notamment dans sa configuration confucéenne ou taoïste, ne saurait ni avoir de modèle ni servir de modèle, elle ne saurait s'accommoder d'un quelconque universalisme ou de formes démocratiques tout aussi universelles, qui seraient impulsées depuis Londres, Paris ou New York. Il s'agit d'une contribution originale au développement durable.

Un « contrat-social » de type nouveau (terminologie que nous avons retrouvée avec intérêt sous la plume de Frédéric Bobin dans le journal *Le Monde*) pourrait bien être à l'ébauche en Chine. Jean-Jacques Rousseau n'est pas loin, à ceci près que l'universalisme de ce dernier et des « lumières » n'est plus de mode dans nos sociétés postmodernes [6]. Ni un saint Augustin, de raison et de foi, avec son dieu unique, ni Auguste Comte, avec son unique

....

(6) « Post-moderne » : on entend par là que les grands schémas de la pensée moderne élaborés depuis la Renaissance (correspondant à des idées de vérités et de savoirs qui seraient absolus, universels) seraient aujourd'hui contestés par l'élaboration d'un savoir plus incertain, élaboré par tâtonnement, en relation avec des situations concrètes, au sein de systèmes en devenir aléatoire. *Cf.* Michel Maffesoli : « *Si une définition, provisoire de la postmodernité devait être donnée, ce pourrait être : la synergie de phénomènes archaïques et du développement technologique. C'est ainsi, que pour reprendre les grands thèmes explicatifs de la modernité : État-nation, institution, système idéologique, on peut constater, pour ce qui concerne la post-modernité, le retour au local, l'importance de la tribu et le bricolage mythologique* ». http://www.miviludes.gouv.fr/IMG/pdf/Michel_Maffesoli.pdf

raison, ne sauraient rendre compte de la fragmentation du monde contemporain : celui-ci a besoin de cadres de pensée plus ouverts, de schémas d'organisation évolutifs, de méthodes d'approches empiriques et non dogmatiques. Effectivement, il y a vingt ans, à l'autre bout du monde, Deng Xiaoping a formulé un mouvement qui ne renie ni la pensée chinoise contradictoire traditionnelle (Yin et Yang), ni la philosophie postmoderne la plus affirmée (*cf*. Edgar Morin : « La méthode »). Ce n'est pas être naïf de vouloir que les droits et services essentiels soient assurés partout et pour chacun dans le monde, si nous le faisons en prenant la mesure de chaque situation particulière. Il n'est pas abusif de dire que l'Occident est souvent dogmatique et qu'il manque un peu de mesure. Nous pouvons à la fois aimer la Chine et ne perdre en aucune façon nos propres intérêts de vue. Et lorsque nous la regardons, il ne faut pas oublier de prendre en considération ce que disait, en substance, le sage et utilitariste Mo Tseu (V[e] siècle b.c.), sur l'amour universel : « *aimez votre prochain comme vous-même, pour votre mutuel avantage*. » [7].

Jean Claude LÉVY [8]

ÉCONOMIE

....

(7) *Cf*. Alexandra David-Neel. *in Le philosophe Mo Tseu et l'idée de solidarité. Socialisme chinois*, Londres, Luzac et Cie, 1907).

(8) Jean Claude Lévy est historien et géographe. Depuis 2005, il est chargé, par le ministre des Affaires étrangères, d'une mission sur la coopération décentralisée (Chine, développement durable, coopération de région à région, de ville à ville...@), il est également conseiller spécial auprès du délégué pour l'Action extérieure des collectivités locales.

La chaîne hiérarchique du ministère public

Jean-Marie HUET
Jean-Amédée LATHOUD
François MOLINS

La direction des Affaires criminelles et des Grâces :
Une institution au cœur du ministère public français

Jean-Marie HUET
Magistrat, directeur des Affaires criminelles et des Grâces

Existant sous cette dénomination depuis 1814, la direction des Affaires criminelles et des Grâces (DACG) du ministère de la Justice constitue l'une des composantes les plus emblématiques du ministère public « à la française ». L'éventail de ses missions est pourtant méconnu, d'autant qu'elle ne suscite l'intérêt des médias que pour ses attributions dans le domaine de la conduite de l'action publique, à raison de son rôle, supposé ou réel, dans les affaires individuelles qui défraient la chronique.

Perçue comme le « bras armé » du ministre de la Justice en matière répressive, la DACG incarne, aux yeux de certains, la mainmise du pouvoir politique sur l'autorité judiciaire. Force est d'ailleurs de constater que cette idée reçue est parfois érigée en vérité par de supposés « sachants ». C'est ainsi que le célèbre site *Wikipédia* – qui, à défaut de jouir d'une autorité incontestée, constitue l'une des principales sources de renseignement de nombre d'internautes – définit la DACG comme « [...] *une administration du ministère de la Justice français* [qui] d*onne des instructions de poursuite au parquet, c'est-à-dire les procureurs généraux et les procureurs de la République* [et que de ce fait], *elle juge donc de l'opportunité des poursuites* ». Nul juriste pénaliste n'ignore l'inexactitude de cette définition puisque si le garde des Sceaux peut donner des instructions aux fins de poursuites, ni lui ni ses services ne peuvent demander le classement d'une procédure, le procureur de la République restant le seul vrai juge de l'opportunité des poursuites.

La vérité sur les missions de la DACG se trouve dans les dispositions de l'article 30 du Code de procédure pénale aux termes desquelles « *le ministre de la Justice conduit la politique d'action publique déterminée par le Gouvernement. Il veille à la cohérence de son application sur le territoire de la République. À cette fin, il adresse aux magistrats du ministère public des instructions générales d'action publique. Il peut dénoncer au procureur général les infractions à la loi pénale dont il a connaissance et lui enjoindre, par instructions écrites et versées au dossier de la procédure, d'engager ou de faire engager des poursuites ou de saisir la juridiction compétente de telles réquisitions écrites que le ministre juge opportunes* ».

Sont ainsi placés au cœur de l'action quotidienne de la DACG, à la fois le concept de « politique d'action publique », plus couramment désigné sous le vocable de « politique pénale », l'objectif de cohérence dans l'action des parquets généraux et des parquets, et le moyen d'action que constituent les instructions, qu'elles soient générales ou individuelles (avec les limitations qui seront reprises ci-après). S'il est vrai qu'à ce titre, elle est, en elle-même, actrice des procédures judiciaires et partie prenante de la justice pénale, son champ de compétence ne saurait être réduit au périmètre défini par l'article 30. Elle a aussi pour mission, en effet, de concevoir et de mettre en œuvre les outils de la justice pénale qu'il s'agisse des normes, nationales et internationales, ou des « outils » pratiques utilisés par les parquets dans leur action quotidienne. Investie de la totalité des missions du ministère de la Justice dans le champ pénal, la DACG est donc tout à la fois au service de la conception et de la mise en œuvre des outils, ainsi que partie prenante de la justice pénale .

La DACG, conceptrice des outils de la justice pénale

La DACG est une direction législative à raison de ses compétences en matière normative. Elle est aussi au service des juridictions et des magistrats de terrain pour lesquels elle conçoit des outils d'action .

Les outils normatifs

Direction du droit pénal, la DACG a pour première mission de participer à l'élaboration des normes répressives nationales et internationales.

La norme nationale

S'agissant des normes nationales, la DACG a la mission d'élaborer, sous l'autorité du garde des Sceaux, les textes pénaux voulus par le Gouvernement, qu'il s'agisse de modifier les règles de fond ou d'adapter celles de forme. À titre d'illustration, la direction s'est particulièrement investie, à la demande des ministres successifs, dans la lutte contre la récidive avec l'adoption des lois du 12 décembre 2005 relative au traitement de la récidive des infractions pénales, du 10 août 2007 relative à la lutte contre la récidive des majeurs et des mineurs, et du 25 février 2008 relative à la rétention de sûreté et à la déclaration d'irresponsabilité pénale pour cause de trouble mental.

Cependant, l'élaboration des normes répressives n'étant pas l'apanage du seul ministère de la Justice, la DACG est appelée à mettre son expertise à disposition des autres départements ministériels. Celle-ci a par exemple été sollicitée dans le cadre de l'élaboration des textes sur l'interdiction de fumer dans les lieux publics ou, plus récemment, pour la préparation du projet de loi relatif aux organismes génétiquement modifiés.

La norme internationale

Depuis 2005, la DACG est aussi chargée de la négociation des normes pénales internationales. Dans ce domaine, l'Union européenne présente une part prépondérante. Ainsi, dans le cadre de la Présidence française de l'Union, la DACG porte l'action de la France tendant à l'adoption de nouvelles décisions-cadres visant par exemple pour l'une à permettre l'exécution dans un pays membre des décisions de contrôle et d'assistance prises avant jugement, pour l'autre à autoriser la reconnaissance et l'exécution mutuelles des peines impliquant un suivi de mesure de probation, et pour une troisième, à consolider le statut et à renforcer les prérogatives des représentants nationaux auprès d'Eurojust.

L'activité « pré-normative »

L'appréhension dans sa globalité de la mission normative de la DACG nécessite d'évoquer son investissement dans la sphère « pré-législative », c'est-à-dire au stade où praticiens et théoriciens du droit s'unissent pour expertiser l'état du droit positif et dessiner son évolution future.

Forte de l'expérience que lui confère son suivi de l'activité des parquets et des parquets généraux, la DACG est régulièrement missionnée pour constituer des groupes de travail chargés d'une évaluation ou d'une réflexion particulière. C'est ainsi que la direction a récemment pris une part essentielle aux travaux relatifs à la dépénalisation de la vie des affaires, comme à la réflexion confiée à Serge Guinchard sur la déjudiciarisation et la réorganisation des contentieux. C'est à ce titre qu'elle participe aussi aux travaux de refonte de l'ordonnance du 2 février 1945 relative aux mineurs délinquants.

Les outils pratiques de l'action pénale

Les fichiers

Le plus emblématique des outils mis à la disposition des juridictions est, à l'évidence, le Casier judiciaire national (CJN) sis à Nantes. Partie intégrante de la DACG dont elle constitue l'une des trois sous-directions, le CJN enregistre, après un contrôle strict de légalité et de cohérence, les condamnations prononcées par les juridictions françaises ou étrangères, et les restitue sous forme d'extraits appelés bulletins de casier judiciaire.

Enregistrant plus d'un million de décisions par an et délivrant annuellement près de huit millions de bulletins, le CJN n'a cessé de moderniser son offre de service au bénéfice des juridictions et des justiciables. Les téléprocédures et les traitements automatisés se sont ainsi développés au profit des demandeurs de bulletins améliorant la célérité du service rendu. En outre, l'interconnexion des casiers judiciaires européens, opérationnelle depuis le 31 mars 2006, relie désormais la France à l'Allemagne, l'Espagne, la Belgique, au Grand-duché du Luxembourg et à la République tchèque.

En application de la loi du 9 mars 2004, le chef de service du CJN assure enfin la tenue du Fichier judiciaire

national automatisé des auteurs d'infractions sexuelles ou violences (FIJAIS), créé dans le but de prévenir le renouvellement de ces infractions et de faciliter l'identification de leurs auteurs. Au 30 avril 2008, ce fichier contenait 41 356 personnes, 500 nouveaux dossiers étant enregistrés chaque mois.

Les outils d'enquête

Travaillant très étroitement avec la direction générale de la Police nationale (DGPN) et la direction générale de la Gendarmerie nationale (DGGN), la DACG est particulièrement soucieuse de l'amélioration de l'exercice de la police judiciaire. Elle a notamment contribué à la réforme de la formation des candidats à l'obtention de la qualité d'officier de police judiciaire (OPJ) afin de donner une dimension plus opérationnelle à la formation.

En outre, plusieurs projets sont en cours de réalisation, qu'il s'agisse de l'harmonisation des référentiels de compétences des OPJ de la police et de la gendarmerie, de la mise en place d'un programme commun de formation ou de la rédaction d'un guide méthodologique du compte rendu téléphonique au parquet.

La médecine légale et l'évolution de son organisation constituent aussi un chantier prioritaire de l'action de la DACG qui participe notamment aux travaux du Conseil supérieur de la médecine légale dont elle assure le support logistique.

Enfin, la DACG se doit de mettre au service des juridictions des outils modernes et innovants d'action, en s'inspirant parfois des exemples étrangers. Ainsi, à l'instar des exemples nord-américains que la direction a mis en place le système Alerte enlèvement qui permet de mobiliser le plus grand nombre lors des enlèvements de mineurs.

L'entraide pénale internationale

Au-delà de son activité courante concernant la diffusion des commissions rogatoires internationales ou l'émission des mandats d'arrêt européens ou internationaux, la DACG axe plus particulièrement son action en la matière sur la lutte contre la criminalité organisée et le terrorisme. À cette fin, elle a mis en place plusieurs groupes de travail bilatéraux avec des pays comme le Maroc, l'Egypte, la Russie et elle prend part aux réunions des instances européennes spécialisées. De même, la DACG a abondamment développé les protocoles d'accord portant sur les équipes communes d'enquête en particulier avec l'Espagne, la Belgique, la Grande-Bretagne, le Portugal, les Pays-Bas, la Bulgarie et Chypre.

La DACG, actrice de la justice pénale

Si l'on excepte ses missions dans le domaine législatif, c'est bien à raison de son activité dans les domaines de la politique pénale et de l'animation et de la coordination de l'action publique que la DACG est souvent le mieux identifiée par ses interlocuteurs. La sensibilité et l'actualité de la question conduisent toutefois à préciser son rôle dans le domaine de l'exercice du droit de grâce du président de la République.

La politique pénale

La politique pénale consiste en la définition, par le garde des Sceaux, des priorités retenues pour la conduite et l'exercice de l'action publique, et en la détermination des conditions d'une application cohérente de la loi pénale sur l'ensemble du territoire national. Il appartient à la DACG d'assurer la mise en œuvre, sur l'ensemble du territoire national, des instructions du ministre. Pour ce faire, ses interlocuteurs sont les procureurs généraux qui portent la responsabilité de la mise en œuvre, au niveau régional, de la politique pénale.

Plus précisément, la mission de la DACG en ce qui concerne la politique pénale est triple : elle doit assister le garde des Sceaux dans la détermination des priorités de politique pénale ; elle doit assurer la mise en œuvre des instructions du ministre ; elle doit enfin dresser un bilan et une évaluation de la mise en application de cette politique.

La détermination de la politique pénale

La politique pénale est, en tout premier lieu, l'expression de la volonté politique du Gouvernement et plus particulièrement du garde des Sceaux. C'est ainsi que dès sa nomination, Rachida DATI, ministre de la Justice et garde des Sceaux, a distingué quatre priorités dans le domaine pénal : la lutte contre les discriminations, la prévention de la récidive des majeurs et des mineurs, la lutte contre la délinquance des mineurs et le renforcement de l'aménagement des peines.

La définition d'une priorité de politique pénale est souvent liée à l'adoption d'une nouvelle norme législative. Pour lutter contre la récidive, par exemple, le garde des Sceaux a fait adopter par le Parlement la loi du 10 août 2007 instituant les peines dites « plancher » et celle du 25 février 2008 relative à la rétention de sûreté et à la déclaration d'irresponsabilité pénale pour cause de trouble mental. En ce domaine, il est certain que la politique pénale consiste d'abord et avant tout en la mise en œuvre de ces nouvelles dispositions législatives.

Il n'est toutefois pas rare qu'une politique pénale – même innovante – soit définie à droit constant. En matière de lutte contre les discriminations, la politique voulue par le garde des Sceaux – destinée notamment à encourager les victimes à dénoncer les faits à l'Autorité judiciaire – a notamment consisté à demander aux procureurs de la République de créer des pôles de lutte contre les discriminations composés d'un magistrat et d'un délégué du procureur issu du milieu associatif ou désigné en concertation avec lui à raison de sa connaissance de ces problématiques particulières.

Forte de la connaissance que lui confère tant son statut d'interlocutrice privilégiée des parquets généraux que le suivi de l'action publique, la DACG peut utilement conseiller le garde des Sceaux sur les thèmes devant faire l'objet d'instructions particulières de politique pénale, voire prendre l'initiative de telles instructions, notamment lorsqu'il s'agit de sujets techniques. Elle le fait, par exemple, à l'approche de l'organisation, en France, d'un événement majeur telle que la Coupe du monde de rugby afin de coordonner l'action des parquets dans des domaines aussi variés que les violences dans les enceintes sportives, la contrefaçon de marques, le dopage ou le travail illicite.

La mise en œuvre de la politique pénale

Une fois définie par le garde des Sceaux, une politique pénale est portée par la DACG qui a la responsabilité de la mettre en œuvre. Elle y procède le plus souvent au moyen d'une circulaire adressée aux chefs de cours, pour instruction en ce qui concerne les procureurs généraux et pour information s'agissant des premiers présidents.

Toutefois la DACG n'a de cesse de varier et de moderniser les outils mis au service de l'action du garde des Sceaux. C'est ainsi que, pour expliquer la politique pénale, elle multiplie les contacts directs avec les magistrats en juridiction, par exemple en participant aux réunions de politique pénale et d'action publique organisées par les procureurs généraux ou en organisant des vidéo-conférences avec ses interlocuteurs.

Le recours à des mémentos pratiques et à des guides méthodologiques – disponibles sur l'Intranet du ministère – permet aussi de mettre à la disposition des praticiens des outils pédagogiques contenant l'ensemble des informations utiles au bon traitement judiciaire d'un contentieux particulier qu'il s'agisse, par exemple, des infractions en matière de racisme, d'antisémitisme et de discrimination, ou des violences conjugales.

L'évaluation de la politique pénale

La culture de l'évaluation des politiques publiques en général et de la politique pénale en particulier est devenue une réalité quotidienne. L'exigence de bonne gouvernance de la chose publique, l'objectif unanimement admis d'une meilleure évaluation de la norme, la révision générale des politiques publiques et les contraintes budgétaires constituent autant d'incitations à développer l'évaluation de l'action des administrations.

Les pouvoirs publics nationaux – exécutif et législatif – ne sont pas les seuls demandeurs de statistiques et autres indicateurs d'activité. Certaines autorités administratives indépendantes, les instances de l'Union européenne, le Conseil de l'Europe, les différentes commissions de l'Organisation des Nations unies mais aussi les médias sont fréquemment demandeurs d'éléments précis sur l'activité de l'institution judiciaire.

À cette fin, la DACG comporte en son sein un pôle d'évaluation des politiques pénales qui est chargé de suivre des indicateurs permettant d'évaluer l'activité des parquets et des parquets généraux et de mesurer l'impact des réformes. Ainsi, des outils structurels tels que l'observatoire des juridictions qui retrace l'activité des parquets, ou l'observatoire de recouvrement des amendes sont complétés par des outils destinés à mesurer la mise en œuvre de nouvelles dispositions comme, par exemple, les peines dites « plancher » ou les pôles de l'instruction. L'évaluation de la mise en œuvre de la politique pénale ne saurait toutefois se cantonner à une approche générale et statistique. Le suivi de l'action publique permet donc à la DACG de s'assurer de la cohérence de l'action des parquets généraux et des parquets à travers le territoire national.

L'action publique

La mise en œuvre de l'action publique, cœur de métier du ministère public, s'exerce dans le cadre d'une chaîne hiérarchique composée du ministre de la Justice, des procureurs généraux et des procureurs de la République.

Placé au sommet de cette structure hiérarchique, le garde des Sceaux est concerné au premier chef par la mise en œuvre de l'action publique. Le suivi que la DACG en assure pour son compte obéit à une finalité déterminée et s'effectue en fonction de critères précis.

Les finalités du rôle de la DACG

L'intervention de la Chancellerie dans la sphère des « affaires individuelles » répond à deux exigences principales :

D'une part, elle permet de s'assurer que les instructions générales de politique pénale sont mises en œuvre. S'il ne saurait être question de remettre en cause le pouvoir d'appréciation des magistrats du ministère public et l'évidente nécessité d'adapter ces instructions, générales et impersonnelles, à des situations particulières et individuelles, il importe tout autant, sous peine de vider les dispositions de l'article 30 précité de toute substance, de veiller à ce que l'action des parquets obéisse à une certaine cohérence et s'inscrive dans un cadre commun, défini au niveau national. Il s'agit là d'une condition de l'égalité des citoyens devant la Loi.

D'autre part, le suivi de certaines affaires individuelles par la DACG est le seul moyen permettant d'assurer une mise en pratique effective des pouvoirs du garde des Sceaux en matière d'instructions individuelles. Dans les faits, ces instructions – moins d'une dizaine par an en moyenne – concernent le plus souvent des décisions relatives à la bonne administration de la justice, qu'il s'agisse de faire requérir un dessaisissement ou un regroupement de procédures. Il peut aussi s'agir d'instructions tendant à l'exercice d'une voie de recours ou aux fins d'enquête, notamment dans le domaine très particulier du droit de la presse.

Au-delà de ces deux objectifs principaux, le suivi de l'action publique par la DACG l'amène à acquérir une expérience et un savoir qui bénéficient à l'ensemble de l'institution judiciaire puisqu'il permet de tirer les enseignements d'une pratique ou d'une expérience locale et de la généraliser, ou encore d'identifier une difficulté juridique et de préparer les innovations normatives destinées à répondre aux attentes des praticiens.

Les critères d'intervention de la DACG

S'il va de soi que la DACG peut être à l'initiative d'une demande de renseignements, il appartient surtout aux procureurs généraux de déterminer les affaires devant être signalées à la Chancellerie. Informés par les parquets des actes de délinquance significatifs commis sur leur ressort, ils doivent en effet identifier les affaires dont il leur paraît justifié, à raison de leur importance, de leur sensibilité ou de leur singularité, qu'elles soient portées à la connaissance de la DACG

Il existe toutefois des critères communément admis qui permettent de guider l'action des procureurs généraux dans ce domaine. Il s'agit notamment de la gravité intrinsèque des faits, de la particulière gravité du trouble causé à l'ordre public par l'infraction, du lieu de l'infraction (par exemple, lorsqu'elle a été commise dans un palais de justice ou dans une école), de la personnalité de l'auteur ou de la victime, du nombre élevé de victimes, du lien existant entre l'infraction et l'actualité ou l'une des priorités de la politique pénale, du caractère inédit de la criminalité constatée ou encore de la complexité d'un problème juridique posé par la procédure.

Le droit de grâce [1]

Si le droit de grâce constitue une prérogative constitutionnelle du président de la République, les dispositions de l'article R.133-1 du Code pénal prévoient que les recours en grâce sont instruits par le ministre de la Justice après, le cas échéant, avis préalable du ou des ministres intéressés. Selon une pratique très ancienne, il est procédé à une élimination préalable des recours en grâce qui ne sont pas de nature à retenir l'attention du Chef de l'État.

Ainsi, le ministre de la Justice, qui décide en dernier lieu de proposer à l'agrément du président de la République, soit une mesure de grâce, soit le rejet de la requête, possède aussi le pouvoir de décider de ne pas faire cette proposition par une décision de rejet sans en référer au chef de l'État. La décision ainsi prise n'est que préalable, en ce qu'elle laisse subsister dans son intégralité le pouvoir de faire grâce qui appartient au seul président de la République.

(1) À l'heure où ces lignes sont rédigées, le débat parlementaire sur la réforme constitutionnelle est toujours en cours, et le devenir du droit de grâce constitutionnellement conféré au président de la République n'est pas encore connu.

Une étude menée en 2007 sur les 7 018 recours en grâce reçus à la DACG démontre que 858 d'entre eux étaient irrecevables, soit environ 12 %. 65 % des demandes adressées concernaient des sanctions pécuniaires, 21,54 % des peines d'emprisonnement et le reste portait sur des peines privatives de droit. Le recours en grâce n'est recevable que s'il vise d'une peine au sens de droit pénal (ce qui exclut, par exemple, les mesures éducatives en faveur des mineurs ou les mesures disciplinaires) et que la condamnation concernée est exécutoire et définitive.

Traditionnellement, la Chancellerie privilégie les procédures de droit commun (aménagements de peine, échelonnement du paiement de l'amende...) qui permettent d'aboutir à une solution satisfaisante, et rendent donc inutile l'intervention d'une mesure de grâce, de manière à ce que celle-ci conserve un caractère exceptionnel et subsidiaire.

Les critères d'octroi de la grâce, qui doivent révéler une situation exceptionnelle, sont de nature variable. Il peut s'agir de motifs humanitaires, de politique pénale gouvernementale (exclusion des délits de circulation routière...), de motifs tenant à l'intérêt de la société (réadaptation sociale, régularisation de la situation, indemnisation de la victime...) ou à la rigueur de la procédure qui peut avoir bloqué la situation (ex. : condamnation prononcée par itératif défaut...).

Conclusion

Loin de tout stéréotype, la direction des Affaires criminelles et des Grâces est donc d'abord et avant tout la direction du droit pénal. Placée sous l'autorité du garde des Sceaux pour la mise en œuvre de la politique pénale du Gouvernement, elle est aussi largement tournée vers les juridictions et plus particulièrement vers les magistrats du ministère public pour les aider et les soutenir dans leur mission d'exercice de l'action publique.

Interlocutrice privilégiée de ces magistrats en général et des procureurs généraux en particulier, au contact direct des partenaires institutionnels de la justice pénale, reconnue pour son expertise sur la scène européenne et internationale, la DACG est au cœur de la justice pénale, au service des justiciables.

VIE DES ORGANISATIONS

À quoi servent les procureurs généraux ?

Jean-Amédée LATHOUD
Procureur général près la cour d'appel de Versailles

À notre époque de communication en temps réel, les interventions au journal télévisé des magistrats ont remplacé, dans l'esprit du public, le cérémonial traditionnel des audiences solennelles en robe rouge, pour faire connaître l'activité de l'institution judiciaire.

Si le rôle et les pouvoirs propres du procureur de la République - assisté de ses substituts - sont relativement bien perçus de l'opinion (direction de l'exercice de la police judiciaire, appréciation de l'opportunité des poursuites, réquisitions devant les juridictions judiciaires du premier degré, participation aux politiques publiques territoriales de prévention...), par contre les attributions du procureur général près la cour d'appel - assisté de ses avocats et substituts généraux -, sa place dans l'organisation judiciaire, sont souvent mal connues de nos concitoyens.

Les Français savent, il est vrai, que les magistrats du parquet général requièrent l'application de la loi devant les magistrats du siège de la cour d'appel près laquelle ils sont nommés (chambre des appels correctionnels, chambre de l'instruction, chambres civiles...), qu'ils soutiennent l'accusation devant la cour d'assises du siège de la cour. Mais ils ne mesurent pas toujours l'étendue des responsabilités des procureurs généraux des trente-trois cours d'appel de notre pays, qui, s'inscrivant dans la structure hiérarchique du ministère public, sont situés entre le ministre de la Justice et les procureurs de la République.

Des attributions significatives en matière de gestion ont été confiées en 2004, conjointement au premier président et au procureur général, ordonnateurs secondaires des dépenses de fonctionnement de leur ressort (cour d'appel, tribunaux de grande instance, conseils de prud'hommes, tribunaux de commerce, etc.). À ce titre, les chefs de cour

mettent en œuvre le budget qui leur est attribué par le ministère de la Justice dans le cadre de la LOLF ; c'est ainsi que la maîtrise des dépenses de frais de justice, en matière de police judiciaire, est une préoccupation permanente des parquets généraux. Conjointement avec le premier président, le procureur général est aussi responsable des marchés publics passés dans son ressort ; il a enfin la co-responsabilité de gestion des ressources humaines, dans le cadre des ETPT [1] qui sont accordés au ressort de la cour (par exemple, à Versailles, 1 160 agents...) ; il évalue les fonctionnaires, il recrute les vacataires, etc.

Mais l'essentiel des responsabilités du procureur général est défini par l'article 35 du Code de procédure pénale : « *Le procureur général veille à l'application de la loi pénale dans toute l'étendue du ressort de la Cour d'Appel et au bon fonctionnement des parquets de son ressort* ». C'est dans le cadre de ses attributions hiérarchiques que le procureur général, magistrat nommé en Conseil des ministres et qui, la plupart du temps, a exercé antérieurement dans sa carrière des responsabilités de procureur de la République, va orienter son action suivant trois axes :

- animation et coordination ;
- surveillance et contrôle ;
- circulation de l'information.

Animation et coordination

Le procureur général « *anime et coordonne l'action des procureurs de la République, en ce qui concerne tant la prévention que la répression des infractions... ainsi que la conduite de l'action publique par les parquets de son ressort* [2] ». C'est ainsi que dans le cadre de relations quotidiennes, écrites ou téléphoniques et de rencontres régulières, les magistrats du parquet général et des parquets se concertent pour harmoniser leurs pratiques, mettre en cohérence les orientations de la politique pénale, dont les grandes lignes sont fixées par le ministère de la Justice. Par exemple, ces derniers mois, dans le ressort de la cour d'appel de Versailles, qui comprend quatre parquets et plus d'une centaine de magistrats du ministère public, des orientations générales ont été définies en matière de violences scolaires, de délinquance des mineurs, en ce qui concerne les relations avec les commissaires aux comptes, responsables de la révélation de faits délictueux, ou encore (en liaison avec l'INHES) d'intelligence économique, ou de lutte contre les violences urbaines.

Ce rôle de coordination des procureurs généraux, d'incitation à promouvoir « les bonnes pratiques », a pour objet de renforcer la cohérence des réponses pénales entre les différents parquets, afin qu'au-delà de l'individualisation des poursuites, les politiques pénales soient « lisibles » de nos interlocuteurs judiciaires, administratifs, des élus locaux, etc. Des orientations écrites sont régulièrement adressées aux parquets pour harmoniser leurs choix d'action publique.

Les relations régulières nouées par les procureurs généraux avec les responsables régionaux des services de l'État et des collectivités territoriales permettent d'éclairer les politiques pénales déclinées localement par les procureurs de la République.

On sait que depuis la loi du 5 mars 2007, ont été créés, dans un nombre limité de tribunaux de grande instance, des pôles de l'instruction, seuls compétents pour connaître des informations pour crimes ou d'affaires justifiant la co-saisine de plusieurs juges d'instruction. Le procureur général doit veiller à la coordination de l'action des procureurs de son ressort qui dirigent une enquête, et qui ensuite pourront saisir le pôle d'une autre juridiction. Veiller à l'harmonisation des critères de saisine des différents services d'enquête (DRPJ, DDSP, gendarmerie...) préconisée par des protocoles interministériels nationaux, puis des protocoles départementaux, est encore une responsabilité de procureur général.

La loi du 9 mars 2004, a institué en France huit juridictions interrégionales spécialisées (JIRS) pour connaître des procédures de délinquance organisée et d'infractions financières de très grande complexité. L'efficacité de ces JIRS dépend de la bonne circulation de l'information, dès le début de l'enquête entre les parquets des diverses juridictions. Le principe de compétence concurrente, entre la juridiction spécialisée et les tribunaux de grande instance de plusieurs cours d'appel, exige de la part des procureurs généraux concernés, une implication personnelle.

Surveillance et contrôle

Les fonctions de surveillance et de contrôle du procureur général s'inscrivent elles aussi dans les missions judiciaires de défense de l'intérêt général, et de garantie des libertés individuelles qui incombent aux magistrats du ministère public. Plusieurs domaines illustrent ces attributions.

....

(1) ETPT : équivalent temps plein salarié.

(2) Art. 35 du Code de procédure pénale.

Le procureur général doit s'assurer du bon fonctionnement des parquets : à ce titre, le dialogue qu'il noue avec les procureurs, les conseils qu'il est amené à prodiguer, les contrôles et les évaluations qu'il effectue sont utiles au bon fonctionnement de la justice. Les justiciables adressent fréquemment au parquet général, une demande de réexamen de certains classements sans suite, décidés par les procureurs de la République. C'est ainsi que le procureur général peut enjoindre aux parquets, par instructions écrites, versées au dossier, de reprendre l'enquête, d'engager des poursuites ou de saisir la juridiction compétente de réquisitions écrites, opportunes pour le bien de la justice.

Cette surveillance et ce contrôle concernent l'exercice de la police judiciaire, puisque l'habilitation et la notation des officiers de police judiciaire représentent une responsabilité importante des chefs de parquets généraux. En matière disciplinaire, le parquet général peut utiliser les pouvoirs de sanction, définis par le Code de procédure pénale. Les réunions de travail que le parquet général tient régulièrement avec, notamment, les responsables régionaux de la police et de la gendarmerie, lui permettent de se tenir informé sur les conditions de travail de ces services, leur politique d'emploi, leur bonne coordination dans l'exercice des missions de police judiciaire.

La surveillance des établissements pénitentiaires est également une responsabilité à laquelle sont attentifs les procureurs généraux, à l'occasion de la visite des lieux d'exécution de peines, du suivi des incidents en détention et des rencontres qu'ils animent semestriellement à la cour pour favoriser le développement des mesures d'aménagement de peine (travail d'intérêt général, chantiers extérieurs, bracelets électroniques, etc.) avec l'ensemble des magistrats du siège et du parquet, les responsables de l'administration pénitentiaire...

Les officiers publics et ministériels font enfin l'objet d'un contrôle attentif, à l'occasion notamment des rapports annuels d'inspection de comptabilité, et d'un dialogue régulier avec les organes disciplinaires de la profession (compagnies régionales des notaires, des huissiers, des avoués...).

Circulation de l'information

Une circulation de l'information prompte et de qualité est également nécessaire à la bonne coordination des politiques d'action publique. Elle conditionne également la pertinence des décisions prises par les parquets. Le procureur général doit veiller à la qualité, à l'exactitude et à la rapidité des échanges. Une information mutuelle entre les différents parquets du ressort est indispensable pour permettre de mettre en œuvre des politiques de saisine claires des services de police, pour favoriser des regroupements éventuels de procédure (par exemple agressions en série, délits commis par des malfaiteurs itinérants, ou en bande organisée...)

Un certain nombre de procédures pénales, civiles ou commerciales sont « signalées » par les parquets aux parquets généraux, en raison de leur gravité pour l'ordre public, de leurs difficultés juridiques ou de leur raisonnance médiatique. Par exemple, les conditions d'application concrètes de nouvelles dispositions législatives concernant le droit ou la procédure pénale, les phénomènes criminels émergents (vols de métaux non ferreux, violences entre bandes, blanchiment, cybercriminalité...) justifient des comptes rendus. En retour, les conseils du parquet général, au regard de sa connaissance de la jurisprudence de la cour ou de l'expérience acquise peuvent être utiles aux procureurs de la République.

À son tour, dans le cadre d'un dialogue permanent avec le ministère de la Justice, le procureur général rend compte des affaires qui lui paraissent importantes pour l'ordre public ou le renseigne sur la teneur exacte des procédures largement médiatisées. Cette information de la Chancellerie porte non seulement sur ces affaires individuelles, mais aussi sur la mise en œuvre des politiques pénales (un rapport annuel d'activité est établi). Des statistiques de résultats (Objectifs, performances...) sont transmises régulièrement.

L'attention enfin que les parquets généraux portent aux associations d'aide aux victimes, en liaison avec les magistrats du siège (élaboration de contrats d'objectifs ; attribution de subventions, ainsi, pour la cour d'appel de Versailles, 284 000 € en 2008) reflète l'importance attachée à l'information des justiciables, essentielle pour que nos concitoyens aient la conviction que l'autorité judiciaire est aussi un service public. Les parquets généraux sont aujourd'hui, eux aussi, impliqués dans les efforts définis par la révision générale des politiques publiques (RGPP) (dématérialisation des procédures, visio-conférence, etc.) mis en œuvre par la Chancellerie et les parquets.

On a pu dire que les procureurs généraux au XIX^{e} siècle étaient de « redoutables sentinelles de l'ordre ». Aujourd'hui, dans le cadre institutionnel qui est le nôtre, ils sont devenus, avec leurs équipes, de véritables acteurs du changement, au service d'une Justice qui modernise ses méthodes, pour être plus efficace et plus humaine.

Les missions du procureur de la République

François MOLINS
Procureur de la République près le tribunal de grande instance de BOBIGNY

Le ministère public est un corps de magistrats établi près les juridictions de l'ordre judiciaire, dont le rôle est de veiller, au nom de la société et dans l'intérêt général, à l'application de la loi lorsqu'elle est pénalement sanctionnée, en tenant compte, d'une part, des droits des individus et, d'autre part, de la nécessaire efficacité du système de justice pénale. Ces deux impératifs constituent le fondement de toute société démocratique et ont été repris dans la recommandation n°2000-2019 sur le rôle du ministère public dans les systèmes de justice pénale, adoptée par le Conseil de l'Europe le 6 octobre 2000.

L'organisation du ministère public obéit au principe de la subordination hiérarchique : « *les magistrats du parquet sont placés sous la direction et le contrôle de leurs chefs hiérarchiques et sous l'autorité du garde des Sceaux, ministre de la justice* [1] ». Tous les magistrats du ministère public sont donc unis par un lien hiérarchique dont la plus haute autorité est le garde des Sceaux, ministre de la Justice qui, en cette qualité, a autorité sur le procureur général qui a des pouvoirs identiques sur les procureurs de la République de sa cour d'appel, dont il a mission d'animer et de coordonner l'action, tant en ce qui concerne la prévention que la répression des infractions à la loi pénale. Cette subordination hiérarchique constitue la garantie de la cohérence de la politique pénale conduite au sein d'un même parquet.

L'exercice de l'action publique est l'attribution essentielle du ministère public. Chargé de la poursuite des infractions, il lui appartient de mettre en mouvement l'action publique en saisissant la juridiction d'instruction ou de jugement et de l'exercer, c'est-à-dire de la poursuivre à l'audience jusqu'à la décision définitive et de la faire exécuter. Le rôle et le métier du parquet ont connu, au cours de ces dernières années, des évolutions très importantes sur deux plans.

Le rôle du procureur de la République avant le déclenchement des poursuites

Si les fonctions du procureur de la République sont extrêmement variées et ses attributions multiples en matière pénale, civile, commerciale, voire administrative, sa fonction essentielle est de mettre en mouvement et d'exercer l'action publique. Ses fonctions s'appliquent donc depuis la recherche de l'infraction jusqu'à l'exécution de la sanction pénale.

Les missions et compétences du procureur de la République s'inscrivent dans une démarche dynamique. En indiquant dans l'article 40 du Code de procédure pénale que « *le procureur de la République reçoit les plaintes et les dénonciations et apprécie les suites à leur donner* », le législateur en a fait la plaque tournante de la justice pénale. En effet, le procureur de la République a le pouvoir d'apprécier l'opportunité des poursuites, mais aussi celui de diriger les enquêtes, de décider du principe et des modalités des poursuites. Il a donc la possibilité de donner aux services de police et de gendarmerie des directives générales pour rechercher et constater les infractions. Le procureur de la République est juge de l'enquête mais il est avant tout un acteur de la politique pénale.

La règle de l'opportunité des poursuites suppose en effet que soit respecté un principe essentiel : celui de l'égalité entre les citoyens, ce qui implique l'existence d'une politique de l'action publique. La politique d'action publique consiste, face à la délinquance existante, à orienter les moyens disponibles vers les infractions les plus nuisibles à l'ordre social. Ainsi définie par le gouvernement et conduite par le ministre de la Justice, la politique pénale est mise en œuvre sur l'ensemble du territoire par les procureurs généraux et par les procureurs de la République. Il appartient à ceux-ci de définir, au plan local, une politique d'ensemble fixant clairement aux services enquêteurs les priorités, et précisant les modes de traitement judiciaire des infractions sur la recherche et la poursuite desquelles l'accent aura été mis. Cette politique pénale doit être la déclinaison au plan local de celle fixée par le garde des Sceaux et ce, en fonction des moyens disponibles et de la nécessaire adaptation de ces choix à la réalité du ressort territorial et à ses problèmes spécifiques. Ainsi, les problématiques des violences urbaines ou de l'habitat indigne ne présentent pas les mêmes caractéristiques ni la même importance dans un département très urbain et dans une zone rurale et n'appellent donc pas les mêmes protocoles de travail.

(1) Ord. du 22 décembre 1958 portant loi organique relative au statut de la magistrature.

C'est dans ce domaine de la politique pénale que la fonction de procureur de la République a connu ses évolutions les plus importantes. Il y a trente ans, le procureur de la République intervenait essentiellement dans la gestion des affaires individuelles, et peu sur le terrain de la politique pénale. Les années 1980 ont vu un élargissement notable du champ de ses missions : traitement de la prévention de la délinquance, protection des victimes, développement de la troisième voie constituée par les réponses alternatives aux poursuites, participation à la politique de la ville et à de nombreuses politiques publiques (toxicomanie, lutte contre l'insécurité routière, habitat indigne...). Dans le cadre de ces nouvelles missions, les parquetiers sont sortis des palais de justice pour aller à la rencontre des autres acteurs.

Les lois de 2001, 2003, 2004 et 2007 ont encore accentué ces évolutions. Dès le début des années 2000, est apparue la notion de « co-production de sécurité » émanant à la fois du préfet et du procureur de la République, ainsi que de l'ensemble des administrations concernées. Le préfet est effectivement chargé d'animer et de coordonner la prévention de la délinquance et l'ensemble du dispositif de sécurité intérieure. Il fixe, à cet effet, les missions autres que celle relatives à l'exercice de la police judiciaire [2]. Peu à peu, de la notion de co-production de sécurité, a émergé l'idée d'une politique dont une partie du contenu peut être concertée avec d'autres autorités et partenaires, et notamment le préfet, dans le cadre des conférences départementales de sécurité ou autres structures de prévention. Si bien que la justice pénale est de plus en plus perçue comme l'instrument privilégié du droit à la sécurité.

Cette participation aux politiques publiques et aux différentes structures de prévention de la délinquance (contrats locaux de sécurité et de prévention de la délinquance, conseil départemental de prévention de la délinquance), mais aussi les responsabilités nouvelles d'animation et de coordination de la politique de prévention de la délinquance dans sa composante judiciaire que lui a donnée le législateur [3] ont encore accentué ce phénomène en développant considérablement les relations entre les maires et le parquet : désormais, en effet, le maire peut être informé par le procureur de la République des suites apportées aux infractions commises dans sa commune et connaître toute décision dont la communication paraît nécessaire à la mise en œuvre d'actions de prévention, de suivi ou de soutien.

Le procureur de la République, juge de l'enquête

C'est pour permettre de mener à bien une politique d'action publique déterminée et parce qu'il est constitutionnellement, en sa qualité de magistrat, gardien des libertés individuelles, que le législateur a confié au procureur de la République la direction de l'exercice de la police judiciaire et le libre choix du service de police ou de gendarmerie auquel il entend confier l'enquête qui sera menée sous sa direction. Ainsi, le procureur de la République coordonne et dirige l'action des officiers de police judiciaire chargés de rechercher les auteurs des infractions, et ce pouvoir peut se manifester par des instructions en vue de procéder à des investigations dans le cadre de la direction de l'enquête.

Mais surtout, les parquets ont fait leur révolution, celle du temps : afin de supprimer tout temps mort dans la gestion des procédures, ils ont adopté et organisé le système dit du « traitement en temps réel » qui repose sur deux principes :

- toute infraction pénale, qu'elle soit élucidée ou non, doit faire l'objet d'un compte rendu téléphonique immédiat au parquet par le service enquêteur ;

- toute affaire dont il est ainsi rendu compte doit faire l'objet d'un traitement immédiat par le parquet.

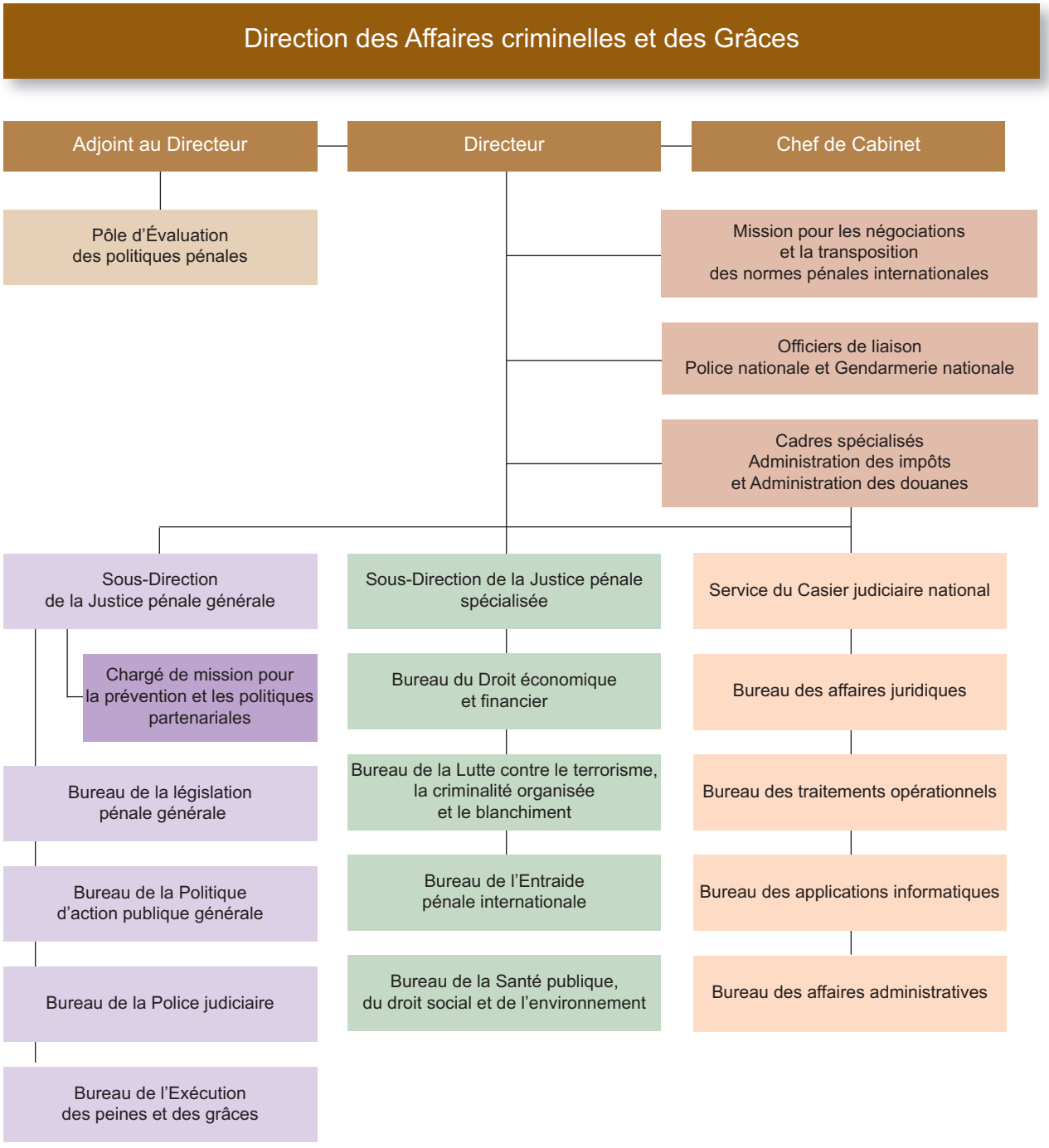
Le traitement en temps réel qui repose sur une conception globale de l'action publique, intégrant l'immédiateté de la réponse judiciaire, a permis une amélioration considérable de la qualité et des délais des réponses pénales, diversifiées et mieux adaptées dans le cadre d'une politique globale d'action publique, au prix d'une totale réorganisation des parquets qui est aujourd'hui surtout construite autour de la notion de l'urgence. Le magistrat du parquet est ainsi devenu le premier juge, celui de l'enquête.

Enfin, la fonction du parquet elle-même a évolué dans le champ du procès pénal avec l'instauration de la procédure de comparution sur reconnaissance préalable de culpabilité qui, même si le pouvoir de juger reste au juge du siège chargé d'homologuer ou de refuser d'homologuer l'accord passé entre le parquet et la personne poursuivie, lui reconnaît un pouvoir accru dans la proposition de la

....

(2) Loi n°2003-239 du 18 mars 2003 pour la sécurité intérieure.
(3) Code de procédure pénale, art 39-1 résultant de la loi du 5 mars 2007 relative à la prévention de la délinquance.

sanction et reconnaît encore davantage le procureur de la République comme une autorité judiciaire. Cette nouvelle procédure, ajoutée à celle de la composition pénale, doit favoriser de nouvelles relations entre le siège et le parquet pour parvenir à l'émergence d'une véritable « politique de juridiction » dans laquelle, dans des conditions compatibles avec les moyens humains et matériels dont ils disposent, sont déclinées, tout en assurant la nécessaire indépendance des magistrats du siège et leur liberté absolue de décision dans les affaires qui leur sont soumises, les grandes orientations de la juridiction.



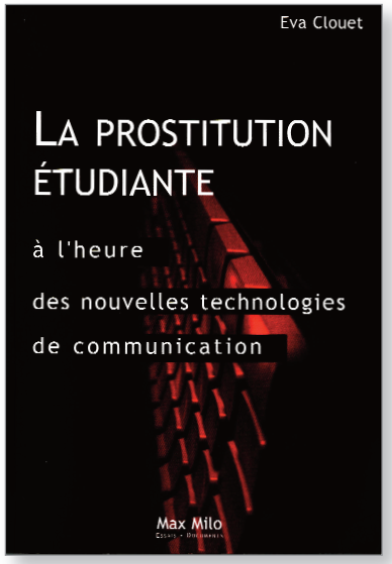
La prostitution étudiante à l'heure des nouvelles technologies de communication

Eva CLOUET

Un nouveau phénomène de société, la prostitution étudiante, a défrayé l'actualité, notamment lors de la campagne à la présidentielle de 2007. Les politiques comme les médias se sont emparés de la question. Le Figaro titrait ainsi le 30 octobre 2006 : « *La prostitution gagne les bancs de la Fac* ». Ils seraient environ 40 000, selon les statistiques des syndicats étudiants, ces jeunes des universités se livrant à la prostitution.

Cet essai sociologique est le produit d'un rapport de stage réalisé par une étudiante de Master 2 de l'université Toulouse II, Eva Clouet, durant l'année 2005-2006. L'auteur souligne que sa recherche s'oriente alors vers la connaissance de « la *prostitution des femmes immigrées en occident* ». Elle décide alors d'effectuer son stage à la délégation de Nantes du Mouvement du Nid. Son ouvrage se découpe en trois parties identiques, traitant successivement : le cadre de l'enquête, les étudiants se prostituant grâce au net : un milieu à part ?, les motifs et les motivations de cette prostitution étudiante.

« *La prostitution est avant tout un fait individuel avant d'être un phénomène social* ». Deux éléments évidents et cumulatifs suggèrent le fait prostitutionnel : « *le rapport sexuel et le rapport marchand* ». Les deux rapports font l'objet d'un processus de domination, tant masculine que socio-économique.



2007, Éditions Max Milo, 192 p., 16,00 €

Le concept de prostitution est analysé globalement, jusqu'à évoquer les régimes qui lui sont attachés : le régime réglementariste (servant à encadrer la dite activité), le régime abolitionniste (qui favorise les liens mafieux, la clandestinité, et contourne l'idée d'étiquetage administratif), enfin, le régime prohibitionniste.

La prostitution a plusieurs visages. L'image de cette activité, et des personnes qui s'y livrent, change avec les mœurs d'une société en constante évolution (libertinage, sida, réseaux internationaux de prostitution). On préfère plutôt parler des « prostitutions ». L'*escorting* est une des conséquences du développement des nouvelles technologies, notamment Internet (rapide, facile, discret, anonyme, sécurisant). Cette prostitution se veut indépendante et individuelle.

L'auteur va tenter de tisser des relations avec ses personnes qui se prostituent, en s'inscrivant sur un forum de discussion, puisque l'internet est « *la vitrine de l'escorte* » (certaines escortes ont parfois leur propre site ou blog).

Cette activité d'escorte se caractérise, en général, par une pratique non professionnelle et occasionnelle, l'enjeu étant « *d'arrondir les fins de mois* ». La difficulté réside dans le fait que ce type de prostitution est difficilement perceptible, cette catégorie n'étant pas connue des services sociaux. Souvent, ces personnes ont une double activité professionnelle. Compte tenu de cette vulnérabilité économique qui touche les étudiants, on comprend qu'une telle activité soit attractive du fait des sommes envisagées (selon l'Observatoire de la vie étudiante, un étudiant sur deux travaille, 45 000 se trouvent dans un état de pauvreté grave ou durable et 225 000 peinent à subventionner leurs études).

Cette découverte va amener l'universitaire à traduire une préoccupation générale en un thème plus limité : « *La prostitution étudiante à l'heure des*

nouvelles technologies de l'information ». L'étude se complique d'autant que cette catégorie de prostitution (les escortes étudiantes) s'appréhende plus difficilement : non perçue par le service universitaire de médecine préventive et de promotion de la santé, difficilement décelable dans les « *bars à bouchon* » ou bars à hôtesses. Le Forum devient le seul terrain de recherche abordable.

Ces étudiants qui se prostituent, via Internet, peuvent-ils être considérés comme des « *prostitués à part* » ? Leurs niveaux scolaires et leurs origines sociales sont très hétérogènes. Cette dérive s'explique par une volonté très forte de se valoriser socialement, et rompre avec la tradition familiale (parents sans diplôme, situations précaires). Julien, Ambre, Claire veulent tous faire des études poussées, avec pour objectif de devenir quelqu'un.

En quête de reconnaissance, et de légitimité dans notre société, ce devenir professionnel est une priorité (approcher, voire intégrer la classe dirigeante). Parfois, cette prostitution masque un manque, une carence, un abandon (perte d'un parent par décès, par rupture des liens familiaux). Julien a ainsi trouvé un refuge dans la prostitution de rue, mais son image s'est fortement dégradée.

Généralement, les étudiants se prostituent comme escortes. Cela n'a qu'un caractère provisoire et permet de préserver son temps pour les études. L'Internet est un moyen d'organiser, depuis son domicile, des rencontres avec des clients soigneusement sélectionnés, et de pouvoir fixer ses conditions et attentes. La sélection du client est une étape cruciale : connaître la personnalité du client, se familiariser avec la personne, éviter les mauvaises rencontres, etc. L'escorte privilégie les rencontres longues, ce qui reste plus naturel. L'homme, qui s'offre les services de l'escorte, entre dans la catégorie des 40-55 ans, souvent marié, ayant une bonne situation professionnelle. L'auteur observe qu'outre « *gagner de l'argent pour poursuivre leurs études* », l'escorte féminine prend « *une revanche sur les hommes avec qui elle aurait entretenu des relations gratuites* ».

Mais c'est surtout le phénomène de paupérisation des étudiants qui est dénoncé, avec le rapport Dauriac de 2000 fixant la mise en place d'un « *plan social étudiant* » [1].

Les parents peinent à les aider financièrement. Afin de concilier études et travail rémunéré, ces étudiants choisissent la voie de la prostitution pour palier les manques sociaux et financiers. Ce choix d'existence offre des aspects séduisants pour l'étudiant : des rencontres informelles avec des clients sympathiques, des personnes établies, cultivées qui influent et parfois aident à la carrière de l'escorte. C'est aussi la possibilité pour ces étudiants prostitués de s'offrir leur indépendance et de fuir les contraintes familiales ou des parents trop conservateurs.

Forme d'« *évasion* », où l'on brave l'interdit, où l'on préserve son image en dissimulant son autre vie.

Il ressort de cette étude qu'il n'existe pas une prostitution type, mais plusieurs formes de prostitution. L'escorte étudiante est une catégorie à part entière, avec pour toile de fond, l'Internet. Les causes génératrices sont très diverses, mais cela traduit manifestement un véritable « *malaise de société* ».

La prostitution est un sujet qui dérange, d'autant qu'il s'agit de traiter d'un thème resté longtemps tabou, la prostitution étudiante. Cette analyse, bien documentée, aborde ce sujet si délicat avec franchise et une prétendue désinvolture pour masquer la complexité des relations humaines et l'existence d'un mal être étudiant. On ne peut rester insensible à cet ouvrage, qui est, du reste, aéré et structuré. On apprécie de même l'excellente bibliographie et l'accès aux jargons des forums de discussion internet et de la prostitution, donnés en annexe. C'est un ouvrage qui mérite qu'on s'y attarde.

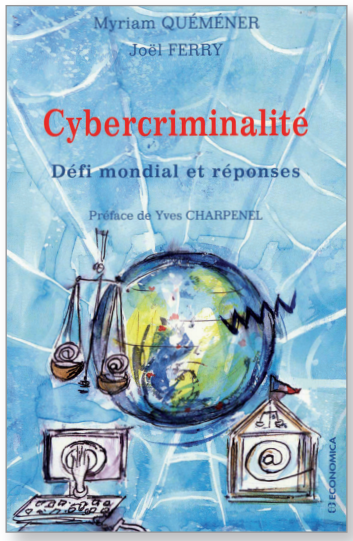
Caroline BOUILLART

(1) Ce plan, rendu public le 14 février 2000, avait été demandé par le ministre chargé de l'Enseignement supérieur, Claude Allègre à Jean-François Dauriac, directeur du Crous de Créteil.

Cybercriminalité

Défi mondial et réponses

Myriam QUÉMÉNER et Joël FERRY



2007, Economica, 281 p., 19 €

La montée en puissance de la dynamique internet à l'échelle planétaire et la diversité des pratiques des acteurs ne sont pas sans conséquence sur le développement d'une cybercriminalité transfrontière en constante évolution. En effet, le fonctionnement intrinsèque du réseau pose des problèmes majeurs de sécurité, et n'est pas sans créer de nouvelles déviances. Face à ces nouvelles réalités virtuelles, Myriam Quéméner, Substitut général au service criminel de la cour d'appel de Versailles, et Joël Ferry, colonel de gendarmerie, commandant la Section de recherches de Versailles, se proposent de dresser un constat pour le moins fidèle de cet environnement si particulier de la cybercriminalité, en insistant tant sur la connaissance du phénomène que sur sa représentation protéiforme. Cette étude s'affine et s'achève sur une troisième partie dédiée aux moyens de lutte.

L'attrait des réseaux de communication séduit toujours davantage, avec un recensement de 1,1 milliard d'internautes à travers la planète. Dans le rapport annuel de la Commission européenne de 2006 sur l'économie numérique, les auteurs notent que « *les technologies de l'information et de la communication (TIC) drainent la moitié de la croissance des 27 États membres de l'Union européenne* ». Cette technologie internet offre accès à de nouveaux services : le WAP (lecture de contenus en ligne sur mobile), l'IPTV (télévision sur mobile). Cet intérêt général marqué pour le numérique a suscité l'attention des États qui instaurent leur propre contrôle sur cette ressource. D'autant qu' « *Internet véhicule un certain nombre de contenus potentiellement préjudiciables et illégaux et peut se prêter à la diffusion d'activités délictueuses* » [1]. Internet est devenu un réel vecteur de risques et d'agissements illicites (piratages, terrorisme, fraudes...), qui dépasse largement la compétence et le cadre d'action de l'État par ses enjeux transfrontaliers. L'absence d'harmonisation des législations pénales et le caractère international de l'utilisation du réseau constituent autant d'entraves juridiques et techniques au sein des territoires nationaux.

Le président de la République française a placé cette cybercriminalité au cœur des préoccupations nationales. Pour comprendre ce phénomène, l'ouvrage nous livre une définition du cybercrime donnée par l'Organisation des Nations unies, précisant qu'il s'agit de « *tout comportement illégal faisant intervenir des opérations électroniques qui visent la sécurité des systèmes informatiques et des données qu'ils traitent* ». Une inquiétude demeure quant à l'augmentation du nombre d'accès (développement du haut débit, et accessibilité des ménages).

Une première partie est consacrée à la connaissance d'un espace ouvert à la cybercriminalité. On y découvre les prémices d'Internet ou l'émergence des réseaux numériques, les offres de services et leurs dangers, enfin, les différents intervenants. Internet est né d'un concept militaire américain développé dans les années 1960, avec la création du réseau ARPANET qui favorisait la communication militaire. Son succès est devenu planétaire ; il est devenu aisé pour tout particulier d'accéder à Internet, par les technologies XDSL (Internet haut débit). Il est permis d'échanger et de mettre en

....

(1) Catinat (M.), 2000, « La politique européenne de promotion d'Internet et quelques considérations pour la France », *Revue du Marché commun et de l'Union européenne*, n° 435, p.87, février.

relation les ordinateurs distants, grâce au protocole TCP/IP. Les services Internet sont extrêmement variés : web, courrier électronique, forum de discussion, blog... La contrepartie est pourtant moins séduisante pour l'utilisateur victime d'attaques informatiques (vers, cheval de Troie, bombe logique...). Outre les internautes citoyens cités par les auteurs, la toile se livre à divers intervenants :

- les prestataires des réseaux numériques (fournisseurs d'accès à Internet, hébergeurs...), qui ne peuvent être tenus responsables des contenus hébergés, transportés ou stockés, n'étant pas producteurs et, à défaut, d'avoir connaissance de contenus illicites ;

- les autorités indépendantes, telles la CNIL, l'ACERP, la mission pour l'économie numérique, la délégation aux usagers de l'Internet... ;

- enfin, les internautes délinquants.

Dès 1988, la France se pourvoit d'une législation destinée à lutter contre le crime informatique. En ce sens, la loi Informatique et Libertés a fait l'objet d'un toilettage par l'entrée en vigueur de la loi du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, et dans un souci de nécessaire conciliation entre l'impératif de sécurité et la préservation des libertés individuelles. La CNIL voit son pouvoir d'intervention renforcé. Concernant les atteintes aux systèmes automatisés de données, la loi pour la confiance dans l'économie numérique du 21 juin 2004 a permis de durcir l'action pénale, dans le cadre de fraude informatique. Face aux risques encourus, la cryptologie se développe pour assurer la confidentialité des informations.

Néanmoins, la menace informatique est plus diffuse. Cette technologie porteuse de déséquilibre engendre de graves dérives à géométrie variable. Les systèmes d'information sont utilisés à des fins criminelles. Une loi du 23 janvier 2006 relative à la lutte contre le terrorisme, et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, tient compte de cette réalité numérique, et notamment, en faisant peser sur toute personne susceptible de proposer à titre commercial une connexion internet à sa clientèle les mêmes obligations que celles envisagées pour les opérateurs de communications électroniques. Les États sont donc très perméables à ce type d'intrusions. Un exemple éloquent mérite d'être souligné, celui de l'Estonie, pionnière de l'Internet, qui a souffert de son ouverture sur réseau, du fait de nombreuses attaques de sites étatiques.

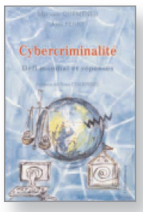
Sont recensés et répertoriés des actes malveillants ayant trait aux droits des personnes (usurpation d'identité, vol de données...), aux personnes (proxénétisme, esclavage sexuel...), aux droits de propriété intellectuelle (contrefaçon, téléchargements illicites...), et toutes les atteintes aux biens (jeux, loteries, fraude à la carte bancaire...). En avril 2006, un étudiant ayant filmé et diffusé via Internet l'agression de l'un de ses professeurs se voyait condamner à une peine ferme d'emprisonnement et au paiement d'une amende. La loi du 5 mars 2007 relative à la prévention de la délinquance est venue, par la suite, réprimer les actes d'enregistrement et de diffusion d'images d'agressions. L'activité normative de l'État se greffe sur l'actualité et évolue au gré des circonstances. Pour parfaire cette étude, les auteurs discernent et recensent comme autres formes de cybercriminalité, servant de « *support* » à cette dernière : la pédopornographie, le racisme, la xénophobie, les infractions de presse...

Enfin, cette lutte contre la cybercriminalité ne saurait être efficace sans recours à des structures, des services spécialisés, tant nationaux qu'internationaux, en charge de garantir l'action d'État. La charpente institutionnelle se dévoile sous deux angles complémentaires : dispositif national et coopération internationale, actions policières et judiciaires. Puis, sont déclinés les outils procéduraux et les instruments juridiques internationaux propres à la résolution de cette criminalité si particulière.

Considérant l'aspect institutionnel, les organes de coopération policière internationale ont été « *regroupés* » au sein d'une section centrale de coopération opérationnelle de police. Il s'agit d'Interpol, d'Europol et du système d'information Schengen. L'analyse de l'action policière se recentre sur le noyau national, notamment par le concours des services traditionnels, Police nationale, Gendarmerie nationale, Douane... Quant au cadre judiciaire, il se définit par l'exercice d'une entraide transfrontalière (Eurojust, Réseau judiciaire européen, OLAF [2]...).

S'agissant de l'adaptation des outils procéduraux, on s'attarde sur l'inviolabilité des frontières et le problème d'incompétence territoriale, avant d'envisager l'autre barrière, celle de la constitution de la preuve. La dématérialisation des éléments de preuve nécessite un renforcement du régime de droit commun pour les infractions commises sur Internet. Ainsi, en plus de la preuve par tous moyens, s'ajoute un nouvel outil : l'obligation de conservation des données (comme prévu par la loi pour la confiance en l'économie numérique précitée). Les

(2) L'Office européen de lutte anti-fraude.



récentes lois sur la sécurité ont influé sur l'activité policière, en adaptant les compétences des services aux difficultés engendrées par l'ère numérique.

La dernière interrogation porte sur l'évolution des instruments juridiques internationaux. La cybercriminalité ne dépend pas d'un périmètre national cloisonné, mais s'identifie telle une menace qui irradie par-delà des frontières. La lutte contre ce fléau doit s'organiser entre les États, par des actions ciblées de l'Union européenne, des Nations unies, de l'Organisation de coopération et de développement économiques (OCDE), du G8, voire même du Conseil de l'Europe qui a adopté à Budapest, le 23 novembre 2001, une convention sur la cybercriminalité. Malgré la densité des informations fournies, les auteurs se livrent à un dernier exercice, en évoquant quelques exemples de législations issues du droit comparé.

En conclusion, les auteurs rappellent l'importance d'un réel engagement de l'État, et l'avantage de promouvoir un partenariat public-privé en matière de lutte contre la cybercriminalité. L'État doit relever le défi d'asseoir les nouvelles perspectives d'une société bercée dans le numérique, tout en offrant un cadre protégé et rassurant d'utilisation des moyens de communication.

« *Tel Janus, Internet est à la fois l'accès à la connaissance et à la pornographie, l'excellence et la boue* » [3]. Les réseaux numériques sont un atout fabuleux d'échanges de tout ordre, qu'il est nécessaire de préserver et de promouvoir. Comme le souligne Pierre Lévy : « *Qu'il faille inventer les cartes et les instruments de navigation pour ce nouvel océan, voilà ce dont chacun peut convenir. Mais il n'est pas nécessaire de figer, de structurer* a priori, *de bétonner un paysage par nature fluide et varié : une excessive volonté de maîtrise ne conduirait, comme souvent, qu'à l'aveuglement et à la destruction. Les tentatives de fermeture deviennent pratiquement impossibles ou trop évidemment abusives* » [4].

En tout état de cause, cet ouvrage présente un intérêt certain, où l'on s'approprie un domaine jusque-là mal maîtrisé ou incompris. Avec ténacité et rigueur, les auteurs s'évertuent à dresser un constat de situation et réalisent la difficile conciliation entre le technique et le juridique. Cet ouvrage présente l'avantage d'être exhaustif sur les moyens et les modes opératoires déployés dans la lutte contre la cybercriminalité.

Caroline BOUILLART

NOTES DE LECTURE

....

(3) « La France, la corégulation et Internet », *Le Figaro*, 26 août 2003.
(4) Lévy (P.), 1997, *Cyberculture*, Paris, Odile Jacob.

La Société de défiance

Comment le modèle social français s'autodétruit

Yann ALGAN et Pierre CAHUC

Sous le titre *La société de défiance*, c'est un petit livre dont l'importance est inversement proportionnelle à son volume que publie le Centre pour la recherche économique et ses applications, sous les signatures de Yann Algan et Pierre Cahuc [1]. Bien que les informations qu'il apporte aient été rassemblées dans une perspective d'analyse socio-économique, elles sont lourdes de signification dans divers domaines, notamment en ce qui concerne les problèmes abordés dans cette revue.

2007, Editions Rue d'ULM, 65 p., 5,00 €

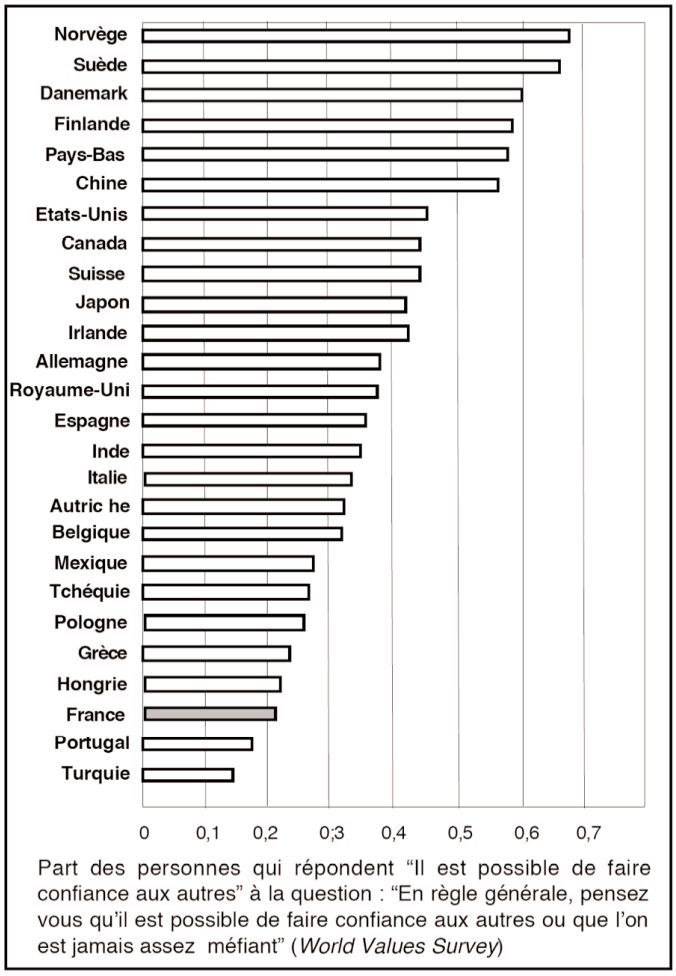
Cet ouvrage confronte les résultats d'études d'opinion menées dans des termes semblables dans la plupart des pays développés. Celles-ci révèlent que l'opinion française se caractérise par un taux record de défiance à l'égard des institutions publiques qui encadrent la vie sociale. À l'égard du parlement, des syndicats ou de la justice, les attitudes critiques sont en France nettement supérieures à ce qu'elles sont dans d'autres pays. Presque un quart des Français déclare ainsi « *n'avoir absolument pas confiance* » dans le parlement et, dans l'expression de cette méfiance, la France arrive en 4e position sur les 24 pays étudiés. La proportion est analogue et le classement identique concernant l'attitude à l'égard des syndicats. De même, 54 % des Français déclarent n'avoir « *aucune* » ou « *peu* » confiance dans le système judiciaire, contre seulement 22 % des Danois, et ils ne sont dépassés en la matière que par la Belgique et la Turquie.

Déjà inquiétante à l'égard des institutions, cette défiance concerne aussi, plus largement, l'ensemble de la vie sociale et s'étend aux personnes, puisque 52 % des Français estiment que, dans la société, « on ne peut parvenir au sommet sans être corrompu », contre 10 % seulement d'opinions semblables en Norvège ou 20 % au Canada ou aux États-Unis. Plus grave encore, à la question « *En règle générale, pensez-vous qu'il est possible de faire confiance aux autres, ou que l'on n'est jamais assez méfiant* », seuls 21 % des Français déclarent faire confiance aux autres, ce taux de confiance réduit les situant au 24e rang sur les 26 pays de l'Organisation de coopération et de développement économiques (OCDE).

C'est là qu'apparaît une conclusion importante pour la perspective abordée ici : « *les informations disponibles indiquent que les Français se défient plus les uns des autres parce qu'ils respectent moins les règles de vie en société que les habitants des autres pays riches* ».

Les données sur ce point, du propre aveu des Français, sont éloquentes. À des questions concernant le jugement à porter sur le fait « *d'acheter un bien dont on sait qu'il a été volé* » ou « *d'accepter un pot-de-vin dans l'exercice de ses fonctions* », la condamnation de ce type de comportement classe la France au dernier et à l'avant dernier rang des 22 pays concernés. De même, il n'y a que 38 % des Français à considérer qu'il n'est « *jamais justifié* » de réclamer indûment des aides publiques, alors que ce chiffre est de 89 % au Danemark ou 59 % en Allemagne. À cet incivisme déclaré correspond un incivisme constaté. Ainsi une expérimentation, consistant à « égarer » un portefeuille, avec l'équivalent de 50 dollars en monnaie locale et

(1) Paris, Editions Rue d'Ulm – Presses de l'École normale supérieure.



Part des personnes qui répondent "Il est possible de faire confiance aux autres" à la question : "En règle générale, pensez vous qu'il est possible de faire confiance aux autres ou que l'on est jamais assez méfiant" (*World Values Survey*)

l'adresse du supposé propriétaire, montre qu'il y a 100 % de restitution dans les pays nordiques pour un résultat de 61 % en France, ce qui la situe au 11e rang sur les 15 pays testés, la lanterne rouge appartenant ici à l'Italie. Une étude de corrélation montre que, dans l'ensemble des pays, il y a un lien très étroit entre cet incivisme et le niveau exprimé de défiance à l'égard des autres, l'incivisme étant d'autant plus grand que la confiance dans les autres est faible.

On l'a dit, cette étude est faite dans des perspectives socio-économiques. Elle s'interroge sur les causes de cette situation, dont elle fait remonter l'origine à la Seconde Guerre mondiale, cette exception française semblant beaucoup moins sensible auparavant. En se référant à un certain nombre d'indicateurs, l'étude tend à établir un lien entre les phénomènes évoqués précédemment et le degré d'étatisme et de corporatisme des sociétés étudiées. Le premier facteur est celui de l'intervention de l'État dans la vie sociale et économique, mais ce n'est pas le plus important, car on retrouve, par exemple, un interventionnisme équivalent dans les pays scandinaves. Selon cette analyse, c'est le mode d'intervention « corporatiste » de l'État qui est le plus décisif et le plus caractéristique de la situation française. Au lieu de procéder à une distribution universaliste des ressources publiques, indépendamment des corps, des statuts et des positions sociales, la redistribution corporatiste – un euphémisme, sans doute, pour ne pas dire clientéliste - « *consiste généralement à accorder des avantages particuliers à certains groupes, souvent au détriment du dialogue social, du respect des règles de la concurrence et de la transparence des mécanismes de solidarité* » [2].

Par là, on retrouve le déficit de confiance évoqué précédemment et le mécanisme qui, selon cette analyse, en induit le développement. « *Dans la logique corporatiste, chaque profession défend ses intérêts dans un système dont la complexité rend très difficile la connaissance précise des acquis des autres. Ce phénomène favorise le développement d'une suspicion mutuelle, car la transparence des droits et des devoirs est essentielle à la consolidation de la confiance et du civisme* ». Par là, aussi, s'enclenche, par exemple dans la vie économique, un processus de méfiance à l'égard du marché et des relations contractuelles et, corrélativement, de recours à l'État : « *Les habitants d'un pays étant d'autant plus enclins à faire contrôler les marchés qu'ils suspectent leurs concitoyens de ne pas respecter spontanément les règles morales dans les échanges* ».

En renvoyant pour ses aspects économiques au livre lui-même, on retiendra surtout ici les conséquences plus générales de ces observations pour l'ensemble des relations sociales, dans la mesure où celles-ci permettent de rendre compte et d'éclairer un certain nombre de phénomènes relatifs à la façon dont s'organise la régulation sociale ou le contrôle social dans la société contemporaine. On voit bien comment cette étude met en évidence l'érosion des mécanismes d'auto-contrôle et d'autodiscipline, que traduisent les manifestations d'incivisme déclaré et constaté qui sont recensées, comme les doutes

(2) La gestion de l'actualité pétrolière, il y a quelques mois, peut être considérée comme une illustration de cette tendance « corporatiste ».

manifestés par les Français concernant le civisme de leurs concitoyens. Par ailleurs, c'est aussi l'affaissement du poids du conformisme sociétal qui est souligné, puisque les Français, non seulement ne s'interdisent pas un certain nombre de comportements inciviques, mais ne les « *condamnent* » pas et les tolèrent chez les autres, même s'ils en déplorent les conséquences pour ce qui est de la « *confiance* » qu'ils peuvent faire à autrui. En tout cas, on voit bien les dysfonctionnements qui peuvent résulter de ce rapport ambigu avec les règles de la vie sociale et comment le non-respect de celles-ci compromet les relations des individus entre eux, en mettant en cause non seulement le « civisme » des comportements, mais aussi, plus prosaïquement, peut-on ajouter, leur prévisibilité.

Par ailleurs, cette analyse éclaire les conséquences sociales qui résultent de cet affaiblissement du rôle des mécanismes de régulation informels, dans la mesure où cette défiance des individus les uns à l'égard des autres, tenant au non-respect des règles qui organisent la vie sociale, les conduit paradoxalement à souhaiter une multiplication des normes juridiques contraignantes pour leur garantir ce qu'ils n'attendent plus des comportements spontanés de leurs concitoyens. D'où cette inflation juridique [3] et réglementaire, qui constitue un des traits caractéristiques de la France contemporaine, avec la policiarisation et la juridiciarisation croissantes de la vie sociale qui en sont les corollaires. L'individualisme que traduisent ces réactions de défiance ayant donc pour conséquence paradoxale une croissance des interventions institutionnelles. D'où un processus circulaire, dans lequel cette évolution, issue de la défiance qu'éprouvent les individus les uns pour les autres, contribue aussi à nourrir et à développer cette même défiance. « *Le déficit de confiance mutuelle nourrit la nécessité de l'intervention de l'État. Mais, en réglementant et en légiférant de façon hiérarchique, l'État opacifie les relations entre citoyens. En court-circuitant la société civile, il entrave le dialogue social et détruit la confiance mutuelle* ».

On le voit, ce livre et les constats qu'il opère posent des questions importantes, et le système formé par le couple défiance/incivisme qu'il met en évidence – et dont les manifestations confinent parfois au nihilisme [4] - éclaire d'un jour particulier les problèmes que soulève la régulation contemporaine des relations sociales. En notant, d'ailleurs, que les remarques faites ne concernent pas que la vie sociale, dans la mesure où les mêmes enquêtes montrent également une très forte corrélation entre le sentiment de satisfaction et de bonheur subjectif éprouvé par les individus dans leur vie personnelle et le niveau de défiance entre les individus constaté dans les pays étudiés. Là encore, les pays nordiques se placent au premier rang, suivis par les pays anglo-saxons, alors que le niveau personnel de « satisfaction » déclaré en France classe celle-ci au 17e rang sur les 23 pays analysés !

Jean-Louis LOUBET DEL BAYLE

Professeur des universités, Toulouse I
Centre d'études et de recherches sur la police

NOTES DE LECTURE

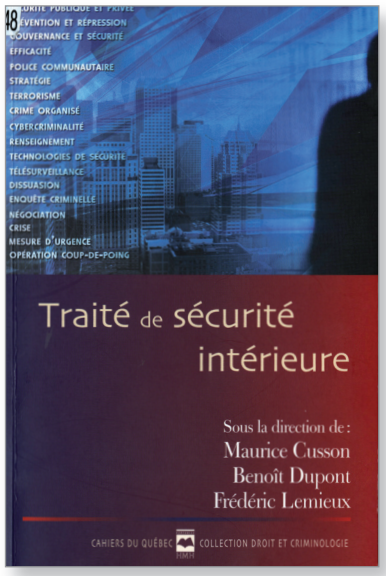
(3) Qui commence à se prolonger en inflation constitutionnelle.

(4) *Cf.* par exemple dans ce sens les remarques récentes de P. A Taguieff : « L'esprit critique, inséparable de l'invention de la liberté, s'est retourné en mode de dissolution de toutes les convictions fortes. L'examen critique s'est radicalisé en posture hyper-critique ne laissant rien subsister dans le champ des valeurs et des normes. Le questionnement s'est fait ricanement, tandis que l'inquiétude qui pousse à la recherche devenait la stérile arrogance de celui « *à qui on ne la fait pas* ». L'ultime aboutissement de l'interrogation socratique, ce pourrait être l'incrédulité généralisée des individus post-modernes » (*Julien Freund. Au cœur du politique*, Paris, La Table ronde, 2008, p. 94).

Traité de sécurité intérieure

Maurice CUSSON, Benoît DUPONT, Frédérick LEMIEUX

Un événement éditorial exceptionnel mérite d'être signalé à tous ceux qui s'intéressent, dans l'exercice de leur fonction, aux questions sécuritaires : la sortie récente d'un *Traité de Sécurité intérieure*, qui a réussi, à la fois, à *publier en français* et à faire collaborer des chercheurs spécialisés, des universitaires et des professionnels des deux rives de l'Atlantique. Ceci n'est pas courant et constitue même un exploit...



2007, Éditions Hurtubise, coll. « Cahiers du Québec : Droit et criminologies », 714 p., 35 €

Nous sommes là en présence d'une véritable « encyclopédie », au sens du *Traité de Police* de Nicolas de La Mare (1707-1738), irriguée par tous les savoirs et pratiques sur et de la police anglo-saxonne, comme par ceux et celles issus de la Vieille Europe, France comprise. Elle fait pendant à l'ouvrage *Histoire et dictionnaire de la Police, du Moyen âge à nos jours*, avec un avant-propos de Nicolas Sarkozy, publié en 2005, qui apparaît tout à fait complémentaire, mais profondément différent dans son optique [1]. Forte de 710 pages, l'entreprise a été dirigée, après un travail de sept années, par Maurice Cusson, qui en a été l'initiateur, Benoît Dupont et Frédéric Lemieux, regroupant, côté Amérique du Nord, dix professeurs et neuf chercheurs du Centre international de criminologie comparée (CICC) de l'université de Montréal et cinq professionnels de la sécurité ; côté européen : cinq professeurs (dont deux Français, du CERP [2] de Toulouse 1, François Dieu et Jean-Louis Loubet del Bayle), trois chercheurs du CNRS (Fabien Jobard, Christian Mouhana, Sébastian Roché) et quatre policiers (un Belge de la police fédérale et trois Suisses de Lausanne et de Genève). Le *Traité* offre, en outre, une bibliographie qui dépasse les mille titres et contient un index thématique fort utile pour sa lecture croisée. Incontournable, il concerne les praticiens de la sécurité, de la justice, de la criminologie, les responsables politiques et associatifs, les journalistes... comme, bien sûr, le monde universitaire et de la recherche dans son ensemble. Il va sans dire que, par son ampleur de réalisation et ses ambitions, cet ouvrage aborde de façon exhaustive les questions sécuritaires, rendues plus complexes dans le contexte de la mondialisation d'aujourd'hui. En épuise-t-il toutes les dimensions ?

Une initiative novatrice

Le contenu, dont les articulations doivent être d'abord présentées, s'annonce passionnant, pour deux raisons *a priori*.

(1) *Cf. Histoire et dictionnaire de la police, du Moyen-âge à nos jours*, Michel Auboin, Arnaud Teyssier, Jean Tulard (dir.), Paris, Robert Laffont, col. « Bouquins », 2005.

(2) Centre d'Études et de Recherche sur la Police de l'Université Toulouse 1. Rappelons que, dans un classement des 400 départements mondiaux de Science politique révélé par Simon Hix (« European Universities in a Global Ranking of Political Science Departments », *European Political Science*, 3 (2), 2004, p. 5-23), cette université, grâce notamment aux recherches internationales du CERP, est classée au 335e rang, devancée seulement par l'IEP de Paris et par l'INSEAD au niveau français. Signalons aussi que le ministère de l'Enseignement supérieur et de la Recherche a décidé, en juin 2007, d'intégrer administrativement le CERP, seul centre à travailler en France sur la police, qui avait accumulé des résultats scientifiques sans précédents, depuis sa création en 1976 par le professeur Jean-Louis del Bayle, au CRSG (Centre de recherche sur la sécurité et la gouvernance) de l'université de Toulouse 1.

Cet ouvrage perpétue une tradition de publications pionnières et de référence : celle de la célèbre École criminologique québécoise, avec notamment le *Traité de criminologie empirique*, publié en 1994 aux Presses universitaires de l'université de Montréal, dirigé par Denis Szabo et Marc Leblanc (auquel plusieurs contributeurs du Traité de 2007 avaient participé, dont Jean-Paul Brodeur et Maurice Cusson), mais aussi avec la revue *Criminologie*, aux mêmes éditions, de réputation scientifique internationale.

Ensuite, de par l'expérience accumulée depuis des années par tous ses auteurs, il se réfère, sur le plan intellectuel, à *une conception moderne de la criminologie*, qui souhaite intégrer l'apport des sciences humaines et sociales et leurs acquis sur la sécurité intérieure – éloigné en cela d'une conception française paralysée souvent par un juridisme pénaliste. Il déploie volontiers un savoir interdisciplinaire de sociologie des organisations, de science politique, de droit, de science administrative, de psychologie... sur les nombreux sujets abordés. Nous sommes en présence d'un *ouvrage de référence à plus d'un titre*. Quel en est l'essentiel sur le plan du contenu ?

On peut diviser la matière abordée, qui est immense, en *deux grands blocs* parfaitement articulés par une écriture claire et homogène de tous les auteurs (qui dénote l'importance de la relecture, de l'articulation et de l'harmonisation de la part des maîtres d'œuvre qui ont réalisé un beau travail éditorial !) :

– Le premier ensemble de contributions (« *Connaître et penser la sécurité* ») synthétise une approche « universitaire », théorique, du sujet, rendant compte des résultats de toutes les recherches de pointe, tant anglo-saxonnes que francophones en la matière. Il est composé de onze chapitres sur les thèmes suivants : l'action de sécurité (réflexion anthropologique de Maurice Cusson), le rapport indissociable entre sécurité et contrôle social (posé théoriquement et comparativement par Jean-Louis Loubet del Bayle), la construction de modèles de gouvernance (étudiée de façon novatrice par Benoît Dupont), un comparatif concernant le processus de construction historique des polices européennes (mené autour de sept États par Jean-Paul Brodeur), la présentation des organismes de sécurité intérieure du Québec (par Maurice Cusson et Marie-Ève Diotte), l'analyse du phénomène nord-américain de la « police communautaire » (décortiqué par Benoît Dupont), les modalités d'évaluation des interventions policières (définies par Étienne Blais et Maurice Cusson, qui insistent notamment sur les actions originales de prévention de la violence dans divers secteurs), le concept fondamental de « stratégie policière » (exploré par Maurice Cusson), l'exposé des tâches policières quotidiennes, écartelées entre négociation verbale et sanction (par Christian Mouhana), l'intégration du travail gendarmique (par « son » spécialiste, François Dieu), la coopération policière internationale au niveau judiciaire (par Nadia Gerspacher).

– Le second groupe de contributions, alimenté par la réflexion théorique initiale, comprend cinq parties séparées, qui résument *les grandes fonctions concrètes et théoriques, tout à la fois, de la sécurité intérieure*, à partir de descriptions et d'analyses intellectuelles concernant tous les professionnels des secteurs publics et privés :

1) *Les parades et les menaces,* cernées à travers six chapitres stimulants, qui collent tout à fait avec la réalité de l'insécurité dans les sociétés modernes de masse, tant dans les conurbations urbaines déployant des systèmes de sécurité multidimensionnels complexes – mais fragiles –, que dans l'espace international, géopolitique ou cybernétique, porteur de nouvelles insécurités exigeant des contre-mesures adaptées. Le premier chapitre aborde la psychopathie des délinquants « persistants et prolifiques », enclins aux récidives (Jean-Pierre Guay et Maurice Cusson) ; le second traite du crime organisé, des maffias, et des stratégies de lutte à leur encontre (Carlo Morcelli, Mathilde Turcotte, Guillaume Louis) ; le troisième décrit les différentes formes de terrorisme ainsi que les moyens à actionner pour les éradiquer (Stéphane Leman-Langlois) ; le quatrième se confronte à la criminalité économique et à sa régulation (Jean-Luc Bacher, Nicolas Queloz) ; le cinquième analyse la question sociale des banlieues et des « points chauds », en s'efforçant d'évaluer l'impact des plans d'action en la matière (Sébastian Roché) ; le sixième soulève la question de la cybercriminalité et des actions à lui opposer (Solange Ghernaouti-Hélie, chercheuse idoine en la matière).

2) L'étude de *l'intelligence policière* (« le renseignement et l'analyse »), nécessaire pour faire face à toutes les menaces, est ordonnancée autour de neuf chapitres. Le premier approfondit la définition du renseignement policier en tant que tel, en traitant de sa production sociale, soit par le moyen des informateurs, soit par celui des technologies, complémentaires en soi (Jean-Paul Brodeur) ; le second, du même auteur, évoque deux exemples d'erreurs dans la phase du renseignement concernant le cas dramatique du 11 septembre 2001 ; le troisième resserre la question autour du renseignement en matière de criminalité, en insistant notamment sur la pertinence et les performances en la matière (Frédéric Lemieux) ; le quatrième synthétise l'apport au renseignement criminel de la « forensique », c'est-à-dire de la police scientifique des « traces », à travers notamment des

développements stimulants sur le « profilage » (Olivier Ribaux et Pierre Margot) ; un cinquième définit les priorités en matière criminelle à partir du modèle belge (présenté par Paul Wouters et Martine Pattyn), détaillant de façon inédite les nouvelles méthodes de saisie ; un sixième différencie renseignement sécuritaire et renseignement criminel (Stéphane Leman-Langlois, Frédéric Lemieux) ; un septième livre une approche comparée (belge, suisse et canadienne) des « services stratégiques » et de développement (Didier Froidevaux) ; un huitième reprend la méthode de définition et d'identification des facteurs d'insécurité intentionnelle (Stéphane Leman-Langlois) ; enfin, est présentée la question de la protection des organisations et des audits de sécurité (Sylvain Mignault).

3) La fonction sécuritaire de *prévention* en tant que telle est ensuite passée au crible de cas concrets. Le niveau d'observation se resserre à travers les dix chapitres qui lui sont consacrés : le premier reprend les grands principes de la prévention policière (Maurice Cusson) ; le second s'interroge sur les méthodes et les techniques de la « prévention situationnelle » (Maurice Cusson) ; le troisième, sur l'efficacité de la surveillance et de la contre-surveillance (Maurice Cusson) ; le quatrième se penche sur les techniques de protection des espaces et leur évaluation (Stéphane Léman-Langlois et Lucie Dupuis) ; le cinquième dégage les fonctions et réfléchit sur l'usage de la télésurveillance (Maurice Cusson) ; le sixième offre une monographie concernant une société de sécurité privée mondialisée et performante, *Securitas* (Massimiliano Mulone, Maurice Cusson et Mélanie Beaulac) ; le septième fait surgir le thème fondamental pour les forces policières de l'usage de la force (traité par Fabien Jobard) ; le huitième révèle les différents genres d'enquêtes criminelles (Jean-Paul Brodeur) ; le neuvième décortique les « entrevues policières » plus ou moins « judiciaires » (Michel Saint-Yves et Michel Tanguay) ; le dixième scrute les « opérations coup-de-poing » (Maurice Cusson et Éric La Penna).

4) La quatrième fonction sécuritaire analysée au concret est celle du *maintien de l'ordre et de la gestion des crises*, ramassée autour de cinq chapitres sur : les situations de gravité, afin d'évaluer les outils de gestion des risques et de l'urgence (Frédéric Lemieux) ; les problèmes de maîtrise des « événements festifs » (Frédéric Diaz) ; le thème de la manifestation, démocratiquement acceptée lorsqu'elle est pacifique, réprimée en cas de débordements (François Dieu) ; la négociation de crise en tant que telle (Michel Saint-Yves) ; la transposition du problème au niveau de la sécurité privée (Éric Boucher).

Il n'est pas aisé de résumer en quelques lignes les objets traités par cette encyclopédie de la sécurité intérieure qui n'avait pas jusqu'ici d'équivalent, même en littérature anglo-saxonne. Recentrons alors quelques remarques autour de la méthode déployée, impressionnante et heuristique.

Une méthode heuristique

L'objet était d'autant moins facile à maîtriser que le *Traité* confronte deux systèmes policiers assez différents : celui de l'Amérique du Nord (où, notamment, la privatisation de la sécurité est forte) et celui de l'Europe continentale (le modèle anglais étant un peu délaissé, reconnaissons-le). Par ailleurs, les auteurs constatent tous un éclatement des acteurs publics et privés de la sécurité (ils dénombrent par exemple 345 organismes rien qu'au seul Québec !). Ils décrivent parfaitement les multiples tâches de « *policing* » assumées (notons l'importance donnée à la description des pratiques de prévention, aux nouveaux savoirs sur l'enquête criminelle, aux sciences forensiques, qui ont bouleversé la police criminelle moderne...). Ils introduisent aussi une réflexion, qui concerne la France d'aujourd'hui (qui élabore sa RGPP dans toutes les administrations, police et armée en tête), en traitant de *l'évaluation des politiques de lutte contre la criminalité et la délinquance, ou des politiques de réinsertion*. À ce propos, Benoît Dupont insiste sur les limites des approches strictement « gestionnaires » émanant du « NMP » (*New Management Public*) de l'Amérique néolibérale (p. 67-80) [3]. *A contrario*, explique-t-il, la sécurité implique des catégories, des valeurs, des logiques de fonctionnement totalement éloignées et indépendantes du monde de l'entreprise privée [4]. Les policiers ou les gendarmes ne sont pas, en effet, des « burelains », pour parler comme Max Weber : ils doivent affronter l'urgence, l'imprévisibilité. Leur calendrier d'action n'est pas celui de la bureaucratie. En raison des circonstances, ils sont contraints de déployer sur le terrain un pouvoir discrétionnaire, une liberté très humaine d'appréciation, un esprit de sang-froid et d'initiative. Dans ses tâches et sa temporalité, la police se situe en partie « hors administration », d'autant que, pour fonctionner rapidement, elle doit déployer des réseaux

(3) Transposées en France via la fameuse loi organique relative aux lois de finance (LOLF)*, portée par le lobby du parlement français contre les ministères parisiens qui traitaient directement leur programme financier avec la Commission de Bruxelles...

(4) Cela reste aussi valable notamment pour l'univers de la pédagogie et de la recherche universitaire.

relationnels efficaces afin de contourner les blocages administratifs et gestionnaires officiels, qui n'administrent, en définitive, eux, que des règlements, du papier et de l'argent public. L'univers policier repose sur des valeurs spécifiques. Il implique aussi la maîtrise de relations suivies et réciproques avec la population, voire avec les délinquants (*cf.* la dialectique gendarme/voleur dont parle Maurice Cusson, p. 52-57). Il doit encore gérer la violence, notamment celle, introvertie et extravertie, résultant de l'usage des armes (*cf.* la communication importante de Fabien Jobard à ce propos, p. 530-540). Ces valeurs, tous les savoirs acquis, sont investis dans la durée, transmis d'une génération de policiers à l'autre, par des strates multiples de personnels professionnalisés. Le métier sécuritaire reste aussi « forfaitaire » au niveau des tâches quotidiennes, en termes de temps de travail, dérogatoire aux statuts officiels, généralement non « rentable » du fait qu'il est lié au devoir de secours porté également et gratuitement à autrui, jour et nuit, même si certaines forces peuvent être amenées à vendre des services de sécurité aux particuliers. Tirant les leçons de la sociologie des organisations, les auteurs du *Traité* repèrent encore les décalages entre public et privé, ainsi que les difficultés liées à « l'atomisation de la gouvernance de la sécurité ». Plus on avance dans la lecture des passages concernant l'Amérique du Nord, plus on sent que l'on se trouve en face d'un système éclaté, aux valeurs différentes, dont on se demande comment il peut fonctionner harmonieusement, être « dirigé » et coordonné, en opposant la police « par les technologies » (notamment mobiles, hertziennes, aériennes – les hélicoptères ! –, cybernétiques, de télésurveillance, voire satellitaires), à la police « par les hommes » – les indicateurs et le travail quotidien d'information basique. Le cas du 11 septembre 2001, au niveau de la sécurité des aéroports des États-Unis, brillamment analysé par Jean-Paul Brodeur – dans deux contributions qui sont un modèle du genre –, renforce évidemment cette impression d'éclatement et de flottement (p. 278-289). Mais ce n'est peut-être qu'une impression, perçue depuis la Vieille Europe...

En tout cas, face à un tel défi, les auteurs nous proposent une définition, disons « positiviste », de la police, influencée – à juste titre – par les évolutions fascinantes de la police scientifique dans les enquêtes criminelles, hyperrationnelles, aux résultats souvent spectaculaires. Par une méthode efficace, ils redonnent ainsi une unité au réel. D'où l'importance de l'épistémologie institutionnaliste et fonctionnaliste conjuguée dans le premier bloc de contributions. Impressionnant est ici le réseau de concepts qui décortique « organes », « structures », « fonctions ». On comprend vite que la sécurité est « une structure ternaire » de rôles – protecteur, protégé, menaces – et un ensemble de cinq fonctions – le renseignement et l'analyse ; la prévention et la surveillance ; l'investigation et la répression ; la gestion de crise face aux cinq catégories de risques (altercations, bagarres, rixes ; rassemblements ; incivilités, blessés, enfants perdus, personnes en détresse ; catastrophes naturelles ou techniques), et, enfin, la polyvalence, réunissant éventuellement plusieurs de ces quatre autres fonctions. On voit apparaître clairement les « structures sociales » de la « gouvernance » sécuritaire (l'État, le marché, les réseaux), ainsi que les différents « niveaux de gouvernance », selon les types d'acteurs (le public, central et local, le privé, l'associatif) dans chaque *modèle* : la micro-gouvernance, la gouvernance interinstitutionnelle, la gouvernance internationale. Chaque palier obéit par ailleurs à une « typologie relationnelle » fondée, pour l'État, sur l'obligation (ou « tierce police »), pour le secteur privé, sur la délégation et la satisfaction des intérêts des clients, pour les réseaux associatifs, sur le don et l'échange, le problème étant de faire cohabiter la « rationalité utilitariste » de la sécurité privée et la « rationalité de justice et d'égalité » de la sécurité publique (qui fonctionne au blâme, à la punition, à la réparation). Typologie pertinente, à la manière d'une sociologie maîtrisée qui veut donner l'impression que nous sommes en présence d'un objet bien huilé. Mais est-ce vraiment le cas ? Serait-ce une illusion d'optique ?

Le risque, avec cette méthode quasi mathématique, à dominante analytique et synthétique, pourrait être de ne pas assez repérer les emboîtements, les hiatus, les problèmes de terrain (vécus par les policiers comme par les victimes, voire par les délinquants), les difficultés de cohabitation et d'adaptation des acteurs multiples, les statistiques « non conformes », les éléments systémiques aussi entre les fonctions dégagées (même si le modèle théorique met en avant le concept de « polyvalence »)... En gros, quels liens établir, par exemple au niveau macrosociologique, entre trafic de drogue, maffias et terrorisme, ou entre sécurité intérieure et sécurité extérieure, ou encore – objet un peu délaissé – entre police et justice...? Ne faudrait-il pas déployer également une grille de lecture moins officielle et « institutionnelle », qui assimilerait les pratiques « tribales » en milieu urbain [5], comme les représentations de la société « d'en bas », porteuses de formes nouvelles de socialité, voire de sociabilité, pas nécessairement décelables en termes de « délinquance prolifique » potentielle, même si elles peuvent être à l'origine de comportements antisociaux, anomiques, au sens durkheimien (pensons aux jeunes *nikikomori* japonais qui se coupent de leur famille et s'isolent dans leur chambre, pour partager un

(5) *Cf.* à ce sujet, notamment, l'ouvrage de Michel Maffesoli, *Le Temps des tribus,* 1988, Le Livre de Poche, 1991.

monde virtuel dans le cyberespace). *Quid*, alors, à ce propos, de la question des liens complexes et troublants entre individu, technique et ville moderne (grille pressentie par Jean-Louis Loubet del Bayle dans sa contribution, p. 65-66) ? Ne faudrait-il pas là convoquer aussi, à rebours, une sociologie plus « compréhensive », qui ne négligerait pas les idéologies de la sécurité, s'efforçant de recomposer les stratégies, notamment assurantielles et financières privées, dans l'élaboration et l'imposition d'une « société du risque » ? Ou encore des analyses plus phénoménologiques [6], attentives à une sociologie des victimes et de la victimisation, aux trajets des « individus incertains », centrés sur eux-mêmes, hantés par l'insécurité, le risque, « l'urgence », l'entropie, démunis de modèles, de repères et d'intégration sociale [7]? Ne faudrait-il pas également approfondir les thèmes du *Traité* autour d'une réflexion scientifique – non idéologique ou politique ! – sur le lien, occulté par les tenants du « politiquement correct » à la française, entre délinquance, criminalité et degré d'intégration des « communautés », notamment *ethniques* (celles-ci, dont l'on ne peut nier l'existence en Amérique du Nord comme en Europe, ne sont pas repérées dans l'*Index*, qui ne retient que les communautés « altruistes », « géographiques » et « d'intérêt » [8]) ? Cela, par exemple, à travers un bilan de l'histoire évolutive du cas états-unien, ou encore, pour la France, à partir d'un recoupement *objectif* et *comparatif*, dans l'espace et dans le temps, des statistiques pénitentiaires, sociales, scolaires, judiciaires, policières ? En définitive, sans tabous et sans avoir peur de la réalité telle qu'elle est, en déployant un engagement peut-être plus proche des valeurs des réseaux associatifs que de la logique réglementaire ou punitive de l'État, ou de celle, intéressée, du marché, ne faudrait-il pas mettre l'accent également sur les causes, plutôt que sur les conséquences des « menaces » contemporaines en termes de sécurité intérieure ?

Autre question, en relation cette fois avec la méthode comparative mise en œuvre par l'ouvrage : la police est traitée abstraitement dans toutes ses fonctions, un peu hors de tout contexte (à part, assurément, les contributions portant sur des cas situés). N'y a-t-il pas de liens entre structure et fonction ? Les modalités organisationnelles ne déterminent-elles pas le « système policier » dans son fonctionnement, et donc dans son efficacité et son évaluation ? A-t-on vraiment les mêmes structures et les mêmes fonctions dans le système nord-américain et dans le système européen ? La différence entre ceux-ci n'est-elle pas reconnue en ces termes par Jean-Paul Brodeur : « *Bien qu'il soit difficile de prévoir ce que l'avenir nous réserve, il est tout de même raisonnable de penser que les systèmes policiers de l'Europe continentale et des pays anglo-américains, plutôt que d'accentuer leurs différences, partageront de plus en plus de traits communs* » (p. 88) ? Ne serait-ce pas là, formulé en creux, le postulat central du *Traité* ? Ce rapprochement est-il si évident ? Les contributions du second bloc, concernant le détail de chaque fonction policière, rencontrent à plusieurs reprises ces questions, tournent autour, les esquivent parfois, ou nous permettent, dans le pluralisme des objets et des approches, de les dépasser et d'y répondre en partie. Le *Traité*, en tout cas, en son genre et en sa matière, renouvelle l'actualité du regard porté par Alexis de Tocqueville sur les différences qui séparent les sociétés et les systèmes de valeurs des deux rives de l'Atlantique, réalité qu'un Max Weber, universitaire déprimé en son temps, découvrit à son tour, lors de son voyage en Amérique...

Un esprit pointilliste, « bête à chagrin », pourrait regretter que l'ouvrage ne comporte que peu de statistiques sur la criminalité comparée, qu'il n'y ait pas de cartes (si utiles en sociologie de la délinquance et de la criminalité, comme l'a montré l'École de Chicago dans ses travaux sur la ville) – alors que sont dessinés de nombreux tableaux, diagrammes et organigrammes. Que certains sujets « actuels » aient été délaissés – mais le *Traité* a été commencé en 2000 ! - par exemple, la corruption de la police, la criminalité sexuelle, la délinquance à l'école, la police environnementale, le travail policier des douanes, les méthodes d'action de la police financière, la surveillance satellitaire, l'organisation et les méthodes des services de renseignement, etc. Mais aussi, et surtout, les nouvelles approches en termes de « sécurité globale » (concept ignoré de l'*Index*, issu des théories des relations internationales) – bien mises en évidence en France, récemment, par le rapport iconoclaste d'Alain Bauer, aux conséquences théoriques et institutionnelles incalculables [9]. De même pour ce qui

....

(6) Comme celle du beau livre de Pierre Sansot, *Poétique de la ville*, Paris, Petite Bibliothèque Payot, 2004.

(7) *Cf.* notamment les travaux d'Alain Ehrenberg, *L'Individu incertain*, Paris, Hachette Littérature, Pluriel sociologie, 1995 ; de Nicole Aubert, *Le Culte de l'urgence. La société malade du temps*, Paris, Flammarion, coll. Champs, 2004 de David Le Breton, *Anthropologie du corps et modernité*, Paris, PUF, Quadrige, 1990 ; *Passions du risque*, Paris, Métaillé, 1991 ; *Signes d'identité. Tatouages, piercings et autres marques corporelles*, Paris, Métaillé, 2002 ; *Conduites à risque. Des jeux de mort au jeu de vivre*, Paris, Quadrige, 2002.

(8) Alors que la contribution de Sébastian Roché, « Restaurer la sécurité dans les banlieues et les points chauds » aborde en partie – mais en partie seulement – le problème, p. 235-245.

(9) Rapport sous la direction d'Alain Bauer, remis au Président de la République et au Premier ministre, *Déceler – Étudier – Former : une voie nouvelle pour la recherche stratégique. Rapprocher et mobiliser les institutions publiques chargées de penser la sécurité globale*, avril-juin 2008, publié dans le supplément au numéro 4 des *Cahiers de la Sécurité*.

est des représentations régulatrices, identitaires et compensatoires de la criminalité et de la police dans les médias et dans les arts (pensons à Edward Munch, à Otto Dix, à Fritz Lang, à Charlie Chaplin, à *M le maudit*, à *Big Brother*, à *Matrix*, à *RoboCop*, etc.). Une théorie criminologique du « délinquant isolé » coupé de tout « milieu » (p. 175-184), très « psychopathologique » certes, n'apparaît-elle pas parfois trop limitative ? Mais tout ne pouvait être abordé, sur un thème qui se révèle, à la lecture de cet ouvrage collectif, en fait, inépuisable, profondément actuel... et inquiétant quant à l'humanité d'aujourd'hui, perçue en ses pratiques, individuelles et collectives, délinquantes et criminelles, de façon profondément réaliste.

Ce *Traité de sécurité intérieure* nous offre ainsi une image de la police moderne en action – au-delà des différences des modèles nord-américains et européens –, avec un point de vue exhaustif sur ses tâches, ses problèmes, ses engagements, ses obligations, sur les difficultés de ses personnels, sur ses méthodes, ses moyens, ses limites aussi. La réussite de cette encyclopédie cohérente, c'est de démontrer, par le déploiement d'une méthode sans faille – même si elle peut être approfondie sur certains points – que les questions de sécurité relèvent bien d'une certaine « intelligence » des problèmes de violence sociale, délinquante et criminelle, comme, en réponse, d'une « stratégie » et d'une politique de « contre-mesures » – pour utiliser un langage de sous-marinier. Cette leçon dépasse ainsi les conceptions empiriques, pragmatiques, analytiques éclatées, juridiques, normatives, comme celles moralisatrices, manichéennes et idéologiques dans lesquelles on a souvent « enfermé » la police et les hommes qui la servent... En cela, *cet ouvrage mérite bien d'être comparé à celui de Nicolas de La Mare, en son temps...*

Cette référence au passé fait paradoxalement surgir, en contre-point, une question symptomatique : le *Traité*, qui se cantonne à l'Amérique du Nord et à l'Europe (en écartant l'Amérique du Sud, l'Asie, l'Afrique, ou d'autres civilisations...), ne laisse guère de place à l'histoire de la police et de la sécurité. Serait-ce en raison d'une hypertrophie de la méthode fonctionnaliste – la sociologie, on le sait, étant souvent « fille de l'instant », comme aimait à le répéter Fernand Braudel ? Certes, quelques analyses sont consacrées au développement de la division du travail policier (p. 32-34) et une brève esquisse (condensée en douze lignes !) est proposée, concernant la construction des polices continentales de l'Europe. Mais sans poser des liens avec celle, indissociable, des structures territoriales des États, si différenciées d'un pays à l'autre, sans s'intéresser à l'étatisation de la police [11], sans se référer non plus au poids des deux guerres mondiales sur le système policier européen... Une approche historique plus dense eût été utile au moins à trois niveaux. D'abord, pour éclairer, précisément, les différences organisationnelles et fonctionnelles des polices analysées, au-delà de leurs fonctions communes contemporaines – même si, en milieu urbain, les fonctions de police semblent identiques depuis toujours. Ensuite, pour approfondir les liens, dans le passé lointain, récent, ou dans le présent, entre des systèmes de valeurs, les codes culturels ou civilisationnels et les *modèles d'ordre public* qui structurent pendant un temps une société donnée, la sécurité intérieure étant évidemment concernée par l'ensemble des mécanismes de contrôle social – point sur lequel insiste pourtant, au début de l'ouvrage, Jean-Louis Loubet del Bayle (p. 58-66) [12]. Enfin, au-delà de la question du poids plus ou moins durable des processus de construction des modèles du passé sur les systèmes policiers publics, privés ou réticulaires contemporains, pour analyser les mécanismes de violence sociale, de délinquance, de criminalité, de transgressions, d'effervescences collectives, qui peuvent être tout de même comparables d'une époque à une autre.

Autant de questions intellectuelles, parmi beaucoup d'autres, qui sont ainsi ouvertes par la lecture de ce *Traité de Sécurité intérieure*, dont on ne peut que recommander vivement la lecture, *urbi et orbi*, pour les raisons ici présentées et critiquées – selon la tradition de l'ancienne scolastique universitaire.

Michel BERGÈS
Professeur des Universités
Bordeaux IV

NOTES DE LECTURE

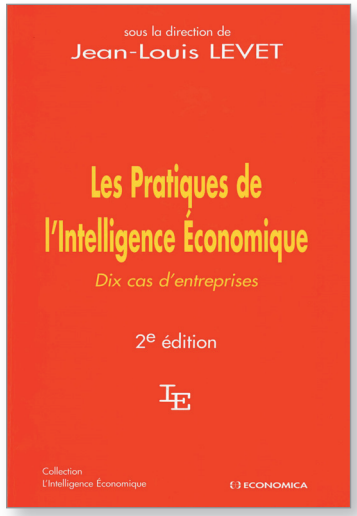
(11) Le *Traité* ne cite aucun des ouvrages classiques en français concernant l'histoire de la police, ni non plus des travaux comparatistes de socio-histoire sur le processus de construction de l'État. Sur un sujet délaissé, à savoir l'identification et les papiers d'identité, on peut consulter un ouvrage paru juste avant la publication du *Traité*, Gérard Noiriel (édit.) *L'Identification. Genèse d'un travail d'État*, Paris, Belin 2007, qui ouvre un « nouveau chantier ».

(12) *Cf.* à ce sujet, l'ouvrage illuminateur de Jean Delumeau, *Rassurer et protéger. Le sentiment de sécurité dans l'Occident d'autrefois*, Paris, Fayard, 1989.

Les pratiques de l'Intelligence économique

Dix cas d'entreprise

Sous la direction de Jean-Louis LEVET



2008, Economica, Coll. L'Intelligence économique, 162 p., 19 €

Cet ouvrage réalisé sous la direction de Jean-Louis Levet, l'un des pionniers de l'intelligence économique, se veut concret et présente des analyses de cas allant de la PME au groupe international. Le lecteur y trouve la relation d'expériences de terrain rapportées par des responsables en prise directe avec l'aléa économique et la concurrence.

Premier enseignement : le taux d'imprégnation de l'intelligence économique dans l'entreprise dépendrait notablement de la taille de celle-ci. Il est également proportionnel à la capacité d'innovation, facteur déterminant de la mise en place d'une stratégie d'intelligence économique. Ceci est une donnée constante à l'échelle française et européenne aussi bien dans l'industrie et les services liés que dans les services financiers, les banques et les assurances.

La propension de l'entreprise à consommer de l'information pour la transformer en connaissance détermine ainsi trois catégories de petites et moyennes entreprises : traditionnelle, taylorienne et cognitive. La dernière classe a vocation à se développer dans des activités innovantes de haute technologie et regroupe les entités privilégiant la logique d'apprentissage et de compétence alliée à une recherche permanente d'informations. Ce sont les plus performantes en terme d'anticipation et de maîtrise de leur environnement.

Si la motivation première de ces entreprises innovantes demeure l'accroissement des parts de marché, l'élargissement de leur gamme de produits et l'amélioration de la qualité comptent de plus en plus dans la maîtrise des marchés conquis et dans le développement à l'international.

Les expériences présentées dans l'ouvrage relèvent de trois réalités différentes en fonction de la taille et de l'activité développée :

1. Une relation structurée entre l'intelligence économique et la réflexion stratégique dans les grands groupes (EADS, RENAULT, L'OREAL, PSA, VALEO).

Ces grandes entreprises favorisent le passage d'une culture opérationnelle traditionnellement orientée vers l'action à une autre fondée sur la réflexion anticipatrice des signaux faibles et des ruptures incertaines. La sensibilisation et la coordination des acteurs internes au partage et à l'exploitation collective de l'information renforcent leur mobilisation interne. Les personnels de ces firmes sont ainsi étroitement liés par la prospective à la vision stratégique de l'upper management dans les mutations inéluctables d'origine identitaire ou technologiques.

Les stratégies d'influence et de communication se développent au cœur de leur démarche de survie et de leur développement à l'international. Elles coexistent avec des pratiques de partage de veille technologique, sociétale ou concurrentielle (coopération-compétition) pour maintenir ou sauver des parts de marché, renforcer l'entreprise dans ses pratiques d'économie d'échelle et de faire face aux nouveaux ordres de grandeur des investissements dans les développements des nouvelles technologies. L'expérience du MISTE 1 en

....

(1) Jean-Louis LEVET est un économiste reconnu, ses travaux portent plus largement sur l'économie industrielle. Ancien conseiller industriel à Matignon, il a exercé de multiples responsabilités dans le secteur public et dans le secteur privé. Il est actuellement directeur général de l'Institut de recherches économiques et sociales (IRES). Ses essais animent régulièrement le débat public : *Sortir la France de l'impasse* (1998), couronné par l'Académie des Sciences morales et politiques, *L'économie industrielle en évolution : les faits face aux théories* (2004).

(2) Mastère « intelligence scientifique, technique et économique » de l'Ecole supérieure d'ingénieurs en électronique et électrotechnique (ESIEE).

2004 est la démonstration d'une veille technologique mutualisée de qualité sur les composants des vidéo-capteurs entre RENAULT, PSA, l'équipementier VALEO et l'IESEE.

2. La personnalité du dirigeant influe fortement sur les pratiques d'intelligence économique développées dans les PME-PMI (SISLEY, DACRAL).

Le domaine d'activité est le facteur important du degré d'imprégnation des fondamentaux de la veille scientifique, commerciale ou technico-juridique dans les PME. Une entité *leader* et représentative du secteur des cosmétiques a associé son personnel à la recherche et à la transmission de l'information utile et en retour lui restitue les effets du processus sur la bonne marche de l'entreprise.

Encore faut-il que ces données soient bien utilisées dans le processus de décision et que les circuits de l'information aient bien été définis entre les départements de la recherche, du marketing et de la vente.

À ce niveau d'organisation du circuit de l'information, le dirigeant de PME innovante est le principal stimulateur du dispositif et de la culture de partage de l'information utile par des modes plus ou moins formels. Confirmation par les faits, l'intelligence économique est plus affaire d'état d'esprit que de taille dans les secteurs évolutifs très concurrentiels et fortement innovateurs.

Les actions des syndicats professionnels peuvent susciter, renforcer, structurer et coordonner les stratégies collectives de développement des petites structures principalement par la mise en place d'une veille collective « tous azimuts » et l'échange d'expertise, deux fonctions facilement mutualisables.

En mettant à leur disposition des pratiques coopératives de l'intelligence économique comme le *lobbying* à l'égard des décisions publiques et des outils tels les réseaux sociaux inter-entreprises, les portails Internet, ces structures visent la complémentarité des compétences et apportent des gains de temps appréciables dans la prise de décision.

3. L'intelligence économique, levier de l'identité et de la pérennité de l'entreprise à l'international. (RAYMOND, SALOMON, MARCAL).

L'acquisition de parts sur les marchés émergents rend particulièrement productives les collaborations d'entreprise de type joint venture ou les groupements d'intérêts économiques. L'union de leurs forces permet le regroupement des homologations et des brevets, des commandes, des connaissances et des ressources en matière d'investissement et de transfert technologique de manière à atteindre la taille critique sur des marchés aussi difficiles et concurrentiels que le marché chinois ou indien et d'y proposer une offre sur mesure.

Les pratiques d'intelligence économique des PME ou des TPE sont aussi centrées sur la surveillance des marchés, de leurs évolutions en termes d'offre, de types d'acteurs et de substitutions entre des lignes de métiers et la surveillance de la concurrence par des moyens légaux. Elles doivent aboutir à dégager des « potentiels de situation » permettant de tirer profit des forces et des faiblesses des acteurs sur les marchés complexes. Les coûts d'accès à l'information et aux compétences leur deviennent plus accessibles grâce à la démocratisation des technologies de l'information. Mais l'efficience des méthodes de management renouvelées de prise de décision stratégique dépend surtout dans ces entités de la conviction du dirigeant à les mettre en œuvre et à adopter les pratiques d'intelligence économique comme mode de fonctionnement.

En résumé, trois caractéristiques se dégagent de ces expériences accumulées et affirmées de l'intelligence économique :

- les pratiques sont multiples et aboutissent à des modes d'organisation adaptés à la trajectoire de chaque entreprise, et ce, quelle que soit sa taille, PME ou grand groupe ;
- leur mise en œuvre n'est en aucune façon une question de moyens ;
- l'intelligence économique est un facteur déterminant de la performance durable de l'entreprise et de son insertion dans son environnement.

Un regret qui, nous le pensons, est dû à une omission volontaire. Celui de voir que les expériences relatées ne mentionnent à aucun moment de séquences de collaboration avec les réseaux d'acteurs territoriaux chargés d'organiser et de provoquer la coopération, favoriser la circulation, l'échange d'informations au plan local et au cœur des territoires. C'est en effet là que se dessinent les constellations entre responsables économiques, universitaires, élus, fonctionnaires qui produisent la plupart du temps une dynamique positive, que l'on peut appeler développement local.

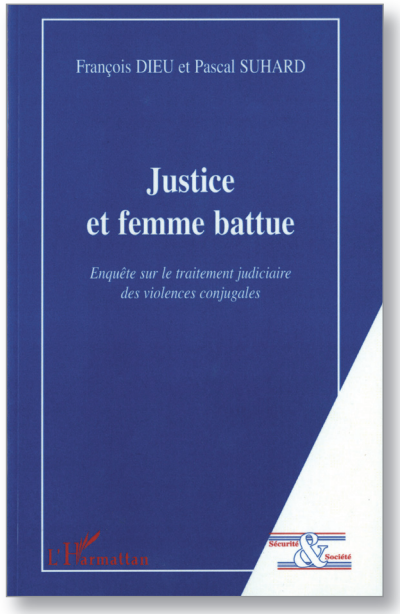
Cette 2e édition constitue donc la suite logique consacrée à l'analyse globale de l'intelligence économique et aux fondements méthodologiques de sa mise en œuvre. S'il devait se synthétiser à l'extrême, le message premier à intégrer de la part des lecteurs se résumerait au fondamental suivant : toute entreprise quelle que soit sa taille, son activité, son degré d'internationalisation peut et doit intégrer une démarche d'intelligence économique, laquelle peut aller jusqu'à faire système et est destinée à améliorer le processus de décision et donc la performance économique.

Alain AUMONIER
INHES

Justice et femme battue

Enquête sur le traitement judiciaire des violences conjugales

François DIEU et Pascal SUHARD



2008, L'Harmattan,
130 p., 13,00 €

En France, selon le secrétariat d'État aux droits des femmes, une femme sur dix (âgée de plus de vingt ans) serait victime de violences conjugales. Les enquêtes de victimation ont participé à la reconnaissance d'un phénomène longtemps occulté. L'évolution des textes législatifs concernant les violences conjugales apparaît significative de cette prise de conscience collective, allant de la loi du 23 décembre 1980 réprimant le viol conjugal, jusqu'à celle du 4 avril 2006 renforçant la prévention et la répression des violences au sein du couple, puis celle du 10 août 2007 sur la récidive. Les auteurs ont pris le parti d'étudier le traitement judiciaire des violences entre conjoints, en respectant la chronologie de la procédure judiciaire : direction de l'enquête, puis orientation des poursuites judiciaires, et sanctions prononcées par les tribunaux. L'ouvrage se divise ainsi en trois grandes parties :

- le profil des victimes et le dépôt de plainte ;

- les constatations médicales ;

- le profil des auteurs de violences conjugales.

Le profil des victimes démontre que les violences conjugales ne touchent pas seulement les milieux défavorisés, même si les populations les plus précarisés et fragiles demeurent surreprésentés. La victime est, dans 98 % des cas, une femme. Toutes les tranches d'âge sont concernées, mais avec une faible représentation des moins de 25 ans (7,1 % des victimes) et des plus de 60 ans (4,3 %). Les 25 à 45 ans sont très majoritairement touchées (60,3 %), car ils concentrent les moments clés de la vie pouvant entraîner des ruptures : mariage, naissance d'un enfant, chômage, séparation, etc. Toutes les catégories socioprofessionnelles sont concernées, mais, là encore, existe une surreprésentation de la classe moyenne et des milieux défavorisés (81,5 %). Il est donc manifeste que la précarité financière de la femme victime contribue à sa vulnérabilité. Ces données et le fait qu'elle soit mère de famille, dans 78,5 % des cas, expliquent aussi que plus d'une femme sur quatre (26,5 %) reprend la vie commune après avoir subi ces violences.

La plupart des enquêtes menées traitent les violences conjugales au travers des sanctions prononcées par les tribunaux correctionnels :

- 53,6 % des mis en cause reconnaissent les faits de violences sur leur partenaire ;

- ces violences sont à 79 % sans incapacité temporaire de travail (ITT) ;

- dans 84,2 % des cas, les auteurs n'ont pas de casier judiciaire.

Le nombre de plaintes pour violences entre conjoints a connu une croissance d'environ 30 % entre 2005 et 2006 dans les deux tribunaux de grande instance d'un département rural (Tarn) que recoupe cette enquête (Albi et Castres). Toutefois, il est impossible de préciser s'il s'agit d'un accroissement de cette forme de délinquance ou des effets de la politique de sensibilisation des victimes pour qu'elles dénoncent davantage ces faits, ainsi que l'incitation des forces de l'ordre et de la justice à mieux les traiter.

Les tribunaux s'inscrivent dans une logique répressive qui participe de la prévention générale de la délinquance. Pour l'année 2005, au niveau national, les condamnations en correctionnelle pour violences conjugales se répartissaient de la manière suivante :

- 85,1 % assorties d'une peine d'emprisonnement ferme ou avec sursis ;

- 15,5 % assorties d'une peine d'emprisonnement totalement ou partiellement ferme ;

- 69,6 % assorties d'une peine d'emprisonnement entièrement avec sursis.

Cette enquête montre combien la question des violences conjugales est une problématique le plus souvent familiale. La réponse judiciaire doit tenter d'apporter une solution pour la famille entière et pas uniquement pour l'auteur des violences, en tenant compte des conséquences au plan économique et relationnel tenant à l'éclatement des liens familiaux.

Les deux auteurs, François Dieu, professeur des universités et Pascal Suhard, magistrat, formulent quelques orientations prospectives à partir d'une enquête qu'ils qualifient de « recherche-action » :

- prendre en compte d'une manière plus effective la problématique des violences conjugales dans les instances en charge du partenariat local ;

- construire un partenariat entre les institutions judiciaires et les instances sanitaires et sociales en charge de la lutte contre l'alcoolisme, compte tenu de la place de l'alcool dans les violences conjugales ;

- recourir plus systématiquement à la médiation si victimes et auteurs souhaitent reprendre la vie commune ;

- faciliter l'éloignement des conjoints violents ;

- encourager les actions de prévention en direction des enfants pour casser la spirale de la reproduction des violences ;

- sensibiliser les professionnels de l'enfance, enseignants et travailleurs sociaux, aux problèmes des enfants exposés aux violences dans le couple ;

- sensibiliser les professionnels de santé afin qu'ils expliquent aux victimes l'intérêt du certificat médical dans la procédure judiciaire ;

- élaborer un outil statistique afin de mieux cibler l'action publique.

Au final, cet ouvrage offre un panorama complet et objectif des principales questions touchant aux violences conjugales. Toutes les thématiques ne pouvant être abordées en profondeur, le lecteur désireux d'approfondissement pourra se référer au grand nombre de publications et de sites internet cités par les auteurs.

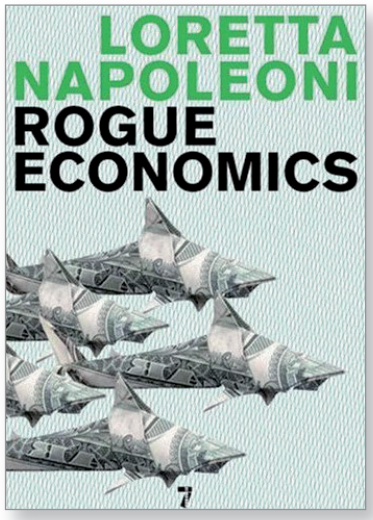
Corinne FAYOLLE
INHES

En savoir plus sur...

Quoi de neuf dans le capitalisme sauvage ?

Un système économique mal régulé laisse facilement la place aux comportements criminels les plus extrêmes, parfois à très grande échelle, et ce au point de déstabiliser des secteurs entiers. Déjà, souvenons-nous, la grande crise financière japonaise dans les années 1980 fut surnommée à juste titre la « récession Yakusa », tant la mafia nippone y avait joué un rôle central. Un nouvel exemple vient de surgir aux États-Unis quand le ministre de la Justice (*attorney general*) s'est publiquement interrogé, en mai 2008, sur le rôle du crime organisé dans la hausse du prix des matières premières. Manifestement, une spéculation de grande ampleur et très organisée pourrait expliquer en partie cette augmentation périlleuse pour les économies occidentales. On sait depuis le XIX[e] siècle – les *robber barons* américains – et plus récemment avec l'expérience russe des années 1990 que le capitalisme devient vite « sauvage », s'il n'est pas encadré par des lois.

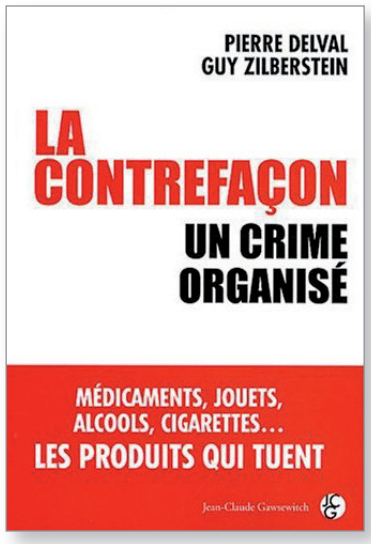
La journaliste et essayiste Loretta Napoleoni, à qui l'on devait déjà un livre intéressant sur le financement du terrorisme – *Terror Inc. : Tracing The Money Behind Global Terrorism* –, propose cette fois avec *Rogue Economics* une plongée dans les « marchés sauvages » de l'après-guerre froide. L'auteur s'interroge ainsi sur la manière dont le monde est en train d'être profondément transformé par ce qu'elle désigne



2008, Seven Stories Press, 336 p., 18,19 €

comme des « forces économiques obscures » qui piègent des millions de consommateurs à travers le monde. Quels sont ces nouveaux marchés sauvages et noirs du capitalisme contemporain ? La réponse proposée est large et entraîne le lecteur des prédateurs capitalistes les plus ordinaires jusqu'à des organisations criminelles aux dimensions de puissances constituées : l'industrie pornographique et la prostitution mondialisée, le commerce de la « malbouffe » et l'obésité, la piraterie maritime et les pêches illégales destructrices des réserves halieutiques, les contrefaçons de médicaments et autres, la crise du crédit et de l'endettement irréel aux États-Unis, les gangs urbains d'Amérique centrale et nord-américaine, etc. Un tel catalogue pourrait laisser penser que l'auteur se laisse aller sans fil conducteur à des descriptions de la modernité. Il s'agit, au contraire, d'une interrogation souvent dérangeante sur la puissance de forces économiques, parfois réellement criminelles, parfois simplement immorales, mais toujours plus débridées et destructrices : en un mot, « sauvages » (*rogue*). Ce que redoute Loretta Napoleoni, c'est en fait une mort de la politique, au profit d'un économisme sans frein et peu respectueux de l'homme. Certes, les criminologues ne se satisferont pas d'une charge aussi politique contre la globalisation et « l'État-marché ». Cependant, le tableau ici dépeint est suffisamment glaçant pour que l'on s'y arrête.

Parmi toutes les *rogue economics*, les contrefaçons occupent une place de choix comme l'expose également le livre de Pierre Delval et Guy Zilberstein : *La contrefaçon, un crime organisé*. Les auteurs rappellent que la contrefaçon ne touche plus seulement l'industrie



2008, Jean-Claude Gawsewitch, 180 p., 18,19 €

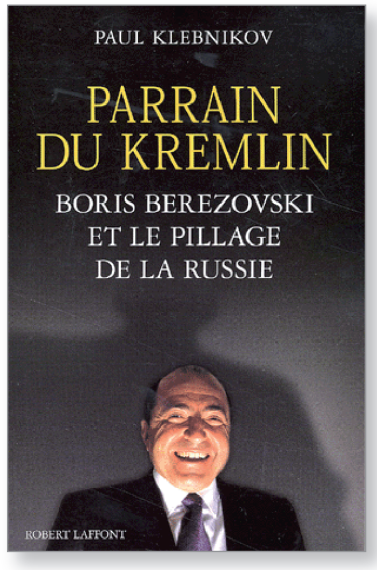
du luxe. En 2008, le marché du luxe ne représente que 8 % du chiffre d'affaires des contrefacteurs. Les contrefaçons s'attaquent aussi à des secteurs plus sensibles, car touchant directement la santé et la sécurité des consommateurs. Les cibles nouvelles de la contrefaçon se retrouvent par exemple dans les biens alimentaires, le cinéma, les médicaments ou les jouets. Désormais, les contrefaçons ne se contentent plus de supprimer des emplois (dans le luxe), elles tuent et blessent : alcool frelaté, faux médicaments et faux vaccins sans effets thérapeutiques, pièces détachées contrefaites provoquant des accidents, fausses cigarettes cancérigènes, etc. Ce secteur criminel en plein développement est très lucratif, puisque les auteurs évaluent son chiffre d'affaires à 500 milliards de dollars. La contrefaçon est une menace protéiforme : économique en supprimant des emplois ; sociale en favorisant le travail clandestin et le crime organisé ; intellectuelle en tuant l'innovation. Ce livre bref, clair et nourri d'exemples n'omet pas de rappeler que ce crime si moderne est souvent entre les mains de véritables organisations criminelles.

Cependant, derrière ces phénomènes de *rogue economics* se dissimulent des individus. L'un d'entre eux, le Russe Roman Abramovitch, vient de faire l'objet d'une courte biographie d'Alban Traquet : *Roman Abramovitch, Football, pétrole, pouvoir*. Né en 1966, très tôt orphelin, Roman Arkadievitch Abramovitch possède aujourd'hui la première fortune de Russie, estimée à 15,7 milliards de dollars en 2007 par le magazine *Forbes*. Cette réussite spectaculaire a débuté au début des années 1990, lors de l'effondrement de l'URSS, quand une petite caste d'hommes d'affaires et d'ex-apparatchiks s'approprie les entreprises nouvellement privatisées. Ce sera ni plus ni moins un grand hold-up.

Ce « capitalisme de bandits » donne alors naissance à d'immenses fortunes, détenues par quelques dizaines de personnages liés au pouvoir de Boris Eltsine. Une sociologue russe les appellera les « oligarques ». Roman Abramovitch est l'un d'eux. Il croît dans l'ombre de Boris Berezovski mais, à la différence de son mentor, en conservant un profil bas. Il saura ainsi ne pas s'aliéner le successeur de Boris Eltsine, Vladimir Poutine. Fortune faite dans le secteur de l'énergie et de l'acier, l'oligarque achète en 1993 le club de football de Chelsea (Angleterre). Puis, il se fait élire en 2000 gouverneur du district autonome de Tchoukotka, une région de l'extrême est russe, à 7 000 kilomètres de Moscou. On le voit désormais s'intéresser au marché de l'art et au monde du cinéma américain. Mais, ce parcours spectaculaire est plein de zones d'ombres que ce livre ne parvient pas à lever. Discret et silencieux, Roman Abramovitch sait que la respectabilité est une des clefs de la réussite. Il aime ainsi répéter cette devinette qui en dit long sur le personnage : « *Connaissez-vous la différence entre un rat et un hamster ? Pas de différence, juste une affaire de relations publiques* ».

2008, Les éditions du Toucan, 253 p., 17,00 €

Concernant son mentor Boris Berezovski, il convient de lire ou de relire un ouvrage important de Paul Klebnikov qui, au-delà de l'histoire de cet oligarque désormais réfugié à Londres, brosse un tableau passionnant de la Russie des années 1990 : *Parrain du Kremlin, Boris Berezovski et le pillage de la Russie*. Depuis, Paul Klebnikov est mort assassiné à Moscou...



2001, Robert Laffont, 386 p., 21,20 €

Violence et état faible : les femmes et les enfants d'abord

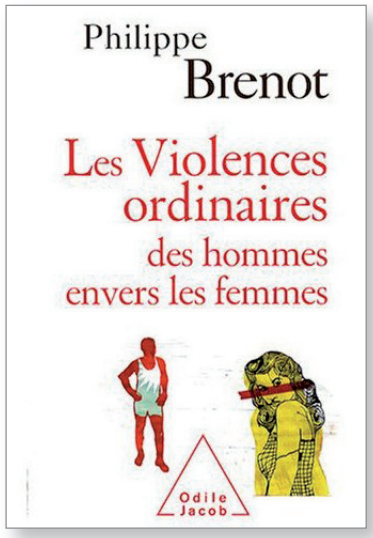
Comme nous l'avons déjà écrit précédemment [1], les violences faites aux femmes représentent un fléau social. Régulièrement, des études et des ouvrages en apportent la démonstration. Ainsi, l'Institut national d'études démographiques (INED) a publié, en mai 2008, une étude détaillant la montée des violences sexuelles en France. Cette vaste enquête sur les conduites sexuelles, menée

(1) *Les cahiers de la sécurité*, n° 4, avril-juin 2008.

auprès de 12 000 personnes en 2006, nous apprend que sur 100 femmes françaises âgées de 18 à 69 ans, 7 ont été violées ; et que 9 autres ont été victimes d'une tentative d'agression sexuelle. Entre 50 000 et 120 000 femmes auraient subi un rapport sexuel imposé ou une tentative durant la période étudiée, alors que seules 9 993 plaintes ont été déposées. Le « chiffre noir » des violences sexuelles est donc considérable.

Cependant, un sujet aussi important et délicat ne peut se satisfaire du seul regard, toujours froid, des enquêtes sociologiques et des études statistiques. La lecture du livre du médecin psychiatre Philippe Brenot, *Les violences ordinaires des hommes envers les femmes*, permet d'aborder ce thème sous un jour différent. Ce point de vue est celui d'un thérapeute dont le propos est à la fois clair et militant : « *Depuis plus de vingt ans, j'écoute des femmes, des hommes, des couples faire part de ce qui les déchire, les éloigne et les sépare. Certains hommes sont violents par névrose, par psychose, par mélancolie. Ils sont peu nombreux. Je dénonce plutôt la violence des hommes qui le sont par modèle, par habitude, par répétition, par ignorance, par aveuglement.* » Si Philippe Brenot se place résolument sous les auspices de la sociologie de Pierre Bourdieu, la « domination masculine », son propos est le fruit de ses longues observations de praticien. Son livre présente d'abord le mérite de disséquer le comportement violent des hommes. Il décrit ce qu'il nomme « *leur aveuglement congénital* », puis propose une typologie des différentes formes de violence exercées sur les femmes par : le physique, les mots, le silence, l'absence, la négligence, le désir, l'immobilisme et la résistance au changement. Après cette inquiétante typologie du « mal » masculin, comme diraient des Lacaniens, le médecin thérapeute se pose l'inévitable question : comment réagir à ces différentes formes d'agressions dans le couple ? Il conseille alors concrètement à ces femmes violentées une série de réponses adaptées, en les détaillant : ne pas réveiller, devant la force, la force ; ne pas réveiller, devant les mots, les mots ; ne pas opposer au silence, le silence ; ne pas opposer à la violence, la frustration ; ne pas opposer à la fuite, le harcèlement.

Philippe Brenot s'interroge ensuite sur les moyens d'enrayer la violence. Il lui semble indispensable de les dénoncer, et ce de différentes manières : les dire dans le couple ; refuser le silence ; oser dire non ; expliquer ; comprendre ; dialoguer. Il conseille également de les dépasser, en trois temps, par : la prise de conscience, l'accompagnement, et les thérapies. Paraphrasant Simone de Beauvoir, le thérapeute se dit convaincu que : « *on ne naît pas homme, on le devient* », sous-entendu, la violence des hommes est un apprentissage social. Il s'en explique longuement et de façon convaincante, sans tomber, loin de là, dans les travers à la mode prônant l'indifférenciation des sexes. Centré sur le couple et la psychologie, ce livre complète utilement des rapports officiels toujours impersonnels.

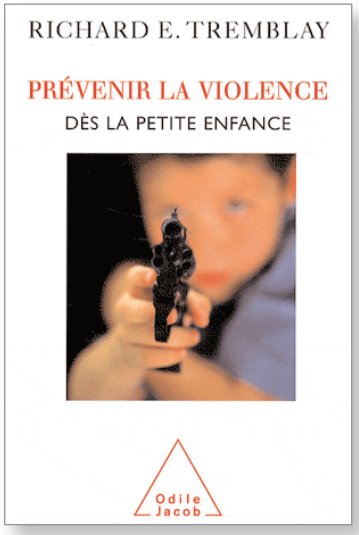


2008, Odile Jacob, 219 p., 19,90 €

Comment prévenir la délinquance des jeunes ? Cette question taraude la criminologie occidentale depuis l'explosion des chiffres de la criminalité et le développement des gangs urbains d'adolescents. Le professeur Richard E. Tremblay propose une réponse originale dans son livre, *Prévenir la délinquance dès la petite enfance*. Le cœur de sa thèse peut se résumer ainsi : les enfants n'apprennent pas à agresser par imitation de modèles vus à la maison, à l'école, dans la rue ou dans les médias. L'origine de la violence des adolescents se situe plus en amont, dans l'enfance. Les agressions physiques sont plus fréquentes avant la puberté qu'après la puberté. Les enfants qui sont sur une trajectoire d'agression physique élevée pendant l'adolescence étaient déjà sur cette trajectoire élevée au début des années d'école primaire. Les études à la petite enfance prouvent, selon lui, que la très grande majorité des êtres humains a eu recours à l'agression physique avant d'atteindre l'âge de 24 mois. Les études des trajectoires d'agression chronique permettent d'identifier des facteurs de risque pendant la grossesse qui caractérisent les familles à haut risque d'avoir un enfant situé sur une trajectoire d'agression physique chronique. Cependant, tant les gènes que l'environnement sont impliqués dans ces mécanismes d'agression. L'environnement facilite ou inhibe l'expression des gènes dès le début de la vie. Ces effets de l'environnement sur les gènes sont particulièrement importants pour le développement de la capacité de régulation des comportements d'agression. Le professeur Richard E. Tremblay remet donc en question les efforts de prévention de la délinquance en général et de la violence en particulier qui, depuis le XIX^{e} siècle, concentrent leurs efforts sur les adolescents. Il préconise des programmes de prévention centrés sur le soutien aux parents et aux enfants, depuis la grossesse jusqu'au début de l'école primaire. Il s'agit d'une

intervention ciblée dès la petite enfance consistant : d'une part, à déceler les troubles du comportement de l'enfant et les facteurs de risques chez les parents (âge, sexe, éducation, pauvreté), et d'autre part, à accompagner les familles et les enfants concernés. Selon le professeur Tremblay, tous les jeunes enfants utilisent spontanément l'agression physique à partir de la fin de la première année, mais la très grande majorité d'entre eux réduit la fréquence de leurs agressions après la troisième année, à mesure qu'ils apprennent des conduites alternatives à la violence. Les mécanismes impliqués dans ces apprentissages sont complexes : maturation du cerveau (développement du langage, régulation des émotions), réaction des victimes et des adultes, expérience de la douleur physique, apprentissage de l'agression indirecte, et capacité à transformer les gestes d'agression en activités ludiques. Plaçant donc l'origine de la violence des adolescents dès la prime enfance, le professeur Tremblay s'inscrit en faux contre l'idée répandue de l'effet criminogène des médias :

« *L'idée que les jeunes apprennent à être violents par consommation d'œuvres de fiction à contenu agressif ou par pratique de jeux de combat (réels ou électroniques) s'appuie sur la théorie de l'apprentissage social de l'agression. Mais il est difficile de défendre cette idée une fois qu'on a constaté que la fréquence des agressions physiques est à son maximum au début de la vie et qu'elle diminue avec l'âge, alors que la consommation d'œuvres de fiction à contenu agressif ou de jeux de combat augmente avec l'âge. Il est fort possible que les jeux qui simulent la violence (jeux de combat, sports, théâtre, romans, cinéma, jeux vidéos) jouent un rôle important dans notre apprentissage des moyens de vivre sans violence aussi bien que dans le soutien de notre capacité à utiliser la violence quand elle est nécessaire. Les recherches sur le sujet tentent de démontrer les effets négatifs de la fiction*



2008, Odile Jacob, 269 p., 25,00 €

à contenu violent. On gagnerait à étudier sérieusement l'idée que la fiction à contenu violent puisse avoir des effets bénéfiques pour la majorité d'entre nous, même si elle est nuisible à une minorité. » Le professeur Tremblay nie ainsi l'influence des contenus violents des médias (télévision, cinéma, Internet) au moyen d'un argument discutable. Selon lui, l'usage à haute dose de produits de grande consommation à forts contenus violents ne s'est pas accompagné d'une hausse proportionnelle à la violence des mineurs. Il en tire donc pour conséquence que cette violence adolescente doit trouver ses origines ailleurs et en amont. On pourrait contester aisément ce propos. Le professeur Tremblay s'appuie sur l'idée popularisée par Norbert Elias dans *La Civilisation des mœurs*. Cependant, cette pacification séculaire des mœurs connaît depuis plusieurs décennies, en Occident, une involution indiscutable qui n'est pas le fruit d'un effet de loupe politique, médiatique ou statistique. De même, le professeur Tremblay balaie, un peu rapidement semble-t-il, les travaux ayant permis de réfuter les prétendus effets cathartiques de la violence médiatique. La Commission Kriegel (2002) sur « La violence à la télévision » avait été claire à ce sujet.

On reconnaîtra probablement, dans ce bref exposé du livre du professeur Tremblay, une partie des idées contenues dans le rapport de l'Institut national de la santé et de la recherche médicale (Inserm) qui, en 2005, suscita une vive controverse : *Expertise collective. Trouble des conduites chez l'enfant et l'adolescent* (Les éditions Inserm, 2005). Le professeur Tremblay participa, en effet, au comité d'experts de l'Inserm sur les troubles des conduites. D'ailleurs, dans une postface, le professeur Tremblay revient longuement sur la polémique que le rapport de l'Inserm provoqua.

Le grief principal contre le rapport collectif de l'Inserm, et donc contre le livre du professeur Tremblay, a été résumé récemment dans Le Monde (mai 2008) par le professeur de psychanalyse et de psychopathologie Roland Gori : « [Or], *en s'éloignant du soin, la santé mentale utilise des indicateurs extrêmement hybrides. Ainsi de l'expertise collective de l'Inserm (2005) qui préconisait le dépistage systématique du "trouble des conduites" chez le très jeune enfant pour prévenir la délinquance : elle mélangeait des éléments médicaux, des signes de souffrance psychique, des indicateurs sociaux et économiques, voire politiques. On aboutit ni plus ni moins, sous couvert de science, à une véritable stigmatisation des populations les plus défavorisées. Ce qui en retour naturalise les inégalités sociales.* »

Quoi qu'il en soit, le livre du professeur Tremblay mérite d'être lu et critiqué. Son point de vue est suffisamment original pour qu'il fasse l'objet de discussions. On peut d'ailleurs s'étonner, à l'aune de la polémique de 2005, que ce livre n'ait pas suscité depuis sa sortie de réactions plus nombreuses.

Jean-François GAYRAUD
Chargé de mission, INHES

NOTES DE LECTURE

JOURNEES EUROPEENNES
EUROPEAN DAYS

Compte rendu des XVe journées européennes des représentants territoriaux de l'État

29 - 31 mai 2008 - Venise

Avec la participation de :

Miguel ALEJO VICENTE, Delegado del gobierno de España en Castilla y Leòn ESPAGNE
Francisco ALVAREZ MARTINEZ, Subdelegado del Gobierno de España en Leòn ESPAGNE
Barbara ANDRACCHIO, Staff - ANFACI ITALIE
Hans ANGERER, Regierungspräsident von Oberfranken ALLEMAGNE
Thierry AUMONIER, Administrateur délégué AERTE
Svein BERBU, Deputy Director General - Ministry of Government Administration and Reform NORVEGE
Migle BERNOTIENE, Adviser of the Government Office LITUANIE
Yvan BLOT, Inspecteur général de l'administration - Ministère de l'Intérieur FRANCE
Jean-Michel BRUNEAU, Sous-préfet de Lisieux FRANCE
Stuart BURGESS, Chairman and Rural Advocate - Commission for Rural Communities ROYAUME-UNI
Marc CABANE, Préfet des Pyrénées-Atlantiques FRANCE
Daniel CANEPA, Préfet de la région Nord-Pas-de-Calais, président de l'association du corps préfectoral FRANCE
Solange CARMONA, Secrétaire générale, AERTE
Gabriella CASACCIO, Vice prefetto aggiunto - ANFACI ITALIE
Andreas CHRISTODOULIDES, District Officer of Paphos CHYPRE
Teresa CIMADEVILLA MARTINEZ, Asesora del Delegado del Gobierno - Leòn ESPAGNE
Lodewijk DE WITTE, Gouverneur - Province Vlaams-Brabant BELGIQUE
Aimée DUBOS, Sous-préfète d'Argenteuil FRANCE
Danièle EVEN, Chef du secrétariat permanent - Association du corps préfectoral FRANCE
Daniel FEREY, Préfet de la Creuse FRANCE
Andrea FERRAZZI, Vice-presidente - Province di Venezia ITALIE
Michel FORET, Gouverneur - Province de Liège BELGIQUE
Imre FORGACS, Head of Central Hungarian Regional Public Administration Office HONGRIE
Giancarlo GALAN, Presidente - Regione Veneto ITALIE
Graham GARBUTT, Chief Executive - Commission for Rural Communities ROYAUME-UNI
Rafaella GISSI, Staff - ANFACI ITALIE
Anne HAUDRY de SOUCY, Conseillère Europe - Caisse des Dépôts et Consignations FRANCE
Christoph HILLENBRAND, District President of Upper Bavaria ALLEMAGNE
Alain LARANGE, Inspecteur général de l'Administration - Ministère de l'Intérieur FRANCE
François-Gilles LE THEULE, Directeur du Centre des études européennes de Strasbourg - ENA FRANCE
Sven LINDGREN, Governor - Kalmar County SUEDE
Hanja MAIJ-WEGGEN, Her Majesty's Governor in the province of Noord-Brabant HOLLANDE
Pascal MAILHOS, Préfet, secrétaire général adjoint, directeur de la modernisation et de l'action territoriale - Ministère de l'Intérieur FRANCE

Association Européenne de Représentants Territoriaux de l'État
Association sans but lucratif selon la loi belge du 27 Juin 1921

Secrétariat Général des Journées européennes : 8, rue Fallempin, 75015 Paris – France
Tel: +33(0)1 45 78 36 17 – Fax: +33 (0)1 45 77 69 65
www.journees.europeennes.org

Claudio MEOLI, Prefetto ITALIE
Juan-Antonio MOLL GOMILA, Jefe Area Extranjeria – Ministerio de administraciones publicas ESPAGNE
Mario MORCONE, Prefetto – presidente – ANFACI ITALIE
Alexandre MOUTON, Chargé d'études, INHES FRANCE
Guido NARDONE, Prefetto di Venezia ITALIE
Hans NEUHOFER, Professor, University of Vienna AUTRICHE
Jacques NICOD, Préfet du District de Lausanne – Canton de Vaud SUISSE
Kari NORDHEIM-LARSEN, County Governor of Telemark NORVEGE
Rasa NOREIKIENE, Undersecretary – Ministry of the Interior LITUANIE
Olga PALACIO GARCIA, Jefa del Gabinete del Delegado del Gobierno en Castilla y Leòn ESPAGNE
Véronique PAULUS de CHATELET, Gouverneur de Bruxelles BELGIQUE
Michele PENTA, Prefetto, segretario generale, ANFACI ITALIE
José Luis PEREZ BECARES, Coordinator de Area – Ministerio de Administraciones Publicas ESPAGNE
Agnès PINAULT, Sous-préfète de Morlaix FRANCE
Ignazio PORTELLI, Vice prefetto, vice segredario nazionale ANFACI, ITALIE
Raoul PRADO, Directeur – DG Regio COMMISSION EUROPEENNE
Roberta PREZIOTTI, Vice prefetto – ANFACI ITALIE
Jean-Marc REBIERE, Préfet de la région Alsace FRANCE
Juan Antonio REDONDO PARRAL, Jefe de la Unidad de Relacioners Institucionales – Ministerio de Administraciones Publicas ESPAGNE
Charles RICQ-CHAPPUIS, Professeur, COER SUISSE
Luis Carmelo RINCON MIRANDA, Jefe de prensa de la delegacion del Gobierno de España en Castilla y Leòn ESPAGNE
Hans J. RØSJORDE, Governor – County of Oslo and Akershus NORVÈGE
Graham RUSSELL, Director – Commission for Rural Communities ROYAUME-UNI
Serge SANDT, Commissaire du district de Grevenmacher LUXEMBOURG
Frank SCHERER, Regierungsvizepräsident von Freiburg ALLEMAGNE
Alvydas SEDZIUS, Governor of Siauliai County LITUANIE
Michela SIGNORINI, Vice prefetto – ANFACI ITALIE
Lars SILSETH, Senior advisor – Ministry of Government Administration and Reform NORVEGE
Eino SIURUAINEN, Governor – Province Office of Oulu FINLANDE
Paulius SKARDZIUS, Director of public administration department – Ministry of the Interior LITUANIE
Perla STANCARI, Prefetto ITALIE
Jean-Claude VACHER, Préfet du Maine-et-Loire FRANCE
Michele VIANELLO, Vice sindaco di Venezia Italie
Luc VILAIN, Sous-préfet de Saint-Julien en Genevois FRANCE
Jacques-André VULLIET, Secrétaire général – IDHEAP SUISSE
Bernard ZAHRA, Directeur – IRA de Bastia FRANCE
Janusz ZALESKI, President of the board – Wroclaw Regional Development Agency POLOGNE

Les 29, 30 et 31 mai 2008 se sont tenues à Venise les XVe journées européennes des représentants territoriaux de l'État (JERTE). Cette année, le thème en était « le rôle du représentant territorial de l'État (RTE) dans l'intégration européenne ». Accueillis sur l'île de San Servolo par Guido Nardone, préfet de Venise, Andrea Ferrazzi, vice-président de la Province de Venise, Michele Vianello, maire adjoint de Venise, Mario Morcone, préfet et président de l'ANFACI et Michele Penta, secrétaire général de l'ANFACI, les participants ont pu se livrer à des échanges riches d'enseignement.

Trois intervenants représentaient la France : Jean-Claude Vacher, préfet du Maine-et-Loire, Jean-Marc Rebière, préfet de la région Alsace et vice-président de l'Association française du corps préfectoral, et Marc Cabane, préfet des Pyrénées-Atlantiques. La délégation française, comprenait entre autres Thierry Aumonier, administrateur délégué de l'Association européenne de représentants territoriaux de l'État (AERTE), Daniel Canepa, préfet de la région Nord-Pas-de-Calais, président de l'Association française du Corps préfectoral, et Solange Carmona, secrétaire générale de l'AERTE.

Les interventions ont eu pour thèmes :

- le RTE dans l'application de la réglementation européenne au travers de l'exemple de l'environnement,
- le RTE et les fonds européens,
- le RTE dans la coopération transfrontalière.

Au préalable, Michele Penta a présenté le rôle du préfet en Italie. La fonction publique italienne a en effet été l'objet, au cours des quinze dernières années, de nombreuses réformes, marquant une nouvelle étape dans les relations entre les pouvoirs publics et leurs usagers. Les citoyens sont ainsi devenus acteurs à part entière du service public à l'exécution duquel ils participent désormais. Ce mouvement s'est accompagné d'une décentralisation accrue de la décision publique. À la fois garant de la cohésion sociale, institutionnelle et territoriale, le préfet a été au cœur de ces réformes. Les récentes lois, notamment celles de 2004, ont ainsi redéfini son rôle, mettant l'accent sur ses fonctions de coordinateur des activités des antennes de l'État sur le territoire dont il a la responsabilité.

Interlocuteur de l'ensemble des administrations locales et, de plus en plus, de la société civile, ses fonctions vont bien au-delà de celles, traditionnelles, de garant de la légalité et de l'ordre public. Il est ainsi à la fois le médiateur de l'ensemble des conflits et le promoteur d'une certaine idée du droit, dont il veille aussi à la bonne exécution. Ces multiples attributions, dont toutes n'ont pas été formalisées par écrit, s'accompagnent chez le préfet d'une connaissance fine de sa circonscription. Attentif aux besoins émergents, soucieux de servir au mieux les intérêts du citoyen, le préfet contribue ainsi à garantir à la fois l'unité d'action de l'État et de l'Union européenne (UE).

Le RTE et l'environnement

Quelle place pour le représentant territorial de l'État dans l'application de la réglementation européenne ? Cette interrogation, l'AERTE avait, cette année, décidé de la soumettre aux intervenants au travers de l'exemple de l'environnement. Par nature transverses, ces questions ne connaissent en effet pas davantage de frontières administratives qu'elles n'en ont de géographiques. Le rôle du RTE dans le respect des normes relatives à la protection de l'environnement, dont l'UE a fait l'un de ses principaux objectifs, sa place dans l'application du programme « *Natura 2000* », constituaient la trame des interventions de cette première demi-journée. Les débats se sont déroulés sous la présidence de Hanja Maij-Weggen, commissaire de la Reine – province du Nord Brabant (Pays-Bas).

Christoph Hillenbrand, *Regierungspräsident* de Haute-Bavière (Allemagne) a exposé quelques-unes des actions entreprises dans sa région en faveur de l'environnement. Avec une superficie de 17 529 Km², la Haute Bavière est la région la plus étendue de la République fédérale d'Allemagne. Ses 4,2 millions d'habitants en font la troisième plus peuplée. Le cadre juridique en matière de qualité de l'air repose à la fois sur la réglementation européenne, entre autres la directive 96/62/EC, et sur la législation nationale. Trois villes de la Haute Bavière sont tout particulièrement concernées par ces réglementations : Munich, Ingolstadt et Burghausen.

La directive européenne fixe à la fois des seuils en matière de pollution de l'air et un maximum autorisé de dépassements de ces seuils par an. Ces limites étaient au départ très peu respectées. Un premier plan d'action intitulé « *Qualité de l'air* » a donc été mis en œuvre le 20 décembre 2004 à Munich. Ce plan prévoyait, entre autres, des mesures concernant les installations industrielles (systèmes de chauffage, centrales d'énergie...) et comportait un certain nombre de dispositions destinées à mieux gérer le trafic routier : meilleure gestion des parcs de stationnement, promotion des transports publics ou des véhicules écologiques au sein de l'administration municipale... Les mesures prises ont cependant rapidement

révélé leurs limites. Les autorités de Haute-Bavière ont, par conséquent, adapté leur stratégie. Celle-ci s'est déclinée en trois étapes. Premièrement, l'interdiction des camions de transit supérieur à 3,5 tonnes dans Munich et leur déviation ont permis d'éviter la circulation dans la ville de tous les poids lourds qui n'avaient pas celle-ci pour destination finale. Deuxièmement, une « Zone environnementale » a vu le jour, dont l'objectif était de réduire le taux d'émission des gaz polluants à l'intérieur de la « Middle Ring Highway ». Le troisième volet a consisté à sensibiliser plus largement l'ensemble des acteurs locaux aux questions liées à la qualité de l'air.

La nécessité de prévoir des voies de contournement était en effet devenue une priorité pour les autorités. Munich est un point nodal au sud du réseau européen d'autoroutes longues distances. L'important flux de marchandises en provenance ou à destination de la France, l'Espagne, l'Autriche et la Suisse (partie occidentale) transitait auparavant par Munich. Ce flux est à présent détourné. Une amende a été instituée pour les contrevenants, s'élevant à vingt euros. Son effet dissuasif réside cependant moins dans son montant que dans le temps d'immobilisation du véhicule nécessaire aux contrôles. Ces mesures ont prouvé leur efficacité. L'autoroute de la *Middle Ring* est largement moins empruntée par les poids lourds qu'elle ne l'était avant. Elles ont également permis la réalisation d'une « Zone environnementale » qui consiste à interdire l'accès du centre-ville de Munich aux véhicules particulièrement polluants, quel que soit, par ailleurs, leur gabarit. Ainsi, en application des normes européennes, les véhicules automobiles devront indiquer le groupe d'émission de polluants auxquels ils appartiennent. Divisés en quatre groupes différents, les véhicules du premier groupe ne pourront plus circuler dans la zone protégée. La troisième étape a consisté à étendre les zones concernées par le plan « Qualité de l'air ». Ceci implique notamment que les comtés fédéraux voisins soient sensibilisés à ces questions et s'engagent à améliorer leur situation. L'ensemble de ces actions feront l'objet d'une évaluation en 2009 et 2010.

Hans Neuhofer, professeur à l'université de Vienne, axe son intervention sur une présentation de la répartition des compétences en Autriche concernant la protection de l'environnement rappelant que la norme européenne est soit directement applicable en droit interne, soit doit faire l'objet de mesures de transposition, il explique qu'en Autriche, c'est aux autorités fédérales ou aux *Länder* qu'il revient d'en assurer la transposition, selon les domaines concernés. L'intervenant souligne ensuite l'importance de la question de l'environnement, à la fois pour l'UE, dont la réglementation en la matière, réunie en un CODEX, dépasse les mille pages, et pour les autorités autrichiennes. Dans ce pays, la protection de l'environnement fait en effet partie des normes constitutionnelles. Hans Neuhofer précise dans son propos liminaire que, en Autriche comme en Allemagne, ces questions sont sensibles et suscitent bien souvent des réactions vives de la part de l'opinion publique.

La loi fédérale constitutionnelle fait obligation aux neuf *Länder* de la République fédérale d'Autriche et à ses 2 358 municipalités de veiller à la protection et à la préservation de l'environnement, notamment de la qualité de l'air, de l'eau et des sols. Les compétences en matière d'environnement y sont partagées entre les autorités fédérales, les *Länder* et les municipalités. Conformément aux dispositions contenues dans la constitution fédérale, la Fédération exerce, dans ce domaine, une compétence générale touchant notamment aux activités industrielles et minières, aux transports, à la protection de l'eau et de l'air, à la gestion des déchets dangereux... L'Office fédéral de protection de l'environnement publie régulièrement ses conclusions.

Les compétences dévolues en ce domaine aux *Länder* sont moins étendues que celles de la Fédération. Elles n'en demeurent pas moins importantes. Ainsi interviennent-ils directement sur les questions tenant à l'aménagement du territoire, à la protection des sols, de la nature et à la préservation des paysages, à l'approvisionnement en eau, à la gestion des eaux usées, au traitement des déchets ménagers... Les *Länder* ont également compétence en matière d'énergie et traitent de questions liées à l'électricité, aux politiques d'économie d'énergie, aux installations industrielles polluantes... Ils interviennent, à ce titre, dans le domaine de la recherche et sont très impliqués dans la promotion des énergies alternatives et non polluantes.

Enfin, les municipalités exercent aussi de nombreuses missions dans ce domaine : aménagement local du territoire, police des bâtiments, réglementation incendie, approvisionnement en eau, transports et traitement des déchets et des eaux usées... Elles interviennent notamment en matière de tri sélectif. Sans aller jusqu'à faire œuvre de jurislateur, elles peuvent, si la situation l'exige, édicter des règlements de police dans ces divers domaines. Les collectivités locales ont également pour mission de responsabiliser et tenir informés leurs administrés.

Quoique non-membre de l'UE, l'exemple de la Norvège est cependant intéressant à plusieurs égards. Il illustre d'une certaine façon ce que peut être l'effet d'entraînement de l'UE sur son entourage immédiat. Les autorités norvégiennes, a indiqué Hans Røsjorde, gouverneur du Comté d'Oslo et d'Akershus, sont en effet particulièrement

attentives aux questions liées à l'environnement. Parce que ces questions ne connaissent par définition pas de frontières, la Norvège veille à la convergence des politiques qu'elle initie dans ce domaine et des politiques européennes. L'attention qu'elle y porte se traduit par une réglementation nombreuse, comportant à ce jour près de deux cent cinquante actes juridiques. Ces dispositions sont généralement prises au niveau national.

En tant que relais entre le pouvoir central et les collectivités locales, les gouverneurs de région assurent l'exécution des politiques nationales. Ils sont également chargés du contrôle de légalité dans leur circonscription. Par conséquent, ils jouent un rôle essentiel en matière d'environnement. Ainsi, pour ne citer que quelques exemples, les gouverneurs de Norvège délivrent les autorisations aux entreprises industrielles et en contrôlent l'activité. Ils veillent à la bonne gestion des équipements et des infrastructures routières. Ils sont également responsables de la protection des espaces agricoles, ou de la gestion des eaux et des ressources en eaux... D'une façon plus générale, ils sont garants de la protection de l'environnement et de la sécurité du citoyen (prévention des pollutions diverses, santé, mais aussi développement durable et changements climatiques par exemple).

Hans Røsjorde évoque ensuite le cas des directives européennes sur la biodiversité. La Norvège ne fait en effet pas parti du réseau « Natura 2000 » mis en place par l'UE. Cela n'empêche pas que la Norvège suive l'exemple de ce dispositif dans ce qu'il offre de meilleur et participe aux indicateurs de la biodiversité fixés par l'UE pour l'année 2010. La Norvège est par ailleurs associée aux actions de l'Agence européenne pour l'environnement. Enfin, elle met en œuvre d'autres approches stratégiques telles que le réseau « Émeraude » par exemple, en application de la convention de Bernes.

C'est ensuite au tour de Jean-Claude Vacher, préfet français du département du Maine-et-Loire, de rappeler tout d'abord brièvement ce que sont les compétences du représentant territorial de l'État en France. Celui-ci a pour mission d'appliquer les lois votées par le Parlement et de veiller à leur respect par les autorités locales. Dans le domaine de l'environnement, cette compétence se traduit par l'examen de très nombreuses décisions prises par les administrations locales. Il s'assure ainsi de la conformité de celles-ci non seulement avec la législation strictement française mais aussi, et peut-être prioritairement, avec la réglementation internationale, en particulier européenne. Le préfet du Maine-et-Loire présente ensuite trois exemples en matière d'environnement.

Le premier est relatif à l'application de la directive SEVESO sur les installations industrielles présentant potentiellement, soit en raison des matières utilisées, soit en raison de leurs productions, de graves dangers pour les populations et pour l'environnement. Cette réglementation SEVESO a été modifiée et précisée de nombreuses fois, tant au plan européen que national d'ailleurs. Comment le préfet remplit-il son rôle dans ce domaine ? Comment peut-il, par exemple, autoriser ou refuser l'extension ou la création de telle ou telle entreprise ? Le préfet doit tout d'abord ici pouvoir compter sur l'entreprise elle-même dont il attend qu'elle participe au processus d'autorisation. Ainsi, celle-ci doit-elle réaliser les études d'impact et de danger préalables, montrer que les plans d'intervention ont été prévus aussi bien à l'intérieur de l'entreprise qu'à l'extérieur, pour les populations riveraines par exemple. D'une manière plus générale, le préfet exerce un contrôle de légalité. Il veille par conséquent à ce que les décisions prises par toutes autorités administratives locales soient conformes au droit en vigueur. De fait, si le permis de construire relève de la compétence du maire, le préfet doit s'assurer qu'il respecte la législation en termes de sécurité environnementale, par exemple concernant le respect des distances minimales imposées entre les sites industriels concernés et les habitations les plus proches. Le préfet a par ailleurs pour tâche de faciliter la connaissance par le public, les usagers, les associations... des produits fabriqués dans ces entreprises et des mesures de protection prises pour assurer leur sécurité. Il s'appuie, pour l'exécution de cette mission d'information, sur les Commissions locales d'information et de contrôle (CLIC), composées à proportion égale de représentants d'associations, d'élus et d'administrations diverses de l'État. Ces CLIC ont un rôle très important, notamment pour éviter que ne se répandent des rumeurs ou de fausses informations.

Le deuxième exemple porte sur le traitement des eaux résiduaires urbaines. Une réglementation européenne fournie, dont les premières directives datent de 1991, faisait obligation aux États membres, selon un calendrier échelonné jusqu'en 2005, de s'assurer que les eaux retournant à la nature répondent à certaines prescriptions, en particulier quant à leur teneur en phosphore et en nitrate. Or, la France a récemment été condamnée par la Cour de justice des communautés européennes (CJCE) pour ne pas avoir été suffisamment diligente dans la mise en œuvre de ces directives. Le gouvernement français a par conséquent donné instruction aux préfets afin que les autorités locales accélèrent la mise aux normes des stations de traitement des eaux polluées des villes et agglomérations. Dans le département du Maine-et-Loire, Jean-Claude Vacher aura ainsi dû prendre des décisions obligeant sept villes de plus de dix mille habitants à se

conformer selon un calendrier précis, à l'obligation qui leur est faite de moderniser leurs installations d'épuration. L'objectif assigné aux préfets ici est de répondre, avant la fin de l'année 2008, aux prescriptions fixées par l'UE en la matière.

Le troisième et dernier exemple porte sur la directive concernant la réduction des gaz à effets de serre. Cette directive, issue du protocole de Kyoto (1997), encourage le recours aux énergies propres et renouvelables. Elle fait par ailleurs obligation aux États membres d'augmenter la part d'énergie électrique produite par ces sources nouvelles dans les dix prochaines années. La France s'est conformée aux prescriptions européennes d'une double façon. Elle a d'abord obligé l'entreprise publique EDF, avant l'ouverture du marché de l'électricité à la concurrence, à acheter plus chers les kilowatts produits par ses sources d'énergie propres dans le but d'inciter des projets alternatifs à voir le jour. De plus, une législation française récente fait du préfet l'autorité décisionnaire en matière de schémas éoliens. Il est, de fait, l'autorité d'agrément dans le département des schémas de développement éolien qui lui sont présentés par les autorités locales. Non seulement le préfet peut-il refuser d'entériner le projet, mais il peut en demander la modification. Par ailleurs, si ce schéma n'est pas de la compétence directe du RTE, c'est lui qui en délivre les permis de construire. Dans le département du Maine-et-Loire, les services préfectoraux ont accompagné les procédures en cours de la rédaction d'un cahier des bonnes pratiques de l'éolien. Celles-ci prennent notamment en compte l'existence de sites paysagers protégés, souvent par d'autres règles elles-mêmes européennes, telles que celles posées par « Natura 2000 », ou internationales, concernant la vallée de la Loire par exemple. Ce cahier des bonnes pratiques constitue un outil précieux pour le préfet du Maine-et-Loire et les collectivités locales dans leurs réflexions sur le sujet. Cette collaboration en amont des projets permet d'en assurer le succès. Depuis 2006, Jean-Claude Vacher a ainsi été amené à prendre quatre décisions d'autorisation et un seul refus.

Pour finir, de nombreux participants ont exprimé leur désarroi face à une réglementation européenne qui, en matière d'environnement, peut parfois avoir pour effet de bloquer de nombreux projets. Une certaine insécurité juridique semble en effet régner dans ce domaine. Ainsi, Christoph Hillenbrand signale qu'il faut, en Allemagne, parfois trente ans pour réaliser certaines infrastructures routières. De même, le préfet du Maine-et-Loire évoque-t-il le cas des aéroports internationaux en France pour lesquels les délais sont aussi longs. Ces projets de longue haleine s'accommodent parfois mal d'une réglementation environnementale évolutive qui peut compromettre leur réalisation. Janusz Zaleski, président de l'Agence de développement régional, Wroclaw (Pologne), dénonce les effets inhibant de ces réglementations vis-à-vis des investisseurs, qui hésitent désormais à se lancer dans de grands projets qu'ils ne sont pas certains de pouvoir mener à terme.

Deux autres points appellent quelques remarques. D'une part, Janusz Zaleski souligne les effets parfois pervers de certaines réglementations qui, par souci d'exhaustivité, finissent par être en contrariété avec le droit national. Ainsi, des zones géographiques non protégées en Pologne sont concernées par « Natura 2000 », rendant, du même coup, irréalisables certains projets pourtant en cours d'élaboration. Inversement, certaines zones protégées par la législation nationale ne figurant pas dans le schéma défini par « Natura 2000 », une incertitude pèse désormais sur leur avenir. D'autre part, de nombreux intervenants, notamment français et allemands, ont convenu que l'environnement était devenu un sujet politiquement très sensible et chargé d'émotions, obligeant les RTE à davantage de vigilance et de prudence encore.

Le RTE et les fonds européens

Si les fonds européens ont, quel que soit le pays, généralement la même destination et sont liés au développement économique et social des régions les moins avancées, leur gestion présente, suivant les cas, des particularités. Ce sont ces particularités, agrémentées d'exemples concrets et nombreux, que les intervenants de cette seconde demi-journée ont exposées. Celle-ci aura également été l'occasion pour Raoul Prado, directeur général à la Commission européenne en charge de la gestion des fonds structurels européens pour le Portugal, l'Espagne, l'Italie et Malte, d'exposer le point de vue de l'UE sur cette question. Au-delà des aspects strictement techniques et financiers, il s'agissait aussi de réfléchir aux outils concrets dont l'UE dote les RTE pour favoriser l'efficacité de leurs actions, ainsi que l'a souligné le président de séance, Graham Garbutt, président de la Commission pour les communautés rurales (Grande-Bretagne).

Rasa Noreikiene, secrétaire d'État au ministère de l'Intérieur lituanien est intervenue tout d'abord pour présenter l'usage qui est fait des fonds structurels européens dans son pays. En Lituanie, comme dans la plupart des États européens à forte culture centralisatrice, ce sont les RTE qui administrent les fonds européens. Dans la mesure

où ces fonds sont utilisés pour le développement socio-économique local et régional, ils viennent s'ajouter aux dispositifs nationaux et, de fait, supposent nécessairement pour leur mise en œuvre un rapprochement des administrations locales et centrales, notamment entre gouverneurs de comtés et municipalités. En Lituanie, les fonds européens permettent d'assurer une certaine péréquation du territoire. Ils contribuent ainsi non seulement à réduire les écarts entre régions, mais aussi, au sein d'une même région, entre les villes et les campagnes. De fait, outre les effets immédiats de ces fonds, ils créent les conditions de multiples partenariats locaux, aussi bien pour ce qui concerne la gestion des projets que pour la définition des besoins et des attentes qui ont prévalu à leur lancement.

S'agissant de la mise en œuvre de ces projets, le Fonds européen de développement régional (FEDER) contient un document stratégique principal destiné à orienter la mise en œuvre des politiques nationales au niveau des comtés. Il précise les utilisations possibles de ces fonds au niveau régional. Un projet de plan régional contenant des propositions d'actions est rédigé par l'administration du gouverneur du comté et approuvé par le conseil régional. Le pilotage de l'emploi des fonds est assuré par le Conseil de développement régional. Celui-ci comprend le gouverneur, qui en assure la présidence, les maires des municipalités concernées et des membres délégués par leurs conseils municipaux. Les RTE administrent ces fonds au seul bénéfice des régions. Ils contribuent ainsi à consolider et encourager le développement régional en même temps qu'ils permettent de résoudre les difficultés dans les zones les plus défavorisées. La Lituanie est l'un des grands bénéficiaires de ces fonds. Le FEDER totalise pour la période 2007-2013 près de 6,7 milliards d'euros dans ce seul pays, ce qui correspond au budget annuel de l'État lituanien.

Le cas italien, présenté par Roberta Preziotti, sous-préfète au département pour les libertés civiles et l'immigration au ministère de l'Intérieur (Italie), est souvent cité comme exemple par l'UE. Les autorités italiennes affectent une quote-part importante des ressources provenant des communautés européennes au développement économique et social des régions les plus en retard par rapport à la moyenne européenne. De fait, depuis le milieu des années 1990, le gouvernement italien a procédé au lancement d'une série de programmes nationaux et régionaux pilotés par les administrations centrales et locales.

Parmi ceux-ci, l'intervenant italien a notamment cité le Programme opératif national (PON) Sécurité pour le développement/Objectif de convergence (PON-Sécurité), couvrant la période 2007-2013 et confié pour sa réalisation au ministère de l'Intérieur. D'un montant total de près de 1,158 milliard d'euros, ses financements sont à la fois nationaux et européens. Ces derniers se répartissent en deux catégories : la première, comprenant les investissements productifs essentiellement affectés à la réalisation d'infrastructures lourdes, soit près de 90 % du total, relève du Fonds européen de développement régional. La seconde, regroupant les financements couvrant les coûts liés à la production normative et aux actions de formation, soit environ 10 % du total des montants alloués, relève pour sa part, du Fond social européen.

La particularité de l'approche italienne tient à son caractère fortement intégré. Le PON-Sécurité a ainsi pour territoire d'application quatre des régions italiennes les plus pauvres, à savoir la Campanie, la Calabre, les Pouilles et la Sicile. Ces régions connaissent, en effet, un retard structurel du double point de vue économique et social pour d'évidentes raisons tenant à leur histoire, leur culture, leurs caractéristiques sociales, leur criminalité et, phénomène plus récent, les flux migratoires dont elles constituent sinon la destination finale, du moins un point de passage important.

Les interventions du PON-Sécurité touchent à de nombreux domaines (construction d'infrastructures, développement des réseaux de communication, formation...). L'objectif est d'assurer la sécurité au sens large des territoires visés afin d'en faciliter le développement économique. Le ministère de l'Intérieur y tient, par conséquent, un rôle d'impulsion central. Il concourt également à la constitution d'un partenariat socio-économique fort. En sa qualité de RTE, le préfet exerce une compétence générale. Il est chargé de coordonner les actions de l'ensemble des administrations concernées par le PON-Sécurité et de veiller à ce qu'elles intègrent, dans leur application, les contraintes locales. Le PON-Sécurité contient, par ailleurs, un important volet relatif à l'immigration, touchant à la sécurité, l'accueil et l'intégration des populations immigrées.

Si la cohérence des actions entre elles est essentielle, l'intervenant italien a également insisté sur la nécessité de veiller à leur bonne articulation avec les autres actions européennes entreprises dans ce domaine et notamment celles du Fond européen pour les réfugiés tendant à soutenir et promouvoir les actions des États membres en matière d'accueil des réfugiés demandant l'asile, du Fond européen pour le rapatriement, contribuant à l'amélioration de la gestion des rapatriements dans le respect des droits fondamentaux de la personne, du Fond européen pour l'intégration de citoyens de pays tiers et du Fond pour les frontières extérieures.

Le préfet français de la région Alsace, vice-président de l'association du corps préfectoral, s'est ensuite exprimé, soulignant le rôle majeur, en France, des RTE dans la déclinaison des politiques européennes. En effet, ils n'en constituent pas seulement les relais indispensables, ils en sont aussi les véritables promoteurs. Cette promotion, l'Europe en a d'autant plus besoin qu'elle connaît un déficit de légitimité auprès des citoyens européens. Les fonds européens sont, dans cette optique, de précieux outils sur lesquels ils peuvent s'appuyer. Ces fonds constituent par ailleurs un moyen privilégié pour accompagner et compenser les impacts des restructurations liées à la mondialisation. Ils contribuent à moderniser les systèmes d'évaluation et de contrôle des gestionnaires publics, État et collectivités territoriales. Ils constituent de nouveaux vecteurs d'influence et d'intervention dans des secteurs stratégiques qui échappaient d'une certaine façon à l'action du RTE. Parce qu'elle concentre les interventions financières d'aide au développement local sur les investissements de recherche-développement, d'innovation, etc. qui sont autant de priorités inscrites au cœur de la stratégie de Lisbonne, l'Europe fait du RTE un acteur des enjeux modernes. Les préfets français tiennent aujourd'hui lieu de véritables « *catalyseurs* » des pôles de compétitivités et d'excellence. Jean-Marc Rebière a exposé, à titre d'exemple, les résultats d'une expérience conduite dans sa région : le pôle biovalley. Financé à hauteur de 30 % par le FEDER, celui-ci porte sur les « *innovations thérapeutiques* ». Il fait partie des quinze pôles de compétitivité mondiaux à vocation mondiale. Centré sur l'Alsace, il reste ouvert aux collaborations transfrontalières. Pôle technologique, la recherche publique y est très présente aux côtés de nombreuses *start-up* locales. Son ambition est de faire de l'Alsace un pôle international de référence dans la découverte et le développement des nouveaux produits et outils de la médecine de demain. De nombreux secteurs sont ainsi concernés : sciences de la vie, chimie, sciences physiques, sciences de l'information, robotique, communication... L'idée est de favoriser la création d'entreprises et l'implantation en Alsace d'industries pharmaceutiques, biotechnologiques ou dont les activités ont un lien avec le secteur médical. Les axes de recherche publique-privée du pôle se développent selon deux axes complémentaires : concevoir de nouveaux traitements à partir des connaissances actuelles et futures en chimie et en biologie, dans le but de tendre vers une médecine personnalisée ; développer des outils innovants pour la médecine (chirurgie mini-invasive assistée par ordinateur, télémédecine...).

Le RTE est ainsi conforté dans son rôle de garant de la bonne affectation des fonds européens et de « *porteur de la stratégie de renforcement de la cohésion territoriale, économique et sociale* ». L'Europe gagnerait à s'appuyer davantage sur les RTE, notamment sur leurs compétences régaliennes telles que celles relatives à la sécurité civile, la sécurité publique ou la sécurité environnementale et sanitaire. Le préfet d'Alsace a conclu sur l'avantage qu'il y aurait à construire un lien plus visible et plus stable entre RTE et la Commission européenne, « *afin de mieux faire ressortir ce qui dans leur action résulte des orientations et prescriptions* » de l'UE. L'Union européenne, en effet, souffre auprès des populations d'un grave déficit de légitimité et de crédibilité que les RTE peuvent contribuer à résorber.

Parmi les six principaux pays de l'UE en termes de surface et de population, la Pologne est, pour la période 2007-2013, l'un des principaux bénéficiaires de la politique de cohésion de l'UE (63,7 milliards d'euros). L'Espagne l'avait été pour la période précédente (2000-2006). Dès son intégration dans l'UE, la Pologne a d'ailleurs largement bénéficié de la politique de cohésion puisqu'elle a reçu, pour les années 2004 et 2006, près de 11,2 milliards d'Euros. Ces financements proviennent essentiellement du Fonds de cohésion et des Fonds structurels de l'UE. Jointes aux financements nationaux et locaux, ces sommes sont essentiellement consacrées au développement socio-économique du pays et des régions. Afin d'en optimiser l'utilisation, le gouvernement polonais a fait de ses représentants territoriaux les principaux gestionnaires de ceux-ci. Les voïvodes (RTE polonais) s'appuient, pour ce faire, sur un organe consultatif. Ils sont ainsi au cœur de la gestion de ces fonds. Une loi du 21 avril 2004 précise leurs missions. Présents à chacune des étapes des projets impliquant des fonds structurels européens, ils en apprécient l'utilisation, en déterminent les conditions d'emploi et en contrôlent le bon usage. Ils sont également responsables du transfert des fonds européens aux petites et moyennes entreprises.

À l'avenir, le voïvode est appelé à devenir autorité certificatrice au niveau régional. Le gouvernement polonais a en effet décidé d'augmenter les fonds européens mis en œuvre au niveau des régions et d'en décentraliser la gestion. Les voïvodes sont ainsi appelés à se recentrer sur leur fonction de contrôleur, l'État restant, quoi qu'il en soit, responsable en cas de mauvaise utilisation des fonds. En conclusion, le rôle des RTE évolue en Pologne. Le mouvement de décentralisation à l'œuvre dans ce pays explique largement cette évolution.

Imre Forgacs, directeur de l'Office d'administration publique régionale de Moyenne Hongrie, représentant la Hongrie, insiste, quant à lui, davantage sur l'intérêt que présentent pour son pays les fonds structurels européens en cas de catastrophes, qu'elles aient des causes naturelles ou non. Ainsi, le gouvernement hongrois a-t-il pu profiter

d'une aide de quinze millions d'euros de la Commission européenne suite aux inondations des fleuves du Danube et de Tisza au printemps 2006. Imre Forgacs souligne ici le rôle positif de ces aides, rapidement mobilisées. Par ailleurs, le RTE hongrois a largement évoqué l'utilité, indirecte, de tels fonds pour son gouvernement dans la redéfinition des équilibres territoriaux, encore à trouver. La restructuration de la Hongrie s'est effectivement faite au cours des vingt dernières années. Or, rappelle l'intervenant, la Hongrie a une histoire institutionnelle marquée par les conflits entre l'État central et les collectivités territoriales. Sept régions ont été créées dans les années 1990, au départ en charge essentiellement de l'aménagement du territoire. Une réforme intervenue en 2007 a permis une véritable décentralisation de la décision publique au profit de ces régions. Les RTE sont, par conséquent, naturellement appelés à jouer un rôle central dans la gestion de ces fonds et, plus généralement, dans la mise en œuvre des politiques européennes.

C'est à Raoul Prado, directeur général des programmes Régions pour le Portugal, l'Espagne, l'Italie et Malte à la Commission européenne, qu'il est revenu de clore cette deuxième demi-journée. Il a articulé sa présentation autour de trois questions. Il a présenté tout d'abord ce que sont les relations des RTE avec à la fois l'État, la population et la Commission européenne, puis a rappelé succinctement ce que prévoit la réglementation européenne en matière de fonds structurels, enfin, il a abordé ce que peuvent être les rôles différents du RTE, à la fois technique et politique, dans la gestion de ces fonds.

Raoul Prado commence par insister sur l'inexistence d'un schéma de travail en matière de fonds structurels mais d'environ une centaine, c'est-à-dire autant qu'il y a de programmes mis en œuvre impliquant de tels fonds. En effet, l'UE compte aujourd'hui vingt-sept États membres, soit autant de schémas de travail différents au départ. À cela s'ajoute qu'il existe deux types de programmes structurels, les uns, régionaux, et les autres, nationaux, même s'ils peuvent avoir une base régionale tels que celui présenté par l'intervenant italien. Enfin, au sein même de chaque État, les régions peuvent ne pas avoir toutes le même statut ainsi que c'est le cas en Italie ou en Espagne par exemple. Responsable du FEDER et de la politique de cohésion pour les quatre États mentionnés plus haut, Raoul Prado insiste sur l'extrême hétérogénéité des situations auxquelles il est lui-même confronté. Les quatre pays dont il suit les programmes présentent en effet la particularité de recouvrir toute la gamme des situations possibles. Au Portugal, pays à forte culture centralisatrice, les régions sont de simples régions administratives. Elles n'ont pas d'existence politique propre. Le processus de décentralisation y est de fait quasi inexistant. Aussi, lorsque les représentants de la Commission se rendent au Portugal, ils n'y rencontrent et n'y discutent qu'avec des représentants de l'État. À l'inverse, l'autonomie des régions étant très aboutie en Espagne, ces programmes régionaux ne supposent pas, au moment de leur définition, une participation poussée des RTE. Dès lors, quel thème fédérateur retenir ici ? L'une des approches possibles réside dans le principe de subsidiarité auquel Raoul Prado invite l'assistance à réfléchir. En effet, une définition uniforme du rôle des RTE dans l'UE serait contre-productive. Vu le nombre de situations différentes, une certaine cohérence ne peut être obtenue que par des voies différentes, tenant compte des spécificités des pays. C'est ce qui fait aussi la richesse et la force de la construction européenne, insiste Raoul Prado.

Second point, la réglementation européenne ne dit que peu de chose concernant les modalités de gestion de ces fonds par les autorités nationales. L'article 12 du règlement de base des fonds précise simplement que les fonds structurels sont mis en œuvre au niveau territorial approprié, selon la Constitution de chaque État membre. La réglementation européenne indique simplement que ces fonds supposent, pour leur gestion, un large partenariat des autorités et, pour ce qui est des programmes régionaux, l'implication des autorités régionales, élues dans la mesure du possible. La Commission européenne ne peut raisonnablement envisager d'être plus précise. Ce serait d'ailleurs, pour elle, courir le risque qu'on lui reproche son ingérence, reproche qui lui est par ailleurs déjà largement adressé.

Troisième et dernier point enfin, Raoul Prado évoque ce que sont ici selon lui les deux rôles des RTE : « *mécanique* », participant, en tant que fonctionnaires, à la mise en œuvre de ces fonds, et « *politique* ». La Commission européenne, quant à elle, distingue trois fonctions, essentielles au fonctionnement de l'ensemble de ses politiques : une de gestion, une de certification et une d'audit.

S'agissant des programmes nationaux, les choses sont relativement simples. Ce sont les ministères qui les gèrent. La situation se complique en revanche dès lors que l'on aborde la question des programmes régionaux. Dans la plupart des États membres, l'autorité de gestion reste au sein de l'État. Ce sont les RTE ou leur équivalent qui en assurent la fonction. La région d'Alsace en France en est d'ailleurs un contre-exemple puisque, à titre d'expérimentation, c'est au conseil régional que la gestion des fonds structurels a été confiée pour cette collectivité. Partout ailleurs, à l'exception notoire de l'Espagne ou c'est le président de région qui assure cette fonction, c'est le RTE

qui est autorité de gestion. Ce système fonctionne. Les choses sont moins évidentes s'agissant des contrôles. Chaque État est en effet tenu, douze mois après l'adoption d'un programme, de transmettre aux services de la Commission une description de ses systèmes de gestion et de contrôle. Leur approbation par ces services conditionne la suite des versements. En procédant ainsi, la Commission s'assure de l'existence d'outils administratifs permettant un pilotage efficace des programmes. Les difficultés surviennent ici lorsque de telles conditions ne sont pas remplies. Les services de la Commission doivent alors inviter l'État concerné à revoir certains de ses modes de gestion et de contrôle, ce qui peut naturellement prendre plus ou moins de temps et être plus ou moins couronné de succès.

Raoul Prado enfin aborde le rôle « *politique* » des RTE dont il souhaite un investissement, en amont des projets, plus important. Ainsi, si toutes les régions ont, sans exception, une représentation à Bruxelles et si la commissaire européenne en charge de la question des fonds se déplace souvent en région pour y rencontrer leurs élus ou autorités, peu de contacts directs sont établis avec les RTE. Les services de l'UE n'ont-ils pas, au même titre que les RTE, pour dessein d'assurer la cohésion territoriale et sociale ? Partenaires naturels, Raoul Prado regrette qu'ils n'œuvrent pas davantage directement ensemble.

Quant au reproche fait aux institutions européennes par les États membres d'une trop grande complexité des contrôles dans la bonne utilisation de ces fonds, Raoul Prado n'en nie pas la réalité. Il relève cependant que de tels contrôles sont nécessaires. Un moyen de les simplifier serait, comme cela se fait dans le secteur privé, l'adoption par les administrations publiques de normes et de standards communs pour certains types de dépenses. Les contrôles seraient ainsi grandement facilités.

De nombreux participants ont enfin pris la parole pour compléter les propos des intervenants, soulignant notamment que le déficit de légitimité dont souffrent la construction européenne et ses institutions est structurel et provient à la fois de la complexité de son histoire, des domaines qu'elle couvre et de l'absence de relais entre elle et le citoyen. Disposant de peu d'agents, le principe de subsidiarité y joue un rôle important. De fait, on assiste à ce que François-Gilles Le Theule, directeur du centre des études européennes de Strasbourg, qualifie d'« *européanisation rampante des fonctions publiques* ». Par ailleurs, c'est aux RTE notamment qu'il convient de porter les projets européens et d'en assurer l'exécution. Sur cette question, les avis divergent, certains estimant avec Bernard Zahra, directeur de l'Institut régional d'administration de Bastia, que si sous l'effet des politiques européennes, la culture de l'évaluation s'est imposé dans l'ensemble des administrations des États membres, la gestion des fonds structurels demeure un fait national et local. En effet, le partenariat nécessaire à leur pilotage suppose que l'UE se tienne en retrait. De plus, les institutions européennes souhaitent s'appuyer sur une responsabilité unique, celle des États, quelle que soit par ailleurs leur organisation. La représentante des Pays-Bas estime, quant à elle, qu'ici aussi les RTE ont un rôle essentiel à jouer, en communiquant davantage sur les politiques européennes et sur l'emploi et les succès des fonds structurels européens. Au final, la construction européenne, dont l'objectif premier était la sécurité, au sens large, de ses ressortissants, ne doit jamais perdre de vue cette mission première qui est la sienne, faute de quoi, elle perdrait toute légitimité aux yeux de ceux dont elle est censée défendre les intérêts.

Le RTE et la coopération transfrontalière

Question centrale, la coopération transfrontalière est de celles avec lesquelles les RTE sont le plus directement aux prises. L'Europe ne connaît pas de frontières. Le citoyen européen se satisfait de moins en moins de ces ultimes divisions administratives. Dès lors, quels instruments de coopération transfrontalière développer ? Comment le RTE participe-t-il aux initiatives bi ou multilatérales ? Quelle coopération entre RTE pour une meilleure sécurité des frontières dans ces conditions ? Autant de questions que les différents intervenants de cette dernière demi-journée se sont attachés à explorer, sous la conduite de Lodewijk de Witte, président de séance et gouverneur de la province de Vlaams Brabant (Belgique).

Miguel Alejo Vicente, délégué du gouvernement en Castille et León (Espagne), a envisagé dans sa présentation la coopération transfrontalière sous l'angle de la sécurité et a insisté tout particulièrement sur la question de l'immigration. Placés sous la responsabilité du ministre de l'Administration publique espagnol et responsables de la politique du gouvernement dans leur circonscription territoriale, les délégués du gouvernement espagnol sont garants de la sécurité. Ils disposent pour ce faire du concours des forces de sécurité de l'État et de l'ensemble des administrations compétentes en matière de séjour et d'accueil des étrangers, tels que les « bureaux des étrangers » par exemple. Or, la crise de l'État-nation, la mondialisation économique et ses conséquences posent aux autorités publiques de nouveaux défis. Ils ont notamment mis en

relief les difficultés pour les structures administratives classiques de faire face aux risques émergents. Actuellement, l'Espagne est confrontée à deux problèmes de sécurité importants : le terrorisme international, ETA restant une menace pour les populations et les autorités, et les phénomènes migratoires. Vu la dimension prise par ces problèmes, les autorités publiques doivent constamment adapter leurs moyens de réponse supposant toujours davantage de coopération entre États. Miguel Alejo Vicente estime de plus que la plupart des problèmes auxquels les États font face isolément ont pris une dimension globale et les concernent, de fait, désormais tous. Terrorisme, pauvreté ou absence de démocratie sont des phénomènes étroitement liés qui impliquent une réponse coordonnée des États, à la fois sous l'angle politique, économique, social, et en termes de sécurité.

Cette réflexion prend tout son sens quand on aborde, par exemple, la question migratoire. De pays d'émigration, l'Espagne est devenue un pays d'immigration. La population de nationalité étrangère résidant en Espagne représente aujourd'hui 9 % du total de la population espagnole.

L'Agence Européenne FRONTEX, créée en 2004, est une première réponse et constitue un précieux outil de coopération. Elle contribue à la sécurité des frontières en renforçant la coordination des actions des États membres dans l'exécution des mesures communautaires relatives à la gestion des frontières extérieures pour éviter l'entrée d'immigrants illégaux. Ce genre d'outils, pour être pleinement efficace, doit cependant être accompagné d'une véritable politique européenne en matière d'immigration que l'Espagne appelle de ses vœux, notamment en matière de séjour, d'intégration et d'aide au développement.

D'une manière plus générale, les accords de Schenghen, signés en 1985, supposent que les contrôles aux frontières extérieures de l'UE soient renforcés. Ces accords ont considérablement approfondi les rapports entre États mitoyens. L'Espagne a ainsi été conduite à développer ses relations avec la France et le Portugal. Le 20e sommet franco-espagnol, qui s'est tenu au mois de janvier 2008, a par exemple permis à ces deux gouvernements d'aboutir à un accord décisif concernant la lutte antiterroriste, en permettant notamment la constitution d'équipes d'enquête permanentes, communes aux deux États. De même, le dernier sommet hispano-portugais de 2008 a vu la naissance du Conseil hispano-portugais de sécurité et de défense. Celui-ci devrait permettre de développer des opérations militaires communes notamment sur des théâtres d'opération extérieurs, et de constituer des équipes de police judiciaire mixtes.

Le préfet des Pyrénées-Atlantiques, dont la circonscription a une frontière commune avec l'Espagne, est parti, quant à lui, d'un constat simple. La frontière, du fait des évolutions économiques et juridiques des rapports entre États voisins membres de l'UE, ne constitue plus une limite aux activités. Tout au contraire, elle est à ce point banalisée que les populations locales ne lui prêtent plus aucune signification symbolique ou pratique. Mieux, elle détermine des comportements d'opportunité : fiscalité plus avantageuse, tarifs différents pratiqués sur des mêmes produits, prix de l'immobilier différencié, etc.

Sur le littoral Basque, une conurbation de près de 600 000 habitants s'est constituée des deux côtés de la frontière autour d'une autoroute longeant la côte. Mais si la dynamique économique et sociale de ce territoire tend à l'unifier, les services publics sont plus source de rupture que de continuité. Par exemple, le citoyen espagnol propriétaire de biens immobiliers en France ne peut pourtant pas s'acquitter de ses impôts locaux par simple voie de prélèvements opérés par le Trésor public français auprès de sa banque espagnole. De même, la personne accidentée du côté de la frontière sera rapatriée par les services d'urgence sur l'établissement hospitalier du territoire de l'accident et non sur celui où elle est habituellement prise en charge et qui peut être éventuellement plus proche. Enfin, les rapports de voisinage de l'aéroport de San Sebastián avec la ville d'Hendaye que 80 % de son trafic survole sont réglés par un accord international entre les deux pays dont les modalités ne sont pas soumises aux acteurs locaux. À cet égard, l'évolution institutionnelle des deux pays – autonomisation des régions espagnoles et décentralisation en France – a compliqué la donne, les compétences laissées en France au RTE étant importantes.

Le traité de Bayonne de 1995 avait tenté d'apporter des réponses en proposant de multiples outils de coopération français (GIP) ou espagnols (*consorcio*). Toutes laissaient de côté l'État, garant en France de nombreux éléments essentiels à la vie de ses ressortissants. Un mécanisme de coopération original a pu cependant voir le jour à l'initiative des autorités locales. Créée le 1er mars 2007, cette coopération a pris la forme d'une association regroupant l'ensemble des collectivités locales concernées (région Aquitaine et département des Pyrénées-Atlantiques, Autonomie basque et députation du Guipúzcoa) dans laquelle les représentants de l'État Français ont été nommés membres de droit. Cette formule a reçu la validation des ministères des Affaires étrangères français et espagnol. Il a permis de donner un cadre et une couverture juridique à des échanges qui jusque-là étaient du domaine exclusif des diplomates. Cet outil de coopération a ainsi permis à de nombreux chantiers communs aux autorités de part et d'autre de la frontière d'émerger. Ces coopérations

multiples portent principalement sur l'échange d'informations et la mise en place d'outils de gestion communs. Ainsi, par exemple, la coordination de la gestion des grands axes routiers transfrontaliers a été améliorée. De même, le plan de secours de l'aéroport Fontarabie espagnol a été communiqué aux autorités françaises et des exercices communs ont été programmés. Une réflexion est actuellement en cours pour équiper le bassin versant espagnol des rivières littorales frontalières (Bidassoa) ou débouchant en France (Nivelle), en instruments de prévision des crues. De même, les questions épidémiologiques, notamment dans le domaine de la santé animale telles que la fièvre catarrhale ovine, dite aussi maladie de la « langue bleue », ont été abordées.

La coopération ne s'est pas limitée aux seules questions de police administrative. Les sujets économiques et sociaux se sont ainsi rapidement imposés. Très concrètement, un rapprochement a été organisé entre l'URSSAF de Bayonne (organisme privé chargé en France de recouvrir les cotisations sociales) et la Trésorerie générale de sécurité sociale du Guipúzcoa dans l'intérêt des acteurs économiques établis dans la région. Ici, les pistes sont nombreuses : information des salariés et des entreprises de part et d'autre de la frontière sur les droits et obligations en matière de cotisations sociales, observation des flux de travailleurs et d'entreprises franchissant la frontière, lutte contre la fraude et le travail illégal... De même, une réflexion sur la coopération hospitalière est en cours, afin de développer une logique de complémentarité entre établissements hospitaliers de chaque côté de la frontière.

Enfin, les thèmes liés à l'environnement ne manquent pas non plus d'être évoqués par cette instance de concertation. La place particulière du préfet en France, représentant l'État mais aussi potentiellement animateur et conseil auprès des autorités locales, lui confère une responsabilité particulière dans la coopération transfrontière. Encore faut-il qu'il soit habilité à le faire par son gouvernement et que les autorités étatiques du pays voisin le souhaitent également.

Frank Scherer, *Regierungsvizepräsident* – Freiburg – Baden Württemberg (Allemagne) a évoqué la coopération transfrontalière mise en œuvre par la région du Haut-Rhin avec la France et la Suisse. Avec six millions d'habitants et 165 milliards d'euros de PIB par an, cette région, située au cœur de l'Europe, bénéficie d'une forte croissance économique. Il rappelle tout d'abord que l'un des éléments clés des politiques régionales européennes réside dans la coopération territoriale. Celle-ci repose sur une meilleure communication entre collectivités situées de part et d'autre des frontières (rencontres, conférences sur des sujets variés...) et sur la réalisation de projets communs. Ces projets bénéficient du concours de nombreux fonds européens. Ainsi, les fonds INTERREG IV A prévus pour l'ensemble de l'UE pour la période 2007-2013 s'élevent à 7,75 milliards d'euros. L'enveloppe INTERREG A destinée à la région du Haut-Rhin comprend, quant à elle, 67 millions d'euros. Ajoutée aux financements nationaux allemands, français et suisses, cette somme est portée à 144 millions d'euros. Ces fonds sont destinés à assurer le financement de projets de coopération transfrontalière, lesquels supposent le concours des administrations territoriales et d'État. Ils touchent à de nombreux sujets : policiers, douaniers, culturels, universitaires, économiques... Frank Scherer cite de nombreux exemples : réalisation d'infrastructures lourdes telles que le pont reliant les villes de Strasbourg et de Kehl ; coopération universitaire entre les universités de Bâle, Fribourg-en-Brisgau, Karlsruhe, Strasbourg et Mulhouse, réunies au sein d'une confédération européenne des universités du Haut-Rhin ; coopération policière et douanière renforcée entre la France et l'Allemagne basée à Kehl et portant sur l'échange de renseignements et d'informations relatives aux enquêtes menées par ces différents services.

Coopération et programmes structurels européens impliquent par ailleurs que les administrations s'adaptent et évoluent. Le rôle du RTE est ici très étendu dans le Haut-Rhin, à tel point qu'il est qualifié de « petit ministère des Affaires étrangères » par l'ensemble des autres administrations locales. Ces multiples coopérations ont nécessité, pour leur réalisation, la création de quatre euro-régions dont le Haut-Rhin est membre. Chacune est dotée d'un statut différent, et une seule dispose de la personnalité morale, la région Pamina, les autres consistant davantage en des plateformes de communication. Enfin, Frank Scherer termine en insistant sur le fait que ces coopérations doivent aussi pouvoir être initiées depuis le terrain. À l'avenir le rôle du RTE, déjà très important aujourd'hui, est appelé à croître. Ses fonctions sont aujourd'hui de donner un cadre juridique et administratif approprié à ces projets et d'en garantir une partie des financements. Son rôle devrait évoluer à l'avenir vers davantage de lobbying en direction des autorités de Bruxelles.

Paulus Skardzius, directeur du département de l'administration publique au ministère de l'Intérieur lituanien, a commencé par situer géographiquement son pays. La Lituanie a quatre pays limitrophes : la Biélorussie, l'Estonie, la Pologne et la Lettonie. La Lituanie compte dix comtés dont un seul n'a pas de frontières avec un autre État. Ses coopérations transfrontalières ont pour fondement la convention de Madrid, signée et ratifiée en 1997, et son protocole additionnel signé en 2002. À cela, s'ajoutent les nouveaux règlements de la Commission européenne 10-82 sur la coopération territoriale.

Pour la Lituanie, la coopération transfrontalière constitue une chance. Les communautés locales lituaniennes sont ainsi invitées à développer des accords avec les collectivités étrangères limitrophes. Les gouverneurs de comté ont pour fonction de coordonner les projets régionaux. Ils s'appuient pour ce faire sur le Conseil de développement régional et animent des groupes de travail au sein des nombreuses commissions intergouvernementales. Ils interviennent également dans le financement de certains de ces projets et disposent de nombreuses compétences dans le domaine de l'aménagement du territoire.

Les outils de la coopération transfrontalière sont nombreux : Euro-régions, programmes transfrontaliers cofinancés par l'UE, groupement européen de coopération territoriale (GECT), ainsi que les multiples instances de coopération internes aux administrations lituaniennes. Des accords de coopération transfrontalière ont été signés entre la Lituanie et ses voisins ayant pour objet de promouvoir et faciliter les collaborations entre les collectivités territoriales de chaque État. Des instances nationales dédiées suivent les progrès de ces coopérations. Par exemple, une commission intergouvernementale lituano-polonaise, créée en 1996, suit l'ensemble des projets de coopération entre les régions de ces deux pays. Elle intervient à tous les stades de ces coopérations et en initie parfois certaines. Elle peut en accompagner le développement, par exemple du point de vue de l'aménagement du territoire. Elle intervient au niveau juridique pour déverrouiller certains blocages. La Lituanie s'appuie par ailleurs largement sur ses six Euro-régions. Ainsi, une quarantaine de communes sur un total d'environ soixante, et six comtés sur dix font partie d'une Euro-région.

Ces coopérations ont divers objets tels que le développement économique, les infrastructures de transports, les questions sociales, environnementales ou énergétiques. Elles disposent de financement nombreux. Outre les financements nationaux, l'ensemble de ces projets intègre de nombreux crédits européens. Ainsi en est-il par exemple du programme couvrant la période 2007-2013 relatif au co-développement des régions transfrontalières lituano-polonaises, portant sur la cohésion sociale, la compétitivité et la productivité de ces régions, et pour lequel la contribution totale de l'UE s'élèvera à sept millions d'euros d'ici à 2013. De nombreux financements internationaux ont également permis ces coopérations, notamment celles établies avec les pays non-membres de l'UE et avec lesquels les projets ne sont pas moins nombreux, par exemple, avec la Biélorussie, concernant la protection de l'environnement et le développement du tourisme.

Dans ce vaste mouvement, les RTE, placés à la tête des nombreuses instances de concertation et de pilotage (conseils de développement régional, groupes de travail divers...) ont un rôle de coordination. Ils sont à la fois initiateurs et forces de proposition. Ils approuvent les projets qui leur sont soumis par les autorités locales. *In fine*, l'intervenant lituanien insiste sur le fait que, au-delà des thématiques nombreuses couvertes par ces coopérations, l'intérêt est de rapprocher les États entre eux, y compris ceux qui ne font pas partie de l'UE.

Enfin, Perla Stancari, préfète, directrice centrale pour les droits civils, la citoyenneté et les groupes minoritaires au ministère de l'Intérieur italien, est intervenue pour présenter la coopération transfrontalière en Italie. Elle rappelle que l'Italie, fervent partisan de l'Europe, a été l'un des premiers États membres à signer la Convention cadre de Madrid du 21 mai 1980. Élaboré sous l'égide du Conseil de l'Europe, cet accord reconnaît, notamment aux collectivités ou autorités locales, compétence pour conclure en leur nom propre des conventions avec des autorités territoriales transfrontalières de même rang. Ces formes de coopérations localisées ont le soutien des institutions communautaires qui y voient un outil privilégié pour la construction européenne. En témoigne le développement, dans les années 1990, des nombreux projets de coopération ayant pu bénéficier de programmes de financement INTERREG. De même, la création d'outils juridiques dédiés tels que les Groupements européens de coopération territoriale (GECT) montre le souci de l'UE de faciliter de tels rapprochements.

Relevant du ministère de l'Intérieur, le préfet en Italie est garant de l'intérêt général. À ce titre, il assure la coordination de l'activité des administrations publiques présentes sur le territoire de la Province dont il a la charge. Il est garant de l'ordre public et de l'exercice des libertés. De par sa position, le préfet est à la fois relais et médiateur, entre administrations locales et centrales et entre celles-ci et le citoyen. Il peut aussi être à l'initiative de nombreux projets. Son statut en fait un acteur central dans la coopération transfrontalière aujourd'hui. En effet, la complexité et la diversité croissante des domaines concernés par cette coopération font du préfet le trait d'union naturel entre l'ensemble des projets conduits et des partenaires impliqués. Ainsi, selon les termes mêmes de Perla Stancari, le préfet a vocation à établir des « *passerelles* » entre espaces frontaliers. Cette coopération transfrontalière est aujourd'hui non seulement essentielle à la bonne administration des territoires que ces frontières coupent, mais elle revêt une dimension géopolitique. L'élargissement progressif de l'UE implique en effet de nouvelles frontières à la fois intérieures et extérieures.

La coopération transfrontalière concerne aujourd'hui l'ensemble des sujets retenant le plus l'attention de l'opinion

publique. Ainsi en est-il de la sécurité, pour laquelle le ministère de l'Intérieur italien a conclu des accords bilatéraux avec l'Autriche, la Suisse, la France et la Slovénie. De nombreuses instances communes à différents pays ont ainsi vu le jour sur ces questions. La Commission franco-italienne pour l'entretien de la frontière nationale et le Comité franco-italien de coopération transfrontalière ont permis un rapprochement entre les préfets d'Impéria pour l'Italie et des Alpes-Maritimes pour la France. De nombreuses opérations de police conjointes ont ainsi vu le jour. Ces opérations ont porté aussi bien sur la surveillance que sur le contrôle de réseaux routiers et ferroviaires. Elles ont également concerné les zones côtières. Des brigades autoroutières communes à ces deux pays ont également été créées.

Ces coopérations s'étendent désormais à la protection civile et aux questions touchant à l'environnement. Ainsi, par exemple, la Commission italo-slovène pour l'hydro-économie a permis à ces deux pays d'élaborer une stratégie commune en matière d'équilibre des ressources en eau, ce qui inclut non seulement les barrages situés dans les zones transfrontalières mais aussi les phénomènes de pollution. De même, la Commission internationale pour la protection des eaux italo-suisses contre la pollution, concernant, entre autres le Lac Majeur et le Lac de Lugane, et la Commission franco-italo-monégasque pour la sauvegarde de la qualité des eaux du littoral méditerranéen (RAMOGE), permettent une meilleure connaissance des phénomènes de pollution et une plus grande sensibilisation des différents acteurs concernés aux questions liées à l'environnement.

S'agissant de la culture et de la formation, la coopération transfrontalière offre le moyen de surmonter les divisions historiques et les stéréotypes. Ces divisions et préventions doivent être vaincues non seulement dans l'intérêt d'un rapprochement entre citoyens européens, mais aussi dans l'intérêt d'une meilleure coopération économique. À cette fin, le Bureau de la coopération internationale et des zones frontalières a lancé en 2005 une initiative intitulée « Pour favoriser la connaissance mutuelle – Comment promouvoir la connaissance de la langue et de la culture du voisin dans la zone frontalière ». Cet événement, organisé en collaboration avec la préfecture de Trieste et le Conseil de l'Europe, a rassemblé de nombreux responsables de politiques liées à l'éducation venant d'Autriche, de Croatie et de Slovénie, ainsi que des représentants de la région Frioul Vénétie-Julienne, de l'université de Trieste, de la chambre de commerce et du centre européen pour les langues vivantes de Graz et de l'Académie linguistique de Maastricht.

Ce sont au total de nombreuses initiatives qui ont ainsi pu voir le jour grâce à la coopération transfrontalière. Ainsi que le souligne Perla Stancari dans son propos, la frontière aujourd'hui est « *moins un élément de division qu'un élément de jonction* ».

Ces journées se sont terminées sur les mots de conclusion de Thierry Aumonier et de Daniel Canepa. Ainsi que le premier l'a rappelé, derrière le thème de cette 15e rencontre – les préfets dans l'intégration européenne – une autre question se profilait, celle du rôle de « *médiateur des RTE entre l'Europe et les citoyens* ». Cette question, Thierry Aumonier se félicite que les différents participants l'aient « *débusquée* ». Ce rôle nouveau, a-t-il souligné avec force, les RTE sont prêts à l'endosser et ils l'appellent même de leurs vœux. Cette place redéfinie du RTE se justifie par la nature transversale des sujets traités par l'UE, par le rôle croissant des régions dans la construction européenne et par l'importance que prennent de plus en plus les questions de sécurité dans le débat européen. De par les multiples attributions qui sont les siennes, juridiques, financières, politiques... le RTE n'est-il pas naturellement appelé à occuper une position clé dans l'architecture européenne de demain ? Passerelle, lien... les qualificatifs sont nombreux pour décrire cette fonction qui est déjà la sienne. En conclusion, le représentant territorial de l'État est aussi celui de l'Europe, et il est prêt à en assumer la charge.

En définitive, conclut Daniel Canepa, cette forte demande des RTE à jouer un rôle nouveau et renforcé dans la construction européenne n'est peut-être que le reflet de celle, plus large, des citoyens qui d'ailleurs ignorent bien souvent tout de l'Europe, mais n'en attendent pas moins beaucoup d'elle. Cette recherche d'un meilleur service rendu au citoyen, est commune à l'ensemble des représentants territoriaux des États membres de l'UE, et constitue une sorte de trait d'union qui les réunit tous et les guide vers un même but.

Alexandre MOUTON
Chargé d'études à l'INHES

JOURNEES EUROPEENNES
EUROPEAN DAYS

XV^th European Days of State territorial representatives

May 29-31 – Venice – Italy

Role of the STR in the European integration

Miguel ALEJO VICENTE, Delegado del gobierno de España en Castilla y Leòn ESPAGNE
Francisco ALVAREZ MARTINEZ, Subdelegado del Gobierno de España en Leòn ESPAGNE
Barbara ANDRACCHIO, Staff - ANFACI ITALIE
Hans ANGERER, Regierungspräsident von Oberfranken ALLEMAGNE
Thierry AUMONIER, Administrateur délégué AERTE
Svein BERBU, Deputy Director General - Ministry of Government Administration and Reform NORVEGE
Migle BERNOTIENE, Adviser of the Government Office LITUANIE
Yvan BLOT, Inspecteur général de l'administration - Ministère de l'Intérieur FRANCE
Jean-Michel BRUNEAU, Sous-préfet de Lisieux FRANCE
Stuart BURGESS, Chairman and Rural Advocate - Commission for Rural Communities ROYAUME-UNI
Marc CABANE, Préfet des Pyrénées-Atlantiques FRANCE
Daniel CANEPA, Préfet de la région Nord-Pas-de-Calais, président de l'association du corps préfectoral FRANCE
Solange CARMONA, Secrétaire générale, AERTE
Gabriella CASACCIO, Vice prefetto aggiunto - ANFACI ITALIE
Andreas CHRISTODOULIDES, District Officer of Paphos CHYPRE
Teresa CIMADEVILLA MARTINEZ, Asesora del Delegado del Gobierno - Leòn ESPAGNE
Lodewijk DE WITTE, Gouverneur - Province Vlaams-Brabant BELGIQUE
Aimée DUBOS, Sous-préfète d'Argenteuil FRANCE
Danièle EVEN, Chef du secrétariat permanent - Association du corps préfectoral FRANCE
Daniel FEREY, Préfet de la Creuse FRANCE
Andrea FERRAZZI, Vice-presidente - Province di Venezia ITALIE
Michel FORET, Gouverneur - Province de Liège BELGIQUE
Imre FORGACS, Head of Central Hungarian Regional Public Administration Office HONGRIE
Giancarlo GALAN, Presidente - Regione Veneto ITALIE
Graham GARBUTT, Chief Executive - Commission for Rural Communities ROYAUME-UNI
Rafaella GISSI, Staff - ANFACI ITALIE
Anne HAUDRY de SOUCY, Conseillère Europe - Caisse des Dépôts et Consignations FRANCE
Christoph HILLENBRAND, District President of Upper Bavaria ALLEMAGNE
Alain LARANGE, Inspecteur général de l'Administration - Ministère de l'Intérieur FRANCE
François-Gilles LE THEULE, Directeur du Centre des études européennes de Strasbourg - ENA FRANCE
Sven LINDGREN, Governor - Kalmar County SUEDE
Hanja MAIJ-WEGGEN, Her Majesty's Governor in the province of Noord-Brabant HOLLANDE
Pascal MAILHOS, Préfet, secrétaire général adjoint, directeur de la modernisation et de l'action territoriale - Ministère de l'Intérieur FRANCE

European Association of State Territorial Representatives - EASTR
Non-profit association constituted under the 27 June 1921 Belgian law

General Secretariat of the European Days: 8, rue Fallempin, 75015 Paris – France
Tel: +33(0)1 45 78 36 17 – Fax: +33 (0)1 45 77 69 65
www.european-days.org

Claudio MEOLI, Prefetto ITALIE
Juan-Antonio MOLL GOMILA, Jefe Area Extranjeria – Ministerio de administraciones publicas ESPAGNE
Mario MORCONE, Prefetto – presidente – ANFACI ITALIE
Alexandre MOUTON, Chargé d'études, INHES FRANCE
Guido NARDONE, Prefetto di Venezia ITALIE
Hans NEUHOFER, Professor, University of Vienna AUTRICHE
Jacques NICOD, Préfet du District de Lausanne – Canton de Vaud SUISSE
Kari NORDHEIM-LARSEN, County Governor of Telemark NORVEGE
Rasa NOREIKIENE, Undersecretary – Ministry of the Interior LITUANIE
Olga PALACIO GARCIA, Jefa del Gabinete del Delegado del Gobierno en Castilla y Leòn ESPAGNE
Véronique PAULUS de CHATELET, Gouverneur de Bruxelles BELGIQUE
Michele PENTA, Prefetto, segretario generale, ANFACI ITALIE
José Luis PEREZ BECARES, Coordinator de Area – Ministerio de Administraciones Publicas ESPAGNE
Agnès PINAULT, Sous-préfète de Morlaix FRANCE
Ignazio PORTELLI, Vice prefetto, vice segredario nazionale ANFACI, ITALIE
Raoul PRADO, Directeur – DG Regio COMMISSION EUROPEENNE
Roberta PREZIOTTI, Vice prefetto – ANFACI ITALIE
Jean-Marc REBIERE, Préfet de la région Alsace FRANCE
Juan Antonio REDONDO PARRAL, Jefe de la Unidad de Relacioners Institucionales – Ministerio de Administraciones Publicas ESPAGNE
Charles RICQ-CHAPPUIS, Professeur, COER SUISSE
Luis Carmelo RINCON MIRANDA, Jefe de prensa de la delegacion del Gobierno de España en Castilla y Leòn ESPAGNE
Hans J. RØSJORDE, Governor – County of Oslo and Akershus NORVÈGE
Graham RUSSELL, Director – Commission for Rural Communities ROYAUME-UNI
Serge SANDT, Commissaire du district de Grevenmacher LUXEMBOURG
Frank SCHERER, Regierungsvizepräsident von Freiburg ALLEMAGNE
Alvydas SEDZIUS, Governor of Siauliai County LITUANIE
Michela SIGNORINI, Vice prefetto – ANFACI ITALIE
Lars SILSETH, Senior advisor – Ministry of Government Administration and Reform NORVEGE
Eino SIURUAINEN, Governor – Province Office of Oulu FINLANDE
Paulius SKARDZIUS, Director of public administration department – Ministry of the Interior LITUANIE
Perla STANCARI, Prefetto ITALIE
Jean-Claude VACHER, Préfet du Maine-et-Loire FRANCE
Michele VIANELLO, Vice sindaco di Venezia Italie
Luc VILAIN, Sous-préfet de Saint-Julien en Genevois FRANCE
Jacques-André VULLIET, Secrétaire général – IDHEAP SUISSE
Bernard ZAHRA, Directeur – IRA de Bastia FRANCE
Janusz ZALESKI, President of the board – Wroclaw Regional Development Agency POLOGNE

The 15th EDSTR (European Days of State Territorial Representatives) were held in Venice May 29-30, 2008. This year's theme was "*the role of the State Territorial Representative* (STR) *in European integration.*" Welcomed to the island of San Servolo by Guido Nardone, prefect of Venice, Andrea Ferrazzi, vice-president of Venice Province, Michele Vianello, deputy mayor of Venise, and Michele Penta, prefect and secretary general of ANFACI, all of the participants enjoyed informative networking in a calm and peaceful atmosphere conducive to the thought process.

France sent three speakers this year: Jean-Claude Vacher, prefect of Maine-et-Loire, Jean-Marc Rebière, prefect of the Alsace region and vice-president of the French Association of Prefects, and Marc Cabane, prefect of Pyrénées-Atlantiques. The large French delegation included Thierry Aumonier, managing director of EASTR, Daniel Canepa, prefect of the Nord-Pas-de-Calais region, president of the French Association of Prefects, and Solange Carmona, secretary general of EASTR.

Their talks focused on the following topics:
- the STR in applying European regulations through the example of the environment,
- the STR and European funds,
- the STR in cross-border cooperation.

For a better understanding, we will look at how these themes were presented.

First, Michele Penta described the role of the prefect in Italy. Over the last fifteen years the Italian civil service has undergone many reforms, marking a new stage in relations between government and its users. Citizens have now become full-fledged actors in public service and participate in its delivery. This movement has been accompanied by increased devolution of public decision-making. As guarantor of social, institutional and territorial cohesion all at once, the prefect has been at the heart of these reforms. Recent laws, especially those of 2004, have redefined his role, emphasising his functions as activities coordinator for the State's outposts throughout the territory for which he is responsible.

As the natural point of contact for local governments and, increasingly, civil society, his functions go well beyond the more traditional ones of guarantor of the rule of law and the public order. He is thus both mediator of all conflicts and promoter of a certain idea of the law, whose proper execution he also oversees. These multiple attributes, not all of which have necessarily been formalised in writing, are accompanied in the prefect by a detailed familiarity with his district. Attentive to emerging needs, wanting to best serve the interests of citizens, the prefect contributes to ensuring the unity of action of the State and the European Union (EU).

The STR and the environment

What role is there for the State Territorial Representative in applying European regulations? This year EASTR decided to put this question to the participants using the example of the environment. These questions, which by their nature are interconnected, are no more bound by administrative boundaries than by geographic ones. The STR's role in complying with regulations regarding environmental protection, which the EU has made one of its primary objectives, and its place in application of the *Nature 2000* programme were a common thread in the talks given during this first half-day. The debates were presided over by Hanja Maij-Weggen, Queen's Commissioner, province of North Brabant (Netherlands).

Christoph Hillenbrand, Regierungspräsident for Upper Bavaria (Germany), described some of the environment-friendly efforts undertaken in his region. With an area of 17,529 Km², Upper Bavaria is the largest region in the German Federal Republic. Its 4.2 million inhabitants make it the third most populous. The legal framework in the area of air quality relies both on European regulations, including Directive 96/62/EC, and on national legislation. Three cities in Upper Bavaria are most especially affected by these regulations: Munich, Ingolstadt and Burghausen.

The European directive sets thresholds for air pollution as well as an authorised maximum number of times these thresholds may be exceeded per year. Initially, these limits were poorly observed. The first *Air Quality* plan of action was implemented on December 20, 2004, in Munich. Among other things, this plan called for measures concerning industrial installations (heating systems, energy plants) and included a certain number of provisions intended to better manage highway traffic: better management of parking areas, promotion of mass transit or ecological vehicles within the Munich government.... The measures taken soon showed their limitations, however. Consequently, the authorities in Upper Bavaria had to adapt their strategy. It was broken down into three stages. First, trucks of more than 3.5 tonnes were prohibited from passing through Munich, and the rerouting of these trucks to Highway A99 made it possible to keep

out all trucks not having the city as their destination. Second, an "Environmental Zone" was created, the purpose of which was to reduce emissions of polluting gases inside the Middle Ring Highway. The third phase consisted of making all local actors more aware of issues associated with air quality.

The need to provide bypass routes in fact became a priority for the authorities. Munich is a hub in the southern part of the European long-distance roadway system. The major flow of goods coming from or going to France, Spain, Austria and Switzerland (western) previously passed through Munich. This flow has now been detoured. Because this is a 27-kilometre detour, this measure required many phases of coordination, especially with the road transport companies. A fine of 20 Euros was instituted for violators. Its dissuasive effect lies not so much in the amount, however, as in the time that the vehicle is stopped for the necessary controls. These measures have proven their effectiveness. The Middle Ring road is far less used by heavy goods vehicles than it was previously. They have also made it possible to create an "Environmental Zone." This consists of prohibiting access to the centre of Munich for severely polluting vehicles, regardless of their size. Also, under European regulations, motor vehicles must indicate the pollutant emissions group they belong to. Of the four different groups, vehicles in the first group may no longer circulate in the protected area. The third stage consists of expanding the areas involved in the *Air Quality* plan. In particular, this means that the neighbouring federal counties have to be made aware of these issues and commit to improving their situation.

Finally, all of these efforts together will be evaluated in 2009 and 2010.

Hans Neuhofer, a professor at the University of Vienna, focused his speech on a presentation of the distribution of powers in Austria in the area of environmental protection. He began by noting that the European regulations are either directly applicable in domestic law or are subject to conversion measures. In Austria the federal authorities or Länder are responsible for ensuring this conversion, according to the areas in question. The speaker then stressed the importance of the environmental issue both for the EU, whose environmental regulations, combined in a CODEX, exceed a thousand pages, and for the Austrian authorities. In this country, environmental protection is actually part of the constitution's norms. Finally, Hans Neuhofer noted in his prefatory remarks that in Austria as in Germany these issues are sensitive and often arouse sharp reactions in public opinion.

The federal constitutional law requires the nine Länder of the Federal Republic of Austria and its 2,358 municipalities to oversee the protection and preservation of the environment, especially air, water and soil quality. Environmental powers are shared between the federal authorities, the Länder and the municipalities. According to the federal constitution's provisions, the Federation exercises overall authority in this area, especially affecting industrial and mining activities, transport, water and air protection, and hazardous waste management. The federal Environmental Protection Office regularly publishes its conclusions. These reports, the latest of which dates from 2007, provide a good overall view of the Austrian situation.

The powers assigned in this area to the Länder are less extensive than the Federation's. But they are no less important. They are directly involved in matters concerning territorial development, protection of the soil and nature and landscape preservation, water supply, wastewater management, and household waste treatment. The Länder also have authority in energy matters and deal with issues associated with electricity, energy-saving policies, polluting industrial facilities.... As such, they are involved in the area of research and especially in promoting alternative, non-polluting energy sources.

Finally, the municipalities also perform numerous missions in this area: local development, building police, fire regulations, water supply, transport and waste and wastewater treatment. They are especially involved in waste sorting. Without actually doing the work of the courts and legislators, if the situation warrants it they can set police regulations in these various areas. Local communities also have the task of making their citizens aware and keeping them informed.

Though not an EU member, Norway's case is nonetheless interesting in several respects. It is in some way illustrative of the spill-over effect the EU has on its immediate neighbours. According to Hans Røsjorde, governor of Oslo and Akershus County, the Norwegian authorities are in fact particularly attentive to environmental issues. Since by definition these issues know no borders, Norway is closely overseeing the convergence of policies it has initiated in this area with European policies. Its attention to these matters translates into many regulations encompassing some two hundred fifty acts to date. Most of these measures are taken nationwide.

As intermediaries between the local communities and the central government, the region governors implement national policies. They are also responsible for monitoring compliance within their districts. Consequently, they play an essential role in environmental matters. To cite just a few

examples, Norway's governors issue authorisations to industrial firms and monitor their activities. They ensure compliance with the prescribed pollution thresholds and treatment of their industrial wastes. They oversee proper management of highway facilities and infrastructures. They are also responsible for protecting agricultural areas, or managing water and water resources... More generally, they are guarantors of environmental protection and citizen safety (prevention of various kinds of pollution, health, as well as sustainable development and climate change, for example).

Hans Røsjorde also noted the case of the European directives on biodiversity. Norway is not in fact part of the *Natura 2000* network set up by the EU. That does not keep Norway from following the example of the best that this system has to offer, and it participates in the biodiversity indicators set by the EU for 2010. Norway is also associated with the efforts of the European Environment Agency. Finally, it implements other strategic approaches, such as the *Emerald* system, for example, in application of the Berne Convention.

It was then the turn of the French prefect of Maine-et-Loire to speak. Jean-Claude Vacher first briefly described the duties and powers of the State Territorial Representative in France. He is responsible for applying the laws passed by the Parliament and monitoring compliance with them by local authorities. In the area of the environment, this authority takes the form of a review of a great many decisions taken by local governments. He thus ensures their compliance not only with strictly French legislation but also, and perhaps most importantly, with international and especially European legislation. The prefect of Maine-et-Loire then presented three examples in the area of the environment.

The first relates to application of the SEVESO directive on industrial facilities which, because of the materials used or because of what they produce, present serious hazards for populations and the environment. These SEVESO regulations have been amended and clarified several times, both at the European level and nationally. How does the prefect perform his role in this area? For example, how can he authorise or reject the expansion or creation of this or that enterprise? First of all, the prefect has to be able to count on the enterprise itself, which he expects to participate in the authorisation process. Hence the enterprise has to conduct impact and hazard studies in advance, and show that its plans were developed both for the enterprise itself and for its surroundings, for local populations, for example. More generally, the prefect monitors compliance with the law. Consequently he ensures that the decisions taken by local administrative authorities comply with current law. If the building permit falls under the mayor's jurisdiction, the prefect has to make certain that the mayor complies with legislation in terms of environmental safety, for example concerning compliance with minimum distances between industrial sites and the nearest homes. The prefect also has the task of facilitating awareness among the public, users and associations of the products manufactured in these enterprises and of the protective measures taken for their safety. For this informational mission, he relies on the local Local Information and Control Commissions (LICC) made up of associations, representatives, elected officials and various State agencies in equal proportions. These LICCs play a very important role, especially in preventing the spread of rumours and false information.

The second example cited by the Maine-et-Loire prefect involved the treatment of urban wastewater. Abundant European regulations, the first directives of which date from 1991, required the member States to make certain that water returning to nature met certain conditions, especially regarding phosphate and nitrate content, following a calendar that stretched into 2005. France recently condemned the Court of Justice of the European Communities (CJEC) for not having been sufficiently diligent in implementing these directives. The French government has consequently instructed its prefects to ensure that local authorities speed up implementation of these standards at municipal wastewater treatment facilities. In the Maine-et-Loire department, Jean-Claude Vacher has therefore had to take decisions requiring seven cities with populations over ten thousand to meet a precise schedule in meeting their obligation to modernise their treatment facilities. The objective set for the prefects here is to respond before the end of 2008 to the instructions set by the EU in this area.

The third and final example involves the directive on reducing greenhouse gases. This directive, which came out of the Kyoto Protocol (1997), encourages the use of clean and renewable sources of energy. It also requires the member States to increase the amount of electricity produced by these new sources within the next ten years. France has complied with the European prescriptions in two ways. First, it required the public utility EDF, before the opening up of the electricity market to competition, to buy at a higher price the Kwatts produced by clean energy sources in order to stimulate the growth of alternative projects. In addition, a recent French law makes the prefect the decision-making authority in matters of wind-power plans. He is in fact the department's authorising authority for wind-power development plans presented to him by the local authorities. Not only can the prefect refuse to approve a project but he can also ask

that it be modified. In addition, although this plan does not fall under the direct jurisdiction of the STR, he is the one who issues the construction permits. In Maine-et-Loire, the prefectural offices have supported the procedures under way for the drafting of a manual of good practices for wind power. These take into account in particular the existence of landscapes that are protected, often by other European rules, such as those established by *Natura 2000*, or international rules concerning the Loire Valley for example. This manual of good practices is an invaluable tool for the Maine-et-Loire prefect and the local communities in their consideration of the project. This collaboration ahead of the project ensures the project's success. Since 2006, Jean-Claude Vacher has taken four decisions to authorise and just one to reject.

Finally, many of the participants expressed their distress with regard to European regulations which, in environmental matters, sometimes have the effect of blocking many projects. A certain amount of legal uncertainty seems in fact to prevail in this area. Christopher Hillenbrand pointed out that in Germany it sometimes takes thirty years to complete certain highway infrastructures. The Maine-et-Loire prefect likewise cited the case of France's international airports, for which the delays are also long. These long-range projects sometimes fit poorly with changing environmental regulations, whose provisions can compromise their implementation. Janusz Zaleski, chairman of the Regional Development Agency of Wroclaw (Poland), decried the inhibiting effects of these regulations on investors, who now hesitate to take up large projects which they are uncertain they can complete.

Two other points elicited some comments. Janusz Zaleski underscored the sometimes perverse effects of certain regulations which, out of a desire to be comprehensive, end up conflicting with national law. Some unprotected areas in Poland are affected by *Natura 2000*, thereby making certain projects that are already under way unrealisable. Conversely, some areas protected by national legislation that do not appear in the system defined by *Natura 2000* now face an uncertain future. In addition, many speakers, especially French and German, agreed that the environment had become a politically very sensitive and emotionally charged subject requiring even more vigilance and caution of the STRs.

The STR and European funds

While European funds are generally applied in the same way regardless of country and are associated with the economic and social development of less advanced regions, these funds are managed in different ways in different cases. The speakers for the second half-day explained these differences and provided many concrete examples. This session was also an opportunity for Raoul Prado, director general of the European Commission responsible for managing European structural funds for Portugal, Spain, Italy and Malta, to explain the EU's viewpoint on this issue. Beyond the strictly technical and financial aspects, consideration was also given to the concrete tools the EU gives to the STRs to promote the effectiveness of their efforts, as was quite rightly pointed out by the session's chairman, Graham Garbutt, chairman of the Commission for Rural Communities (Great Britain).

Rasa Noreikiene, secretary of State with the Lithuanian Interior Ministry, spoke first to describe the use made of the European structural funds in her country. In Lithuania as in most of the European States with a strong centralising culture, it is the STRs who administer the European funds. To the extent that these funds are used for local and regional socioeconomic development, they are added to the national systems and in fact necessarily assume a close relationship between local and central government offices for their implementation, especially between county governors and municipalities. In Lithuania, the European funds ensure a certain cross-subsidisation of the country. They contribute not only to reducing gaps between regions but also within a given region between villages and the countryside. In fact, aside from the immediate effects of these funds, they create conditions for multiple local partnerships, both with regard to project management and to the definition of the needs and expectations that prevailed when they were launched.

As this involves the implementation of these projects, the European Regional Development Fund (ERDF) contains a principal strategic document intended to guide the implementation of national policies at the county level. It specifies possible uses of these funds at the regional level. A draft regional plan containing proposed measures is drafted by the office of the county governor and approved by the county's regional council. Guidance for the use of these funds is provided by the Regional Development Council. It includes the governor, who serves as its chairman, the mayors of the concerned municipalities and members delegated by their municipal councils. The STRs administer these funds for the sole benefit of the regions. They thereby contribute to consolidating and encouraging regional development while at the same time making it possible to resolve problems in the most disadvantaged areas. Lithuania is one of the great beneficiaries of these funds. For the 2007-2013

period, the ERDF totals some 6.7 billion Euros in that country alone, which corresponds to the annual budget of Lithuania.

The Italian case, presented by Roberta Preziotti, under prefect with the department of civil liberties and immigration in the Interior Ministry (Italy), is often cited as an example by the EU. The Italian authorities assign a significant share of the resources from the European communities to the economic and social development of regions that are more backward than the European average. In fact, since the mid-1990's, the Italian government has launched a series of national and regional programmes run by the central and local authorities.

Among these, the Italian speaker cited in particular the National Operative Programme (NOP) Security for Development / Convergence Objective (NOP-Security), covering the 2007-2013 period and assigned to the Interior Ministry for implementation. With a total of nearly 1.158 billion Euros, its operations are both national and European. The latter fall into two categories: the first, including productive investments mainly applied to creation heavy infrastructure, or more than 90% of the total, comes from the European Regional Development Fund. The second, including operations covering costs associated with regulatory production and training efforts, or about 10% of the total amount allocated, comes from the European Social Fund.

The uniqueness of the Italian approach has to do with its highly integrated character. NOP-Security applies to four of the poorest Italian regions, Campania, Calabria, Puglia and Sicily. These regions are in fact structurally backward both economically and socially for obvious reasons having to do with their history, culture, social characteristics, crime rate, and – a more recent phenomenon – the influx of immigrants for whom they are if not the final destination at least a major point of passage.

The NOP-Security measures affect many areas (infrastructure construction, development of communication networks, training...). The objective is to ensure security in the broad sense for the targeted territories so as to facilitate their economic development. The Interior Ministry consequently plays a role as central driving force. He also contributes to establishing a strong socio-economic partnership. As STR, the prefect has overall authority. He is responsible for coordinating the efforts of all the agencies involved in NOP-Security and for ensuring that they integrate local constraints into their application. NOP-Security also includes an important immigration-related aspect affecting the security, reception and integration of immigrant populations.

While it is essential that these efforts be consistent with one another, the Italian speaker also stressed the need to ensure that they are properly associated with other European efforts undertaken in this areas, especially those of the European Refugee Fund aimed at supporting and promoting the efforts of the member States in receiving refugees seeking asylum; the European Repatriation Fund, contributing towards improving management of repatriations in compliance with fundamental human rights; the European Fund for the Integration of Third-Country Citizens; and the Foreign Borders Fund.

The French prefect for the Alsace region, vice president of the Association of Prefects, spoke next, emphasising the major role of the STRs in France in applying European policies. In fact not only are they indispensable intermediaries, they are also the real promoters of these policies. Europe needs this promotion all the more because of its perceived lack of legitimacy among European citizens. From this standpoint, the European funds are invaluable tools that they can rely on. These funds are also a favoured means of supporting and compensating for the impacts of the reorganisations associated with globalisation. They contribute to modernising systems for evaluating and monitoring public managers, the State and local communities. They are new vectors of influence and intervention in strategic sectors that in some way escape the efforts of the STR. Because it focuses financial measures to assist local development on investments in R&D, innovation, etc., which are all priorities included within the Lisbon strategy, Europe makes the STR a key player in modern issues. Today French prefects serve as veritable *catalysts* for competition and excellence. By way of example, Jean-Marc Rebière explained the results of an experiment conducted in his region: the BioValley centre. With 30% of its funding from the ERDF, it focuses on *therapeutic innovations*. It is part of the fifteen worldwide competitiveness centres. Located in Alsace, it is open to cross-border cooperation. As a technological centre, public research is very much present there, alongside many local start-ups. Its ambition is to turn Alsace into a key international centre in the discovery and development of new products and tools in the medicine of tomorrow. Hence many sectors are involved: life sciences, chemistry, physical sciences, information sciences, robotics, communications... The idea is to promote enterprise creation and to set up pharmaceutical and biotech industries, or others linked to the medical sector, in Alsace. The centre's public-private research focuses on two complementary approaches: designing new treatments based on current and future knowledge in chemistry and biology, with the goal of moving towards personalised medicine; developing innovative tools for medicine (minimally invasive computer-assisted surgery, telemedicine...).

The STR is thereby assisted in his role as guarantor of the proper allocation of the European funds and "*promoter of the strategy for reinforcing regional, economic and social cohesion.*" Europe would benefit from relying even more on the STRs, especially on their sovereign-state authorities such as those relating to civil security, public safety or environmental and health safety. The Alsatian prefect concluded with the advantage of establishing a more visible and stable link between the STR and the European Commission "*in order to better highlight which aspect of their efforts derives from the guidelines and prescriptions*" of the EU. In fact the EU does suffer from a serious lack of perceived legitimacy and credibility among citizens, which the STRs can contribute to reducing.

Of the six main EU countries in terms of area and population, Poland, for the 2007-2013 period, is one of the main beneficiaries of the EU's cohesion policy (63.7 billion Euros). Spain had been for the previous period (2000-2006). With its integration into the EU, Poland also greatly benefited from the cohesion policy, receiving nearly 11.2 billion Euros for the years 2004 and 2006. These funds came mainly from the EU's Cohesion Fund and Structural Funds. Added to national and local funds, these monies were devoted mainly to the socioeconomic development of the country and its regions. To optimise their use, the Polish government made its territorial representatives the managers of these funds. The *voivods* (Polish STRs) are supported by a consultative body for this purpose. Hence they are deeply involved in managing these funds. A law of April 21, 2004, spells out their missions. Present at every stage in projects involving European structural funds, they appraise their application, determining the conditions for their use, and monitor their proper use. They are also responsible for transferring European funds to small and medium enterprises.

In the future, the *voivod* will become the certifying authority at the regional level. The Polish government has in fact decided to increase the European funds applied at the regional level and to decentralise their management. The *voivods* will therefore be required to refocus on their function as comptroller, with the State in any case remaining responsible in the case of improper use of the funds. In conclusion, the role of the STR is evolving in Poland. The devolution movement under way in these countries is the main explanation for this evolution.

Imre Forgacs, director of the Regional Public Administration office of Middle Hungary, representing Hungary, emphasized instead the value for his country of the European structural funds in the event of catastrophes, natural and otherwise. The Hungarian government benefited from 15 million Euros in aid from the European Commission following the flooding of the Danube and Tisza rivers in spring 2006. Here Imre Forgacs stressed the positive role of this aid, which was quickly mobilised. Furthermore, the Hungarian STR described at length the indirect usefulness of these funds for his government in redefining territorial balances, still under way. Hungary's reorganisation has been going on for the last twenty years. The speaker noted that Hungary has an institutional history marked by conflicts between the central State and the local communities. Seven regions were created in the 1990's, originally responsible mainly for development. A 2007 reform made it possible to truly devolve public decision-making to these regions. Of course the STRs are consequently called on to play a key role in managing these finds and more generally in implementing European policies.

Raoul Prado, general director of Regional Programmes for Portugal, Spain, Italy and Malta with the European Commission, brought this second half-day to a close. His presentation focused on three issues. First he described the relations the STRs have with the State, the populace and the European Commission. He then briefly described what European legislation has to say about structural funds. Finally, he dealt with the various roles that the STR may play, both technical and political, in managing these funds.

Raoul Prado began by stressing one point. This is no one approach to structural funds but rather about a hundred; that is, as many as there are programmes implemented using these funds. Indeed, the EU now has twenty-eight member States, meaning that many starting approaches. In addition, there are two types of structural programmes: regional, whose management in one form or another depends on the region and for that matter generally bears the region's name, and national, even though these may have a regional base like the one presented by the Italian speaker. Finally, within each member State, the regions may not all have the same status, which is the case in Italy or Spain, for example. Raoul Prado, who is responsible for ERDF and for the cohesion policy for the four States mentioned above, stressed the extreme heterogeneity of the situations he has to deal with. The four countries whose programmes he monitors in fact are unique in covering the entire range of possible situations. In Portugal, a country with a highly centralising culture, the regions are merely administration regions. They have no political existence of their own. The devolution process is in fact virtually nonexistent there. Hence when representatives of the Commission head for Portugal, they meet and discuss only with representatives of the State. Conversely, with the regions being strongly autonomous in Spain, these

regional programmes, when they are being formulated, do not assume intense participation by the STRs. So what sort of federating theme should be adopted here? One possible approach lies in the principle of solidarity, which Raoul Prado invited the audience to consider. A uniform definition of the role of the STRs would in fact be counterproductive. Given the number of different situations, a certain consistency can be obtained only by different means, taking into account the unique aspects of the different countries. This is also what makes European construction so rich and powerful, Prado insisted.

The second point is that European regulations do not say much about how these funds are to be managed by the national authorities. Article 12 of the basic funds regulations states simply that the structural funds are implemented at the appropriate territorial level, according to the constitution of each member State. This European regulation does not prescribe any manner in which to proceed. It simply indicates that, for their management, these funds assume a broad partnership among the authorities and, for regional programmes, the involvement of regional authorities, elected to the extent possible. The European Commission cannot reasonably expect to be more precise. For the Commission, it would run the risk of being criticised for interference, which for that matter has already happened.

As his third and final point, Raoul Prado mentioned what for him are the two roles of the STRs: "*mechanical*," participating as functionaries in implementing these funds, and "*political*." For its part, the European Commission distinguishes three functions essential to the functioning of all its policies: a management function, a certification function, and an audit function.

As these are national programmes, things are relatively simple. The ministries run them. The situation gets complicated when we get into the matter of regional programmes. In most of the member States, management authority lies with the State. The STRs or their equivalent serve this function. France's Alsace region is a counter-example, actually, since it is the regional council that was entrusted with management of the structural funds, on an experimental basis, for this region. Everywhere else, with the notable exception of Spain where the region's president serves this function, it is the STR who is the management authority. This system works. Things are less obvious in the case of controls. Twelve months after the adoption of a programme, each State is in fact required to send to the Commission offices a description of the management and control functions. Their approval by these offices determines subsequent payments. By operating this way, the Commission makes certain of the presence of administrative tools that allow effective steering of the programmes. Problems arise when these conditions are not met. The Commission's offices must then invite the State in question to review certain of its management and control procedures, which of course may take more or less time and meet with more or less success.

Finally, Raoul Prado talked about the "*politial*" role of the STRs, saying he hoped for a greater investment upstream from the projects. While all the regions, without exception, are represented in Brussels, and while the European commissioner in charge of the matter of funds often travels to the regions to meet with their elected officials and authorities, there are few direct contacts with the STRs. Do not the EU's offices, just like the STRs, have the same goal of ensuring territorial and social cohesion? Although they are natural partners, Raoul Prado regrets that they do not work more directly together.

As for the criticism made of the European institutions by the member States of excessively complex controls over the proper use of these funds, Raoul Prado did not deny their reality. He noted however that such controls are necessary. One means of simplifying them would be – as is done in the private sector – to have the administrative bodies adopt common norms and standards for certain types of expenditures. Controls would thus be greatly facilitated.

Finally, many participants took the floor to add to the speakers' remarks, in particular underscoring that the lack of perceived legitimacy afflicting European construction and its institutions is structural and derives from both the complexity of its history, the areas it covers, and the lack of intermediaries between it and the citizen. With few agents, the principle of subsidiarity plays a major role. In fact, we are seeing what François-Gilles Le Theule, director of the Centre for European Studies in Strasbourg, calls the "*rampant Europeanisation of public functions*." Furthermore, it is especially to the STRs that projects should be taken to implement them. On this question opinions differ; some, like Bernard Zahra, director of the Regional Institution of Administration of Bastia, believe that, while under the effect of European policies the culture of evaluation has imposed itself on all the governments of the member States, management of structural funds remains a national and local fact. Indeed, the partnership necessary to steering them assumes that the EU will hold itself back. Further, the European institutions wish to rely on a single responsibility, that of the States, whatever their organisation. The Netherlands' representative stated that here, too, the STRs have an essential role to play, by communicating more about European policies and about the use and successes of the European

structural funds. In the end, European construction, whose primary objective was the security – in the broadest sense – of its citizens, must never lose sight of this, its primary mission, without which it would lose all legitimacy in the eyes of those whose interests it is supposed to defend.

The STR and cross-border cooperation

The key issue of cross-border cooperation is one that the STRs are directly involved with. Europe knows no borders. The European citizen is less and less satisfied with these last administrative divisions. Given that, what instruments of cross-border cooperation should be developed? How does the STR participate in bi- or multilateral initiatives? What cooperation should there be among STRs for better border security under these conditions? These are the questions that the various speakers during the final half-day sought to explore, guided by Lodewijk de Witte, the session chair and governor of Vlaams Brabant province (Belgium).

In his presentation, Miguel Alejo Vicente, the delegate of the government of Castille and León (Spain), looked at cross-border cooperation from the security angle and most especially stressed the immigration issue. Placed under the responsibility of the Spanish Public Administration Ministry and responsible for the government's policy in their territorial districts, the delegates of the Spanish government are guarantors of security. In this they have the cooperation of the State's security forces and all of the agencies with responsibilities in the area of foreigners' residence and reception, like the "foreigners' offices," for example. Now the crisis of the Nation-State, economic globalisation and its consequences are raising new challenges for the public authorities. These challenges have in particular highlighted the problems for classic administrative structures in dealing with the emerging risks. Currently, Spain is confronted by two major security issues: international terrorism, with ETA still a threat for the people and the authorities, and immigration phenomena. Given the dimension taken on by these problems, the public authorities must constantly adapt their responses, always assuming greater cooperation among States. Miguel Alejo Vicente believes that most of the problems faced by the States in isolation have taken on a global dimension and in fact now concern all. Terrorism, poverty or the lack of democracy are closely linked phenomena that imply a coordinated response by the States, both politically, economically and socially, and in terms of security.

This consideration takes on its full meaning when we deal for example with the immigration issue. From being a country of emigration, Spain has become a land of immigration. The population of foreign nationals residing in Spain today represents 9% of the total Spanish population.

The European agency FRONTEX, established in 2004, is a first response and a valuable tool for cooperation. It contributes to border security by strengthening the coordination of efforts by the member States in carrying out Community measures relating to management of external borders to avoid the influx of illegal immigrants. In order to be fully effective, these types of tools must however be accompanied by a truly European immigration policy which Spain hopes for, especially in the areas of residence, integration and development assistance.

More generally, the Schengen accords signed in 1985 assume that controls at the EU's external borders will be reinforced. These accords substantially deepened relations between adjoining States. They led Spain to develop its relations with France and Portugal. The 20th Franco-Spanish summit held in January 2008, for example, enabled these two governments to reach a decisive agreement on combating terrorism, in particular allowing the creation of permanent investigation teams common to the two countries. Likewise, the last Hispano-Portuguese summit in 2008 saw the establishment of the Hispano-Portuguese Council on Security and Defence. This should make it possible to develop joint military operations, especially in external theatres of operation, and the creation of mixed law enforcement teams.

The prefect of the Atlantic Pyrenees, whose district shares a common border with Spain, started from a simple premise. Because of the economic and legal changes in the relations between neighbouring member States of the EU, borders no longer constitute a limit on activities. On the contrary, they have become so ordinary that local populations no longer consider them to have any symbolic or practical meaning. Rather, they determine behaviours of opportunity: more advantageous taxation, different prices for the same products, different real estate pricing....

On the Basque coast, an urban conglomeration of some 600,000 people has grown up on the two sides of the border along a highway running down the coast. But while the economic and social dynamic of this territory tends to unify it, the public services are more a source of rupture than of continuity. For example, the Spanish citizen who owns property in France cannot pay his local taxes simply by debits made by the French Public Treasury from his Spanish bank account. Likewise, an accident victim along the border will be taken by the emergency

services to a hospital in the district where the accident occurred and not to the hospital where he is ordinarily cared for and which may even be closer. Finally, the neighbourly relations of the San Sebastian airport for the city of Hendaye, which 80% of its traffic flies over, are governed by an international agreement between the two countries whose terms and conditions are not submitted to local actors. In this regard the institutional evolution of the two countries, with autonomisation of the Spanish regions and devolution in France, has complicated the situation, with the powers left to the STRs in France being major.

The 1995 Treaty of Bayonne attempted to provide answers by proposing multiple tools for French (GIP – Public Interest Group) or Spanish (consorcio) cooperation. All of them left out the State, which in France is the guarantor of many essential elements of the life of its citizens. A unique mechanism for cooperation was nonetheless brought to life by the local authorities. Established on March 1, 2007, this cooperation took the form of an association bringing together all of the local communities concerned (Aquitaine region and the department of the Atlantic Pyrenees, Basque Autonomy and the Guipúzcoa delegation) in which the representatives of the French State were appointed members by right. This formula was validated by the French and Spanish foreign affairs ministries. It provided a framework and legal coverage for exchanges which up to then had been the exclusive purview of diplomats. This cooperation tool brought forth numerous areas of common work for authorities on both sides of the border. These multiple realms of cooperation mainly involve the exchange of information and the implementation of common management tools. For example, coordination of the management of the major cross-border highways was improved. Likewise, the rescue plan for Spain's Fontarabie airport was communicated to the French authorities and joint exercises were scheduled. Discussions are currently under way to equip the Spanish-side basin of the rivers of the border coast (Bidassoa) or those flowing into France (Nivelle) with flood-forecasting instruments. Epidemiological issues, especially in the area of animal health such as pseudo foot-and-mouth disease, also known as bluetongue, have also been taken up.

Cooperation has not been limited just to administrative police matters. Economic and social issues quickly imposed themselves. Specifically, a connection was organised between the Bayonne URSSAF (a private body in France responsible for collecting social security taxes) and the General Social Security Fund of Guipúzcoa in the interest of the economic actors operating in the region. Here there are many approaches: informing employees and enterprises on both sides of the border of their rights and obligations in the area of social security taxes, monitoring flows of workers and companies crossing the border, combating fraud and illegal labour.... Hospital cooperation is also being considered so as to develop a complementary approach between hospitals on both sides of the border.

Finally, topics associated with the environment have also been dealt with in this coordination effort. The special place of the prefect in France, as a representative of the State but also a potential coordinator and advisor to local authorities, gives him a unique responsibility in cross-border cooperation. But it is still necessary for his government to authorise him to do this, and for the State authorities of the neighbouring country to wish this as well.

Frank Scherer, Regierungsvizepräsident – Freiburg – Baden Württemberg (Germany), described the cross-border cooperation established by the region of the Upper-Rhine with France and Switzerland. With six million inhabitants and a GDP of 165 billion Euros annually, this region in the heart of Europe enjoys strong economic growth. He noted first of all that one of the key elements of European regional policies is territorial cooperation. This relies on better communication between communities located on either side of the border (meetings, conferences on varied subjects) and on carrying out joint projects. These projects benefit from many European funds. For example, the INTERREG IV A funds provided for all of the EU for the 2007-2013 period amount to 7.75 billion Euros. The INTERREG A envelope assigned to the Upper Rhine region included 67 million Euros. Added to the German, French and Swiss national funding, this amount rises to 144 million Euros. These funds go to ensure funding for cross-border cooperation projects which assume the participation of the territorial administrations and the State. They touch on many subjects: police, customs agents, cultural, universities, economic.... Frank Scherer cited many examples: construction of heavy infrastructure like the bridge linking the cities of Strasbourg and Kehl; university cooperation between the universities of Basel, Fribourg-en-Brisgau, Karlsruhe, Strasbourg and Mulhouse, united within a European confederation of the universities of the Upper Rhine; strengthened police and customs cooperation between France and Germany based in Kehl and bearing on the exchange of information relating to investigations conducted by these various services.

European cooperation and structural programmes also imply that administrations have to adapt and evolve. The role of the STR is very extensive here in the Upper Rhine, so much so that he is called "the little foreign affairs minister" by all of the other local bodies. This manifold

cooperation has required the creation of four Euro regions of which the Upper Rhine is a member. Each one has a different status, and just one has a corporate personality, the Pamina region, while the others consist more of communication platforms. Finally, Frank Scherer ended his remarks by stressing that this cooperation also needs to be initiated on site. In future the role of the STR, which is already significant now, will surely grow. Today his functions include giving an appropriate legal and administrative framework to these projects and ensuring a share of funding for them. His role should evolve in future more towards lobbying the authorities in Brussels.

Paulus Skardzius, director of the public administration department in the Lithuanian Interior Ministry, began his remarks by geographically situating his country. Lithuania has four bordering countries: Belarus, Estonia, Poland and Lattvia. Lithuania has ten counties, only one of which has no borders with another State. Its cross-border cooperation is based on the Madrid Convention signed and ratified in 1997, and its added protocol signed in 2002. In addition there are the new European Commission regulations 10-82 on territorial cooperation.

For Lithuania, cross-border cooperation is an opportunity. The local Lithuanian communities are invited to develop agreements with the bordering foreign communities. The county governors' function is to coordinate regional projects. For this they rely on the Regional Development Council and lead work groups within the many intergovernmental commissions. They are also involved in the funding of some of these projects and have many powers in the area of territorial development.

There are many tools for cross-border cooperation: Euro regions, cross-border programmes funded by the EU, European Groupings of Territorial Cooperation (EGTC), and the many instances of cooperation within Lithuanian government bodies. Cross-border cooperation agreements have been signed between Lithuania and its neighbours aimed at promoting and facilitating cooperation between the territorial communities of each State. Dedicated national units monitor the progress of this cooperation. For example, a Lithuanian-Polish intergovernmental commission was set up in 1996 to monitor all cooperation projects between the regions of these two countries. It is involved at all stages of this cooperation and in some cases initiates it. It is able to support development, for example in terms of land-use planning. It is involved at the legal level in order to resolve certain difficulties. Lithuania also relies heavily on its six Euro regions. Some forty municipalities out of a total of about sixty, and six counties out of ten, are part of a Euro region.

This cooperation covers different objects. They include among others economic development, transport infrastructure, and social, environmental and energy issues. There are many sources of funding. In addition to national funding, all of these projects receive many different European credits. This is the case for example with the programme covering the 2007-2013 period relating to co-development of the Lithuanian-Polish cross-border regions, focusing on social cohesion and the competitiveness and productivity of these regions, for which the total EU contribution will reach seven million Euros by the end of 2013. A great deal of international funding has also made this cooperation possible, especially with EU non-member countries, where the projects are no less numerous, as for example with Belarus, concerning environmental protection and tourism development.

Within this vast movement, the STRs, heading up many different coordination and steering bodies (regional development councils, various work groups) play a coordinating role. They are both initiators and a source of proposals. They approve the projects submitted to them by the local authorities. Overall, the Lithuanian speaker stressed the fact that, beyond the many topics covered by this cooperation, its value lies in bringing the States closer together, including those that are not part of the EU.

Finally, Perla Stancari, prefect and central director for civil rights, citizenship and minority groups under Italy's Interior Ministry, described cross-border cooperation in Italy. She noted that Italy, a fervent partisan of Europe, was one of the first member States to sign the framework Madrid Convention of May 21, 1980. Prepared under the aegis of the Council of Europe, this agreement ascribes jurisdiction to local communities or authorities for concluding conventions in their own behalf with cross-border territorial authorities of equal rank. These forms of localised cooperation are supported by Community institutions, which see in them a preferred tool for European construction. This is shown by the development in the 1990's of the many cooperation projects that benefited from INTERREG funding programmes. Likewise, the creation of dedicated legal tools, such as the European Groupings of Territorial Cooperation (EGTC), shows the EU's desire to facilitate these connections.

Reporting to the Interior minister, the prefect in Italy is the guarantor of the general interest. As such, he coordinates the activities of the administrative bodies present in the Province for which he is responsible. He is the guarantor of public order and the exercise of freedoms. By virtue of his position, the prefect is both contact and intermediary, between local and central government bodies and between these and the citizen. He is also able

to initiate many projects. His status makes him a key actor in cross-border cooperation today. Indeed, the growing complexity and diversity of the areas involved in this cooperation make the prefect the natural liaison between all of the projects implemented and the partners involved. In Perla Stancari's own words, the prefect is responsible for establishing "*bridges*" between border spaces. Today this cross-border cooperation is not merely essential for the proper governance of the territories which these borders cross; it also has a geopolitical dimension. The EU's progressive expansion in fact implies new frontiers, both internal and external.

Cross-border cooperation today concerns all those subjects that are most in the public eye. This is the case with security, for which the Italian Interior minister has concluded bilateral agreements with Austria, Switzerland, France and Slovenia. Many bodies common to different countries have thus been created to deal with these issues. The Franco-Italian Commission for maintenance of the national border and the Franco-Italian Commission on cross-border cooperation have brought the prefects of Imperia for Italy and the Alpes-Maritimes for France closer together. There have been many joint police operations. These operations have involved both surveillance and control of road and rail networks. They have also involved coastal areas. The two countries have also set up joint highway brigades.

This cooperation now extends to civil defence and to matters affecting the environment. For example, the Italo-Slovenian Commission for Hydroeconomy has enabled these two countries to develop a joint strategy in balancing water resources, which includes not just the dams located in border areas but also pollution phenomena. Likewise, the International Commission for the protection of Italo-Swiss waters against pollution, involving Lakes Maggiore and Lugano, among others, and the French-Italian-Monegasque Commission to safeguard water quality on the Mediterranean coast (RAMOGE) provide better knowledge of the phenomena of pollution and greater awareness of the various actors involved in questions associated with the environment.

In terms of culture and training, cross-border cooperation provides the means to overcome historic divisions and stereotypes. These divisions and stumbling blocks must be overcome not just in the interest of bringing European citizens closer together but also in the interest of greater economic cooperation. To this end, in 2005 the Bureau of International Cooperation and Border Zones launched an initiative entitled "T*o promote mutual knowledge - How to promote knowledge of the neighbour's language and culture in border zones*." This event, held in collaboration with the prefecture of Trieste and the Council of Europe, brought together many of those responsible for education policies from Austria, Croatia and Slovenia, as well as representatives of the Friuli-Venezia-Giulia region, the University of Trieste, the Chamber of Commerce and the European Centre for Living Languages of Graz, and the Linguistic Academy of Maastricht.

Hence there are many initiatives that were made possible through cross-border cooperation. As Perla Stancari stressed in her remarks, today the border is "*less a factor for division than a factor for union.*"

These days were brought to a close with the concluding remarks of Thierry Aumonier and Daniel Canepa. As the former noted, behind the topic of this 15th meeting, prefects in European integration, there is another question, that of the role of "*STRS' role as mediator between Europe and its citizens.*" Thierry Aumonier expressed his satisfaction that the various participants had brought this issue to the forefront. This new role, he emphasised, is one the STRs are ready to take on. What is more, they are calling for it. This redefined place of the STR is justified by the interconnecting nature of the subjects dealt with by the EU, by the growing role of the regions in European construction, and by the increasing importance of security issues in the European debate. Given his many attributions – legal, financial, political – isn't the STR naturally called on to hold a key position in the European architecture of tomorrow? Bridge, link... the qualifiers are many to describe his function. In short, the State Territorial Representative is also Europe's representative. And he is ready to take on the task.

In short, concluded Daniel Canepa, this strong demand by the STRs to play a new and strengthened role in European construction is perhaps only a reflection of those broader demands by citizens who are often unaware of everything about Europe but who nonetheless expect much from her. This search for better services rendered to the citizen is common to all of the territorial representatives of the EU member States and constitutes a bond that joins them all and guides them towards the same goal.

LIPSIE Languages

Conclusions du séminaire Euro-Caraïbe en matière de protection de l'euro

Guadeloupe, 28 - 31 janvier 2008

Dans le cadre du programme européen « Périclès », mis en place par l'Office européen de lutte anti-fraude (OLAF) de la Commission européenne, dédié aux actions en matière d'échange, d'assistance et de formation pour la protection de l'euro, l'Office central pour la répression du faux monnayage (OCRFM) de la direction centrale de la Police judiciaire française a organisé sur le site de Saint Anne, en Guadeloupe, du 28 au 31 janvier 2OO8, un séminaire à vocation internationale, consacré à la protection de l'euro et à l'évaluation de la menace dans la zone de l'Arc Caraïbe.

Cette manifestation, qui a réuni un public spécialisé de policiers, de magistrats et de la Banque centrale, a consisté à échanger avec les délégations caribéennes sur l'expérience européenne en matière de protection de l'euro, partagée avec nos homologues des offices centraux européens, soutenue par les institutions européennes : OLAF, ETSC [1], EUROPOL, et internationale : INTERPOL.

Depuis l'adoption de l'euro, en janvier 2002, et l'élargissement d'un marché constitué de plus de 300 millions de ressortissants européens, les contrefacteurs nationaux ont été rapidement concurrencés par d'autres producteurs tout aussi expérimentés en matière d'offset avec, pour certains, leur propre expérience acquise avec la contrefaçon du dollar américain, et tout aussi organisés dans la mise en place des réseaux de circulation et de distribution. L'adoption de l'euro a élargi les frontières de la coopération internationale qu'il s'agisse de l'Europe de l'Est ou de l'autre continent d'Amérique du Sud.

Pour la première fois, grâce au programme Périclès, la région de l'Arc Caraïbe a été appréhendée sur cette problématique spécifique du faux monnayage :
- quel est l'état du faux monnayage dans ces différents pays ?
- quelles sont les voies de circulation et de distribution empruntées pour écouler les faux euros produits depuis ce continent ?
- existe-t-il des liens entre le faux monnayage et les autres trafics criminels majeurs de cette zone : trafic de drogues, immigration irrégulière, traite des êtres humains, blanchiment d'argent ?

Les objectifs suivants ont été visés :
- obtenir une évaluation de la menace de l'euro ; solliciter la mise en place de structures adaptées à la détection et à la protection de l'euro, en proposant aux institutions policières, judiciaires et bancaires les dispositifs mis en place au sein des organisations européennes chargées de la protection de l'euro (centres nationaux d'analyse et de classification des contrefaçons, obligation de recyclage des billets et des pièces par la branche institutionnelle bancaire, centralisation des informations par les offices centraux nationaux, etc.) ;
- s'assurer du maintien de la confiance dans l'euro, par le public, en apportant l'ensemble des informations nécessaires à la reconnaissance de cette monnaie, à une détection optimisée des faux tant par les instituts bancaires, commerciaux, opérateurs de change, que par les usagers ;
- insister sur le renforcement nécessaire de la coopération internationale, policière, judiciaire et autre ;
- retranscrire les besoins spécifiques en formations, échanges formulés par les délégations.

Un séminaire reposant sur le partenariat institutionnel

L'exemple des Antilles françaises

Ce projet a pris en compte une situation géographique particulière, impliquant un partenariat soutenu avec les Pays-Bas et la Grande-Bretagne, ainsi que le soutien d'autres offices centraux nationaux européens. L'idée originale de ce séminaire a été de partir de la situation française constatée au sein des Antilles en matière de faux monnayage et de poursuivre cette réflexion sur l'ensemble de cette zone.

....

(1) L'Office européen de lutte anti-fraude : OLAF ; Centre technique et scientifique européen : ETSC.

S'agissant de la France, des départements d'outre-mer sont rattachés au territoire métropolitain : la Guadeloupe et ses rattachements (Saint-Barthélemy et Saint-Martin), la Martinique et la Guyane française. Partout, l'euro circule de la même façon qu'en métropole. Saint-Barthélemy et Saint-Martin évoluent vers une structure plus autonome, depuis 2007, en devenant des communautés d'outre-mer (COM), régies par l'article 74 de la Constitution française.

Pour la Hollande, les Antilles néerlandaises étaient, jusqu'au 30 juin 2007, un ensemble de cinq îles principales situées dans la mer des Caraïbes : Bonaire, Curaçao, Saba, Saint-Eustache et la partie méridionale de l'île de Saint-Martin (Sint-Maarteen), l'autre partie étant sous souveraineté française. C'est un territoire dépendant des Pays-Bas, formant juridiquement un des trois actuels États du royaume des Pays-Bas, la fédération des Antilles néerlandaises. Depuis le 1er juillet 2007, l'État fédéral autonome des Antilles néerlandaises a amorcé sa dissolution progressive, qui sera effective le 15 décembre 2008, après le transfert complet des compétences de l'État fédéral autonome, soit vers ceux des deux nouveaux territoires autonomes de Curaçao et de Sint-Maarteen (qui formeront alors deux futurs États autonomes au sein du royaume des Pays-Bas, en plus de celui d'Aruba et de l'État des Pays-Bas), soit vers l'État des Pays-Bas pour les trois nouvelles communes néerlandaises à statut particulier : Bonaire, Saba et Saint-Eustache qui pourraient adopter l'euro. C'est ainsi que les îles néerlandaises sont classées en deux groupes suivant leur situation géographique : les îles du Vent avec Sint-Maarten, Saint-Eustache et Saba situées au nord des petites Antilles et à l'est de Porto Rico et les îles sous le vent : Bonaire, Curaçao, Klein Bonaire et Klein Curaçao auxquelles se rattache Aruba, bien qu'elle ne fasse pas partie des Antilles néerlandaises qui sont situées au large de la côte du Venezuela.

Pour ce qui concerne la présence de la Grande-Bretagne dans cette zone, on retrouve les îles d'Anguilla, les îles vierges britanniques, les îles Turks et Caicos, les îles Caïmans et Monsenat.

Les partenaires

Les partenaires opérationnels

L'Office central pour la répression du faux monnayage s'est, en outre, appuyé, pour la réalisation de ce séminaire, sur l'expertise européenne des offices centraux nationaux :
- espagnol : très investi dans un partenariat pérennisé avec la Colombie, tant en matière de formation, que sur un plan opérationnel ;
- italien : doté d'une forte expérience en matière de démantèlement d'officines offset principalement installées dans la partie sud du pays pour les billets et découverte d'ateliers clandestins pour la fabrication des fausses pièces d'euro ;
- Portugais : constituant un modèle d'organisation en matière de protection de l'euro, concerné par les axes de circulation des faux établis entre l'Italie, la France et l'Espagne.

Il convient, par ailleurs de souligner le travail de relais efficace effectué dans cette zone géographique éloignée de la métropole par nos correspondants du Service de coopération technique international de police (SCTIP). Ces derniers ont, en effet, pris en compte nos demandes d'invitation auprès des autorités locales étrangères invitées. Quatre d'entre eux ont participé à la totalité des travaux en raison de l'intérêt porté à la nécessité d'une coopération policière accrue dans cette région et de leur curiosité à mieux connaître, voire à découvrir la thématique particulière en matière de protection de l'euro. (délégation d'Haïti, Sainte-Lucie, Cuba et Miami).

Le *secret service*, quant à lui, a répondu présent à l'invitation, les représentants de Miami et de Porto Rico étaient présents pour évoquer leur propre expérience en matière de contrefaçon du dollar.

L'office central a sollicité, en outre, ses partenaires nationaux institutionnels indispensables au développement d'une politique interministérielle de lutte contre le faux monnayage. L'importance de ce partenariat institutionnel tant avec la Banque de France (BDF) que la Monnaie de Paris a d'ailleurs justifié l'élaboration commune et la signature conjointe d'un protocole d'accord officiel d'assistance mutuelle, d'échange du renseignement et de l'analyse statistique. Ce protocole a été signé avec la BDF à l'occasion du passage à l'euro en janvier 2002, et est actuellement en cours de signature pour la monnaie métallique.

Les instituts d'émission de monnaie

Il s'agit de la Banque de France pour les billets, et plus particulièrement de la direction de l'Industrialisation, de la Recherche et du Développement. En outre, l'Institut d'émission monétaire de Guadeloupe était également mobilisé. Pour les pièces, la Monnaie de Paris, établissement public à caractère industriel et commercial, était représentée par le directeur du Centre national d'analyses des pièces en euro.

Les juridictions interrégionales spécialisées (JIRS)

Les JIRS sont composées de magistrats spécialisés en matière de criminalité organisée. Le faux monnayage en France, comme dans de nombreux autres pays, est apprécié en terme de criminalité organisée. Il rentre, en effet, dans les catégories d'infractions les plus dangereuses (crime de fabrication de fausse monnaie, et délit de mise en circulation commis en bande organisée) nécessitant la mise en place de prérogatives d'enquêtes dérogatoires au droit commun (sonorisation, infiltration, achat de confiance, etc.).

Les organismes internationaux

Ce séminaire a reçu le soutien des organismes internationaux tels qu'Europol et Interpol. Enfin, il convient de souligner la mobilisation des dix-huit délégations étrangères composées à la fois de policiers et de magistrats. Toutes ont répondu présentes et beaucoup d'entre elles ont signalé la nécessité d'améliorer, voire de mettre en place des structures efficientes en matière de tri, de détection et de recensement des faux et de contrôle des opérateurs de change. Très peu d'entre elles connaissent véritablement les signes de sécurité propres à l'euro, et sont demandeurs de formations plus techniques sur ce point. De même, de façon récurrente, la question a été posée de savoir ce qui devait être fait des faux euros détectés et quelles autorités devaient être contactées pour faire remonter l'information.

Certaines des délégations ont présenté un exposé de leur situation locale en matière de faux monnayage, comme la Colombie, le Venezuela, la République dominicaine, la Fédération néerlandaise des Antilles (Curaçao, Saint-Martin), Cuba, Haïti, le secret service de Miami et de Porto Rico ; d'autres ont émis le souhait d'intervenir lors du temps de parole qui avait été aménagé durant la matinée du mardi 29 janvier (Haïti, Suriname, Guyana). Enfin, d'autres délégations ont pu intervenir lors des questions posées à l'issue des interventions.

Le faux monnayage dans l'Arc Caraïbe

L'impression générale dégagée laisse transparaître de façon assez évidente la disparité des situations des différents États composant la zone caraïbe. Les différences linguistiques, culturelles, politiques, économiques sont autant d'éléments qui ont fait de ce séminaire sa difficulté relative et son ambition. Des réflexions spontanées faites par les divers intervenants, il est apparu que ce séminaire avait été véritablement une occasion assez exceptionnelle de réunir la majeure partie de l'Arc antillais élargi, naturellement, aux pays d'Amérique latine avoisinants comme la Colombie et le Venezuela.

Antilles françaises

La direction interrégionale de Police judiciaires des Antilles-Guyane françaises a initié l'action contre le faux monnayage. La DIPJ Antilles Guyane a été mise en place, dans sa structure moderne, à partir de 2004, et existait

© Ministère de l'Intérieur/DCPJ/OCRFM

sous sa forme initiale depuis 1985. Une centaine de fonctionnaires de police sont en poste pour couvrir une zone de compétence comprenant la Guadeloupe et ses dépendances (Saint-Barthélemy et Saint-Martin), la Martinique et la Guyane. Il existe donc un éclatement géographique pour ces entités territoriales. Par exemple, deux cents kilomètres séparent la Guadeloupe de la Guyane. Cependant, l'intégralité des services développés en métropole existe de manière identique au sein de la structure antillaise : une police technique et scientifique spécifique, une division criminelle, une division financière.

La structure Guyane comprend douze fonctionnaires. Elle fait office de Groupe d'intervention régional (GIR) permanent : structure interministérielle réunissant les forces de la Police nationale, de la Gendarmerie nationale, des douanes, de l'administration fiscale et du travail.

Saint-Martin réunit quatre policiers. Il s'agit d'une représentation territoriale en cours de transformation, avec un rattachement prévu à l'antenne de l'Office central pour la lutte en matière de stupéfiants (OCTRIS), et de nature interministérielle (police et gendarmerie).

L'importance fondamentale de la coopération internationale dans cette région donnée a été mentionnée. C'est la raison pour laquelle le siège de la DIPJ installé en Guadeloupe est devenu un sous-bureau d'Interpol. L'ensemble des pays de la zone 8 peuvent ainsi se servir de cette structure pour des échanges qui dépassent largement le domaine de l'informel, mais ont, au contraire, une valeur juridique officielle permettant une intégration des réponses obtenues en procédure. Ce sous-bureau Interpol constitue donc une interface dans cette zone, y compris pour des messages expédiés à destination de la métropole. En outre, la DIPJ fait partie de l'association des chefs de polices de la Caraïbe qui propose un système d'échanges d'informations.

La prise en compte, par la direction centrale de la Police judiciaire française de la nécessité de développer la coopération internationale, s'est traduite par la création d'un poste spécifique de chargé des relations internationales afin d'assurer un suivi optimal des demandes de coopérations internationales. Dans chacune des structures territoriales de la DIPJ existe un représentant fausse monnaie qui a été formé par l'OCRFM (Guadeloupe, Martinique, Guyane).

L'analyse de la criminalité dans cette zone géographique met en évidence un taux moyen des vols égal à celui de la France métropolitaine. Cependant, il existe une véritable difficulté pour la part des vols commis avec armes, deux à trois fois supérieure à la France métropolitaine. Le taux des violences et menaces à personnes est au même niveau qu'en région parisienne. Quant à la criminalité organisée, elle est tournée majoritairement vers le trafic des produits stupéfiants (cocaïne, crack, cannabis). Depuis 2004, la Martinique a été renforcée dans ses structures de lutte contre ce trafic. De même, Saint-Martin est une route obligée des narcotrafiquants pour les flux maritimes à destination de l'Europe et de l'Afrique.

En matière de faux monnayage, l'activité n'est pas préoccupante mais pour autant bien installée, plus particulièrement en Guadeloupe. La fausse monnaie représente 5 % des faits de criminalité organisée. Huit familles de contrefaçons locales ont été créées par la Banque de France pour des billets contrefaits de 20, 50 et 100 euros. Plusieurs affaires mettant en cause des équipes constituées ont été réalisées. En début d'année 2007, par exemple, cinq individus ont été interpellés en Guyane, pour des faits de fabrication et de mise en circulation de faux billets de 50 euros fabriqués localement à partir d'une chaîne graphique. L'intégralité du matériel utilisé a été saisie de même que la fourniture utilisée pour la réalisation du patch holographique. Seuls trente et un billets ont été saisis, l'enquête ayant permis de mettre rapidement fin à cette source de fabrication. Les nationaux mis en cause étaient originaires de Guyane et du Brésil.


© Ministère de l'intérieur/DCPJ/OCRFM

La banque de France a affiné son analyse dans cette zone géographique. Elle constate que les fausses coupures de 20 et 50 euros représentent 89 % de la totalité des contrefaçons décelées dans les trois départements. Dans la part des classes communes, 33 % des fausses coupures sont imprimées en *offset*. Ces classes communes (de nature européenne) représentent elles-mêmes 38 % de la masse totale du faux monnayage, ce qui signifie que le volume majeur restant provient de fabrications locales.

Les cinq premiers indicatifs qui structurent la part des contrefaçons *offset* détectées sont parmi les contrefaçons

les plus répandues sur l'ensemble de la zone euro. Il est intéressant de constater que la contrefaçon EUA 50P20 d'origine colombienne constitue la part la plus importante (16 %). Suivent les contrefaçons *offset* d'origine italienne eua5Op05, eua100p07, eua20p02, puis une autre contrefaçon colombienne eua50p19. La quasi-totalité des contrefaçons eua50p20 colombiennes a été détectée en Guyane. Par ailleurs, des liens techniques ont été révélés par la Banque de France avec trois nouvelles contrefaçons dont les indicatifs suivent : fra 20K175, fra 50K169, fra 100K48. Ces éléments de nature technique laissent à penser que des liens peuvent être faits avec des membres d'une même équipe.

Le département de la Guadeloupe mérite une attention particulière parce qu'il représente la part la plus importante des contrefaçons locales. Pour la Martinique, la répartition entre classes locales et communes est de 50 %. La Guadeloupe représente 60 % du chiffre global, suivie par la Guyane puis la Martinique. En matière de faits constatés police, il existe une recrudescence de 21 % par rapport à 2006.

Colombie

Les représentants des deux services répressifs particulièrement actifs dans la lutte contre le faux monnayage, le Département administratif de la sécurité (DAS), dépendant directement de la présidence de la République colombienne et la direction des Investigations criminelles (DIJIN), unité de lutte contre le faux monnayage, étaient représentés.

L'arsenal juridique mis en place en matière d'incrimination et de peines est le suivant :
- la fabrication de fausse monnaie nationale ou étrangère est punie de 6 à 10 ans d'emprisonnement ;
- le trafic de fausse monnaie est puni de 3 à 8 ans ;
- l'émission est punie de 3 à 10 ans ;
- la mise en circulation est punie de 2 à 4 ans.

Le représentant de la DIJIN a évoqué l'alliance stratégique avec l'Office central espagnol (BIBE), l'OLAF, EUROPOL et INTERPOL, en termes de formations et coopérations opérationnelles. Un listing chronologique des opérations policières de démantèlement d'officines *offset* très significatives en termes d'organisations criminelles ou de montant du préjudice a été produit.

Cependant, les chiffres présentés expriment un préjudice en terme de valeur financière. Les chiffres du nombre de billets saisis, y compris par valeur faciale et par contrefaçon, n'ont pas été communiqués. Une recherche est en cours auprès des services d'Europol.

4 juillet 2004 : opération Eurogreen, démantèlement de la première imprimerie d'euros en Amérique. Saisie en contre-valeur de 54 400 euros.

17 octobre 2004 : opération Atlantique, démantèlement d'une imprimerie représentant, jusqu'en 2006, la quantité en contre-valeur la plus importante : 2 millions d'euros.

31 octobre 2006 : opération Caldas, saisie en contre-valeur de 5 millions d'euros.

14 juin 2007 : opération Eurotree y Greenday, démantèlement de l'organisation criminelle la plus importante en matière de fabrication et de trafic de fausse monnaie. Dix personnes interpellées, des billets de 500 euros ont été imités (contrefaçons référencées eua 50P14, eua 100PO9).

16 juillet 2007 : opération euromedellin, une organisation criminelle est démantelée. Le centre du trafic est situé au cœur de la ville de Medellín. De la monnaie locale, des faux dollars et des faux billets de 100 euros sont fabriqués. Six personnes sont interpellées. La monnaie contrefaite est expédiée dans les villes de Bogotá, Pereira, Barranquilla, Cucuta, et, pour les faux euros à destination des pays suivants : États-Unis, Guatemala, Équateur, Venezuela et Espagne.

26 juillet 2007 : opération Eurocali, fabrication en contre-valeur de 700 000 euros contrefaits, la valeur faciale imitée est de 50 euros. Les investigations ont duré huit mois. Sept personnes ont été interpellées. L'intégralité du matériel *offset* a été saisie (EUA 50P20). D'autres monnaies ont été fabriquées : bolivars, dollars. Les routes de distributions des faux euros ont été organisées par voies postales, grâce à la complicité de pilotes de ligne, à destination de l'Espagne, de la France, du Portugal, de l'Angleterre, de la République dominicaine, des États-Unis et de la Suisse.

11 octobre 2007 : opération Bogotá métal, une fabrique clandestine de fausses pièces de pesos péruviens et de deux euros est démantelée. Les mis en cause avaient une activité professionnelle en relation avec la métallurgie, et étaient également impliqués dans le trafic de cocaïne. Des méthodes identiques de dissimulation et de sortie du territoire étaient utilisées pour les deux types d'activité (sans plus de précision).

De façon plus générale, la grande majorité des imprimeurs *offset* mis en cause dans la fabrication de la fausse monnaie travaillait officiellement dans une société commerciale d'impression et d'édition en tout genre, cartes de visite. Plus rarement, on retrouvait d'anciennes machines *offset* d'occasion rachetées et installées dans des lieux privés.

Les fabrications de fausse monnaie sont, en fait, réalisées par des équipes différentes en fonction des commandes, organisées selon le principe de séparation stricte des tâches pour diminuer les risques : fabrication, transport, mise en circulation. Les euros falsifiés sont logiquement destinés à l'exportation, essentiellement à destination des pays d'Europe : l'Espagne reste une voie d'accès privilégiée en raison, très certainement, d'une langue commune partagée qui facilite d'autant les mises en relations avec les intermédiaires. Cependant, certains pays de l'Arc caraïbe ne sont pas épargnés : Saint-Martin, la République dominicaine. Toutes les voies de transport en fonction des circonstances sont utilisées : voies postales, avions, bateaux.

Selon les déclarations de nos collègues colombiens, il n'existe pas de liens systématiques entre ces organisations criminelles et les mouvements des Forces armées révolutionnaires de Colombie (FARC), car les premiers disposent désormais d'une certaine autonomie et d'un marché de commande bien installé. Il peut, au cas par cas, y avoir des liens avec les trafiquants de stupéfiants, notamment de cocaïne (*cf.* opération eurométal). Les circuits de distribution usités sont alors les mêmes.

Le représentant du Venezuela est venu compléter de manière très intéressante cette analyse de la situation du faux monnayage dans ce secteur géographique. Ce pays constitue, en effet, un canal de distribution des faux dollars à destination de Porto Rico, Haïti et Cuba.

S'agissant des faux euros, il n'a pas été recensé pour l'heure de canaux majeurs de distribution vers les Caraïbes, certainement en raison du fait que le marché est encore mal connu.

Cuba

6 % du faux monnayage est constitué de faux euros. L'influence touristique y est certainement pour quelque chose.

Suriname

Les opérations de change amènent la découverte de faux euros. Ceux-ci proviennent de la Guyane française et du Guyana. Le problème invoqué réside dans le fait que de nombreuses opérations de change se font dans la rue, en dehors de tout contrôle. Quant aux agents de change qui découvrent des faux euros, leur destruction est purement et simplement réalisée, sauf pour un remettant identifié sur une transaction frauduleuse. En outre, ces faux euros ne sont pas comptabilisés. Les faux billets sont bien sûr repérés au niveau des agences bancaires et de la banque centrale du Suriname. L'analyse produite suggère des fabrications en chaîne graphique et essentiellement des impressions laser. L'importance de la coopération internationale et régionale a été rappelée à cette occasion. C'est ainsi que le Suriname a développé une coopération avec la Guyane française et le Brésil.

Haïti

Le représentant de la délégation a indiqué dans ses conclusions que les statistiques haïtiennes en matière de faux euros, bien que très loin derrière la France, n'expriment que les cas de faux monnayage rapportés aux autorités policières et bancaires, et, en cela, ne signifient pas que les risques pour les différentes monnaies nationales et étrangères qui ont cours légal en Haïti ne sont pas importantes.

Au contraire, la position limitrophe d'Haïti avec la Colombie suffit à elle seule pour retenir l'attention des autorités haïtiennes, « *surtout lorsqu'on connaît les liens étroits qui existent entre les secteurs criminels colombiens, dominicains et haïtiens dans le domaine du trafic de la drogue et des véhicules volés* ». Un exemple propre au faux monnayage a été cité, celui d'un Haïtien arrêté en 2005, en possession d'une dizaine de milliers de faux dollars américains, dont la source d'approvisionnement venait de République dominicaine.

Enfin un élément contextuel de taille a été cité : « *par ailleurs, la stabilité retrouvée, l'amélioration du climat de sécurité et la réhabilitation progressive de l'image d'Haïti à l'étranger vont, sans nul doute, replacer bientôt le pays dans les itinéraires touristiques de la Caraïbe. Aussi, les secteurs mafieux haïtiens n'attendront pas longtemps pour faire de la production et du trafic de fausse monnaie une activité criminelle à grande échelle. D'où l'urgence, pour le gouvernement haïtien, de ratifier la convention de Genève de 1929 et de mettre en place un Office central pour la répression du faux monnayage.* »

Il a ainsi été exposé que, dans cette optique : « *l'Office central haïtien devrait être en relation étroite avec les offices centraux des autres pays et les autorités bancaires et d'émission monétaire qui interviennent directement dans le cadre de la lutte contre le faux monnayage, tant sur le territoire qu'à l'étranger, afin d'assurer un système d'alerte rapide et d'échange d'informations techniques et opérationnelles* »

Conclusion

Que faudrait-il retenir de façon prioritaire d'un tel séminaire ?

La disparité des situations nécessite plus que jamais une coopération régionale et internationale accrue, parce que les objets, produits illicites des trafics circulent très facilement d'un État à un autre.

La problématique des faux euros nécessite une approche globale : apprentissage de la reconnaissance de cette monnaie encore étrangère, recyclage des fonds grâce à un système bancaire contrôlé (ce qui est mis en place pour la monnaie nationale est tout aussi profitable pour l'euro), association d'organismes commerciaux importants tels que les agences de change pour recenser les faux, identification de l'autorité auprès de laquelle les faux euros doivent être renvoyés : Interpol, Europol via un État membre.

L'interrogation suivante, particulièrement concrète, a été très souvent posée : que fait-on des faux euros détectés sur notre ressort national ? Quelle autorité internationale doit être contactée ? Cette question est symptomatique du travail de communication véritable, nécessaire sur le traitement réservé aux faux euros.

De la même façon, il ne semble pas qu'Europol ait produit suffisamment de synthèses complètes sur les productions colombiennes en matière de faux euros. Hormis certaines opérations ciblées présentées aux États membres, des historiques plus complets référençant les matériels utilisés, les voies de transport et de mise en circulation usitées, les quantités précises de billets saisies, y compris par valeur faciale, n'ont toujours pas été communiqués.

La présentation, dans la suite de cette première action internationale à vocation généraliste, d'un futur projet à réaliser dans le courant du premier trimestre 2008, dans le cadre du programme Périclès, dans cette même zone géographique, mais à Saint-Martin.

L'implication particulière de nos homologues hollandais dans la perception commune de protection de l'euro, dans cette même zone des Caraïbes, nous permettrait de proposer un projet commun dont la France pourrait être le directeur de projet. Le lieu pressenti serait alors l'île de Saint-Martin pour la partie française et Sint-Maarten pour la partie néerlandaise. L'île de Saint-Martin présente, en effet, cette particularité, depuis 1648, d'être composée de deux parties, sans véritable frontière entre les deux. Saint-Martin est situé sur la route maritime des grands échanges commerciaux, mais surtout sur les voies empruntées en matière de trafic de drogue. Les euros circulent déjà côté français, et ne sont pas étrangers de l'autre partie du territoire. Par ailleurs, les trois nouvelles communes néerlandaises à statut particulier, Bonaire, Saba et Saint-Eustache, devraient être amenées à adopter l'euro d'ici 2008.

Sur cette île, même si les deux langues officielles sont le français et le néerlandais, l'anglais est utilisé dans les deux parties du territoire, ainsi que l'espagnol apporté par des immigrés de République dominicaine. C'est la raison pour laquelle, en plus de la disparité des États environnants, les trois langues de travail français, anglais et espagnol demeurent indispensables.

L'objet du séminaire consisterait à organiser des ateliers de travail portant sur des problématiques plus ciblées (chacun de ces ateliers serait présidé par un représentant français de l'Office néerlandais, espagnol, et anglais) :
- formations techniques à la reconnaissance de l'euro ;
- incitation à la mise en place d'un office central national en matière de faux (avec explication des conditions de fonctionnement, fichiers spécifiques...) ;
- présentation du Centre national d'analyse des billets et des pièces (missions techniques, statistiques et de coopération avec les services d'enquête, et obligation de recyclage des pièces et des billets ;
- axes de coopérations à l'international entre institutions policières, judiciaires.

Cette proposition fera l'objet d'un rapport qui sera soumis prochainement au directeur du chef de l'Unité de protection de l'euro à l'Office de lutte anti-fraude de la Commission européenne.

Valérie MALDONADO

Chef de l'Office central
pour la répression du faux monnayage

Colloque organisé par la Fondation pour l'Enfance en partenariat avec l'association Droit@l'Enfance

Internet : un jeu d'enfant ?

Arnauld GRUSELLE

Le 30 mai 2008, la Fondation pour l'Enfance, en partenariat avec l'association Droit@ l'Enfance a organisé un colloque sur le thème : Internet est-il un jeu d'enfant ? Cette journée de travail réunissant policiers, gendarmes, magistrats, avocats, représentants d'associations et d'administrations, ainsi que de nombreux professionnels de la protection de l'enfance s'est déroulée dans l'amphithéâtre de l'INHES.

Internet et, plus généralement, les nouvelles technologies constituent un progrès considérable en termes de communication et d'information : c'est indiscutable. Mais elles constituent aussi le terrain de nouvelles formes de criminalités, dont les enfants et les adolescents sont la cible facile. Comme l'a développé Florence Marguerite, magistrate à la direction des Affaires criminelles et des Grâces (DACG) au ministère de la Justice, les risques pour les mineurs sont de deux ordres : les contenus qu'ils peuvent recevoir via Internet d'une part, et les contacts avec des agresseurs potentiels d'autre part.

Ce qui apparaît comme rassurant, c'est que la sécurité des enfants sur Internet est aujourd'hui une priorité pour les pouvoirs publics. Ceci a été développé par Olivier Peraldi, adjoint au délégué interministériel à la Famille, qui a rappelé tout l'intérêt que porte Nadine Morano, secrétaire d'État à la Famille, à ce sujet. À cette occasion, la secrétaire d'État a souhaité préciser qu'il est nécessaire d'agir sans cesse pour adapter les lois, identifier et diffuser les bonnes pratiques, sensibiliser les parents et les enfants dans le cadre de démarches partenariales incluant les pouvoirs publics, les industriels, les associations et les parents.

D'ores et déjà, comme l'a rappelé Myriam Quéméner, la France n'a pas à rougir de son arsenal législatif, car celui-ci est tout à fait calqué sur la Convention du Conseil de l'Europe applicable depuis juillet 2004. C'est le premier traité international de lutte contre la cybercriminalité. Depuis dix ans, les choses ont considérablement évolué. La loi du 5 mars 2007 relative à la prévention de la délinquance élargit encore les infractions de la détention à la consultation habituelle d'images pédopornographiques et crée l'infraction de proposition sexuelle à un mineur, qui vise à traquer des criminels cherchant à prendre contact avec un enfant. Pour ce faire, la loi offre la possibilité aux enquêteurs, sous couvert d'un pseudonyme, de participer aux échanges avec des personnes susceptibles de commettre une infraction. Ces échanges peuvent ainsi être conservés et, fait nouveau, être versés à la procédure et servir de preuve si besoin. Ces dispositions ont notamment été utilisées dans le cadre d'une affaire récemment médiatisée dans laquelle plusieurs individus avaient planifié l'enlèvement d'une fillette à laquelle il réservait un traitement des plus sordides. À noter que la Fondation pour l'Enfance s'était constituée partie civile dans cette affaire.

C'est d'ailleurs cette action plutôt méconnue de la Fondation qui a été présentée par Maître Bénédicte Grandin, représentant Maître Olivier Baratelli, avocat de la Fondation pour l'Enfance depuis 2003. Maître Grandin a ainsi rappelé que la Fondation pour l'Enfance s'était constituée partie civile dans plus d'une centaine d'affaires intéressant les faits prévus et réprimés par l'article 227-23 du Code pénal, à savoir la diffusion, la fixation, l'enregistrement, la transmission, la détention, l'importation, l'exportation, la captation d'images d'un mineur présentant un caractère pornographique. L'intérêt de cette action est double : il est répressif, car les dommages et intérêts sollicités et obtenus par la Fondation ont souvent davantage d'impact sur les condamnés que les peines d'emprisonnement avec sursis prononcées ; il est préventif, car il convient de faire comprendre à l'accusé à quel point son intérêt pervers pour ce genre d'image participe activement au fait d'enlèvement, de viol, de séquestration et parfois de barbarie au préjudice des enfants utilisés sur ces images. Ainsi, celui qui consulte ou collectionne ces images participe à ce honteux et lucratif trafic, alors même que, bien souvent, les victimes ne peuvent être identifiées.

Quand on parle de trafic et d'Internet, on comprend bien qu'il s'agit d'une préoccupation dont le traitement des crimes et délits dépasse le cadre national. La nécessité d'une collaboration transnationale est plus que jamais indispensable pour parvenir à lutter efficacement contre ces dérives. Faciliter la collaboration policière au niveau mondial, c'est le rôle d'Interpol OIPC (Organisation internationale de police criminelle) tel qu'il a été présenté par Yves Rolland, officier de renseignements criminels. Cette organisation basée à Lyon regroupe 186 pays et a pour vocation de faciliter la coopération policière criminelle internationale. Interpol travaille dans un cadre juridique précis, composé de textes internationaux dont la Convention internationale des droits de l'enfant, et s'est fixé comme action prioritaire, depuis 1992, la lutte contre les crimes commis contre les enfants. Les outils dont dispose Interpol sont des bases de données, notamment une sur les mineurs victimes d'abus sexuels accessible aujourd'hui à trente pays et comprenant environ 550 000 photos et vidéos d'abus sexuels commis sur des mineurs. Interpol dispose également de notices qui permettent le lancement d'avis de recherche internationaux. Les opérations Vico et Ident menées par Interpol ont été particulièrement médiatisées et ont ainsi permis l'arrestation de deux pédophiles respectivement en Thaïlande et aux États-Unis. Il convient de noter que le succès de ces opérations est conditionné à la participation active des États parties.

Si la France figure au rang des bons élèves avec son arsenal juridique et les moyens qu'elle déploie dans le cadre de la coopération internationale, elle n'est pas en reste en matière de dispositifs proposés pour le signalement des contenus illicites et des moyens mis en œuvre dans le cadre de l'enquête. Ainsi, le commissaire Fabien Lang, adjoint au chef de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) a présenté le dispositif de signalement des sites illicites : le GESIP (Gestion des signalements d'images pédopornographiques) connu du grand public sous l'adresse www.internet-mineurs.gouv.fr. Ce dispositif est actuellement vieillissant, il ne permet que le signalement d'images à caractère pédopornographique, alors que l'on sait aujourd'hui que les contenus illicites et/ou dangereux pour les mineurs sont de nature diverse.

D'autres signalements arrivent par l'intermédiaire de Point de Contact qui est le point de centralisation des signalements de l'Association des fournisseurs d'accès (AFA), ceux-ci ayant l'obligation de donner la possibilité à leurs clients ou utilisateurs de pouvoir signaler un contenu illicite. Ces signalements sont traités par une équipe de policiers et de gendarmes qui analyse la nature juridique des faits commis sur les sites incriminés afin de qualifier l'infraction et d'engager les premières investigations. Le 1er septembre 2008, un nouveau site devrait être lancé en vue du remplacement du GESIP et du Point de Contact.

Le commissaire divisionnaire Frédéric Malon, chef de l'Office central pour la répression des violences aux personnes (OCRVP), a précisé que les angles d'attaque pour lutter contre la pédopornographie étaient nombreux. Tout d'abord, les auteurs d'infraction laissent une trace en visitant un site illicite (l'adresse IP), permettant ainsi leur identification. Par ailleurs, à Rosny-sous-Bois, une cellule de veille de la gendarmerie surveille les réseaux *peer to peer* et une cyberpatrouille est chargée d'infiltrer la toile. Les accès aux sites illicites peuvent être bloqués lorsque ces sites sont hébergés à l'étranger ; ce système fonctionne au Royaume-Uni (30 000 connexions bloquées par jour) et en Norvège (5,5 millions de connexions bloquées par an), la France s'efforce de rattraper son retard à ce jour.

Le travail sur les images permet, quant à lui, d'identifier parfois des victimes, des auteurs, des lieux, des indices. Enfin, le contrôle des flux financiers générés par la pédopornographie est une autre piste d'investigation peu explorée par la France, mais qui peut être intéressante en matière de lutte contre les trafics sur Internet. Leila Ben Debba, directrice des programmes européens à l'ICMEC (*International Center for Missing and Exploited Children*) a d'ailleurs partagé l'expérience américaine menée en ce sens.

Le Lieutenant-colonel Eric Freyssinet de la Gendarmerie nationale a présenté les moyens mis en œuvre par la gendarmerie pour lutter contre cette forme de criminalité. Elle dispose ainsi de 170 enquêteurs spécialisés au niveau national, d'une trentaine de spécialistes au niveau central, d'une équipe dédiée aux analyses de système informatiques ou électroniques et d'une équipe chargée de la surveillance d'Internet au quotidien qui traque notamment les échanges d'images pédophiles sur les réseaux *peer to peer*. Il a, par ailleurs, insisté sur le rôle des prestataires de services internet en matière de prévention, de protection et de responsabilité.

Marc Mossé, directeur des affaires publiques et juridiques de Microsoft France s'est exprimé sur la façon dont cet acteur majeur qu'est Microsoft exerce sa responsabilité autour des différents services qu'il propose aux utilisateurs. Tout d'abord, le système d'exploitation Vista propose un certain nombre de paramétrages permettant une utilisation de l'ordinateur des enfants sous le contrôle des parents. Par ailleurs, la console de jeu X-box autorise la programmation de plages horaires, et interdit ainsi l'accès à des jeux en fonction de l'âge au regard de la classification

européenne PEGI. Enfin, Windows Live Messenger (ancien MSN), dispose également de paramétrages permettant aux parents de contrôler. La technologie est ainsi utilisée comme outil de protection, mais ne remplacera jamais la responsabilité et la vigilance des parents. Pour cette raison, plusieurs actions pédagogiques ont été menées à destination des parents, comme par exemple un guide édité à 2 000 000 d'exemplaires avec l'UNAF (Union nationale des associations familiales).

Jean Delprat, administrateur de l'UNAF, chargé du dossier Media et TIC, a souligné l'importance désormais prépondérante des médias et particulièrement d'Internet dans la construction de l'identité de l'enfant et de sa relation au monde. Un enfant passe ainsi environ 1 480 heures chaque année à utiliser différents médias (TV, radio, Internet, téléphone mobile, jeu vidéo). Les foyers avec des enfants de 6 à 11 ans possèdent en moyenne dix écrans. Jean Delprat précise que derrière la notion d'Internet se cache une multitude d'usages comme la recherche d'information, l'utilisation de messageries en ligne, l'échange de fichiers, la création et la gestion de blog. Du côté des parents, Internet suscite vigilance et interrogations, car les logiciels de contrôle parental proposés ne sont pas toujours d'une grande facilité d'utilisation : alors que 95 % connaissent leur existence, seul 39 % des parents ont installé un logiciel de contrôle parental.

Parmi les activités les plus addictives proposées aux jeunes, figurent les jeux vidéo, qu'ils soient sur console ou en ligne. Maître Nathalie Joffroy, avocate au barreau de Grasse et membre de l'association « Femmes et Enfants du monde » a insisté sur la grande violence de certains jeux vidéo faisant l'apologie du crime, de la drogue et du sexe. Par ailleurs, il est aujourd'hui prouvé que la santé peut être affectée par une consommation excessive de jeux vidéo, il existe désormais des services spécialisés dans certains hôpitaux et réservés aux accros du jeu.

En conclusion et à la lumière des débats de la journée, Maître Marie-Pia Hutin-Houillon, avocate et présidente de l'association Droit@l'Enfance, a souhaité porter au nom des associations un certain nombre de revendications à l'attention des pouvoirs publics et de l'ensemble des acteurs du monde numérique. Tout d'abord, elle a souligné l'attente de coordination entre les acteurs au niveau international pour une lutte efficace contre la criminalité sur Internet. Elle a également insisté sur l'importance et la qualité de l'information qui doit être fournie aux parents pour leur permettre d'exercer eux aussi efficacement leur rôle protecteur. Il est apparu également que la création d'une juridiction spécialisée sur la criminalité numérique serait de nature à renforcer l'efficacité de la lutte contre celle-ci grâce à l'intervention exclusive d'acteurs formés. Enfin, il convient de renforcer les mesures d'information concernant les risques liés à l'usage de ces technologies avec, pourquoi pas, une labellisation de certains sites et jeux garantissant un usage sans danger pour les enfants ou les adolescents.

Loin des clichés et des contre-vérités véhiculés parfois sur Internet, cette rencontre aura permis l'échange entre différents acteurs, dont les préoccupations et les intérêts parfois divergents, semblent néanmoins se retrouver autour de la protection des plus vulnérables : les enfants.

Arnauld GRUSELLE
Directeur de la Fondation pour l'Enfance

Délinquances et changements sociaux, des modes de vie et des pratiques d'intervention Dialogue Sud-Nord

Laurence HERNANDEZ
Audrey BOUSQUET

Tous les deux ans, l'AICLF organise une manifestation scientifique destinée à rassembler en un même lieu criminologues et autres spécialistes du phénomène criminel. Réseau francophone créé en 1987 dans le but de favoriser l'échange et l'interconnaissance en criminologie, l'AICLF prouve bien, depuis sa création, qu'une communauté scientifique peut exister au-delà des réseaux anglophones, non seulement de manière identitaire, mais aussi par le biais de publications (telles que la *Revue internationale de criminologie et de police*) et de rencontres officielles (les colloques bisannuels). Denis Szabo, chercheur québécois et fondateur de l'Association, avait pour objectif le développement des relations entre universitaires et professionnels œuvrant dans les champs d'action couverts par la criminologie, par le biais de la langue française. Le colloque, qui s'est tenu du 11 au 13 mai 2008, ne fait que confirmer la réussite de l'AICLF qui n'avait jamais rassemblé autant d'intervenants. La destination marocaine y a certainement contribué. Capitale administrative du Maroc et grande ville universitaire, Rabat s'est avéré être un cadre idéal pour la rencontre et l'émulation des échanges. L'accueil fort agréable réservé aux participants par l'Association et par l'Université Mohammed V – Agdal, sous l'égide de Mohammed Ghedah, ont très certainement contribué au succès de cette manifestation.

Mais le choix de Rabat comme ville d'accueil revêt surtout un aspect symbolique : pour la première fois, le colloque de l'AICLF s'est tenu dans un pays du Sud. En 2006 déjà, le choix de la ville d'Istanbul avait initié un rapprochement vers des horizons moins classiques de la criminologie francophone, jusque-là majoritairement représentée par le Québec, la Belgique, la Suisse et la France. Motivée par un tel désir d'ouverture, cette 11[e] édition du colloque de l'AICLF aura bien été placée sous le signe de la diversité.

Diversité des participants tout d'abord. Avec quelque 120 intervenants répartis dans 20 ateliers, le colloque a réussi à regrouper le plus grand nombre de chercheurs de toute l'histoire de l'Association. Que le français soit leur langue de communication habituelle ou occasionnelle, ces derniers sont venus d'horizons extrêmement variés : Belgique, Canada, France, Suisse, mais aussi Roumanie, Italie, Grèce, Iran, États-Unis, Corée du Sud, Tunisie, Turquie et Japon. Toutefois, ce sont les pays fondateurs du réseau qui ont, sans commune mesure, été les plus représentés. On peut même s'étonner de l'absence de pays du Sud, particulièrement du Maghreb et d'Afrique Subsaharienne. Le Maroc a toutefois été mis à l'honneur. Le déplacement à Rabat a permis la rencontre avec un pays, avec ses problématiques – anciennes ou émergentes – dans une optique non stigmatisante et décomplexée. Ont été abordés les thèmes de la famille, du terrorisme, de l'immigration, et, plus généralement, les relations du Maroc avec l'Occident.

Diversité des approches ensuite. Le colloque de l'AICLF est, certes, le point de rencontre d'une communauté

scientifique réunie par une langue et des objets communs, mais ces derniers sont disséminés dans le paysage institutionnel et scientifique. Dans le contexte français, un tel éclatement est d'autant plus fortement ressenti que l'absence d'autonomisation institutionnelle (universitaire) de la criminologie a conduit les chercheurs intéressés par le phénomène criminel vers des disciplines variées. Cet éparpillement n'a pourtant pas été un obstacle à la venue en nombre d'universitaires français, chercheurs isolés ou membres de laboratoires. On peut ainsi noter la présence de psychologues du Laboratoire santé individu société et du Centre de recherche et d'éducation par le sport (CERS) de l'université Lyon II, du Centre universitaire de recherche en sciences de l'éducation et psychologie (CURSEP) de l'université Jules Verne de Picardie, du Centre d'études et de recherches en psychopathologie (CERPP) de l'université Toulouse II, ou de l'Institut de criminologie et sciences humaines (ICSH) de l'université Rennes II. Étaient aussi présents des sociologues du Centre interdisciplinaire d'études urbaines (CIRUS) de l'université Toulouse II et du centre de recherche psychotropes, santé mentale, société (CESAMES) de l'université Paris Descartes, ainsi que des politologues du Centre d'études et de recherches sur la police (CERP) de l'université Toulouse I. Enfin, des chercheurs-praticiens de l'École nationale d'administration pénitentiaire (ENAP) ont également participé à la manifestation.

S'il n'est pas aisé de repérer des pratiques et des tendances dominantes, on remarquera cependant que les approches psychosociales tiennent une place toute particulière dans le champ de l'actuelle criminologie francophone. Par ailleurs, la criminologie théorique, qui cherche à expliquer l'action criminelle, ne se fait pas au détriment d'une criminologie appliquée, intéressée par les moyens de lutte contre la délinquance. Ainsi, de nombreuses communications ont présenté les résultats, les objectifs ou les méthodes de recherche-action et de recherche-évaluation.

Diversité des thématiques enfin et surtout. Cette 11e édition avait pour thème la délinquance des sociétés qui connaissent de rapides changements sociaux, économiques et politiques, ces derniers se situant au croisement des phénomènes de mondialisation, d'acculturation, de migration, de déracinement ou d'urbanisation. Impactant les modes de vie et les réseaux de solidarité traditionnels, de tels changements, pour le moins brutaux, tendent à multiplier les occasions de frustration et la perturbation des codes normatifs. À cette problématique générale abordée lors des sessions plénières, dans le cadre d'un échange Sud-Nord, les sessions d'atelier ont été déclinées en une multitude de sous-thèmes qui ont, chacun à leur façon, contribué à l'apport de réponses au questionnement global.

Un échange Sud/Nord sur des problématiques globales

Les exemples de l'immigration et de la délinquance

Deux sessions plénières se sont pleinement intégrées dans la problématique Sud-Nord. La première a interrogé le lien entre migrations et délinquance, et plus précisément, celui des migrations maghrébines. L'oratrice du Nord, Michelle Vatz Laâroussi (université de Sherbrooke) s'est intéressée aux impacts psychosociaux sur les enfants de la disqualification des pères immigrants au Québec. Après avoir insisté longuement sur l'évolution actuelle vers des sociétés de plus en plus mobiles et vers la mondialisation des courants migratoires, elle s'est intéressée au cas des familles maghrébines au Québec. Détaillant les contrastes entre délinquance et première génération d'immigrants et entre délinquance et deuxième et troisième générations d'immigrants, elle a formulé l'hypothèse d'un déficit de reconnaissance concernant ces dernières, tout en affirmant l'importance du contexte d'accueil, d'insertion et d'intégration pour la trajectoire sociale des migrants.

Malika Benradi (université Mohammed V – Agdal), oratrice du Sud, s'est essayée à une analyse critique du discours sur la criminalité des maghrébins en Europe en analysant les « statistiques de la peur ». Elle s'est attachée à étudier la situation des Maghrébins en France, à la fin des années 1970. Son étude a porté sur les statistiques pénales de la ville de Toulouse. Elle a été menée à partir du constat d'un discours sur la violence des Maghrébins dans les pays du Nord. En comparant le groupe de migrants Maghrébins et un autre groupe de migrants d'Europe du Sud, l'intervenante a analysé la surreprésentation des migrants maghrébins dans les statistiques criminelles (et le risque accru de garde à vue et de sanction pénale à leur égard) comme résultant de la réaction sociale particulière dont ils font l'objet.

Si les deux intervenantes ont souhaité montrer l'importance de la stigmatisation des groupes de migrants et de leurs descendants, seule Michelle Vatz Laâroussi a présenté une analyse scientifique actualisée. Elle a tout d'abord distingué quatre types de structures de délinquance liées aux premières générations dans les années 1990 : le terrorisme, la délinquance liée au statut des migrants et à la famille (clandestins, sans-papiers), la délinquance enchâssée dans les politiques nationales de migration (délinquance fonctionnelle, économies souterraines), la délinquance

organisée pour contourner ces frontières (réseaux de passeurs, de prostitutions, de travail clandestin). Ensuite, elle a montré comment la délinquance de deuxième génération est davantage liée à l'urbanisation, à la ségrégation résidentielle et au statut « ethnique » et « racial » des jeunes (selon les termes utilisés par l'oratrice). En explicitant les particularités d'une société canadienne pourtant ouverte à l'immigration, elle s'est intéressée au problème des parents maghrébins qui, depuis 2001, connaissent le taux de chômage le plus élevé. À l'aide d'une grille d'analyse psychosociale, celui-ci a été perçu comme une « impuissance des pères » se soldant par des stratégies défensives et réactives (surprotection de la famille ou « parentification », retrait social et familial) ainsi que par des impacts psychosociaux sur les enfants (marginalisation, exclusion, isolement).

Cette analyse fort contemporaine a contrasté avec l'étude de Malika Benradi, issue d'une recherche effectuée à la fin des années 1970. Alors qu'elle datait de plus de trente ans, la question de la validité actuelle des résultats ou d'un renouvellement de la recherche n'a pas été abordée. Par ailleurs, son imprécision méthodologique a rendu inopérants les résultats de la recherche. La distinction du groupe de migrants maghrébins avec les autres groupes de migrants (espagnols, portugais, etc.) et les Français (d'origine ?) a été menée sans explication concernant la méthode à l'origine de la distinction. Les catégories utilisées n'appartiennent à aucune des typologies exploitées dans le contexte pénal français (femme/homme ; mineur/majeur ; français/étranger). Si elle a eu accès à d'autres informations, comment Malika Benradi a-t-elle discriminé les différentes catégories de population : par les lieux de naissance ? Mais alors, comment est-t-il possible, dans les statistiques françaises, de distinguer un Algérien, un Français ou un Espagnol né à Alger dans les années 1950 ? Par les noms de famille (ce qui reviendrait à rentrer dans la discrimination de fait qu'elle s'est donnée pour mission de dénoncer). De même, lorsqu'elle aborde la thématique de l'immigration, oublie-t-elle de préciser s'il s'agit d'immigration régulière ou irrégulière (pénalement répréhensible), sachant qu'un migrant en situation irrégulière sur le territoire français est délinquant de fait. La question qui se pose alors concerne la nature des faits reprochés au groupe maghrébin par l'appareil répressif et judiciaire, notamment lorsque l'on parle de violence visible.

Par ailleurs – et contrairement à sa consœur du Nord – Malika Benradi n'a proposé aucune piste d'action pour contrer la corrélation « immigration-délinquance » ou les effets de la stigmatisation dénoncée. Michelle Vatz Laâroussi, si elle s'est seulement attachée à la dimension psychosociale d'un problème aux multiples facettes, a, quant à elle, conclu sur la nécessité d'accompagner les stratégies identitaires des jeunes et la reconstruction identitaire des parents, et de favoriser la transmission de l'histoire nationale.

Au-delà de ces limites, la synthèse et la mise en relation de tels exposés suscitent de nombreuses interrogations sur des questions essentielles telles que la stigmatisation des immigrants. La question mérite d'être développée en France, pays qui, contrairement au Canada, peine à faire émerger la question de l'ethnicité, notamment concernant les statistiques policières. Le problème de l'inégalité des individus face aux institutions répressives et pénales ou celui des interactions de normes issues de cultures différentes constituent pourtant des problématiques à développer.

Les violences terroristes

Lors de la session plénière « Violences terroristes », deux communications ont abordé ce thème, chacune évoquant la thématique d'un point de vue différent géographiquement, mais aussi disciplinairement. En effet, Abdessamad Dialmy (université de Fès) a pris place en tant que représentant du Sud, pour évoquer le problème du terrorisme islamique au Maroc sous l'angle de la psychosociologie. Azzedine Rakkah (FNSP-Paris), orateur du Nord, a exposé quant à lui ses recherches sur un échantillon d'Européens se considérant comme militant du djihadisme, en utilisant l'approche de la science politique et de la sociologie. Néanmoins, deux points communs caractérisent ces interventions. Premièrement, elles traitent de la même question, celle de l'engagement dans un parcours de vie pour lequel le djihad devient une croyance directrice et où l'Occident est appréhendé de manière négative. D'autre part, elles analysent toutes deux les histoires de vie et les étapes parcourues par les individus concernés. La confrontation de ces exposés a permis de comprendre que les raisons et l'intensité de l'engagement sont différentes selon les pays concernés, les conditions de vie et le contexte politique. D'ailleurs, il est important de noter que si Abdessamad Dialmy a pris comme objet d'enquête les personnes ayant été jusqu'au bout de la démarche suicidaire au nom de l'Islam, Azzédine Rakkah a interrogé certains militants du djihadisme en insistant sur le fait que tous n'étaient pas candidats au suicide. C'est ainsi que Abdessamad Dialmy a tenté de démontrer comment une frustration habitationnelle peut déboucher sur une frustration sexuelle, puis islamiste. Plus précisément, il a entrepris d'expliquer « *l'étiologie de la violence terroriste suicidaire* ». Cette intervention éclairante a permis de comprendre, tant du point de vue de la religion que de la société marocaine, l'engagement dans cet acte extrême. De son côté, Azzédine

Rakkah a expliqué le parcours de certains Européens qui décident un jour de partir à Damas rejoindre une organisation armée pour s'entraîner au combat. Celui-ci décrit l'engagement sous l'angle des référentiels politiques venant intégrer le domaine religieux, et la manière dont ces jeunes européens sont socialisés à la doctrine djihadiste par le biais de certains imams et d'Internet. Ceux qui décident de partir à Damas le font sous le coup d'Internet et de rumeurs, sans être véritablement dirigés par les groupes du Moyen-Orient et sans véritablement parler la langue arabe. Avant l'année 2006, ces personnes partaient au combat en Irak après être restées une quinzaine de jours en Syrie. Après 2006, la Syrie décidant de coopérer un peu plus dans la lutte contre le terrorisme, arrête les Européens se rendant à Damas, les incarcère, puis les renvoie en Europe. Certains d'entre eux inventent alors une autre histoire, dans laquelle ils auraient réellement combattu, s'autoproclament recruteurs et se pensent investis d'une mission. Ces parcours diffèrent de ceux décrit par Abdessamad Dialmy. Ce dernier énonce quant à lui, comment de jeunes marocains, dans une logique de remise en cause de leur masculinité, sans femme ni logement, s'investissent dans une organisation terroriste. Il explique que cet engagement a plusieurs causes, pas seulement religieuses, mais relevant des conditions de vie, de la manière dont l'organisation terroriste envisage la religion, de la traduction du suicide (interdit par la religion) en martyre, et des appréhensions politiques et historiques vis-à-vis des institutions. Toutefois, une constante est présente dans les carrières décrites, celle de l'extrême minorité de ce type d'engagement autant au Maroc qu'en Europe.

Des sessions d'ateliers aux thématiques variées

Les exemples de la police et des conduites addictives

D'autres thématiques, indirectement rattachées au sujet principal, ont fait l'objet de réflexions et de débats. À titre d'illustration, deux sessions d'ateliers reflétant les réalités actuelles de la recherche en criminologie seront exposées ici.

Police et sécurité

On ne pourra omettre de mentionner dans cette revue l'atelier « Police et sécurité », en raison de son thème et de la présence dominante de chercheurs français. *A priori* peu homogène et relativement marginal, il a été le lieu d'interrogations interreliées et consubstantielles à la problématique générale du colloque. En effet, l'ensemble « police-sécurité » est, lui aussi, touché par de rapides changements sociopolitiques engendrés par des « mutations en cours qui favorisent la rationalité » [1]. Cette évolution se traduit par une prise en compte accrue de la mesure de l'action policière (thème au demeurant largement documenté dans la littérature anglophone). Dès lors, c'est la pertinence de certains « modèles » de police qui a été examinée : police de proximité d'une part, présentée tour à tour comme lieu commun universel [2] et comme enjeu sécuritaire et politique dans les pays d'Afrique francophone Subsaharienne [3] ; police de répression d'autre part, jugée inefficiente dans la lutte contre les incivilités [4]. Mais la mesure de l'action policière concerne également la question de la délimitation des tâches à effectuer. Tel était l'objet de l'analyse du périmètre des tâches de la gendarmerie. Cette institution française est, en effet, contrainte au repositionnement de ses capacités opérationnelles autour d'un socle missionnel plus restreint [5]. Définir des priorités d'actions prend d'ailleurs tout son sens dans le contexte actuel d'augmentation des contraintes budgétaires. C'est aussi dans ce contexte que s'inscrivent les évaluations de l'efficacité des différentes missions policières. Dans cette perspective, la réflexion ne pouvait être menée à bien sans interroger la pertinence du concept de performance appliqué au service public policier. L'évaluation comme objet d'étude a donc supplanté la recherche comme évaluation. Et les intervenants ont tenté de caractériser les orientations prises par l'évaluation dans le contexte actuel des réformes néomanagériales françaises [6]. Ils ont en outre déterminé l'impact d'une culture quantitative « du résultat » sur les pratiques policières en évoquant ses possibles effets pervers [7].

....

(1) Problématique du colloque telle qu'elle a été formulée dans l'appel à contributions.
(2) Communication de Jean-Louis Loubet Del Bayle (CERP, université de Toulouse I).
(3) Communication de Yann-Cédric Quero (CICC et CIPC, université de Montréal).
(4) Communication de Julien Piednoir (université d'Angers).
(5) Communication de François Dieu (CERP,université de Toulouse I).
(6) Communication de Laurence Hernandez (CERP, université de Toulouse I).
(7) Communication de Christian Mouhanna (CESDIP-CNRS).

Le domaine de recherche « police et sécurité » n'a finalement plus à douter de son devenir au sein de la criminologie. Responsable de cet atelier thématique, Maurice Cusson, dans la lignée du récent *Traité de sécurité intérieure* [8] qu'il a codirigé, a souhaité rappeler que la sécurité intérieure est « *un nouveau territoire pour la criminologie* » (titre de son intervention). Fidèle à son approche rationnelle de la déviance, il a démontré qu'il est possible de produire de la sécurité à toutes les étapes du processus de justice pénale, « *avant même que les délits ne soient commis* ». Attaché à une science appliquée, il a soutenu que les criminologues disposaient des connaissances nécessaires pour répondre à ces besoins.

Conduites addictives et criminalité

Si les thèmes de la police et de la sécurité apparaissent à la fois comme marginaux et comme de « nouveaux territoires pour la criminologie », d'autres se révèlent assez classiques et largement exploités par les chercheurs de différents pays. Il en est ainsi de la question « des conduites addictives et de la criminalité » qui a mobilisé deux sessions d'ateliers [9] et plusieurs autres interventions [10], tant du point de vue des pratiques que des actions et des politiques mises en place pour les traiter.

En se penchant sur les interventions consacrées à ce thème, il ressort que le lien entre conduites addictives et criminalité peut être étudié sous plusieurs aspects et en fonction de plusieurs pratiques. Il en a résulté une richesse des interventions et la confrontation des approches. Toutefois, si l'angle criminologique privilégie les études en termes de trajectoires de vie ou d'enquêtes par échantillon (dans le milieu carcéral, par exemple), les études en termes de politiques publiques restent minoritaires. De même, et reflétant par là les réalités universitaires nationales, les chercheurs québécois et belges sont très bien représentés dans ce champ classique de la criminologie alors que les autres nationalités sont quasiment absentes. Pour illustrer ce propos de manière numérique, il peut être opportun de revenir sur les approches abordées lors du colloque : styles de vie et trajectoires de vie (neuf interventions) ; études statistiques sur échantillons (quatre interventions) ; politiques publiques (deux interventions) ; économie souterraine (une intervention). Au total, sur les seize interventions, douze ont été effectuées par des chercheurs canadiens, trois par des Belges et une par un Français. Au-delà de la simple comptabilisation des interventions, la diversité des thématiques reflète l'étendue de ce champ de recherche aussi bien que la prise en compte de problématiques nouvelles par les chercheurs. L'atelier a démontré que cette thématique est évolutive et que la recherche dans ce domaine est capable de s'adapter et de s'intéresser à de nouveaux objets. Ainsi, les questions des jeux de hasard et d'argent [11], du dopage dans le cyclisme [12] ou encore des pratiques addictives chez les Nunavimiuts [13] (populations autochtones du Canada) ont été abordées à côté de thématiques plus traditionnelles, largement connues, telles que celles relatives au rôle et à la place des pratiques addictives aux côtés des pratiques délinquantes [14],

(8) Codirigé avec Benoît Dupont et Frédéric Lemieux. Éditions Hurtebise HMH à Montréal. Distribué en France par Distribution du Nouveau Monde, Librairie du Québec, 30, rue Gay-Lussac, 75005 Paris.

(9) « Drogues, conduites addictives et criminalité ».

(10) « Délinquances et stratégies d'intervention » ; « Nouvelles formes de déviance et de criminalité » ; « Violences, déviances et peuples autochtones ».

(11) Communications de Valérie Beauregard, Serge Brochu, Marie-Marthe Cousineau (CICC - université de Montréal) et Robert Ladouceur (université de Laval) « Les facteurs permettant de prédire la participation et les problèmes avec les jeux de hasard et d'argent parmi les détenus fédéraux du Québec », « Les habitudes de jeux de hasard et d'argent des détenus fédéraux du Québec », « Jouer à l'intérieur des murs de la prison », de Fréderic Ouellet (CICC-Université de Montréal) « Trajectoires de vie et récidive : étude comparative de joueurs compulsifs et de délinquants adultes ».

(12) Communication de Bertrand Fincoeur (service de Criminologie – université de Liège) « Le dopage en cyclisme sur route : un objet d'étude criminologique ».

(13) Communications de Chantal Plourde, Natacha Brunelle, Annie Gendron (université du Québec à Trois-Rivières), Michel Landry (centre Dollard - Cormier et RISQ - Québec), Louise Guyon (INSPQ - Québec) et Cécile Mercier (Centre de réadaptation Lisette Dupras - Québec) « Consommation de drogues chez les Nunavimiuts : méthodologie de la recherche participative et faits saillants du volet d'enquête », de Chantal Plourde, Natacha Brunelle, Stéphanie Eveno (université du Québec à Trois-Rivières), Michel Landry (centre Dollard - Cormier et RISQ - Québec), Louise Guyon (INSPQ - Québec), et Cécile Mercier (Centre de Réadaptation Lisette Dupras - Québec) « Comment se vit l'usage d'alcool et d'autres drogues dans les communautés du Nunavik : points de vue de Nunavimiut », de Chantal Plourde, Natacha Brunelle, Annie Gendron (université du Québec à Trois-Rivières) et Serge Brochu (CICC-université de Montréal) « Trajectoires de consommation de substances psychoactives chez les femmes autochtones incarcérées : portrait comparatif et points de vue exprimés en regard de leur consommation avant et pendant l'incarcération ».

(14) Communications de Michel Born (université de Liège) « La place de la délinquance dans le style de vie des consommateurs de drogues », de Claire Gavray (université de Liège) « Consommations et délinquances : deux expériences complémentaires à l'adolescence ? », de Karine Bertrand, Louise Fines (université de Sherbrooke) et Cinthia Ledoux (université du Québec à Trois-Rivières) « Jeunes délinquants en traitement de la toxicomanie : leur vécu et leurs perceptions quant à leur propre trajectoire de réadaptation », de Michel Landry, Rachel Charbonneau, Hélène Simoneau et France Lecomte (centre Dollard - Cormier – Québec) « L'intervention auprès des personnes judiciarisées toxicomanes ».

à l'incidence de l'économie souterraine du cannabis [15] ou à de celle de la consommation de cocaïne [16].

De ce fait, il est difficile de déceler l'homogénéité des études consacrées aux conduites addictives et à la criminalité. Même si l'organisation en sessions d'ateliers a le mérite de présenter des approches et des thèmes différents aux participants, elle ne facilite pas le repérage des chercheurs, des laboratoires et des approches ni la cohérence des interventions. On peut alors se demander si, concernant les conduites addictives et la criminalité, une organisation par type d'approche ou d'enquête n'aurait pas éclairé davantage cette problématique fort complexe et facilité la compréhension des participants.

Au total, ce colloque, qui ambitionnait de faire dialoguer le Nord et le Sud, s'est avéré être davantage un échange qu'un dialogue pour trois raisons principales : la première, technique, revient au temps très court – ou inexistant – laissé aux débats en fin d'intervention ; la seconde, plus factuelle, tient à la surreprésentation des pays du Nord ; la troisième, « culturelle », concerne les différences de réalités sociales entre les deux aires géographiques Sud et Nord. Si la famille, l'immigration ou la sécurité sont des thèmes universaux, le colloque de Rabat a montré qu'ils étaient aussi dépendants de contextes économiques, sociétaux et culturels. La remarque vaut également à l'intérieur d'une même aire géographique, au sein de laquelle les problématiques ne sont pas transposables d'un pays à l'autre.

Cet échange s'est donc concrétisé autour de postulats partagés. Face à la montée de nouvelles formes de criminalité, la nécessaire neutralité axiologique du criminologue a constamment été rappelée. Dans ce domaine particulièrement sensible qu'est l'étude du phénomène criminel, le chercheur doit se garder des « dangers idéologiques de la confusion [17]», afin de faire la différence entre « rumeurs, stéréotypes sociaux et savoirs scientifiques [18]»... une neutralité dans l'étude du phénomène criminel qui ne doit pas se faire au prix d'une certaine sensibilité. « *Le criminologue ne doit pas être qu'un technicien. Il doit aussi (ap)porter un regard humain sur le monde* » (Georges Kellens, lors de la remise du prix Beaumont-Tocqueville 2008).

Laurence HERNANDEZ
Allocataire de recherches au Centre d'études et de recherches sur la police (CERP), Université de Toulouse I

Audrey BOUSQUET
Allocataire de recherches au Centre d'études et de recherches sur la police (CERP), Université de Toulouse I

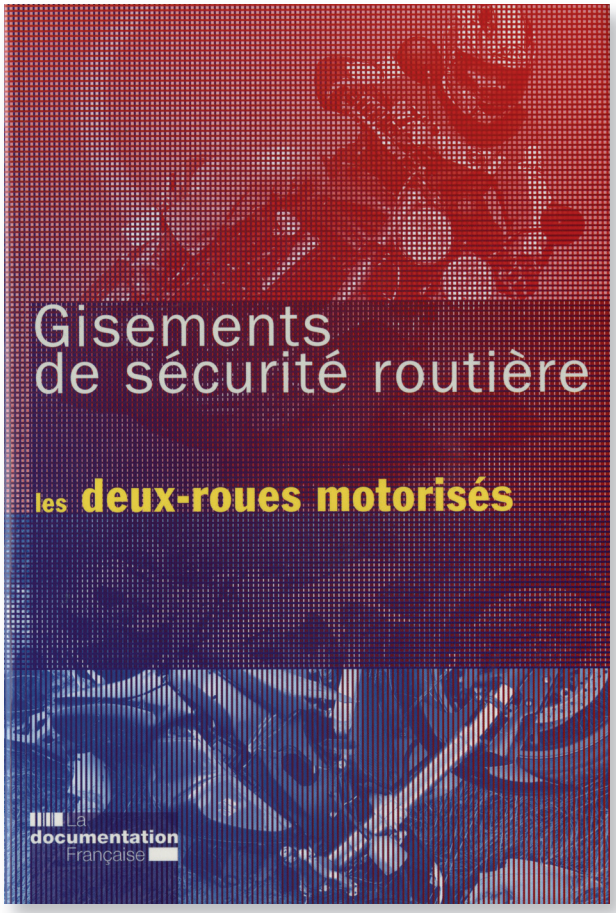
(15) Communication de Marc Alain (université du Québec à Trois-Rivières) et Martin Bouchard (Simon Fraser University) « *Les paradoxes de la culture intensive de cannabis au Québec : lorsqu'une économie développée accapare un marché plus traditionnellement associé aux économies en émergence et en développement* ».

(16) Communication de Mylène Magrelli Orsi, Serge Brochu (CICC-Montréal) et Isabelle Parent (ministère de la Sécurité publique – Québec) « Les trajectoires de vie de consommateurs de cocaïne : analyse phénoménologique des implications criminelles ».

(17) Citation extraite des interventions.

(18) *Idem*.

Un ouvrage de La documentation Française



Gisements de sécurité routière

Sous la direction de **Régis Guyot,**
préfet des Deux-Sèvres

Prix **12** €

Parution : **juillet 2008**

Pagination : **280**

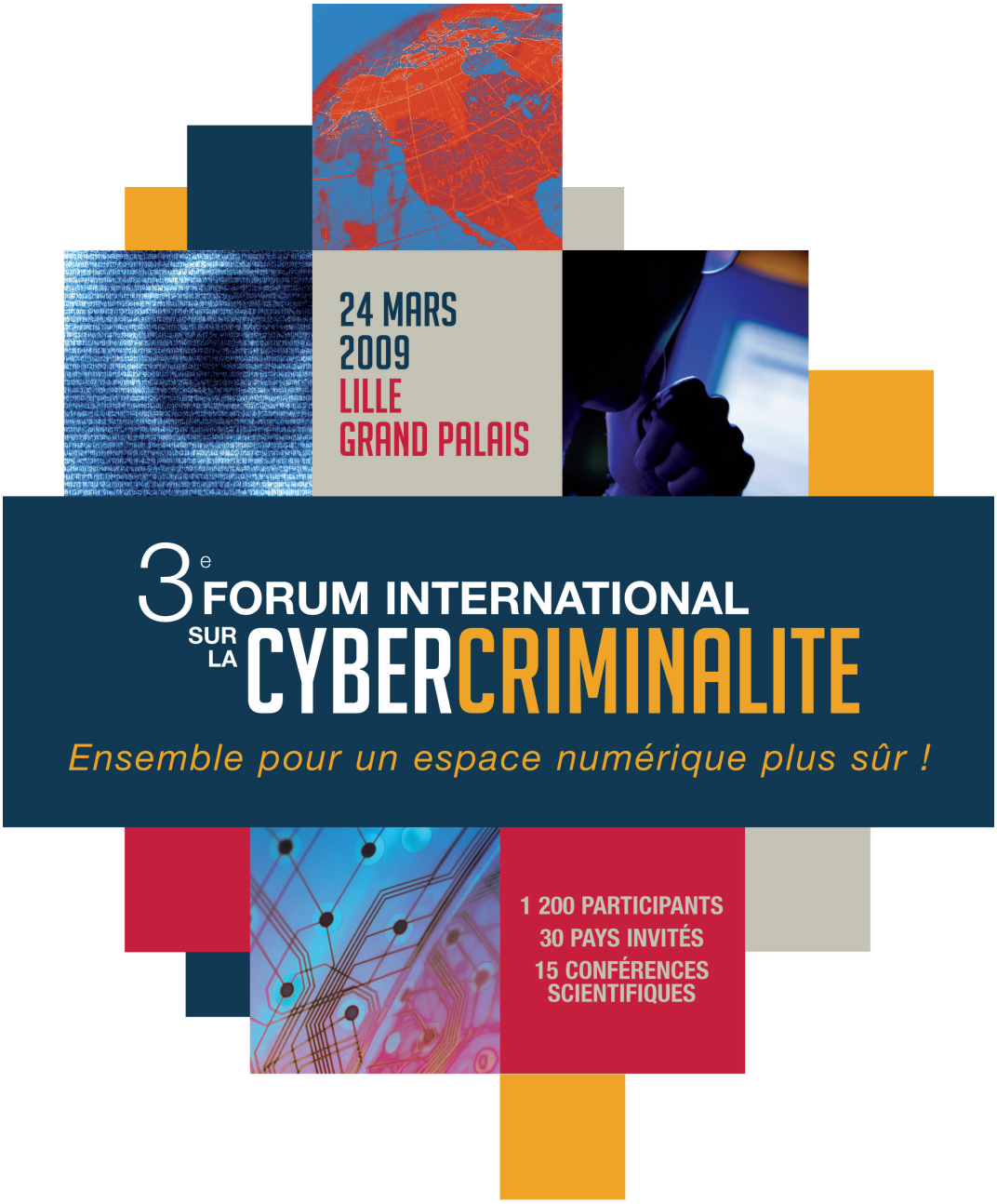
isbn : **978-2-11-006979-5**

Le livre

Après six années globalement très positives pour la sécurité routière, un constat s'impose néanmoins : les utilisateurs de deux-roues motorisés représentent aujourd'hui près d'une personne sur quatre dans les accidents de la circulation routière (contre une sur dix il y a dix ans) et le nombre de blessés graves, cyclomotoristes ou motards, est désormais supérieur à celui des automobilistes. Ce constat préoccupant a conduit les pouvoirs publics à s'interroger sur les causes de cette situation et les leviers d'action possibles. Il a donc été demandé au préfet Régis Guyot, au titre de son expérience reconnue en matière de sécurité routière – notamment depuis la publication en 2002 des *Gisements de sécurité routière* – de réunir un groupe de travail afin de proposer, cette fois-ci, des « gisements » plus spécifiquement orientés vers les deux-roues motorisés.

Ces « gisements » représentent un nombre – plus ou moins facile à évaluer – de vies à épargner et de blessés à éviter. Leur exploitation pour progresser dans ce sens appelle des mesures spécifiques et des recherches nouvelles. Et, cette action particulière doit s'inscrire simultanément dans le cadre plus général des politiques nationale et locale conduites en faveur de la sécurité routière.

Le groupe de travail a mis l'accent sur les « gisements » suivants : développement d'un contrôle-sanction automatisé également dissuasif pour le conducteur d'un deux-roues motorisé et pour l'automobiliste, amélioration de la détectabilité, réduction de la sur-vulnérabilité, interventions sur les infrastructures routières, traitement des obstacles fixes hors agglomération, action auprès des conducteurs novices. Des « gisements » transversaux viennent en outre renforcer la réflexion en s'intéressant à l'enjeu majeur de santé publique que constitue l'accidentalité des motards et des cyclomotoristes, aux insuffisances des données et de la connaissance sur leur sécurité, à l'éducation à la sécurité dans leur formation, enfin aux stratégies locales et partenariales spécifiques aux deux-roues motorisés.



UNION EUROPÉENNE

GENDARMERIE Une force humaine

La région de gendarmerie du Nord-Pas-de-Calais, avec le soutien de l'Union européenne, organise pour la 3e année consécutive le Forum International sur la Cybercriminalité (FIC 2009) le mardi 24 mars 2009 au Grand Palais à Lille (59).

Le succès croissant de la manifestation permet d'envisager une mobilisation encore plus forte de l'ensemble des partenaires publics et privés, nationaux et internationaux, des collectivités territoriales, économiques et juridiques ainsi que des experts en criminalité numérique dans l'optique de développer une approche partenariale et transfrontalière de la lutte contre la cybercriminalité.

L'INHES est associé aux travaux de rédaction du *Livre blanc* sur la cybercriminalité porté par le Forum.

Temps forts : 15 conférences et ateliers scientifiques, un salon exposants, un espace dédié aux démonstrations et la remise du *Livre blanc* « Le chef d'entreprise face aux risques numériques » aux plus hautes autorités présentes.

Informations et inscriptions : www.fic2009.fr

CAHIERS DE LA SÉCURITÉ

http://www.cahiersdelasecurite.fr

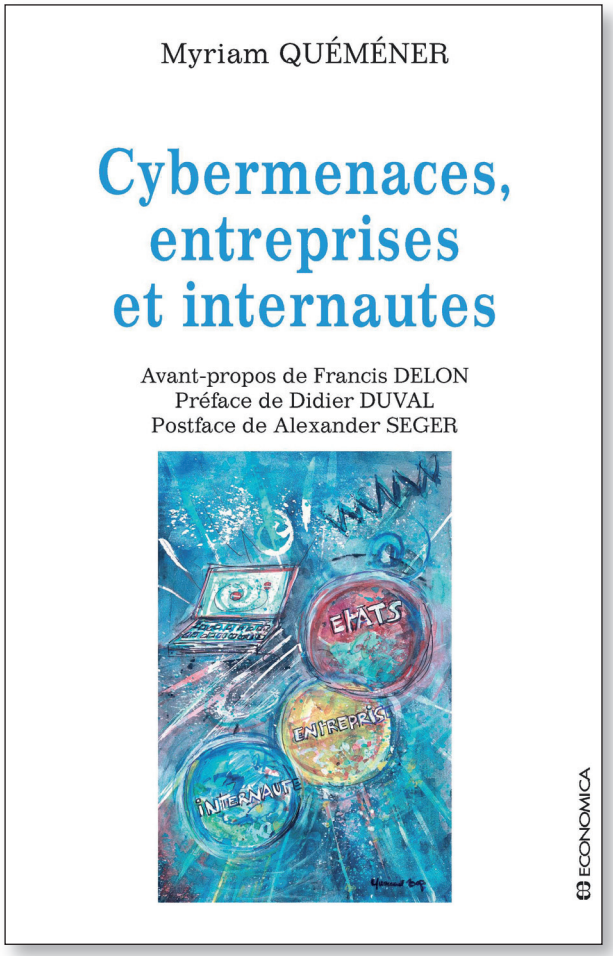
La forme inédite, plus aérée, plus attractive, rejoint notre préoccupation de fond : faire des Cahiers la revue de tous les penseurs et de tous les acteurs de la sécurité.

Notre ambition est de mettre une réflexion sérieuse et documentée au service de tous ceux qui en ont besoin pour penser et pour agir.

Accueil
Web
Lettres
L'intégrale
l'Inhes
Liens

INHES
INSTITUT NATIONAL DES HAUTES ÉTUDES DE SÉCURITÉ
"Les Borromées", 3 avenue du Stade de France
93218 Saint-Denis-La-Plaine cedex
Tél. 01.55.84.53.00 – Fax. 01.55.84.54.26
www.inhes.interieur.gouv.fr

Un ouvrage Economica Éditions



Cybermenaces, entreprises et internautes

Auteur **Myriam QUÉMÉNER**

Prix **19 €**

Parution : **1er novembre 2008**

Pagination : **265**

isbn-13 : **978-2717856422**

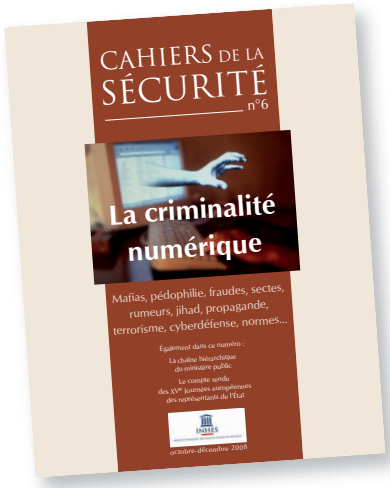
Le livre

Les cyberattaques sont désormais l'un des enjeux majeurs de notre société en visant les technologies de l'information et de la communication (TIC) numériques. Elles nous interpellent tous sur la vulnérabilité de nos sociétés face au réseau mondial qu'est l'Internet et pose la question cruciale de la sécurité du monde actuel. Ces menaces sont universelles et ciblent aussi bien les États, les entreprises et les internautes, sous des formes très variées comme, par exemple, le cyberterrorisme ou la contrefaçon en ligne. Ce livre n'est pas un réquisitoire contre Internet, mais bien au contraire un guide de sensibilisation pour mieux alerter les entreprises et les internautes des dangers des réseaux numériques.

Quelle responsabilité pour les acteurs de l'Internet ? Quelle est la réglementation en matière de cybersurveillance du salarié ? Myriam Quéméner répond à ces questions et présente une typologie des délinquants de la toile, leur façon de nuire ainsi que l'ensemble des cybermenaces actuelles et les réponses juridiques appropriées. Elle fournit également des pistes de réflexion par une mise en perspective de problématiques sous le double regard de l'anticipation stratégique et de l'intelligence économique dans une optique globale de sécurité.

L'auteur

Magistrat depuis 1986, substitut général au service criminel de la Cour d'Appel de Versailles après avoir été précédemment sous-directrice à la direction des Affaires criminelles et des Grâces. Elle participe comme expert à des séminaires internationaux organisés par les ministères et le Conseil de l'Europe sur la cybercriminalité. Elle a écrit plusieurs articles sur la cybercriminalité et publié avec Joël Ferry, en 2007, Cybercriminalité, défi mondial et réponses aux éditions Economica.



Chaque trimestre retrouvez les CAHIERS DE LA SÉCURITÉ

À retourner à La Documentation française 124 rue Henri Barbusse 93308 Aubervilliers Cedex France

Acheter un numéro, s'abonner, c'est simple :

@ En ligne :
www.ladocumentationfrancaise.fr
(paiement sécurisé)

✉ Sur papier libre
ou en remplissant
ce bon de commande
à retourner à l'adresse ci-dessus

En librairies (achat au n°)
et à La Documentation française :

- 29-31 quai Voltaire
75344 **Paris** Cedex 07
01 40 15 71 10

- 165 rue Garibaldi - La Part-Dieu
69001 **Lyon** Cedex 03
04 78 63 23 02

Où en est ma commande, mon abonnement ?

✆ 01 40 15 69 96 de 9h à 12h30

Une information, un renseignement ?

✆ 01 40 15 70 00 de 9h à 18h

✉ La Documentation française
Service Relations clients
124 rue Henri Barbusse
93308 Aubervilliers Cedex France

Bulletin d'abonnement et bon de commande

Je m'abonne aux Cahiers de la sécurité

Un an, 4 numéros soit près de 20 % d'économie

☐ France métropolitaine (TTC) **60,50 €**
☐ DOM-TOM-CTOM,
(HT, avion éco) **66,10 €**
☐ Union européenne (TTC) **63 €**
☐ Autres pays (HT, avion éco) **69,20 €**
☐ Supplément envoi par avion prioritaire pour tous les pays hors d'Europe

Je commande le(s) numéro(s) suivant(s)
des Cahiers de la sécurité
au prix unitaire de **18,90 €**

. . . . . .
. . . . . .
. . . . . .

pour un montant de . . . . . €
participation aux frais d'envoi + 4,95 €
Soit un total de . . . . . €

Voici mes coordonnées ☐ M. ☐ Mme ☐ Mlle

Nom : . . . . . Prénom : . . . . . .
Profession : . . . . . .
Adresse : . . . . . .
Code postal : . . . . . Ville : . . . . . .
Mél . . . . . .

Ci-joint mon règlement de . . . . . €

☐ Par chèque bancaire ou postal à l'ordre de M. l'Agent comptable de La Documentation française
☐ Par mandat administratif (réservé aux administrations)
☐ Par carte bancaire N° |_|_|_|_| |_|_|_|_| |_|_|_|_| |_|_|_|_| Date d'expiration : |_|_|_|_|

N° de contrôle |_|_|_| (indiquez les trois derniers chiffres situés au dos de votre carte bancaire, près de votre signature)

Date Signature