N° 404 OCTOBRE 2009

Le Bulletin de L'ILEC

MENSUEL

Devant la cyberdélinquance : enjeux et moyens

Une mutation du crime organisé

Si le droit pénal en ignore la notion, il ne méconnaît pas les caractéristiques d'un phénomène qui touche aussi bien les Etats, les internautes et les entreprises. L'arsenal juridique s'adapte.

*Entretien avec Myriam Quéméner, magistrat au service criminel de la cour d'appel de Versailles **

Comment définissez-vous la cybercriminalité ?

Myriam Quéméner : C'est la délinquance liée aux réseaux numériques. Elle est transversale et porte aussi bien sur les piratages, les fraudes, les contrefaçons, les infractions dites de contenu comme la pédopornographie ou le racisme. Tout le champ pénal est concerné.

Qui sont les cyberdélinquants ?

M. Q. : Les délinquants classiques se sont mis à utiliser les réseaux numériques, car ils ont vite compris que c'est pratique et peut rapporter gros. L'anonymat et le faible coût d'accès ont créé une aubaine. Il y a les *hackers*, les pirates, les *coders*[1] et les « mules »[2]. Ils se jouent des systèmes juridiques des Etats. La criminalité organisée a installée une hiérarchie, avec des jeunes chargés de récupérer des données personnelles sensibles, au moyen de programmes robots et logiciels malveillants, pour ensuite les revendre. Il s'agit plus d'une reconversion de la délinquance que d'une nouvelle délinquance. Les délinquants s'adaptent grâce aux outils, le *spamming*, le *phishing*, le *pharming*, le *carding*[3]… On constate aussi un fort développement de l'« e-réputation » en matière de concurrence, d'espionnage industriel, pour nuire à des individus ou à des entreprises

Quelles sont les nouvelles formes d'atteinte au droit des sociétés ?

M. Q. : La cybercriminalité est multifacette. Elle vise les entreprises comme les Etats et les internautes. Sur le plan économique, on assiste à une explosion

(suite page 3)

Que font les polices ?

Dans une de ses *Fictions* intitulée « La Bibliothèque de Babel », Jorge Luis Borges imagine le fantasme de tout lettré (par ailleurs cauchemar du général de brigade Stumm von Bordwetz dont les lecteurs ont fait la connaissance le mois passé ; la remarque s'impose étant donnée la puissante représentation de la maréchaussée dans le présent *Bulletin*). Il rêve la bibliothèque idéale, image de l'univers : *« L'Univers (que d'autres nomment la Bibliothèque) se compose d'un nombre indéfini, et peut-être infini, de galeries hexagonales… »* L'interminable théorie des hexagones contient toute la pensée. *« De ces prémisses incontournables il [un bibliothécaire de génie] déduisit que la Bibliothèque est totale, et que ses étagères consignent toutes les combinaisons possibles des vingt et quelques symboles orthographiques, c'est-à-dire tout ce qu'il est possible d'exprimer dans toutes les langues. »* Vertige de l'esprit dont la Tour Bibliothèque, échelle de Jacob inversée, conduit au Logos par le seul secours de l'intelligence humaine. *« Quand on proclama que la Bibliothèque comprenait tous les livres, la première réaction fut un bonheur extravagant. Tous les hommes se sentirent maîtres d'un trésor intact et secret… L'Univers se trouvait justifié. »* Retour à la théologie de la justification. Comme au Paradis, toutefois, le ver était dans le fruit, ou plutôt le serpent rôdait au pied de l'arbre de la connaissance, prototype béatifique de la Bibliothèque de tous les savoirs. En effet, la Bibliothèque comme Internet déréalise le monde : *« La certitude que tout est écrit nous annule ou fait de nous des fantômes. »* Se substitue au monde sensible une mascarade qui se nomme l'univers du virtuel, Babylone immatérielle, lieu de toutes les turpitudes anonymes. Borges en vain nous avait avertis. Désormais, plus sûrement que la couche d'ozone, l'internet enferme la planète dans sa toile, offrant un terrain de jeu à la criminalité, comme si, au terme de la constitution de la Noosphère chère au père Teilhard, n'apparaissait pas l'Omega, mais le péché répété. Est-ce un hasard si le colonel Régis Fohrer fait une allusion au Décalogue, lorsqu'il évoque *« dix recommandations pour la sécurisation de l'espace numérique des entreprises »* ?

Comme vous y allez, diront les sceptiques, Borges est un poète et Teilhard un casuiste. Il faut revenir sur terre et voir ce qui se cache sous le terme emphatique de « cybercriminalité ». René Henri Legret n'atténue pas l'hyperbole lorsqu'il décrit la cybercriminalité comme une *« hydre à plusieurs têtes dont la motivation est le plus souvent financière »*. Les familiers de Maurice Dantec, celui de *Cosmos Incorporated* ou de *Grande Jonction*, en sont déjà convaincus. Notre interlocuteur de préciser : *« Cela va du plus connu, la pédopornographie, le trafic de personnes, de substances illicites, le révisionnisme, au plus opaque : l'activité des organisations criminelles transnationales, le piratage, le terrorisme, l'espionnage, la déstabilisation. »* Il y a aussi selon Myriam Quéméner, *« la contrefaçon en ligne et le téléchargement illicite »*, encore que le terme « crime » dépasse en l'espèce sans doute la pensée de l'auteur. Il y a encore, pour Christian Aghroum, *« la contrefaçon de carte bancaire, la pénétration des réseaux, les fraudes dans le commerce électronique, les escroqueries en ligne »*. Et grandit entre les Etats le spectre de la guerre numérique, dont l'Estonie a été la cible pour avoir déboulonné une statue à la gloire des soldats soviétiques. *« La Corée du Sud et les Etats-Unis,* commente Gilbert Pinte, *ont subi trois importantes vagues d'attaques durant la seule première semaine de juillet 2009. »* Plus besoin de jeter des avions contre le Pentagone, un ordinateur suffirait à paralyser l'hyperpuissance ! Pour couronner le tout, c'est la personne même qui est en jeu, à en croire Eric Freyssinet : *« Les citoyens sont-ils bien conscients de la nature des informations qu'ils diffusent sur la Toile ? Certains évoquent un permis de naviguer comme il existe un permis de conduire. »* Sale temps pour les libertés individuelles. A cet égard, Christian Aghroum ne nous rassure pas lorsqu'il souhaite *« la mise à jour de la loi, qui n'autorise que dans le cadre de la lutte contre le terrorisme et la criminalité organisée, et sous le contrôle d'un magistrat, d'installer des vidéos et des micros chez les criminels organisés »*. Le spectre de Big Brother rôderait-il dans les canaux de l'internet ? Oui peut-être, car l'Etat se cache au bout de la caméra, mais non sans doute, car c'est bien pire. « *N'importe quel Français, connecté depuis chez lui,* assure Eric Freyssinet, *est à la portée des délinquants du monde entier. »* L'homme devient un Big Brother pour l'homme.

Que fait donc la police ? Eh bien, elle se mobilise, tout comme la maréchaussée. Prévert seul pourrait inventorier les services chargés de combattre la cybercriminalité. René-Henri Legret défend les couleurs du CRED. Christian Aghroum celles de l'OCLCTIC. Le vice-amiral Michel Benedettini, qui dirige l'ANSSI, évoque la DGSSI, les OZSSI et le CFSSI. Le colonel Joël Ferry vante l'IRCGN. Le lieutenant-colonel Freyssinet ajoute le STRJD et la MITICOM. Le lieutenant-colonel Fohrer organise le FIC. Le tout constitue un arsenal franco-français qui devrait être complété par des coopérations avec l'étranger – car le phénomène est par nature transnational–, soit sur une base bilatérale, comme avec l'Irlande, soit sur le plan mondial, avec une *« ONU de l'internet »*. Où l'utopie seule paraît répondre à la science-fiction devenue banalité.

Avec l'utopie, le pire n'est jamais loin. Grâce à l'internet, il triomphe, et s'attaque à ce que nous avons de plus précieux depuis l'édit de Villers-Cotteret. Notre pauvre langue. Elle croule sous les anglicismes tombés de la Toile. Entre *« Web »* et *« Net »*, il n'est question que de *« blogs »*, de *« wifi »*, de *« peer to peer »* sous la menace du *« hacker »*, Absalon de service. Faut-il chanter la pavane pour une langue défunte, à la lecture de l'index de l'ouvrage *Cybercriminalité, défi mondial*, où se pressent des termes aussi ésotériques et déplaisants que *« happy slapping »*, *« carding »*, *« pharming »*, *« phishing »*, *« spamming »*, barbares venus d'au-delà du *limes* polluer notre fragile parlure ? La loi Toubon n'a pas été abolie. Elle devrait s'imposer à tous comme une règle de santé publique. Au moins est-elle obligatoire pour les agents de l'Etat. Alors se pose la question subsidiaire, puisque juges et gendarmes cèdent à la tentation du *globish*. Que fait la police des polices ?

Dominique de Gramont

de la contrefaçon en ligne, qui touche aussi bien la contrefaçon de sites que la contrefaçon de marques et de produits. N'oublions pas le téléchargement illicite de films, de musique et de jeux vidéo.

Quand la notion de cybercriminalité est-elle apparue dans le droit français ?

M. Q. : Le terme n'est pas employé dans le droit pénal français, sauf en matière de mandat d'arrêt européen. Le droit français a appréhendé le phénomène avec la loi Godfrain de 1988 sur les atteintes au traitement informatisé de données, mais la loi du 9 mars 2004, qui vise la criminalité organisée transnationale, ne mentionne pas le mot. Trop de juristes sont encore peu sensibles à l'enjeu.

Comment l'arsenal juridique français s'est-il adapté ?

M. Q. : Nous disposons d'un arsenal assez complet, qui s'est adapté, particulièrement après les attentats de 11 septembre 2001, avec la loi sur la sécurité quotidienne de 2001, qui a permis la conservation des données pendant un an, la loi de mars 2003, qui a renforcé les moyens d'investigation, dont les perquisitions informatiques et les interceptions téléphoniques, transposables à la Toile. En matière de compétence territoriale, des précisions doivent être apportées sur le lieu des serveurs et la compétence de la juridiction, car plusieurs juridictions peuvent être simultanément compétentes. La loi d'orientation, de programmation et de performance de sécurité intérieure (Loppsi 2), portée par le ministère de l'Intérieur, va introduire une infraction concernant l'usurpation d'identité en ligne. La France a ratifié la convention du Conseil de l'Europe de novembre 2001, premier traité international en matière de cybercriminalité.

La technologie en ligne se complique tous les jours. Doit-on former une catégorie particulière de magistrats et qui doit s'en charger ?

M. Q. : Des formations continues sont déjà proposées par L'Ecole nationale de la magistrature (ENM) et la Commission européenne développe des certificats de juristes en matière de cybercriminalité. Il serait pertinent d'en spécialiser davantage pour avoir un magistrat référent par parquet. Les sessions de formation proposées par l'ENM devraient être obligatoires pour les magistrats chargés du domaine et surtout pluridisciplinaires, associant des avocats et des magistrats, mais aussi des experts nationaux et internationaux, des services d'enquête spécialisés, des acteurs de la Toile, des associations comme le Clusif, qui dresse chaque année un panorama de la cybercriminalité.

Quel dialogue la justice entretient-elle avec les autres acteurs institutionnels ?

M. Q. : Nous entretenons d'excellentes relations avec de nombreux services spécialisés dont l'IRCGN (Institut de recherche criminelle de la gendarmerie nationale) et l'OCLCTIC (Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication). Ce sont nos fournisseurs de procédures.

Faut-il un ministère public à compétence nationale en matière de cybercriminalité ? Un service spécial au ministère de la Justice ? L'espace judiciaire ne doit-il pas tendre vers une européanisation puis une mondialisation ?

M. Q. : Il faut au moins des pôles spécialisés par régions. Si le juge d'instruction est supprimé, il faudra d'autant plus spécialiser le parquet. Au ministère, il faudrait un service spécial, et il serait judicieux de créer un comité interministériel contre la cybercriminalité pour coordonner les actions de la Justice, de l'Intérieur, de l'Education nationale ou du secrétariat d'Etat au numérique. Des actions sont menées avec le Conseil de l'Europe, qui démarche les pays non signataires de la convention et propose des expertises dans les zones qui rencontrent des difficultés économiques et deviennent des terrains propices à la cybercriminalité, comme l'Afrique noire, l'Amérique latine ou le Maghreb.

Entre 2007, première parution de votre livre, et 2009, se seconde édition, quelles ont été les grandes évolutions ? Et demain ?

M. Q. : En deux ans, il y a eu des modifications législatives, une jurisprudence importante en matière de responsabilité des prestataires techniques, de nouvelles fonctions de l'internet (réseaux sociaux et leurs incidences sur l'usurpation d'identité) et les qualifications pénales. Nous avons mis l'accent sur la coopération public-privé, avec des acteurs comme eBay ou Microsoft. Les enjeux demain seront la protection des données personnelles, et le nécessaire équilibre entre la protection des libertés individuelles, le « droit à l'oubli », et les investigations destinées à réprimer les cyberdélinquants. Il faut aussi renforcer la coopération internationale, ainsi que la formation et la prévention. Réduire cette délinquance suppose que les citoyens maîtrisent les nouvelles techniques de l'information. Dans les entreprises, l'urgence est la protection du patrimoine informationnel et la création d'un vrai dialogue entre les métiers : marketing, juridique, commercial. Souvent, ils s'ignorent.

Propos recueillis par J. W.-A

*Cybercriminalité, défi mondial, *de Myriam Quéméner et Joël Ferry, Economica, 2009 ;* Cybermenaces, Entreprises, Internautes, *de Myriam Quéméner, Economica, 2008*

1. Fouineurs, pirates et installateurs de codes malveillants.

2. Intermédiaires recrutés par le biais de courriels ou de sites, sous couvert de contrats de travail ou de commissions.

3. Courrier indésirable, hameçonnage, détournement d'adresses ou de cartes bancaires.

L'entreprise dans la ligne de mire

Au premier rang des urgences en matière de cybercriminalité figure la guerre de l'information dont sont victimes les entreprises, du fait des attaques de concurrents sans scrupules.

*Entretien avec Joël Ferry, colonel de gendarmerie, commandant la section de recherches de Versailles**

Depuis quand la gendarmerie est-elle impliquée dans la lutte contre la cybercriminalité et quelles sont ses actions ?

Joël Ferry : Elle est impliquée depuis 1998, quand fut publié le rapport du Conseil d'Etat sur les réseaux numériques, dû à Isabelle Falque-Pierrotin, aujourd'hui présidente du Forum des droits de l'internet, et auquel la Gendarmerie nationale a contribué. Son Institut de recherche criminelle s'intéressait au phénomène depuis 1995. Un dossier avait été traité par la section recherches de Paris cette année-là.

La gendarmerie mène des actions de sensibilisation auprès des particuliers, des parents d'élèves, des chefs d'établissement scolaire et des chefs d'entreprise. Mais si Internet est un nouveau vecteur de criminalité, il ne faut pas le stigmatiser et en avoir peur. Il convient de le connaître et de le maîtriser. Sur le plan répressif, la gendarmerie a mis en place depuis 2000 des enquêteurs spécialisés en technologies numériques, chargés d'assister les enquêteurs traditionnels, voire de prendre à leur compte les enquêtes concernant l'usage des réseaux numériques.

« Ne devrait-on pas créer un deuxième Internet où la sécurité serait au cœur du système ? »

Face aux multiples facettes de la cybercriminalité – infractions au système de traitement de données, comme l'intrusion dans un système informatique ; infractions de contenu, comme le stockage d'images pédophiles ; utilisation des réseaux numériques comme supports d'infractions traditionnelles (vols, escroqueries et atteintes à la propriété intellectuelle) –, la gendarmerie, grâce au STRJD (service technique de recherches judiciaires et de documentation), peut procéder au plan national à des rapprochements entre les affaires, et traquer les internautes aux comportements illicites. Un service de veille constate les ventes de produits volés ou contrefaits sur des sites d'enchères ou de commerce. L'IRCGN (Institut de recherche criminelle de la Gendarmerie nationale) se consacre à la police technique et scientifique. Il centralise les données utiles en matière de preuves numériques, coordonne des opérations nationales et met à la disposition des enquêteurs des moyens et des techniques d'investigation spécifiques, comme des logiciels d'aide à l'enquête. La gendarmerie est en mesure de répondre immédiatement aux plaintes d'un chef d'entreprise.

L'arsenal juridique français est-il adapté ?

J. F. : Il est l'un des plus aboutis. Depuis 2002, de nombreuses lois sont venues protéger la société et le citoyen. Sur le plan pénal, l'arsenal est riche et cohérent au niveau français et européen. Le problème se situe aux frontières de l'Union. La convention de Budapest de 2001 est un premier pas, mais elle ne vaut que pour les pays qui l'ont ratifiée : une douzaine en Europe plus les Etats-Unis. Elle ne l'est pas par la majorité des signataires dont le Royaume-Uni, l'Allemagne, l'Italie, le Canada, le Japon ou l'Afrique du Sud, qui ont pourtant participé activement aux négociations. La convention est fondamentale pour la protection de l'enfance, des systèmes automatisés de données et des droits d'auteurs. Elle oblige les Etats à d'instaurer des mesures procédurales et techniques adaptées contre l'usage illégal des techniques numériques. Elle favorise l'entraide policière et judiciaire dès lors que des moyens numériques ont été utilisés dans l'espace international pour commettre une infraction. On peut regretter que, autant l'Europe a été consciente de la nécessité de préserver les données de connexion (un an en France), autant cet enjeu semble ignoré ailleurs. La convention n'oblige pas à la conservation des données de connexion, qui constitue souvent le point de départ de toute enquête.

Les cyberattaques annoncent-elles une nouvelle forme de guerre entre Etats ?

J. F. : C'est une nouvelle forme de guerre. Je doute que deux Etats tentent un jour de s'opposer frontalement sur Internet, mais un Etat peut mener des actions insurrectionnelles, terroristes, ou comme dans le cas de la Géorgie, contre-insurrectionnelles. Internet peut fournir le moyen de déstabiliser un Etat comme une entreprise, en bloquant le système informatique d'une administration, d'un commerce, d'une usine ou d'une banque par déni de service. On peut créer la psychose, en contrôlant des serveurs majeurs du secteur public ou privé pour désinformer ou empêcher les transactions économiques ou commerciales essentielles. L'attaque de 2008 contre l'Estonie, pays largement numérisé, a consisté à bloquer plusieurs heures tous les services essentiels au fonctionnement de l'Etat. Les codes malveillants, « chevaux de Troie », vers et virus, peuvent devenir des armes de perturbation massive.

Depuis la première édition de votre livre en 2007, les menaces numériques sont-elles mieux appréhendées et la cybercriminalité a-t-elle évolué ?

J. F. : Le dispositif législatif s'est renforcé et la jurisprudence s'est enrichie. On s'est interrogé sur la nature des réseaux sociaux : sont-ils hébergeurs ou éditeurs ? Dans un cas ils ne sont pas responsables, dans l'autre ils le sont… La loi Hadopi introduit une approche graduelle de la contrefaçon entre le droit de copier à des fins personnelles et à des fins commerciales. Le défi sera demain le maintien en l'état d'Internet avec la possibilité d'échanges instantanés dans tous les domaines, notamment celui des objets. L'augmentation exponentielle des échanges ne risque-t-elle pas de faire exploser le système ? Pour l'entreprise, la conservation des données et la protection des informations sont déterminantes. Il est nécessaire pour elle de se donner les moyens d'une politique de sécurité solide, élaborée en concertation avec l'ensemble des salariés.

Droits des personnes, des sociétés, de la propriété intellectuelle… Quelle est la priorité ?

J. F. : Tout est urgent, mais ce qui est urgentissime concerne l'intelligence économique, notamment la protection du patrimoine matériel et immatériel de l'entreprise. Les TPE et PME sont les plus vulnérables. Elles ne disposent pas toujours de la compétence, de la disponibilité et des moyens de leur sécurité numérique. La guerre de l'information est prioritaire. Elle a pour cible l'entreprise, avec la conquête par ses concurrents de ses parts de marché, de ses produits, de ses idées et de ses clients.

Propos recueillis par J. W.-A

*Coauteur de *Cybercriminalité, défi mondial, op. cit.*

Information bien gardée, entreprise avisée

La sécurité des systèmes d'information est une nécessité de bon sens pour les entreprises, exposées au vol de données et à la malveillance. Et un avantage concurrentiel pour les premières qui s'en préoccupent.

Par Rémy Février, commandant de gendarmerie spécialiste en intelligence économique, et Joël Ferry, colonel de gendarmerie, commandant la section recherches de Versailles.

Avec une compétition économique mondiale opposant un nombre croissant de pays, l'impact des technologies de l'information, dans une économie de la connaissance où l'information a une valeur intrinsèque majeure, mène à la guerre économique. Celle-ci rend plus cruciale la recherche d'avantages concurrentiels pérennes. Longtemps considérée comme un simple support de la chaîne de valeur de l'entreprise, les systèmes d'information (SI) sont à présent au cœur de l'activité. La mise en place, la gestion et la pérennité d'un SI obéissent à des impératifs de plus en plus complexes. Les réseaux sont soumis à des forces diverses et souvent contradictoires induisant des mouvements dont la méconnaissance peut être très préjudiciable.

Les risques liés à une insuffisante sécurité du SI d'une entreprise sont de deux types : la perte directe d'informations stratégiques et l'atteinte à l'image.

Perte d'informations stratégiques

Alors qu'une gestion optimale du SI devient essentielle, rares sont les dirigeants de PME qui mettent l'accent sur sa sécurité. Pourtant, les modes de captation des informations depuis les serveurs et postes de travail sont multiples, et quelques précautions de bon sens réduiraient beaucoup les risques liés à l'utilisation d'un SI peuvent être envisagés selon une nomenclature récurrente.

Les postes de travail

Un des points fondamentaux mis en évidence par la grande majorité des études relatives aux SI réside dans la méconnaissance, de la part des collaborateurs, des dangers inhérents à leur utilisation. Seuls les périls connus du grand public et faisant l'objet d'une diffusion médiatique récurrente paraissent plus ou moins identifiés. Bien peu de collaborateurs font le lien entre virus et portail ou messagerie électronique : de nombreux utilisateurs naviguent paisiblement sur la Toile sans imaginer que cette connexion est toujours à double sens, du fait d'un échange permanent de fichiers potentiellement infectés (*« cookies »*). De même, l'utilisation désinvolte d'une messagerie électronique peut s'avérer dramatique pour l'ensemble d'un réseau interne, notamment par le téléchargement d'un code infecté présent dans un pièce jointe ou plus rarement dans le corps du message. Ce code est susceptible de provoquer de graves dysfonctionnements dans l'ordinateur cible, de se propager à l'ensemble du réseau, voire d'ouvrir une porte dérobée par laquelle son auteur pourra prendre à distance le contrôle du poste de travail. La conjonction de ces deux utilisations peut devenir

dramatique lorsque le salarié communique, sur un site commercial par exemple, l'adresse de messagerie qui lui a été affectée par son employeur, alors qu'elle peut être détournée au détriment de l'entreprise.

Les « nomades »

Le large succès de l'ordinateur portable en fait une cible de choix. Les portables contiennent souvent des données de première importance, mais la menace n'est pas toujours évaluée correctement. Les efforts de protection des SI sont insuffisants : la plupart portent prioritairement sur le réseau physique interne. Les formalités de mise à disposition d'un ordinateur portable auprès d'un collaborateur se limitent souvent à la signature d'une décharge qui exonère le service informatique de toute responsabilité ultérieure et au choix d'un mot de passe personnel.

Le récipiendaire devrait, au minimum, se voir spécifier l'ensemble des dangers relatifs au vol de son matériel informatique (il faut toujours le conserver à portée de vue en cas de déplacement) ou à l'interception de ses données, ainsi que la nécessité de définir un mot de passe suffisamment long et complexe pour éviter une intrusion rapide dans le système.

Les réseaux sans fil

Le WiFi *(Wireless Fidelity)* constitue une ressource de plus en plus employée dans les entreprises : sa facilité d'utilisation et la mobilité qu'il autorise en font un moyen plébiscité par les utilisateurs. Néanmoins, de par leur nature (ondes radioélectriques), dans le cas d'entreprises de taille modeste, la pénétration des réseaux WiFi alimentés par des connexions particulières est assez simple.

La détermination de la clé de chiffrement « WEP » d'un émetteur WiFi prend, en moyenne, quelques minutes, même avec des clés de 128 bits. La maîtrise des outils nécessaires, accessibles depuis n'importe quel moteur de recherche, est à la portée de n'importe quel utilisateur un peu opiniâtre. Bien que surtout répandue comme support de téléphonie mobile, la technique Bluetooth peut ponctuellement faire l'objet d'interceptions, au travers de failles mises en évidence sur certains téléphones – souvent rapidement colmatées par les constructeurs lors de mises à jour des systèmes d'exploitation.

Les installations physiques

Pour autant, il serait erroné de considérer que seuls les matériels liés à l'utilisateur final sont vulnérables : les réseaux internes proprement dits peuvent constituer des cibles, au travers de failles logicielles ou matérielles : « pare-feu » sous-dimensionné, absence de véritable politique de gestion des mots de passe (changements réguliers et retraits des codes personnels des salariés ayant quitté l'entreprise sont indispensables), manque de sécurité du portail de l'entreprise…

L'usage du réseau

Le réseau est organisé de telle sorte qu'avec la convergence des systèmes les courriers électroniques échangés par les salariés au moyen d'un ordinateur de poche *(PDA)* peuvent donner lieu à captation d'informations permettant de connaître la stratégie ou les avancées techniques d'une entreprise.

Atteintes à l'image

Les autres risques liés à la sécurité défaillante d'un SI sont les atteintes à l'image ou à la réputation d'une entreprise. Le détournement d'un site constitue une arme redoutable dans une lutte opposant des groupes de pression ou ONG à des entreprises, pour les activités industrielles ou commerciales de celles-ci. Si ce type d'attaque est souvent limité à des enjeux médiatiques et sociétaux, il n'en demeure pas moins que n'importe quelle entreprise peut subir une campagne de dénigrement du fait d'une altération de l'intégrité de son SI.

La mondialisation de l'économie, conjuguée à la nécessité de préserver des parts de marché – a fortiori dans un contexte de ralentissement de l'activité – peut pousser des acteurs peu scrupuleux à franchir les limites de l'acceptable en termes de concurrence. L'atteinte à l'image d'une entreprise peut résulter d'une action malveillante visant l'un de ses responsables, qui aura bien du mal à prouver son innocence, tant il est vrai qu'il reste toujours un doute dans l'esprit du public. Que penser de l'envoi au directeur général d'une société de courriers électroniques contenant des images pédophiles ? L'image institutionnelle d'une entreprise et de ses marques commerciales, porteuses d'années d'efforts soutenus en communication, est très vulnérable en cas de menées concurrentielles agressives.

Responsabilité des dirigeants

Depuis plusieurs années, les tribunaux manifestent la volonté de responsabiliser les entreprises et leurs dirigeants, en ne s'intéressant non plus seulement à la faute, mais aussi aux personnes qui auraient pu l'empêcher. C'est la remise au goût du jour de la vieille notion, en droit civil, de *« bon père de famille »*. L'effet recherché est de pousser les dirigeants d'entreprise à prendre conscience du caractère indispensable que revêt la sécurité des SI et à utiliser toutes ressources à leur disposition afin de les protéger. Tel est le cas de la protection des traitements de données à caractère personnel.

La désignation d'un directeur de la sécurité des SI ne suffit pas à dédouaner les dirigeants de leurs responsabilités : le fait de déléguer une tâche ne fait pas disparaître l'obligation qu'a l'employeur de contrôler, au sens du Code civil, la légalité des actes commis par ses collaborateurs. De même, l'utilisation du matériel

informatique à disposition des salariés accordée à titre privé et sur le temps de travail ne l'exonère pas de sa responsabilité de surveillance au sens de l'article 1384 alinéa 5 du Code civil. (TGI de Marseille, 11 juin 2003). Il revient au dirigeant d'insuffler une véritable politique de sécurité des SI dans l'entreprise, et de faire en sorte qu'elle bénéficie d'un fort appui du haut encadrement, afin de susciter par capillarité l'adhésion de l'ensemble des collaborateurs.

La fréquente absence de précautions particulières, dans les entreprises, autour des systèmes d'information, corrélée au nombre et à la diversité des menaces potentielles, fait que l'entité économique soucieuse de protéger son système dispose d'un avantage concurrentiel indirect. Cet avantage est susceptible non seulement de lui permettre de pérenniser son activité en cas de crise majeure, mais aussi d'éviter des mises en cause médiatiques très préjudiciables. Toutefois, l'acquérir n'est envisageable qu'à partir de la définition et de la mise en place d'une politique de sensibilisation de l'ensemble des salariés de l'entreprise. A défaut, tout effort en matière de réduction des risques de perte d'informations stratégiques demeurera d'une efficacité illusoire.

ilec

Un mal inéluctable ?

Le temps est venu d'aborder différemment les problèmes et d'imaginer des réponses originales à la cyberdélinquance.

Entretien avec René Henri Legret, secrétaire général du Centre de recherche et d'études de défense (CRED)

Comment définissez-vous la cybercriminalité ?

René Henri Legret : La cybercriminalité est complexe et ne touche pas un domaine en particulier. Avec Internet et l'usage généralisé de l'informatique, l'intégralité de l'activité humaine est concernée. Toutefois, il faut distinguer de quoi on parle. La cybercriminalité est une hydre à plusieurs têtes dont la motivation est le plus souvent financière. Cela va du plus connu, la pédopornographie, le trafic de personnes, de substances illicites, le révisionnisme, au plus opaque : l'activité des organisations criminelles transnationales, le piratage, le terrorisme, l'espionnage, la déstabilisation…

Dans une entreprise, tous les services sont des utilisateurs de l'informatique et détiennent un savoir, une part parfois non négligeable de la mémoire ou de l'histoire de la société. Ce capital informationnel est vital. La cybercriminalité est une menace d'arrêt de production, de contrefaçon, d'espionnage industriel, de concurrence déloyale, de désinformation, de vol, de chantage ou d'extorsion. Les sites d'entreprise sont des cibles pour la cybercriminalité. Assujettis à l'informatique, vitrines de l'entreprise ou de la marque, marchands ou outils de communication, ils sont prioritairement concernés par les dénis de service. Sur des sites marchands, des attaques peuvent vite se chiffrer en millions d'euros. On sait que 98 % des actes malveillants sont d'origine humaine, et leurs sources se trouvent à l'intérieur de l'entreprise. Une sécurité ne vaut que par son maillon le plus faible. Quelle que soit la serrure, ce ne sera qu'un problème de temps et de moyens pour l'ouvrir. Souvent, l'entreprise ne réalise pas que des données qu'elle pense obsolètes peuvent avoir un intérêt considérable pour un concurrent, un partenaire, un associé. En sécurité économique, on en revient toujours aux valeurs d'usage et d'échange d'une information, donc au prix que le concurrent est disposé à payer pour se l'approprier.

L'entreprise doit s'attacher à une démarche globale de sécurité de l'information et de veille sur l'évolution de la technologie, mais elle doit aussi définir une procédure de supervision de ses hommes clés. Un décès, une rupture, un divorce, un accident, un choc, une mutation, une sanction, un licenciement voire une frustration ou une déception sont autant de facteurs qui peuvent altérer le jugement, la vie, de quelqu'un et le rendre vulnérable. Le temps du petit pirate génial qui, du fond de son grenier, se lançait dans la pénétration d'un système pour jouer est révolu. Les attaques d'entreprises, d'organismes financiers de régulation ou de réseaux de gouvernance sont l'apanage d'acteurs structurés et techniquement à la pointe. Relevant d'Etat ou d'organisations criminelles transnationales, ils peuvent être disséminés en groupuscules de circonstance ou en francs-tireurs. Dans le cas des organisations criminelles transnationales, on ne compte plus les tentatives d'extorsion de fonds auprès de villes et de réseaux de gouvernance. Cela concerne aussi des entreprises. Quand il y a eu vol ou détournement de fichiers, le paiement d'une rançon ne protège en rien d'une fuite de données vers des concurrents.

Quelle est la solution ?

R.-H. L. : Personne ne l'a. Parlons plutôt de gestion et de contrôle d'un espace de liberté démocratique par une volonté politique forte, conjuguée à une volonté des acteurs de la société civile et de chaque

utilisateur. Concernant les moyens de paiement par carte électronique les normes EMV[1] sont complètement déployées, mais c'est loin d'être le cas dans tous les pays européens, a fortiori ailleurs dans le monde[2]. Le talon d'Achille, c'est la piste magnétique. Si une carte est recopiée et son code espionné par un réseau de caméras de surveillance, il est possible à un cybercriminel de réaliser un clone de la carte et de faire des transactions qui seront réputées légitimes (retraits d'argent ou paiement dans un pays étranger). Tant que la carte n'a pas été signalée comme frauduleuse par son propriétaire…

Les principales organisations criminelles spécialistes dans le genre sont des réseaux arméniens, russes, pakistanais. Il y a de fortes probabilités qu'ils alimentent des réseaux terroristes, même si c'est moins rentable que le trafic de substances. Les normes EMV ne sont pas parfaites, mais elles offrent une réponse graduée aux attaques et leur diffusion devrait permettre d'éviter nombre de fraudes. Il faut noter que ce sont les émetteurs de cartes qui ergotent toujours devant le prix pour assurer la sécurité des échanges de leurs clients (remplacement des terminaux, émission de cartes, mise à jour de leur centre de gestion de clés, etc.).

La protection des auteurs et des utilisateurs passe-t-elle par une surveillance accrue ?

R.-H. L. : Plus l'arsenal législatif va se renforcer, plus vont émerger des solutions chiffrées permettant de contourner « l'Etat répressif ». Avec Hadopi, des « fournisseurs » et leurs utilisateurs prêts à tout utilisent différentes méthodes : VPN (réseau privé virtuel), *P2P* (*peer-to-peer*, « d'égal à égal ») chiffré. Les plus aguerris utilisent déjà le réseau TOR (système de connexion anonyme à Internet). Tant que de premières têtes ne sont pas tombées, il est difficile d'anticiper les techniques qui seront utilisées. Dans tous les cas, ceux qui ont des choses à cacher se tourneront vers des solutions alternatives.

Lorsque des millions de personnes utiliseront des méthodes de chiffrement aléatoire, il est probable que de petits malins se fondront dans la masse et le flux pour cacher leurs forfaits. C'est déjà le cas avec le contournement des blocages de sites par les fournisseurs d'accès. La communauté des cyberpirates s'est organisée depuis longtemps pour rendre ces méthodes inopérantes. Faute d'avoir travaillé intelligemment, on se trouve dans une période de fausse ouverture, de prohibition. Qui dit prohibition dit gros profits, mais pas pour l'Etat.

« Les sites d'entreprise sont des cibles pour la cybercriminalité. Assujettis à l'informatique, vitrines de l'entreprise ou de la marque, marchands ou outils de communication, ils sont prioritairement concernés par les dénis de service. »

Que faut-il améliorer pour endiguer la menace ?

R.-H. L. : Des actions sont menées en France et dans d'autres pays de l'Union. La Police nationale a créé deux corps, un pour l'analyse informatique pure, l'autre pour la téléphonie pure. L'idée devrait être étendue à la gendarmerie. Ce sont deux métiers complémentaires, or dans toutes les enquêtes judiciaires il y a présence de la preuve numérique, ne serait-ce que par une carte SIM. Les téléphones cellulaires sont devenus des micro-ordinateurs dont l'exploitation nécessite des connaissances techniques particulières.

La gendarmerie a créé le FIC[3] : ces rencontres méritent d'être encouragées. Elle s'est dotée depuis 2001 de spécialistes, les « NTEC » (nouvelles technologies), répartis dans les régions. Leur travail est impressionnant, et on peut regretter que les départs tardent à être remplacés et que certains moyens ne soient pas complètement dévolus à leur mission première. L'institution gagnerait si, à l'instar des plates-formes régionales de techniciens d'investigation criminelle, elle créait des « plates-formes NTEC ». Elle pourrait envisager de regrouper les unités de recherche spécialisées par départements ou par régions, afin de les doter d'une uniformité de compétence en « zones police » comme en « zones gendarmerie ». Ce serait un début de réponse aux difficultés que soulève la loi Hadopi. Ces groupes d'analyse des supports numériques pourraient avoir des délais raisonnables de transmission, pas plus de trois mois. Car il est préjudiciable pour la justice comme pour le justiciable d'attendre une décision un à deux ans. Et tout le monde aurait à gagner, parquet inclus, à une harmonisation des modalités d'échanges entre services dans une même institution. J'aurai garde d'omettre le renouvellement et le maintien opérationnel du matériel, soumis au règlement de la Commission centrale des marchés publics. Entre l'expression des besoins à un instant T, la rédaction du « *cahier des clauses techniques particulières* » et de l'appel d'offres, sa publication, le temps de réponse, les délais de dépouillement et la notification du marché, nous sommes déjà à T plus six mois. Si l'on ajoute le temps de livraison des fournisseurs, à T plus douze mois quand le matériel est déployé. S'il n'y a pas de problème !

D'autres initiatives méritent d'être relevées comme celles du « *Commissariat du futur* » où des expérimentations sont en cours, ou la création de l'ANSSI[4]. A nouveaux défis, nouveaux moyens. La Toile est un ensemble de voies de communication et d'échange. La raison de la création de la maréchaussée,

en son temps, à été d'assurer la sécurité des grandes voies d'échange et de communication : ports, routes, marchés… Si nous consacrions dix pour cent des effectifs chargés de la répression routière à la cybercriminalité, avec les moyens techniques et les budgets adéquats, nous verrions une amélioration du taux de résolution des affaires. Comme sur la route, les délits contraventionnels ou pénaux doivent être sanctionnés. C'est aussi un des volets de l'instruction civique nouvelle mouture à intégrer dans le cursus des jeunes. C'est une question de volonté politique, et aussi d'approche des problèmes : ouvrons notre esprit pour envisager des réponses graduées et originales à toutes les formes de délinquance. Il faut aussi élargir notre réflexion et notre action à nos partenaires de l'Union, multiplier les initiatives européennes pour fédérer des projets de code source ouvert, seule alternative à long terme pour l'indépendance des utilisateurs privés.

Propos recueillis par J. W.-A

1.www.emvco.com.

2.Voir le rapport 2008 de l'Observatoire de la sécurité des cartes de paiement (www.observatoire-cartes.fr).

3. Cf. p. 14

4. Cf. p. 11

Cyberformation contre cybercriminalité

Face à la cybercriminalité, la gendarmerie porte ses efforts sur la surveillance, l'investigation, la formation et la recherche-développement, en partenariat avec des universités et des entreprises.

*Entretien avec le lieutenant-colonel de gendarmerie Eric Freyssinet**

Quels sont les enjeux de la cybercriminalité ?

Eric Freyssinet : Nous sommes à l'ère de la maturité des réseaux de communication. Le premier enjeu est de faire comprendre à chacun que leurs effets pervers sont une réalité pour beaucoup de gens, car Internet est le support d'une grande partie de la communication économique, sociale ou officielle (on y déclare ses impôts). Le deuxième est économique, puisqu'une grande partie du commerce, dont celui des œuvres, ou des services bancaires sont proposés en ligne. La migration d'une partie de l'activité dans cet espace n'est pas un épiphénomène. Or elle suscite une délinquance qui ne semble pas suffisamment enrayée par les services de l'Etat. Le troisième enjeu est que la cybercriminalité est un défi mondial. Des outils juridiques apparaissent, une coopération se dessine, mais les frontières entre les Etats et leur souveraineté sont des obstacles à une répression efficace. Il existe des paradis numériques, comme la Grande-Bretagne pour la France, ou un Etat fédéré qui possède, aux Etats-Unis, ses propres lois. Le quatrième enjeu tient au type de dossiers. Un quart des enquêtes traitées par les enquêteurs spécialisés de la gendarmerie touche à la pédopornographie. Les autres enjeux sont la formation, les équipements, les outils.

Sommes-nous en présence d'une nouvelle mafia ?

E. F. : On constate l'apparition de nouvelles formes de criminalité organisée, attirées par la possibilité de faire rapidement des profits. On a observé l'année dernière une montée en puissance des publicités pour de faux anti-virus, qui incitent à télécharger un logiciel inefficace conduisant l'utilisateur à fournir son numéro de carte bancaire. Celle-ci peut être débitée plusieurs fois. Pour autant, nous ne sommes pas tant en présence d'une nouvelle mafia que de nouvelles victimes. N'importe quel Français, connecté depuis chez lui, est à la portée des délinquants du monde entier. On le constate avec la délinquance « nigériane », qui auparavant opérait par le papier ou le fax. La délinquance s'est entourée de spécialistes, informaticiens, ingénieurs, sans pour autant être mieux organisée. En matière d'escroquerie à la carte bancaire, c'est la même délinquance itinérante d'Europe de l'Est qui aujourd'hui encore s'empare de marchandises dans les camions.

Comment lutter contre ce qui est anonyme, et à la fois nulle part et partout ?

E. F. : Notre effort depuis plusieurs années est d'éviter que la cybercriminalité ne devienne anonyme. Evidemment, le besoin d'anonymat demeure dans certains pays, les citoyens veulent pouvoir s'exprimer sans crainte d'être repérés et inquiétés pour des raisons politiques. Mais dans le cadre d'une enquête judiciaire, et dans le respect des libertés individuelles, nous devons pouvoir identifier les personnes derrière les réseaux, et conserver des données par l'intermédiaire des opérateurs. Cela a conduit à la loi sur la sécurité quotidienne de 2001 et à une série de directives européennes. Des cyberpatrouilleurs vont à la rencontre des délinquants sur les réseaux et dialoguent avec eux afin de les identifier. Les Français sont à la portée de délinquants qui parlent français et s'abritent à l'étranger. Il reste difficile de demander à un Etat de faire fermer un site illicite. On peut le lui signaler, mais nous n'avons pas d'outils efficaces.

Quel est dispositif de lutte de la gendarmerie contre la criminalité numérique ?

E. F. : Un premier niveau d'intervention regroupe les services spécialisés, dont le laboratoire qui traite

de preuves informatiques, créé en 1992 à Rosny-sous-Bois, à l'Institut de recherche criminelle de la gendarmerie nationale (IRCGN). Une équipe de surveillance d'Internet créée en 1998 dans le service technique de recherches judiciaires et de documentation (STRJD) est chargée de la répression des atteintes aux mineurs et de la surveillance générale. Au niveau local ont été créés en 2001 les enquêteurs en technologie numérique, aujourd'hui au nombre de cent quatre-vingt-dix : leur mission est d'analyser les supports de preuve et de mener des investigations spécialisées. Depuis 2005, leur formation est validée par un diplôme de l'université de technologie de Troyes. Au niveau des compagnies départementales, six cent correspondants en technologies numériques jouent le rôle de relais auprès des soixante-mille gendarmes, pour les aider à acquérir les bons réflexes lorsqu'ils entendent une victime, à maîtriser les supports de preuve numériques et à connaître les outils.

L'IRCGN travaille avec des écoles d'ingénieurs et des universités sur des projets de recherche, certains financés par l'Agence nationale pour la recherche. Avec les universités de Troyes et de Montpellier, les partenariats vont s'intensifier, avec la création, dans le cadre d'un projet européen, d'un centre d'excellence contre la cybercriminalité baptisé 2-Centre, qui va mettre en réseau des centres de recherche et de formation, et former le personnel des opérateurs qui sont nos intermédiaires. La Garda Siochana irlandaise développe un partenariat similaire avec l'université de Dublin et constitue avec nous le pilote de ce réseau européen. Nous avons aussi des partenaires industriels : Thalès, Microsoft et Orange. L'objectif du centre est de développer en France une activité de recherche-développement et de formation, afin que la gendarmerie, la police et la justice dialoguent mieux avec les industriels. Si les outils de défense et de protection sont bien développés, ceux permettent d'identifier les sources le sont moins. Enfin, une « *Mission d'investigation sur les technologies de l'information et de la communication* » (Miticom) a été créée il y a trois ans par le ministère de l'Intérieur. Police et gendarmerie y sont associées en groupes de travail.

Quels sont les moyens d'enrayer la contrefaçon en ligne ?

E. F. : Elle est de trois types : la contrefaçon d'œuvres de l'esprit (musique, films, livres…), celle de produits manufacturés et celle d'objets électroniques (fausses cartes bancaires, appareils de copie de pistes magnétiques…). En matière d'œuvres de l'esprit, nous menons des actions ciblées contre une organisation à quatre niveaux : un groupe de personnes, sur un forum, récupère les copies, un autre pirate des serveurs pour stocker, un troisième anime, enfin des consommateurs adeptes de la culture *warez* (fréquentation de sites de distribution de programmes copiés ou « craqués », c'est-à-dire sans protection). Pour les produits manufacturés, l'équipe de surveillance de Rosny-sous-Bois est vigilante, mais les affaires judiciaires sont rares : les consommateurs ne sont guère sensibles aux enjeux économiques de l'escroquerie, ni aux enjeux sanitaires (faux médicaments).

Certains hébergeurs sont-ils malhonnêtes ?

E. F. : On assiste, notamment aux Etats-Unis, à une dérive d'hébergeurs qui, sous couvert de préserver la liberté d'expression, ne répondent pas aux demandes des services de police pour identifier ceux qui ont des activités malhonnêtes sur leurs serveurs. D'autres hébergeurs ont été créés par des groupes criminels, pour constituer de vraies sociétés avec pignon sur rue.

Contre les paradis numériques, il faut une prise de conscience des responsables politiques. Le phénomène ressemble à celui des paradis fiscaux. Une évolution de la convention sur la cybercriminalité du Conseil de l'Europe serait nécessaire. Le risque est grand du côté des pays émergents, où pourraient ne se développer que des activités économiques illégales sur les réseaux.

Faut-il un ministère public à compétence nationale en matière de cybercriminalité ?

E. F. : Cela faciliterait les choses pour les infractions internationales, mais il serait plus utile de donner des outils plus efficaces au ministère public compétent sur le plan local. Aujourd'hui, un parquet local peut être amené à financer le début d'une enquête (frais de réquisition des opérateurs) qui en réalité ne le concerne pas, ou peu. Il aura tendance à ne pas autoriser les enquêteurs à s'y investir. Il serait pertinent que ces budgets soient nationaux, tout en laissant aux enquêteurs et magistrats locaux la possibilité d'agir dans leur périmètre, de lancer des enquêtes et d'échanger de l'information.

Redoutez-vous de nouvelles formes d'atteinte aux droits des personnes et des sociétés ?

E. F. : Mes préoccupations portent sur les données personnelles, qui échappent de plus en plus à leur émetteur. Les citoyens sont-ils bien conscients de la nature des informations qu'ils diffusent sur la Toile ? Certains évoquent la création d'un permis de cybernaviguer comme il existe un permis de conduire. Cela ne correspond pas à notre culture, mais il faut donner aux jeunes les outils pour comprendre Internet et ses dangers. Mon autre inquiétude concerne la cryptographie, de plus en plus utilisée pour protéger les informations, mais aussi par des groupes criminels, ainsi que le développement des techniques de dissimulation des preuves. La solution passe par la formation et l'innovation.

Propos recueillis par J. W.-A

* Chargé des projets cybercriminalité à la direction générale de la gendarmerie nationale, sous-direction de la police judiciaire (DGGN-SDPJ).

ANSSI, nouvelle arme de l'Etat

Depuis l'été dernier, une agence nationale met en œuvre la politique de défense contre les attaques informatiques, qu'elles soient dirigées vers la sphère publique ou vers le privé.

Entretien avec le vice-amiral Michel Benedittini, directeur général adjoint de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

La création par décret, le 9 juillet 2009, de l'ANSSI participe-t-elle d'une stratégie spécifique en matière de cybercriminalité ?

Michel Benedittini : Oui, mais elle dépasse l'enjeu de la cybercriminalité, pour celui de la cyberdéfense qui l'englobe. Cette création s'inscrit dans la prise de conscience, depuis quelques années, d'une posture de l'Etat insuffisamment puissante face à la montée des risques et à l'enjeu majeur du numérique dans la société, pour la vie économique, sociale, la défense du pays ou le fonctionnement de l'Etat. Ce retard a été souligné par deux rapports parlementaires, celui du député Pierre Lasbordes en décembre 2005 et celui du sénateur Roger Romani en juillet 2008, qui ont joué un rôle de catalyseur. La DCSSI, direction centrale de la sécurité des systèmes d'information, créée en 2001, avait été un premier signe de l'aptitude de l'Etat à répondre aux enjeux du numérique. Avant de se fondre dans l'ANSSI, elle disposait de cent dix personnes. Mais nos homologues anglais ou allemands sont au nombre de cinq à six cents…

« Un rôle de labellisation des prestations de services. »

La prise de conscience s'est également traduite dans les travaux du Livre blanc sur la sécurité et la défense nationale publié en juin 2008. Ce document associait pour la première fois les questions de défense à celles de sécurité. On quittait le domaine militaire pour une vision plus large. Les menaces sur nos systèmes d'information ont été considérées comme un risque majeur pour la France dans les quinze ans à venir. A cette occasion, la décision a été prise de créer l'ANSSI, afin de renforcer les capacités nationales et d'irriguer l'ensemble du territoire, avec la création dans chaque zone de défense et de sécurité d'un observatoire zonal de la sécurité des systèmes d'information (OZSSI). Sous les ordres des préfets de zone, ils déclinent et diffusent les règles et les bonnes pratiques, et font remonter l'information.

Quelles sont les missions de l'agence ?

M. B. : L'ANSSI a cinq grandes missions. La première est de former, au Centre de formation à la sécurité des systèmes d'information (CFSSI), les agents de l'Etat. Nous concevons une politique de diffusion d'un corpus pédagogique proposé aux centres de formation publics et privés qui forment nos experts à la SSI, et à l'ensemble des informaticiens, qui, aujourd'hui, n'ont pas tous conscience des menaces.

Parallèlement, l'Agence est organisée en quatre sous-directions, chacune dotée d'une mission spécifique. La sous-direction stratégie et réglementation a une mission de régulation, d'élaboration de règles, de préparation de textes juridiques et réglementaires. Elle délivre des labels à des produits destinés à la protection des informations classifiées. Elle en délivre également à l'usage de la société civile : les cartes à puce bancaire diffusées en France sont certifiées par l'ANSSI au nom du Premier ministre. Nous avons tout un portefeuille de produits de sécurité informatique pour lesquels nous vérifions les fonctions de sécurité. Nous mettons en place un nouveau type de label de qualification pour les échanges électroniques entre les autorités administratives et les usagers.

Nous allons labelliser des prestataires de services dans le domaine informatique (audit, installation, contrôle) qui respectent des règles et recommandations que nous allons établir dans un référentiel général de sécurité. Ce référentiel s'imposera à toutes les autorités administratives de l'Etat. Toujours dans le cadre du volet régalien de la première mission de l'Agence, un bureau, chargé de la stratégie industrielle, conseille les entreprises françaises, particulièrement les PME, qui œuvrent dans le domaine de la pérennité des systèmes d'information.

La deuxième sous-direction a une mission opérationnelle. Le Centre opérationnel de la sécurité des systèmes d'information suit en permanence l'actualité qui concerne notre domaine. Il assure une fonction essentielle de veille sur les attaques informatiques. C'est la vigie de l'agence. Il a également une fonction d'expertise technique pour préparer les défenses, analyser les ordinateurs attaqués, comprendre comment l'attaque s'est produite. Il élabore un dispositif, recommandé par le Livre blanc, de détection des attaques contre les systèmes de l'Etat. L'objectif est de détecter le plus tôt possible, dans les immenses flux qui transitent entre Internet et les intranets des ministères, les signaux faibles, les attaques, et de les stopper au plus vite. Un bureau inspecte les systèmes d'information de l'Etat, afin d'aider les administrations à améliorer la sécurité des dispositifs opérationnels, notamment les plus sensibles.

Déceler les attaques, mettre en place des règles est une chose, assister ceux qui doivent les appliquer

en est une autre. Aussi la troisième sous-direction, « Assistance, conseil et expertise », a-t-elle pour mission d'anticiper les évolutions techniques, de proposer les innovations nécessaires en matière de sécurité des systèmes d'information, qu'il s'agisse de protocoles, de microcomposants, de logiciels, d'équipements sans fil.

La quatrième sous-direction, « *Systèmes d'information sécurisés* », a pour mission de doter l'Etat de systèmes fiables, résilients et hautement confidentiels pour gérer les crises et relier les grands décideurs de l'Etat. L' « *Intranet sécurisé interministériel pour la synergie gouvernementale* » (ISIS), inauguré il y a un an, est le premier système d'information sécurisé permettant l'échange et le partage de documents classifiés au titre du secret défense entre acteurs gouvernementaux. Le réseau de téléphonie fixe et de télécopie « Rimbaud » (« *Réseau interministériel de base uniformément durci* ») compte quatre mille cinq cents abonnés sur le territoire métropolitain et dans les DOM : ministères, services déconcentrés, centres opérationnels et opérateurs chargés d'une mission de service public d'importance vitale. Il permet la continuité de l'action gouvernementale.

De quels moyens dispose l'agence ?

M. B. : L'objectif, en termes d'effectifs, est de les doubler pour les porter à 250 personnes en 2012, afin de répondre aux besoins d'expertise technique, de conseil et de détection des attaques.

Les nouvelles menaces sont-elles mieux appréhendées aujourd'hui ?

M. B. : Les nouvelles menaces sont bien sûr mieux appréhendées, grâce à un travail de fourmi pour les analyser en permanence, ainsi que les nouvelles vulnérabilités, et en déduire des règles et des pratiques. Mais les menaces se multiplient aussi vite que les technologies se développent. Qui, hier, pouvait prédire que le téléphone portable serait piraté ?

Quels liens l'ANSSI a-t-elle avec d'autres acteurs institutionnels nationaux et internationaux ?

M. B. : Quel que soit son effectif, une agence, seule, ne peut rien. Son travail doit être décliné et mis en œuvre dans l'administration, les ministères, les entreprises et tous les acteurs du monde numérique. Afin de diffuser l'information utile auprès de tous les utilisateurs de l'informatique et conseiller les PME, souvent démunies, nous avons créé un portail, *www.securite-informatique.gouv.fr*. Au-delà des dix commandements de la sécurité informatique, il offre plusieurs niveaux d'entrée et des recettes pratiques. Sur le plan de la formation une expérience pilote est menée avec la chambre de commerce et d'industrie de Valenciennes pour labelliser les formations données dans les centres publics et privés.

L'informatique n'a pas de frontière : une équipe est donc chargée de développer les relations avec nos homologues étrangers et de participer aux négociations internationales. Elle participe à la promotion de la confiance dans la société de l'information, dans le cadre européen et mondial, et prépare la position nationale en liaison avec les administrations concernées. L'ANSSI entretient également des collaborations techniques avec ses homologues, et contribue à l'orientation des travaux de recherche et développement au niveau national.

Propos recueillis par J. W.-A

Vers une cyber-ONU

Depuis le début de la décennie, l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) agit contre la cybercriminalité. Il souhaite aujourd'hui une ambitieuse coordination internationale.

*Entretien avec Christian Aghroum, commissaire divisionnaire, chef de l'OCLCTIC**

Quelles raisons ont présidé à la création de l'OCLCTIC ?

Christian Aghroum : À la fin années 1980, de nouveaux moyens se sont avérés nécessaires, pour les enquêteurs financiers, afin de procéder à des constatations dans les entreprises. Auparavant, le bilan d'une société était inscrit dans un grand livre comptable. L'informatisation des entreprises lui a substitué un grand fichier. Or, en police judiciaire, pour assurer l'authenticité juridique d'un document, il faut réaliser la constatation par soi-même. Il a fallu former des enquêteurs à extraire des données dont l'authenticité ne puisse être en question. Des spécialistes en criminalité informatique ont donc essaimé dans les sections économiques et financières de police judiciaire. Au milieu des années 1990, des enquêteurs ont été formés dans d'autres domaines que la finance, comme celui de la pédopornographie. C'est sur fond de développement de la délinquance informatique et de convention de Budapest sur la cybercriminalité que naît l'Office, en 2000, réponse au besoin de centralisation de l'information judiciaire, et au besoin d'un interlocuteur pour nos partenaires d'Interpol et Europol.

Quelles sont les missions de l'Office ? Quels conseils l'Office apporte-t-il aux entreprises ?

C. A : Composé de policiers et de gendarmes, il a élargi ses compétences, d'une police informatique à une police d'Internet. Ses missions sont de nature stratégique quand il joue le rôle d'interface pour les infractions associées aux nouvelles technologies, qu'il forme des investigateurs en cybercriminalité et qu'il participe à l'élaboration des lois et règlements, et représente la France dans les organismes internationaux. Sur le plan tactique, l'Office dispose de groupes d'enquête sur le piratage, la contrefaçon de carte bancaire, la pénétration des réseaux, les fraudes dans le commerce électronique (de plus en plus sur téléphone mobile), les contrefaçons numériques et les escroqueries en ligne (via eBay par exemple). Nous accueillons la plate-forme de signalement des contenus illicites, qui offre un guichet unique aux particuliers et aux professionnels *(www.internet-signalement.gouv.fr)*. Depuis le début de l'année, nous avons traité 39 000 signalements, mais nous manquons de personnel.

Alors que la Direction centrale du renseignement intérieur a une vocation d'intelligence économique, aider les entreprises françaises à lutter contre l'espionnage industriel, l'Office a une approche plus économique : nous intervenons auprès des directions et de l'encadrement des groupes industriels ou bancaires pour leur faire comprendre qu'ils doivent déposer plainte quand ils sont victimes d'attaques. Il est nécessaire pour l'entreprise d'écouter la direction informatique et la sécurité des systèmes d'information (SSI). Or un problème de langage cloisonne les services, la SSI a parfois un langage de spécialiste proche de la paranoïa, qui s'oppose au marketing, ouvert sur le monde. Il est regrettable que ce qui relève de la SSI soit dans certaines entreprises sous la coupe de la direction informatique, qui parfois le diabolise, alors que cela devrait être intégré dans une vraie direction de la sécurité avec une vision transversale des problèmes. Il est aussi regrettable que la véritable cible des attaques, les PME-PMI, soit la moins bien défendue, faute de moyens et de formation à l'intelligence économique. Installer un antivirus ne suffit pas.

Vous occupez-vous de la contrefaçon ?

C. A. : Les produits contrefaits qui transitent sur la Toile, les faux Vuitton et faux Lacoste, ne sont pas du ressort de l'Office. Notre vigilance porte sur les contrefaçons du numérique, les faux logiciels, les faux boîtiers multiservices, les contrefaçons de données personnelles, les fausses façades. En ce domaine, les entreprises doivent avoir des outils de veille, de détection et d'alerte. Les grands groupes ont leurs propres moyens, mais les PME sont souvent moins bien outillées. Leur salut passe par une action commune, par les fédérations ou l'Unifab, dotés de relais efficaces et de moyens pour aller en justice.

Qu'apporte le projet de « loi d'orientation et de programmation pour la performance de la sécurité intérieure » ?

C. A. : L'Office est promoteur de quelques suggestions. La première porte sur le blocage des sites pédopornographiques, car bon nombre de pays, non coopératifs, refusent de les fermer (Russie, pays d'Asie). Une bulle de protection, sorte de contrôle parental national, va permettre à l'internaute de naviguer librement sans être assailli par des images plus que douteuses. Deuxième proposition : nous demandons l'incrimination de l'usurpation d'identité en ligne, car aujourd'hui nous sommes bloqués dans nos enquêtes. Enfin, nous souhaitons la mise à jour de la loi Perben II, qui n'autorise que dans le cadre de la lutte contre le terrorisme et la criminalité organisée, sous le contrôle d'un magistrat, d'installer des vidéos et des micros chez les criminels présumés. On veut disposer des mêmes outils informatiques, car les criminels ont recours au chiffrement.

« Des moyens de paiement se créent, comme Paypal, qui échappent à tout contrôle et facilitent les réseaux de blanchiment . »

Les enjeux sont à la fois techniques et sociétaux. En France, le taux d'équipement en accès à Internet ne dépasse pas 60 %. La marge de progression est donc grande, comme celle du nombre de victimes et d'infractions. Il faut une capacité de réponse adaptée, qui passe par la spécialisation des policiers, gendarmes et magistrats. Les outils deviennent de plus en plus complémentaires, comme le téléphone mobile et la robotique assistée. Autre source d'inquiétude : le développement d'Internet dans le monde, particulièrement en Afrique, qui, grâce à la norme de réseau téléphonique de troisième génération, peut franchir un âge technique et disposer de l'Internet mobile sans réseau électrique (des téléphones solaires sont commercialisés). Le réseau mondial ne peut pas s'autogérer et la souveraineté nationale n'est pas adaptée. Des moyens de paiement se créent, comme Paypal, qui échappent à tout contrôle et facilitent les réseaux de blanchiment ou d'évasion de capitaux. Face au risque que chaque pays ne déploie une sorte de cyberprotectionnisme, une ONU de l'Internet est nécessaire, avec de vrais pouvoirs d'intervention. Cette force aura à arbitrer la réponse informatique offensive qu'un Etat se verra contraint d'adopter face à des attaques.

Propos recueillis par J. W.-A

** Direction centrale de la police judiciaire.*

Une vigie de la cybercriminalité mondiale

En mars dernier s'est tenue au Grand Palais de Lille la troisième édition du Forum international de la cybercriminalité (FIC). Le succès de cette manifestation, lancée en 2007 à Marcq-en-Barœul par la gendarmerie du Nord-Pas-de-Calais, va croissant.

Entretien avec le colonel de gendarmerie Régis Fohrer, commissaire général du FIC, et les commandants Dominique Schoenher et Rémy Février, commissaires généraux délégués***

Quelles raisons ont présidé à la création du FIC et en quoi consiste-t-il ?

Dans un contexte de mondialisation et de développement d'Internet, la dépendance croissante des entreprises vis-à-vis des technologies de l'information et de la communication (TIC) présente des risques que savent exploiter des délinquants de plus en plus organisés. La gendarmerie est un acteur institutionnel reconnu et légitime dans la lutte contre la cybercriminalité, phénomène récent mais en plein essor, profitant de l'anonymat et de l'ubiquité procurés par les TIC. Dans sa contribution à la politique publique d'intelligence économique, la gendarmerie a identifié la dépendance des entreprises vis-à-vis des TIC et le fait que celles-ci représentent une des vulnérabilités les moins bien gérées, faute de sensibilisation des chefs d'entreprise. Par ailleurs, la cybercriminalité ayant une dimension transnationale, son traitement nécessite une réponse adaptée, ainsi qu'un partage des savoir-faire.

Après ce constat, la solution d'un forum international s'est imposée à la région de gendarmerie Nord-Pas-de-Calais. La question du financement de ce projet d'envergure fut et demeure une préoccupation essentielle. Toutefois, l'intérêt porté à la problématique au niveau national et européen – la lutte contre la cybercriminalité étant une priorité de la direction Justice, liberté et sécurité de la Commission – a permis un cofinancement gendarmerie-UE. Les collectivités locales (conseil régional, municipalité de Lille, Lille Métropole communauté urbaine), ayant saisi les enjeux politiques et économiques de l'événement, ont contribué à son essor par un soutien sans faille et la volonté de faire de l'eurométropole lilloise un pôle d'excellence en la matière. La qualité des travaux, la synergie et la mobilisation des acteurs ont contribué au succès de ce rendez-vous annuel.

Plutôt qu'une grande messe tous publics, l'organisation a pris le parti de multiplier les ateliers couvrant la diversité des atteintes numériques et le développement des parades appropriées. Plusieurs conférences-débats se tiennent simultanément, ciblant des publics différents, afin de garantir une large interaction entre les intervenants (cent vingt au FIC 2009) et leurs auditeurs. Des sujets de fond sont suivis d'une année à l'autre, mais la programmation est arrêtée aussi tard que possible, afin de rendre compte des derniers développements de l'actualité. La quatrième édition se tiendra les 31 mars et 1er avril prochains à Lille. La programmation n'est pas encore arrêtée, mais quelques pistes nouvelles ou d'actualité seront certainement abordées, comme la cyberinfiltration pour les forces de l'ordre, les formations de sensibilisation aux risques d'Internet, la responsabilité du chef d'entreprise dans la protection de son système de traitement automatisé de données, l'émergence d'une cyberdéfense, ou la lutte contre le téléchargement illégal.

Quels sont les principaux enseignements des trois éditions précédentes ?

Les criminels exploitent toujours davantage le vecteur des TIC, alors que l'attention des utilisateurs à la nécessité de se protéger reste très insuffisante. La naïveté, sur le principe « *qui pourrait bien s'intéresser à moi ?* » confine au laisser-aller, voire à l'insouciance criminelle puisque cette attitude facilite le travail des délinquants. Et peu d'usagers sont conscients de leur responsabilité dans l'utilisation des TIC, ce qui freine la mise en place d'une politique de sécurité responsable.

Quelle est l'audience du FIC ? Et ses partenariats ?

La participation a augmenté chaque année de 50 % depuis le lancement. En 2009, le FIC a réuni mille quatre cents personnes, de dix-sept pays, et quatre cent cinquante entreprises, pendant une journée. Pour la prochaine édition, l'organisation table sur deux mille personnes représentant une trentaine de pays sur deux jours. Pour garantir la pertinence des contenus au regard des populations cibles, les organisateurs se sont attachés à développer de nombreux partenariats avec les acteurs nationaux et régionaux de la lutte contre la cybercriminalité. Administrations, associations, collectivités territoriales, universités, industries de la sécurité des systèmes d'information, organismes consulaires, sont autant d'intervenants sollicités dès que la thématique développée entre dans leur champ de compétence. Au plan international, le partenariat avec la Belgique est particulièrement développé. L'organisation s'attache à associer les représentants des autres pays pour identifier les différences d'approche et saisir toutes les opportunités d'échange de bonnes pratiques. L'expérience montre qu'après une première participation à titre d'observateur les pays renouvellent leur partenariat, en tenant un rôle plus actif dans les débats.

Les objectifs et missions du FIC ont-ils évolué ?

L'objectif principal demeure la sensibilisation des populations et des acteurs économiques au risque numérique en vue de développer leur résilience. Un espace d'exposition est réservé aux industriels qui développent des solutions de protection répondant aux besoins des entreprises, des collectivités et des particuliers. Le forum offre l'opportunité de mettre en réseau les parties prenantes (praticiens de la justice et des forces de l'ordre, acteurs économiques, collectivités territoriales, représentants de la société civile, chercheurs et enseignants), avec un partage d'expérience au niveau international. Avec le soutien des autorités françaises et de la Commission, un mandat prospectif s'affirme. Le forum a vocation à devenir un laboratoire d'idées européen, en vue d'une réponse internationale à la cybercriminalité, force de proposition pour la mise en place de politiques anticipant de nouveaux risques numériques.

La troisième édition a donné lieu à la publication d'un guide, *Le Chef d'entreprise face aux risques numériques*, édité en partenariat avec le Clusif[1], et d'une *Lettre ouverte aux dirigeants* présentant dix recommandations pour la sécurité de l'espace numérique des entreprises. Ces documents ont fait l'objet d'une remise officielle aux autorités présentes au FIC 2009 et d'une mise en ligne sur le site *www.fic2009.fr*. Une version papier sera remise aux entrepreneurs présents au FIC 2010. Le guide énumère les principaux risques numériques auxquels sont confrontées les entreprises et formule quelques conseils de base, reposant sur une prudence élémentaire.

Le risque numérique est multiforme, et mal connu des services de répression sur le plan quantitatif, parce que les entreprises hésitent à porter sur la place publique l'exploitation de failles dans la protection de leur système de traitement de données. Il inclut les atteintes au patrimoine informationnel et à l'image de l'entreprise. La responsabilité pénale d'un chef d'entreprise peut être engagée dans le cas de vol de données à caractère personnel, d'hébergement de contenus illicites ou d'utilisation à des fins criminelles par le personnel, si les faits résultent d'une protection insuffisante. La veille et la protection sont les meilleures parades.

Propos recueillis par J. W.-A

** Directeur des contenus scientifiques.*

*** chargés de la cellule intelligence économique de la région de gendarmerie Nord-Pas-de-Calais.*

1. Club de la sécurité de l'information français.

Maîtres-Toile contre cyberbrigands

Contre le vol d'informations en ligne, des métiers se créent. La protection de l'information fait l'objet d'enseignements de plus en plus spécialisés.

*Entretien avec Jean-Paul Pinte, docteur en sciences de l'information et de la communication**

Comment suivez-vous les évolutions d'Internet et comment les transmettez-vous à vos étudiants ?

Jean-Paul Pinte : Mes activités en entreprise et, depuis 2001 à l'Université ont été l'occasion de surveiller des territoires d'information et de mettre en place diverses cellules de veille (commerciale, environnementale, marketing, sociale, technologique…) Dans le cadre de mes enseignements j'intègre cette dimension de veille et de culture informationnelle dans chacune des filières, ainsi que dans trois modules de mastère consacrés à l'intelligence économique.

En tant que futur travailleur du savoir, chaque étudiant doit apprendre à surveiller l'évolution d'un domaine, pour lequel il assure une recherche d'information stratégique à l'aide d'une mallette de veille. Ce module permet de collecter l'information (de façon manuelle ou automatisée), puis de la cartographier, de la trier et de l'analyser à des fins de diffusion sélective, pour une prise de décision au plus haut niveau de l'entreprise. Il faut savoir que 87 % des les internautes ne dépassent pas la première page de Google quand ils y cherchent une information. Ils oublient de visiter le « Web invisible », bien plus important et accessible par les outils que je fais découvrir à mes étudiants. Ce « Web invisible » ou « Web abyssal » est inaccessible aux moteurs de recherche classiques. Il comprend des bases, banques de données et bibliothèques en ligne gratuites ou payantes. Se contenter de la Toile visible, c'est négliger une zone cinq cents fois plus volumineuse que Google, avec des centaines de milliers de ressources de grande valeur. En font aussi partie les pages orphelines, puisque le seul moyen d'y accéder est de connaître leur adresse exacte (URL).

Quelques outils indexent des documents relevant du Web abyssal. Ces instruments permettent de trouver des informations souvent pertinentes car difficiles d'accès. L'efficacité d'une recherche dépend en grande partie des outils utilisés. Des moteurs comme Archives.org, cimetière de la Toile depuis son origine, permet de retrouver des pages remontant à 1993 en France et jusqu'à 1987 ailleurs. Des bases de données gratuites comme Dadi de l'Urfist (Lyon) proposent plus de huit cents bases de données gratuites.

Parmi les catégories accessibles, l'agriculture, les brevets, les marques, la chimie, l'environnement, l'économie, la génétique, l'histoire, l'informatique, la linguistique, les mathématiques, la médecine, les sciences le cinéma, l'art, la photographie… Dans cette lignée s'inscrivent des moteurs comme Turbo10, Xrefer, Profusion, ou Wondir, qui scrute la toile à l'aide d'un millier de moteurs réunis sous une seule adresse.

La cybercriminalité étant protéiforme et son défi, mondial, quels sont les enjeux et quelle formation donner aux étudiants ?

J.-P. P. : L'arrivée du Web 2.0 vers 2005 a engendré pour les « natifs du digital » des comportements plus actifs que sur le Web 1.0, ouvert à la vente à distance dix ans plus tôt. L'arrivée du commerce en ligne, donc du paiement en ligne, a fait naître une catégorie de cyberdélinquants ayant non plus pour objectif de nuire à autrui mais de s'enrichir. Le Web 2.0 ou Web social, c'est une série d'applications qui permettent aux gens de diffuser des contenus. Parmi elles, le blog, les réseaux sociaux comme Facebook et Linkedin, et les outils de microblogage comme Twitter.

C'est donc par des cas concrets que j'apprends aux étudiants à demeurer vigilants, à détecter les sites douteux et non sécurisés, notamment quand ils passent à l'acte de paiement. Ils sont aussi formés à s'assurer de la pertinence de l'information en enlevant le « bruit » (ce qui est en dehors de l'axe de recherche). Avec des outils de cartographie comme Kartoo, Clusty ou Touchgraph ils sont capables de s'assurer de la pertinence des résultats d'une recherche, d'expertiser une identité numérique. Tout cela leur permet, entre autres, d'économiser le temps perdu sur Google.

Les outils de veille sécuritaire ne sont-ils pas sous-utilisés par les entreprises ?

J.-P. P. : Les entreprises ont longtemps boudé les systèmes de veille et bien souvent ne savent pas qu'elles sont surveillées, ni, si elles ont mis un pied dans la veille, qu'elles peuvent se la faire voler ! Les vraies démarches de veille sont assez récentes et commencent seulement à apparaître dans les PME-PMI, mais avec des cellules utilisant des outils de plus en plus élaborés.

Cela requiert-il, dans l'entreprise, une nouvelle fonction ? Doit-elle être attachée à la direction générale ?

J.-P. P. : Il faut créer des profils intégrant tous les atouts de la maîtrise des sciences de l'information et axés sur des concepts d'intelligence économique et de veille. Cette fonction doit être attachée à la direction générale, qui doit en reconnaître l'autorité, et non pas celle d'entités éparpillées réalisant une veille sans capitalisation ni diffusion sélective.

Quelles sont les actes délictueux les plus importants en ligne ?

J.-P. P. : En tête figure l'infection de sites (63 %), devant l'infection de courriels et le hammeçonnage (48 %). Les entreprises semblent avoir pris conscience des dangers des réseaux sociaux. Elles sont moins nombreuses à être sensibles aux fenêtres intempestives.

Le passage progressif au Web 3.0 (l'Internet des objets) va connecter les flux d'information à nos identités réelles pour favoriser nos échanges. Informations professionnelles, médicales, réseaux sociaux, loisirs, vont se trouver de plus en plus connectés à des services nouveaux et connectés entre eux (par WiFi entre autres). Des chercheurs des universités d'Hiroshima et de Kobe disent avoir mis le doigt sur une méthode permettant de craquer en moins d'une minute le système de chiffrement WPA *(Wi-Fi Protected Access)*. Les trafics à la carte bancaire, aux fausses identités sur les réseaux sociaux, vont croître. Grâce aux techniques sans contact (RFID, Bluetooth, géolocalisation…), nous nous connecterons à un nombre croissant d'objets et d'interfaces dans notre vie quotidienne, ce qui va engendrer d'autres risques pour notre identité numérique.

Les entreprises ne savent visiblement pas qu'elles ne possèdent aucune protection efficace contre le vol de données à l'aide du téléphone mobile. Des appareils multimédias comme l'Iphone et le Blackberry seront capables de compromettre leur sécurité. Dans la cyberguerre, la Corée du Sud et les Etats-Unis ont subi trois importantes vagues d'attaques durant la seule première semaine de juillet 2009 contre des sites institutionnels. Ces attaques vont se multiplier. Et chacun va devoir veiller à son identité numérique sur la Toile, car n'importe qui peut, dans une cartographie d'information, se trouver fiché délinquant sans l'être, uniquement parce qu'il laisse une trace sur Internet. Cette trace indélébile pourra être exploitée à mauvais escient pour lui nuire ou le faire chanter. Le « Web sémantique » permettrait même la disparition de l'adresse de messagerie : on pourra envoyer des courriels à quelqu'un en utilisant uniquement son profil de navigation et ses critères de recherche.

Propos recueillis par J. W.-A

* *Maître de conférences et enseignant-chercheur au laboratoire d'ingénierie pédagogique de l'université catholique de Lille, membre de l'Association internationale de lutte contre la cybercriminalité (AILCC). Blog : http://cybercriminalite.wordpress.com.*

Bulletin de l'Institut de liaisons et d'études des industries de consommation

Directeur de la publication : Dominique de Gramont – Editeur : Trademark Ride, 93, rue de la Santé, 75013 Paris (tél. 01 45 89 67 36, fax 01 45 89 78 74, jwa@tmride.fr, www.trademarkride.com) – Rédacteur en chef : Jean Watin-Augouard – Secrétariat de rédaction et contact : François Ehrard (01 45 00 93 88, francois.ehrard@ilec.asso.fr) – Maquette et mise en pages : Graph'i Page (01 39 72 20 28, ividalie@orange.fr)

Imprimé par : Imprimerie A. Mouquet, 2 rue Jean-Moulin, 93350 Le Bourget (tél 01 48 36 08 54) – ISSN : 1271-6200

Dépôt légal : à parution – Reproduction interdite sauf accord spécial

www.ilec.asso.fr