La cybercriminalité en mouvement

Comme beaucoup de formes de délinquance, la cybercriminalité est en perpétuelle évolution. Cependant, elle est particulièrement influencée par les évolutions technologiques et les nouvelles pratiques qui se développent chaque jour. Cela en fait un champ d'expérimentation technique, opérationnel et juridique permanent. Nous nous proposons, dans cet article, de présenter une photographie de la lutte contre la cybercriminalité (point effectué en milieu d'année 2010).

par le lieutenant-colonel Éric FREYSSINET*

LA LUTTE CONTRE LA CYBERCRIMINALITÉ EN 2010

La cybercriminalité recouvre différentes réalités, selon les interlocuteurs. Ainsi, il est bien évident que face au formidable développement qu'a connu et connaît encore l'usage des technologies numériques, les services de police ont dû s'adapter, notamment avec la présence dans presque toutes les enquêtes judiciaires de quelque nature qu'elles soient du téléphone mobile ou d'Internet.
Toutefois, dans le cadre de cet article, nous nous limiterons aux seules infractions commises, exclusivement ou de façon essentielle, grâce aux technologies numériques.

Quelles sont les tendances ?

Aucune étude statistique fiable ne permet aujourd'hui de mesurer l'ampleur des phénomènes cybercriminels, que ce soit à cause des difficultés de définition évoquées ci-dessus ou de la faible propension des victimes à déposer plainte.
Ainsi, la progression éventuelle des statistiques officielles en matière d'atteintes aux systèmes de traitement automatisé de données (1) ou d'escroqueries sur Internet ne saurait être interprétée comme une augmentation significative du nombre de ces faits, mais plutôt comme une meilleure prise en compte collective de ces problèmes.
Toutefois, plusieurs tendances se dessinent nettement.
Le crime organisé est aujourd'hui omniprésent dans toutes les formes de cybercriminalité. D'abord, parce qu'il s'est déplacé sur ces nouveaux médias, soit par intérêt ou soit par nécessité. Il en est ainsi par exemple en matière de vols de voitures – impossibles aujourd'hui sans une certaine maîtrise de l'électronique –, des escroqueries liées à la carte bancaire ou à la nigériane, ou de pédopornographie. Ensuite, parce qu'il est guidé par l'appât des nouveaux gains rendus possibles par l'abus des nouvelles technologies : l'administration et la commercialisation de services criminels au travers des *botnets*, la vente de logiciels abusant la crédulité des victimes (*scareware*) ou, encore, la collecte massive de données personnelles (*phishing*, pourriels…).

* Chef de la division de lutte contre la cybercriminalité, service technique de recherches judiciaires et de documentation de la gendarmerie nationale (X92, Mastère spécialisé SSIR, ENST 2000).

(1) Les atteintes aux systèmes de traitement automatisé de données (ou STAD) recouvrent l'ensemble des infractions définies par les articles 323-1 et suivants du code pénal (anciennement loi Godfrain), lesquelles décrivent les accès frauduleux ou autres modifications frauduleuses de données dans un système informatique (actions trop souvent appelées à tort « piratages »).

Le volume des données à traiter augmente de façon presque exponentielle, avec l'évolution des capacités de stockage (taille des disques durs (2)) ou de transmission des données (Internet haut débit). La conséquence pratique, pour les enquêteurs, est double : l'augmentation des traces potentielles à exploiter, et un accroissement du temps nécessaire à l'analyse des éléments de preuve collectés et, par voie de conséquence, la nécessité de développer de nouvelles stratégies.

L'Internet haut débit est largement accessible et qui plus est en situation de mobilité : l'ADSL largement diffusé, des connexions à Internet de plus en plus courantes dans les entreprises, des points d'accès Wi-Fi en libre service, des abonnements 3G+, des terminaux téléphoniques s'apparentant de plus en plus à des ordinateurs. La conséquence principale de cette évolution est une augmentation mécanique du nombre des victimes potentielles de la cybercriminalité, particuliers ou entreprises. La seconde conséquence tient au développement de nouvelles pratiques, telles que l'hébergement (ou le relais) de contenus ou d'activités illégaux à l'insu des utilisateurs légitimes de connexions Internet.

Outre le développement constant des techniques cryptographiques, commencent à se développer des outils et des pratiques anti-forensiques (3), c'est-à-dire qui cherchent à empêcher la collecte de preuves (4). En effet, le souhait de plus en plus partagé et parfaitement légitime de préserver la vie privée peut aussi avoir un effet favorable sur les activités illégales. Les services d'enquête doivent ici encore adapter leurs méthodes et leurs outils de travail, voire chercher à faire évoluer leurs capacités juridiques, comme nous le verrons plus loin.

En conclusion de cette première section et pour compléter ces tendances de fond, nous soulignerons le fait indéniable qu'aujourd'hui la cybercriminalité est devenue une réalité pour presque tous les citoyens et donc pour tous les acteurs judiciaires (enquêteurs, magistrats, avocats, etc.).

Les acteurs

Les services d'enquête spécialisés en matière d'infractions liées aux technologies numériques, et plus particulièrement en matière de cybercriminalité, ont donc vu leur rôle renforcé. Souvent bien connus du grand public (pour une présentation de ceux-ci, se reporter à l'article cité en [1]), les services spécialisés évoluent et s'adaptent notamment par la formation, et de nouveaux acteurs apparaissent.

Ainsi, la formation des enquêteurs est un axe d'effort permanent. Sur le plan européen, un groupe de travail (le *European Cybercrime Training and Education Group* (5)) est chargé, depuis 2007, de coordonner ces efforts et de faciliter l'échange de bonnes pratiques entre les différents services européens. Ce groupe de travail réunit des services d'enquête spécialisés, des centres de formation ou des universités, ainsi que des entreprises partenaires du secteur des technologies de l'information.

En France, les investigateurs en cybercriminalité de la police nationale ont vu leur formation inscrite au registre national de certification des compétences professionnelles (RNCP) en 2009 (6). La gendarmerie, quant à elle, est engagée dans une démarche de partenariats universitaires. Ainsi, les enquêteurs en technologies numériques (NTECH) de la gendarmerie nationale sont formés, depuis 2005, dans le cadre d'un diplôme d'université délivré en partenariat avec l'Université de technologie de Troyes (UTT). Ce diplôme est devenu cette année (2010) une licence professionnelle reconnue par le ministère de l'Enseignement supérieur et de la Recherche.

La commission nationale de l'informatique et des libertés (CNIL) est une autorité administrative indépendante (bien que rarement identifiée comme telle) qui, parmi d'autres, joue un rôle important dans la lutte contre certaines formes de cybercriminalité. Elle dispose ainsi d'agents assermentés chargés de réaliser des contrôles sur place, dans les entreprises ou dans les administrations. Elle peut aussi décider de sanctionner certaines dérives (7) ou de les porter à la connaissance de l'autorité judiciaire, *via* la saisine du procureur de la République compétent.

Mais de nouvelles autorités administratives ont vu le jour au cours des derniers mois. Ainsi, la Haute Autorité pour la Diffusion des Œuvres et la Protection des droits sur Internet (HADOPI) est chargée d'animer la lutte contre la contrefaçon des œuvres de l'esprit facilitée par Internet, grâce, notamment, à un dispositif de riposte graduée pouvant aller jusqu'à la privation d'accès à Internet. Enfin, l'Autorité de Régulation des Jeux en Ligne (ARJEL) chargée de la régulation des jeux d'argent et de hasard sur Internet, met en œuvre un certain nombre de prérogatives de contrôle des opérateurs

(2) La taille moyenne des disques durs analysés par les enquêteurs en technologies numériques de la gendarmerie est passée de 75 gigaoctets en 2005 à près de 250 gigaoctets en 2009.

(3) Les **sciences forensiques** regroupent l'ensemble des sciences et techniques utilisées dans le cadre de l'enquête judiciaire (ou dans des circonstances analogues, telles les enquêtes internes à des entreprises) pour rassembler, collecter et analyser les éléments et supports de preuve utiles à la manifestation de la vérité. Les techniques dites « anti-forensiques » visent à empêcher ou à rendre moins aisée l'utilisation de ces méthodes. Très utilisée dans le domaine de la preuve numérique, cette terminologie commence à apparaître dans d'autres contextes, comme celui des empreintes génétiques. Cette extension est la traduction du souci manifesté de tous temps par les délinquants de ne pas laisser de traces dans l'exécution de leurs forfaits.

(4) De plus en plus de logiciels grand public incluent des fonctions permettant l'effacement automatique des traces d'historique : ainsi, le navigateur Web de la société Microsoft, Internet Explorer 8, avec son mode de navigation sans traces inPrivate.

(5) Ou ECTEG: http://www.ecteg.eu/

(6) Voir : http://www.cncp.gouv.fr/grand-public/visualisationFiche?format=fr&fiche=6580

(7) Voir à ce sujet le site de la CNIL : http://www.cnil.fr/vos-responsabilites/les-sanctions-de-a-a-z/

de ce secteur et peut demander, *in fine,* le blocage de l'accès à des plateformes de jeux qui contreviendraient à la réglementation française.
De façon moins opérationnelle, mais tout aussi essentielle, l'Observatoire de la Sécurité des Cartes de Paiement (OSCP) (8) réunit des représentants de l'État, ceux des banques et des consommateurs, ainsi que des experts indépendants.

DE NOUVELLES FORMES DE PARTENARIAT

Personne ne peut prétendre lutter seul contre la cybercriminalité. Outre les interactions naturelles entre les différents acteurs concernés, on voit se nouer des partenariats objectifs.

Les partenariats opérationnels

Les opérateurs de téléphonie sont tout particulièrement intéressés à participer à la lutte contre la fraude dont ils sont victimes. L'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) anime ainsi un groupe de travail rassemblant la police, la gendarmerie et les services de lutte contre la fraude constitués par les opérateurs afin d'échanger sur les techniques de fraude et de développer des stratégies d'action concertée, c'est-à-dire de faciliter le dépôt de plaintes par les opérateurs, mais aussi d'agir, par exemple, sur les modes de commercialisation ou les outils de détection de la fraude que ceux-ci peuvent mettre en œuvre.
On ne peut qu'appeler de nos souhaits le développement de tels groupes de travail dans d'autres secteurs économiques.
Un autre angle d'approche pourrait consister à s'attaquer directement aux phénomènes, plutôt qu'à un secteur en particulier. Ainsi, le développement des *botnets* (9) est particulièrement préoccupant étant donné qu'il favorise une grande partie des infractions commises aujourd'hui sur Internet. De nombreux acteurs collectent des informations sur l'activité des *botnets*, mais les services d'investigation officiels sont rarement impliqués de façon efficace. Une présentation [2] réalisée lors du Symposium sur la Sécurité des Technologies de l'Information et de la Communication (SSTIC) de juin 2010 abordait ce problème.
Un exemple récent (le dossier « Mariposa » (10) géré par la *Guardia Civil* espagnole en partenariat avec des entreprises spécialisées dans la sécurité informatique au début de l'année 2010, démontre sans conteste qu'il est possible de faire mieux. Le groupe de travail européen d'Interpol spécialisé en matière de lutte contre la criminalité liée aux technologies de l'information a donc décidé d'initier un projet opérationnel en ce sens courant de septembre 2010 à mai 2011, auquel la police et la gendarmerie françaises participent.

Recherche et développement

La France est particulièrement riche en spécialistes de la cryptographie ou de la sécurité des systèmes d'information. Notre pays n'est toutefois pas aussi présent qu'on pourrait le souhaiter dans le domaine de l'investigation numérique. Ainsi, tous les outils utilisés par les services d'enquête ont été développés à l'étranger. De même, la littérature – essentielle pour la formation des enquêteurs – ou les publications scientifiques sont presque exclusivement éditées en langue anglaise.
Les services spécialisés, tels l'Institut de Recherche Criminelle de la Gendarmerie Nationale (IRCGN), pilotent régulièrement les travaux de stagiaires issus d'écoles d'ingénieurs ou de formations universitaires, mais cela demande un investissement important au niveau du suivi desdits travaux.
De nombreux projets collaboratifs sont régulièrement entrepris, que ce soit dans le cadre (et grâce à) de financements européens ou, plus modestement, au niveau français. Ainsi, parmi les initiatives récentes, on peut citer le projet MAPAP (11), sous la coordination du Laboratoire d'Informatique de Paris 6. Ce projet s'est tout particulièrement intéressé aux pratiques de partage de contenus pédopornographiques sur les réseaux « pair à pair » (*peer to peer*), grâce au financement de l'Agence Nationale pour la Recherche (ANR) et de la Commission européenne.

2CENTRE – projet de centre d'excellence

Mais cela n'est pas suffisant. Aussi, pour contribuer à l'émergence d'une activité de recherche et développement dédiée à l'investigation numérique, les services spécialisés français sont-ils à l'initiative, avec leurs homologues irlandais, de la préfiguration d'un réseau

(8) Le rapport annuel de l'OSCP est publié depuis 2002 sur le site Web de la Banque de France: http://www.banque-france.fr/observatoire/

(9) *Botnet* : réseau constitué par les ordinateurs individuels qui ont été contaminés par un logiciel malveillant donné, lequel a pour particularité de les placer sous la coupe d'un même dispositif de contrôle. Ces *botnets*, qui peuvent regrouper plusieurs centaines de milliers voire plusieurs millions d'ordinateurs dans le monde, servent à relayer toutes sortes d'activités criminelles, comme des campagnes d'envoi de courriers électroniques non sollicités (*spam*), la diffusion de contenus illicites ou des attaques concertées, dites en « déni de service », qui visent à rendre inaccessible un serveur sur Internet.

(10) De nombreux articles de presse en ligne ont couvert cette actualité, comme par exemple celui-ci : http://www.01net.com/editorial/513201/le-reseau-pirate-mariposa-demantele-en-espagne/

(11) *Measurement and analysis of P2P activity against paedophile content*, http://antipaedo.lip6.fr/

de centres d'excellence dans ce domaine, dont les compétences touchent également à la formation.
C'est au sein du groupe de travail ECTEG d'Europol évoqué plus haut que cette initiative a vu le jour. Elle est née du constat qu'il est difficile de diffuser dans chacun des Etats partenaires les bonnes pratiques et produits développés conjointement en matière de formation, du fait d'un manque de formateurs qualifiés – le plus souvent recrutés dans les services spécialisés déjà surchargés – d'où cette nécessité de renforcer la recherche et le développement.
Ainsi, le 2CENTRE (*Cybercrime Centres of Excellence Network for Training Research and Education*) (12) verra le jour dans le même temps en Irlande (University College de Dublin) et en France (autour de l'Université de Technologie de Troyes) au cours de l'année 2010. Il s'agira, à chaque fois, d'animer un réseau de partenaires (Gendarmerie et police nationales, Université de Montpellier, Thalès, Orange France et Microsoft sont les premiers partenaires en France), qui sera certainement amené à s'étendre à d'autres organismes de recherche ou de formation en France ou à des pays francophones, dont certains se sont déjà déclarés intéressés. L'objectif est de développer ensemble des modules de formation, qui, traduits en différentes langues, seront en libre partage au sein du réseau 2CENTRE. Cette philosophie de partage s'adresse aussi à des activités de recherche. Le réseau 2CENTRE devrait intégrer rapidement de nouveaux centres. Ainsi, le ministre de la Justice belge a annoncé la volonté de créer dans son pays un centre d'excellence à l'occasion du Forum International sur la Cybercriminalité qui s'est tenu au mois de mars 2010 [3].

FAIRE ÉVOLUER LA LÉGISLATION

L'ensemble de ces actions est mené dans un cadre juridique nécessaire et particulièrement riche. Et même si le législateur français est souvent précurseur, des adaptations sont toujours nécessaires, ne serait-ce que pour se mettre en conformité avec les exigences européennes.

Les évolutions récentes et en cours

Ainsi, en mars 2007, la loi sur la prévention de la délinquance (13) a introduit un dispositif particulièrement novateur : les cyberpatrouilles. Dans le cadre de ces patrouilles, des enquêteurs spécialement formés à cette fin mènent sur Internet des investigations sous pseudonyme portant sur un certain nombre d'infractions, notamment celles touchant à la protection des mineurs. Plus récentes, et très commentées par les internautes, deux lois, que nous évoquions plus haut, ont permis la création de l'HADOPI et de l'ARJEL.
Plus discrètement, le Parlement européen a voté récemment le « Paquet télécom » qui introduit l'obligation pour certaines entreprises (notamment les opérateurs de communications électroniques) de notifier à une autorité compétente les incidents de sécurité ayant un impact sur les traitements de données à caractère personnel. Le Parlement français a déjà entrepris sa transposition sous la forme d'une proposition de loi adoptée le 23 mars 2009 par le Sénat, en première lecture (14). Cette obligation de notification s'imposerait à l'ensemble des secteurs économiques et devrait avoir un impact fort sur la volonté des entreprises de porter plainte en cas d'atteinte à leur système d'information.
Enfin, un projet de loi présenté par le Gouvernement est l'objet de nombreux commentaires. Il s'agit de la loi d'orientation et de programmation pour la performance de la sécurité intérieure (15). Elle contient des dispositions importantes visant à autoriser le blocage des sites Web pédopornographiques, à mieux lutter contre les fraudes à l'identité ou à autoriser, en matière de criminalité organisée, certains services d'enquête à installer des dispositifs de capture de données (et répondre ainsi, dans certains situations, à l'utilisation par les groupes criminels d'outils de chiffrement).

Les évolutions possibles

Malgré la richesse de cet arsenal législatif, les préoccupations restent importantes et les souhaits d'évolution sont nombreux. En voici quelques exemples.
La lutte contre les courriers électroniques non sollicités (*spam*s ou pourriels) a fait l'objet de dispositions ambitieuses dans le cadre de la loi pour la confiance dans l'économie numérique. Elle prévoit notamment une contravention pour chaque message illégal : il reste néanmoins difficile d'envisager la conduite d'investigations judiciaires poussées en matière de contraventions ; à titre de réponse, on pourrait fixer un seuil au-delà duquel l'infraction deviendrait un délit. Enfin, cette loi ne visait que les pourriels à caractère commercial : les pourriels non commerciaux, tout aussi nombreux et nuisibles nécessitent un encadrement adapté.
Les cyberpatrouilles (investigations sous pseudonyme) ne sont possibles que pour un nombre limité d'infractions : les atteintes aux mineurs, la traite des êtres

(12) Site Web du projet: http://www.2centre.eu/

(13) Loi n°2007-297 du 5 mars 2007 relative à la prévention de la délinquance.

(14) Proposition de loi visant à mieux garantir le droit à la vie privée à l'heure du numérique, http://www.senat.fr/dossier-legislatif/ppl09-093.html

(15) Voir le dossier législatif de la LOPPSI 2 sur le site de l'Assemblée nationale: http://www.assemblee-nationale.fr/13/dossiers/lopsi_performance.asp

© Ludovic/REA

« En mars 2007, la loi sur la prévention de la délinquance a introduit un dispositif particulièrement novateur : les cyberpatrouilles. Dans le cadre de ces patrouilles, des enquêteurs spécialement formés à cette fin mènent sur Internet des investigations sous pseudonyme intéressant un certain nombre d'infractions, notamment celles touchant à la protection des mineurs ». *Un membre de la Division de lutte contre la cybercriminalité de la gendarmerie nationale devant son ordinateur, Rosny-sous-Bois, 19 juin 2009.*

humains et, plus récemment, les jeux d'argent et de hasard sur Internet. Or, de larges champs de la cybercriminalité s'organisent sous la forme de forums en ligne ou d'échanges entre suspects, notamment la contrefaçon d'œuvres de l'esprit, les atteintes aux systèmes de traitement automatisé de données ou la contrefaçon de cartes bancaires. Il paraît donc souhaitable d'étendre le champ d'application des investigations sous pseudonyme à ces infractions.

Enfin, la gravité des sanctions n'est pas toujours dissuasive et ne semble pas toujours adaptée. Ainsi, il pourrait être envisagé de prévoir des circonstances aggravantes supplémentaires dans les cas où des atteintes à des systèmes de traitement automatisé de données ont pour objectif de collecter massivement des données personnelles ou d'escroquer un nombre important de victimes.

L'ensemble de ces évolutions (en cours ou à venir) suscitent d'importants débats et, parfois, des inquiétudes. Pourtant, l'action dans ces domaines est importante. Peut-être faudra-t-il non seulement créer de nouvelles formes de dialogue, mais aussi mieux anticiper ces nécessaires évolutions. Cela pourrait être une des missions du futur Conseil national du numérique, qui devrait remplacer rapidement le Forum des droits sur l'Internet (16).

CONCLUSION

Ce rapide tour d'horizon pourra être utilement complété par la lecture des nombreux blogs [4] ou journaux en ligne qui suivent l'actualité en matière de lutte contre la cybercriminalité. Mais nous vous soumettons quelques idées, en guise de conclusion :

• La lutte contre la cybercriminalité doit absolument être l'occasion de développer des actions en partenariat ;

• La France, même si l'ensemble de ses acteurs sont particulièrement actifs, présente des retards en matière d'innovation et d'indépendance technologique, notamment en ce qui concerne les outils d'investigation numérique, d'édition et de diffusion de publications scientifiques en rapport avec la lutte contre la cybercriminalité ou, encore, d'utilisation des techniques proches de l'investigation numérique dans la gestion des incidents de sécurité des systèmes d'information ;

• Le développement des technologies, des mesures de sécurisation et de lutte contre la cybercriminalité et l'évolution des législations sont interdépendants. Mieux appréhendé, le débat public portant sur ces sujets pour-

(16) Site du Forum : http://www.foruminternet.org/

rait peut-être rendre les législations à la fois plus efficaces et mieux acceptées.

BIBLIOGRAPHIE

[1] FREYSSINET (E.), *Se préparer à la réponse judiciaire contre les attaques informatiques*, Journée de la sécurité des systèmes d'information, 16 mars 2010, http://www.ossir.org/jssi/jssi2010/2B.pdf

[2] FREYSSINET (E.), *Réflexions pour un plan d'action contre les* botnets, SSTIC, du 9 au 11 juin 2010, http://www.sstic.org/2010/presentation/Reflexions_pour_un_plan_d_action_contre_les_botnets/

[3] de CLERCK (S.), Actes du 4e Forum International sur la Cybercriminalité, des 31 mars et 1er avril 2010, page 11, http://www.fic2010.fr/pdf/2010/Les_actes.pdf

[4] FREYSSINET (E.), Blog « Criminalités numériques », http://blog.crimenumerique.fr/