# L'Europe en lutte contre la cybercriminalité

*Éric FREYSSINET, lieutenant-colonel, chef de la Division de lutte contre la cybercriminalité, Pôle judiciaire de la gendarmerie nationale*

Lutter contre la cybercriminalité à l'échelle européenne est à la fois une nécessité et une gageure. La cybercriminalité n'a pas de frontières – même si l'on verra qu'il en subsiste – et les systèmes judiciaires, les cultures, les frontières physiques créent autant de barrières à un contrôle efficace de ces formes de délinquance. Après un peu plus de vingt ans d'actions, d'initiatives et de réussites dispersées mais convaincantes, l'Europe de la lutte contre la cybercriminalité semble vouloir prendre un nouveau virage avec la création d'un véritable outil commun, un Centre Européen de lutte contre la Cybercriminalité – annoncé par le Conseil de l'Union Européenne le 29 avril 2010 et qui devrait voir le jour en 2013. Après avoir parcouru les enjeux et les différentes étapes de cette lutte, nous envisagerons quelques-unes des composantes qui paraissent essentielles pour ces nouveaux outils.

## 1 Les enjeux

### 1.1 Une criminalité dynamique

Aujourd'hui, le tourbillon d'informations qui nous parviennent, de reportages, de témoignages d'amis ou de voisins qui ont été ou croient avoir été victimes de cybercriminels, ne nous permet plus de douter à la fois de l'existence de ce nouveau champ d'observation de la délinquance, mais aussi de sa dynamique qui apparaît presque explosive et donc un peu inquiétante.

#### 1.1.1 Petit retour sur l'histoire

Effectivement, si on regarde l'évolution des trente dernières années, ces phénomènes prennent une ampleur accrue au fur et à mesure de l'acceptation des technologies dans la société. L'outil informatique personnel est apparu à la fin des années 70 et a commencé à se développer au début des années 80. Il a d'abord été un outil professionnel – les applications bureautiques ou scientifiques. C'est donc avant tout comme support de preuve que les enquêteurs ont côtoyé l'informatique, par nécessité pour accéder aux comptabilités des entreprises dans les affaires financières.

Mais ce sont aussi des usages et des objets plus ludiques qui se sont développés[1]. A cette époque, la seule véritable délinquance spécifique était la circulation de copies illégales de logiciels, parfois même vendues par le fournisseur de matériel informatique. Le Minitel et les services télématiques apparaissent aussi à cette époque pour les français, avec la cohorte des factures téléphoniques parfois rallongées grâce à des escroqueries bien organisées.

[1] Voir la liste des ordinateurs personnels dans l'article de Wikipédia : http://fr.wikipedia.org/wiki/Ordinateur_personnel

Dans le même temps, plus discrets, les ancêtres des hackers d'aujourd'hui s'adonnaient au *phreaking*[2], téléphonant gratuitement grâce à des *blue box*[3], ou s'introduisant dans les ordinateurs de sociétés, de banques ou de centres de recherche, en se connectant sur les modems qui permettaient le dialogue entre les systèmes d'alors. Ainsi, en octobre 1984, la sécurité du système télématique britannique Prestel est mise à mal par des journalistes plus curieux et persévérants que les autres qui se sont rendus célèbres en révélant le contenu de la boîte de courrier électronique du Prince Philippe[4]. C'est notamment cet événement qui a motivé le législateur britannique à voter une loi plus adaptée dans ce domaine[5]. Les premiers virus informatiques font aussi leur apparition et se propagent grâce à l'échange de disquettes ou même sur les premiers réseaux informatiques.

La France vit à la même époque une séquence qui lui est presque particulière avec l'arrivée de la carte bancaire à puce et des télécartes à puce au début des années 80. Les deux sont l'objet de convoitises qui vont se concrétiser par des atteintes sérieuses à la fin des années 90.

Les années 90 ensuite connaissent deux événements importants avec l'arrivée de l'Internet grand public et de la téléphonie mobile. C'est aussi à partir de ce moment-là que la cybercriminalité commence à devenir un phénomène qui concerne le grand public et non plus uniquement quelques spécialistes ou des films à sensation. Les escrocs utilisent très rapidement le support électronique pour atteindre leurs victimes, que ce soit sur des forums de discussion ou par courrier électronique.

La pornographie est évidemment très présente, partagée sur les réseaux des universités, puis sur les espaces d'échanges. Même si elle est sujette à caution, elle est légale ou sa diffusion tolérée dans la plupart des pays. En revanche les images représentant des mineurs font évidemment leur apparition et les cassettes vidéo qui circulaient sous le manteau sont peu à peu remplacées par des supports numériques qui circulent plus discrètement et plus facilement sur Internet. D'abord sur des forums électroniques (ou BBS) où l'on se connectait par des liaisons téléphoniques, comme dans l'affaire Long Arm en 1992, où plus de 900 personnes ont été interpellés suite à l'identification d'un tel espace d'échanges au Danemark, jusqu'à l'affaire Cathedral[6] en 1998 qui a permis de révéler le *Wonderland Club* au sein duquel 145 adultes échangeaient plus de 700.000 images grâce à Internet. Enfin, les enfants, les personnes vulnérables en général, sont de plus en plus présentes sur les réseaux de communication, et sont victimes des prédateurs, notamment sexuels.

Les centraux téléphoniques numériques des entreprises sont alors de plus en plus victimes d'intrusions permettant de consommer gratuitement des unités téléphoniques, les techniques classiques des années 70 et 80 ne fonctionnant plus, cette forme de délinquance est encore très présente aujourd'hui et a pris une dimension internationale avec la connexion sur Internet de ces commutateurs, y compris ceux de certains opérateurs.

---

[2] Contraction de phone (téléphone) et freak (monstre de foire ou plutôt ici membre d'une certaine contre-culture).

[3] Dispositifs qui permettaient, grâce à l'émission d'une certaine fréquence sonore, de produire des ordres compris par les commutateurs téléphoniques, et par exemple de téléphoner gratuitement à longue distance.

[4] On trouvera de nombreux exemples du même type dans le chapitre 3 de *A complete hacker's handbook*, Dr. K., Carlton Books, 2002

[5] Computer Misuse Act 1990

[6] Article sur le procès en 2001 de plusieurs suspects britanniques : Child porn ring smashed, The Register, 10 janvier 2001, http://www.theregister.co.uk/2001/01/10/child_porn_ring_smashed/

Les années 2000 sont caractérisées par le développement exponentiel des formes organisées de cybercriminalité qui peu à peu recrutent des techniciens – par exemple dans les réseaux de vol de voiture ou de copie de cartes bancaires. D'autres se développent complètement autour de l'outil informatique – comme les véritables entreprises criminelles qui apparaissent en Russie, en Ukraine ou même aux Etats-Unis. Ainsi, entre 2008 et 2010, plusieurs sociétés ont vu leurs activités illégales mises en lumière : McColo et 3FN aux Etats-Unis, dont les activités ont cessé ou Innovative Marketing[7], basée en Ukraine.

C'est aussi la décennie du développement des réseaux sociaux, avec de nouvelles opportunités pour les délinquants d'atteindre leurs victimes. Ainsi, on y retrouve des escrocs de toute nature ou la diffusion de logiciels malveillants. La question de l'identité numérique devient cruciale, notamment au travers de ces réseaux sociaux. Un nouvel enjeu apparaît enfin très clairement, celui de la communication et de la propagation de l'information et son corollaire négatif, la diffusion de messages de haine ou la diffusion des rumeurs.

### 1.1.2 La cybercriminalité aujourd'hui et demain

#### *1.1.2.1 Tendances*

Après ce balayage très rapide de l'évolution de la cybercriminalité au cours des trente dernières années, citons quelques éléments clés de ce qui caractérise l'environnement dans lequel elle se développe aujourd'hui en 2011.

Le numérique est omniprésent et hyper-connecté. Il est presque devenu indispensable pour les citoyens, les entreprises ou l'administration d'utiliser des outils numériques et la tendance à l'interconnexion est forte, avec un profil que l'on configure sur son ordinateur et que l'on retrouve sur son téléphone, son téléviseur ou même très bientôt dans sa voiture ou à bord d'un avion.

Il résulte du point précédent un enjeu très fort en matière de libertés individuelles, que ce soit la protection des données à caractère personnel, la protection de son identité, la liberté d'expression. Il en découle aussi une dépendance croissante de nos sociétés à ces technologies.

La délinquance organisée est très active. Aussi bien au travers des groupes criminels classiques qui utilisent de façon massive ces nouveaux outils de communication, ou abusent les technologies ne serait-ce que parce qu'elles sont un obstacle à leur activité, qu'au vu de l'émergence de nouveaux groupes criminels complètement tournés vers l'appropriation frauduleuse grâce aux technologies. Le moteur de cette délinquance est évidemment le gain financier de leurs activités, qui présente souvent l'avantage dans un environnement numérique d'être moins dangereux et plus efficace.

La sécurité numérique, qui n'est plus un enjeu uniquement des grandes entreprises ou des Etats comme nous l'avons vu, est toutefois toujours perçue comme un enjeu de sécurité nationale qui est de plus en plus réaffirmé. A la fois face à la menace terroriste, mais aussi face à l'éventualité d'un conflit armé.

[7] Voir à ce sujet l'article de François Paget (McAfee) sur son blog : http://blogs.mcafee.com/mcafee-labs/mafia-style-cybercrime-organizations

### 1.1.2.2 Traduction concrète

***La traduction concrète de ces tendances se joue aujourd'hui au travers des mots-clés suivants : botnets, escroqueries, vie privée, identité numérique et données personnelles, hacktivisme, avec en filigrane de gros questionnements sur le rôle de certains États, la crainte du cyberterrorisme et toujours très présente la nécessité de protéger plus efficacement les mineurs.***

Un **botnet**[8] est constitué de plusieurs centaines à plusieurs milliers de machines de particuliers ou d'entreprises qui ont été compromis par un logiciel malveillant et lorsqu'elles sont connectées à Internet contactent un serveur de contrôle, à l'insu de leur utilisateur. Ces essaims de machines peuvent ainsi être exploitées pour réaliser une grosse partie des actions illégales commises aujourd'hui sur Internet comme la diffusion de courriers électroniques non sollicités (spam), la diffusion de logiciels malveillants ou de contenus illicites de façon discrète ou bien encore des attaques coordonnées contre des serveurs (attaques en déni de service distribué). Ils sont une des formes les plus inquiétantes d'insécurité sur les réseaux à laquelle aucune réponse définitive n'a encore été apportée malgré quelques affaires réussies comme le dossier Mariposa[9] en Espagne ou Bredolab[10] aux Pays-Bas.

Le gain financier est très nettement la motivation d'une grande partie de la cybercriminalité aujourd'hui et sûrement pour les décennies à venir. Plus visibles pour le grand public, les différentes formes **d'escroquerie**[11], notamment celles perpétrées par des personnes vivant en Afrique de l'Ouest, sont aussi une des plus difficiles à résoudre aujourd'hui et pour lesquelles la prévention est certainement un facteur clé de réussite, c'est-à-dire l'information du public de façon massive sur les précautions à prendre lors de leurs échanges financiers avec des inconnus sur Internet.

La **vie privée, la protection des données personnelles et la protection de l'identité** sont évidemment une préoccupation constante, notamment en France depuis la loi de 1978 sur l'Informatique et les libertés. Toutefois, la publication massive et volontaire d'informations personnelles sur les réseaux sociaux, et l'inquiétude sur les abus qui pourraient en découler (ou encore, le vote en France d'une loi[12] protégeant plus spécifiquement l'identité sur les réseaux), le débat sur le statut juridique de l'adresse IP[13], illustrent l'importance de ces sujets pour les années à venir, dans un contexte judiciaire encore balbutiant dans ce domaine, très peu de poursuites ayant été engagées au cours des trente dernières années pour des infractions à la législation sur la protection des données personnelles. C'est aussi un angle d'appréciation

---

[8] Voir article plus complet sur la lutte contre les botnets : *Réflexions pour un plan d'action contre les botnets*, Eric FREYSSINET, SSTIC 2010, http://www.sstic.org/2010/presentation/Reflexions_pour_un_plan_d_action_contre_les_botnets/

[9] Voir le résumé de cette affaire sur Wikipédia : http://fr.wikipedia.org/wiki/Botnet_Mariposa

[10] Voir le résumé en anglais de cette affaire sur Wikipédia : http://en.wikipedia.org/wiki/BredoLab_botnet

[11] Voir à ce sujet la page d'information du ministère de l'Intérieur sur les escroqueries sur Internet : http://www.interieur.gouv.fr/sections/a_votre_service/votre_securite/internet/cybercriminalite/escroqueries-internet

[12] Article 226-4-1 du code pénal, créé par la loi n°2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure

[13] Voir à ce sujet un billet de l'auteur de cet article : http://blog.crimenumerique.fr/2010/02/28/du-statut-juridique-des-traitements-de-ladresse-ip/

nouveau sur la cybercriminalité, avec l'implémentation progressive en Europe des directives du « Paquet Télécom » qui prévoient la notification des autorités et éventuellement des victimes lors d'une atteinte significative à un système d'information ayant entraîné un risque de divulgation de données à caractère personnel[14].

Le **rôle de certains États**, ensuite, est questionné sous deux angles. Ainsi, de la même façon qu'il existe des paradis fiscaux, il existe encore de gros progrès à faire sur l'harmonisation des législations et leur implémentation effective et certains pays sont parfois considérés comme de véritables paradis numériques pour la cybercriminalité. Par ailleurs, dans un contexte où la posture officielle des États est des plus en plus précise et parfois agressive en matière de cyberdéfense, quelques pays ont été accusés d'organiser des opérations d'espionnage cybernétique sous forme d'attaques contre des entreprises ou parfois des infrastructures critiques[15]. Toutefois, il convient d'être prudent et il est tout aussi possible que des groupes criminels organisés, basés dans ces pays soient aussi à l'origine des attaques.

Le corollaire immédiat de ces questions, l'inquiétude d'une possible action terroriste ciblant directement des infrastructures critiques numériques, ce que l'on pourrait alors qualifier de **cyberterrorisme**, ne s'est à ce jour pas réalisé, les premiers signes commencent à émerger[16]. La dépendance croissante des États et des infrastructures au numérique, et la présence très active des groupes terroristes sur Internet pour communiquer, se former et diffuser leur propagande, leur capacité à recruter et à motiver les jeunes générations obligent toutefois les services spécialisés à une vigilance renforcée. Récemment, le terrible attentat d'Oslo – qui avait été revendiqué juste quelques heures avant par un pamphlet diffusé sur Internet[17] – ou, par exemple, l'arrestation par la garde civile espagnole, en août 2011, d'un jihadiste recruté en Espagne[18] par Internet doivent continuer d'alerter.

Beaucoup moins inquiétants évidemment, mais beaucoup plus visibles et actifs, sous la bannière des « Anonymous », puis du groupe plus agressif des « Lulzsec », ils sont parfois qualifiés de groupes **d'hacktivistes**. Ils organisent des attaques en déni de service puis des atteintes plus graves contre de grandes entreprises de dimension internationale, des groupes sectaires ou parfois des États. Ces groupes engendrent parfois des préjudices très importants et ont mobilisé des ressources importantes dans les services d'enquête et devant les tribunaux. Leur motivation affichée est parfois ludique, parfois de l'ordre du mouvement d'humeur et très souvent sous l'angle de la revendication politique et du droit à manifester, avec son cortège de casseurs numériques. **Ces développements posent la question de la maîtrise des débordements numériques des mouvements d'opinion dans les démocraties.**

---

[14] En France, c'est l'ordonnance 2011-1012 du 24 août 2011 qui implémente ce dispositif et introduit un nouvel article 34 bis dans la loi n°78-17 du 6 janvier 1978.

[15] L'Iran et Israël sont ainsi cités comme acteurs principaux dans la diffusion du botnet Stuxnet (http://fr.wikipedia.org/wiki/Stuxnet) et la Chine est souvent pointée du doigt pour son rôle supposé dans des attaques ciblées récentes contre des entreprises et des administrations, comme par exemple suite aux intrusions dans les réseaux des institutions européennes et du fonds monétaire international ou les attaques dont a été victime Google (http://fr.wikipedia.org/wiki/Op%C3%A9ration_Aurora).

[16] On pourra lire à ce sujet les études publiées par le Coordinateur national contre le terrorisme des Pays-Bas : http://english.nctb.nl/themes/Counterterrorism/Terrorism_on_the_Internet/index.aspx?action=0

[17] Voir la synthèse de cet aspect sur Wikipédia : http://fr.wikipedia.org/wiki/Anders_Behring_Breivik#Manifeste_2083

[18] Selon les informations officielles diffusées par le gouvernement espagnole (http://www.lamoncloa.gob.es/IDIOMAS/9/Gobierno/News/2011/17082011JihadistTerrorism.htm) il serait en fait le gestionnaire d'un forum de discussion destiné à la propagande et au recrutement. Certains participants auraient l'intention de préparer des attaques contre des cibles en occident.

**Les plus jeunes, enfin, sont une des cibles privilégiées de la délinquance sur Internet, ou soumis à des risques particuliers.** La diffusion de contenus pédopornographiques est en perpétuelle croissance, ayant évolué des images fixes aux supports vidéos. Elle est très souvent associée à une démarche commerciale. De nouveaux documents sont produits régulièrement et donc autant de victimes, soit pour créer l'intérêt commercial, ou plus simplement dans le cadre d'une émulation collective entre les personnes qui s'adonnent à ces échanges. Les adultes cherchant à entrer en relation avec de jeunes mineurs sont de plus en plus nombreux, s'abritant derrière le relatif anonymat des échanges électroniques. Cette question est prise en compte dans l'évolution de la directive relative à l'exploitation sexuelle et à la protection des enfants[19], notamment en permettant dans toute l'Europe des investigations sous pseudonyme par les services d'enquête concernés.

#### *1.1.2.3 Enjeux techniques*

Les enjeux techniques sont évidemment très nombreux, sous-tendus par une évolution accélérée des progrès technologiques accessibles au grand public, aux entreprises et évidemment aux délinquants.

On peut les regrouper sous trois bannières : le volume de données (explosion des vitesses de circulation des données, de la taille des supports de stockage), l'évolution rapide des règles de fonctionnement de l'Internet (l'arrivée confirmée de l'IPv6[20], la dérégulation progressive des règles de nommage) et de façon plus générale, une pénétration toujours plus importante des outils numériques et de communication.

Ces enjeux techniques ou technologiques sont très souvent associés à des progrès pour la société – y compris en termes de sécurité – et ne sont pas considérés par les services chargés de lutter contre la cybercriminalité comme des obstacles. Toutefois, il convient d'être attentif à ces évolutions, parfois de les anticiper pour prendre des mesures permettant de garantir les capacités d'enquête ou parfois de dialoguer avec ceux qui les développent pour que les problématiques de sécurité soient bien pris en compte. L'impact le plus important est très certainement la nécessité pour une plus grande partie des enquêteurs, quel que soit leur champ d'investigation (de la sécurité routière à la lutte contre le trafic de stupéfiants) de les inclure dans leur démarche de recherche de traces et d'indices.

## 1.2 Les territoires européens

Dans cet environnement particulièrement évolutif, la gestion des territoires est primordiale.

D'abord et comme cela est répété très souvent, la cybercriminalité se joue bien évidemment des frontières, et il s'agit d'un domaine ou les services de police et la justice doivent nécessairement coopérer encore plus efficacement par-delà les frontières. Le cadre de l'Union européenne est particulièrement favorable à cette action, avec les outils très pertinents que sont les agences de coopération (Europol et Eurojust notamment), les outils de procédure communs (dont le tout récent mandat d'arrêt européen, les accords de Schengen pour un nombre croissant de pays).

L'intégration de nouveaux pays au sein de l'Union ou dans des accords de coopération renforcée permet systématiquement de faire de véritables progrès. Ainsi, la convention du Conseil de l'Europe sur la

[19] Voir le site Web de la Commission européenne sur ces questions : http://ec.europa.eu/home-affairs/policies/crime/crime_sexual_en.htm

[20] IPv6 est une évolution du protocole utilisé pour les communications sur Internet, qui va permettre de multiplier les possibilités de connexion d'équipements à Internet, mais implique des technologies de transition qui présentent à la fois des risques en terme de sécurité des systèmes, mais risquent aussi de rendre plus complexes les enquêtes sur Internet.

cybercriminalité, qui concerne des pays plus lointains comme le Japon, les Etats-Unis ou le Canada, est particulièrement utile. Dans le cas où les pays ne sont pas encore partie à ces accords, la coopération existe où se développe. Ainsi, la Russie et la Turquie participent activement depuis quelques années au groupe de travail Européen d'Interpol sur la lutte contre la criminalité de haute technologie.

Mais, comme c'est le cas avec certains pays Africains, de l'Extrême-Orient ou de l'Amérique du Sud, souvent à l'origine ou point de passage de la délinquance sur Internet, il sera nécessaire d'inventer des formes encore plus efficaces de coopération, dans un univers ou une réponse immédiate est nécessaire.

Ainsi, il faut très certainement **repenser Internet et les réseaux numériques de communication comme un véritable territoire à sécuriser**, et nous partageons cette mission avec de nombreux États, parfois lointains, mais aussi avec des entreprises privées, de toutes tailles. La coopération avec les multinationales présentes sur Internet – souvent américaines (de Google à Facebook en passant Microsoft ou Ebay) est ainsi de plus en plus efficace. Ainsi, les réponses aux demandes judiciaires sont très souvent réalisées avec une célérité comparable aux entreprises nationales.

Enfin, de la même façon que tous les territoires d'un même pays n'ont pas accès aussi rapidement aux évolutions technologiques (comme l'accès haut débit à Internet qui n'est pas uniformément réparti), il faut être attentif à offrir aux services d'enquête un accès uniforme aux technologies, aux formations et à l'information nécessaires à la réalisation de leur mission. Pour la France, il s'agit de s'intéresser non seulement aux enquêteurs et aux magistrats des grandes villes mais aussi à ceux des petites villes et des champs, et des départements et collectivités d'outre-mer. Pour nos partenaires étrangers, il faut aussi faire l'effort de leur apporter notre soutien, et c'est ce que permettent notamment beaucoup de projets financés par la Commission Européenne.

# 2 Les étapes de la lutte en Europe

On peut dégager trois grandes étapes dans la façon dont la lutte contre la délinquance numérique s'est construite en Europe : l'ère des pionniers (les années 70 et 80), l'époque de la prise de conscience (les années 90) et la période plus récente de consolidation (les années 2000). Nous verrons qu'une nouvelle étape est nécessaire pour faire face aux nouveaux enjeux de cette époque.

## 2.1 Les pionniers

Jusqu'au début des années 90, ce sont de véritables pionniers qui se confrontent à la cybercriminalité. Parfois déjà très spécialisés, lorsqu'il s'agit de s'en prendre aux premières atteintes complexes contre des systèmes de traitement automatisé de données, comme lors des affaires mettant en cause des personnes liées au *Chaos Computer Club*[21] dans les années 80. Parfois de simples passionnés parmi les enquêteurs plus classiques mettent en œuvre les premières perquisitions informatiques et analyse des données issues de matériels informatiques, notamment parmi les enquêteurs spécialisés en délinquance financière.

Les premiers acteurs ne sont pas que policiers, bien évidemment : sociétés de récupération de données, développeurs de logiciels, experts judiciaires en informatique, des magistrats et des avocats s'intéressent aussi à ce domaine.

[21] Créé en 1981, le Chaos Computer Club (CCC) est une organisation de hackers allemande. Elle organise chaque année des conférences très courues à Berlin.

## 2.2 La prise de conscience

Les passionnés ne sont plus les seuls à se démener, et l'arrivée des premières législations – comme la loi Godfrain en 1988 en France, accompagne une prise de conscience au sein des hiérarchies policières. Un peu partout en Europe, des unités spécialisées se créent au cours des années 90. Leurs représentants créent dès 1990 un groupe de travail hébergé par Interpol (Working party on IT Crime – Europe) qui se réunit toujours aujourd'hui, trois fois par an, rassemblant des représentants des du Portugal à la Russie en passant par la France.

En 1998, l'ENFSI (European network of forensic science institutes)[22], association qui regroupe les laboratoires scientifiques de police européens, crée un groupe de travail dédié à la preuve informatique, le *Forensic information technology working group*.

## 2.3 La consolidation

Les années 2000 voient les différents dispositifs nationaux[23] et internationaux se consolider avec un nombre croissant d'enquêteurs spécialisés, confrontés à de plus en plus d'affaires, comme évoqué au début de cet article. Le service européen de coopération policière Europol, qui a créé en 2002 une équipe chargée d'animer son action contre la cybercriminalité (le *high tech crime centre*, HTCC) voit son rôle dans ce domaine confirmé progressivement entre 2001 et 2007, puis pleinement inscrit dans ses statuts lors de sa transformation en véritable agence européenne au 1er janvier 2010. Europol a la capacité de soutenir des équipes communes d'enquête et gère plusieurs fichiers d'analyse en rapport avec la cybercriminalité, dont Cyborg qui regroupe des informations issues d'enquêtes judiciaires de toute l'Europe.

En matière de formation, les efforts sont aussi menés au niveau européen. Qu'il s'agisse de formations organisées sous l'égide d'Interpol en Europe, que de projets rendus possibles grâce à des financements de la commission européenne (programmes Falcone puis AGIS et ISEC aujourd'hui). Ainsi, depuis 2001, une série de projets – notamment initiés par la police irlandaise – ont proposé une harmonisation des formations européennes à la lutte contre la cybercriminalité. Les structures de formation proposées par ces projets et les modules développés ont alimenté de nombreuses formations en Europe. Aujourd'hui, ce travail est mené sous la coordination d'un groupe de travail hébergé par Europol, avec le soutien du CEPOL (le Collège européen de police) : le *European cybercrime training and education group* (ECTEG)[24].

De nouveaux outils sont à la disposition des enquêtes en matière de cybercriminalité au sein de l'Union européenne. Ainsi, Eurojust, créée en 2002, regroupe 27 magistrats représentant chacun des états-membres et pouvant faciliter la coordination des enquêtes. Autre outil judiciaire, le mandat d'arrêt européen est une réponse particulièrement intéressante dans ce domaine qui se joue très souvent des frontières.

Enfin, l'ENISA a été créée en 2005. Agence européenne de la sécurité de l'information et des réseaux, elle joue un rôle important d'identification des menaces, de sensibilisation des acteurs économiques et des Etats sur les risques en matière de sécurité. Elle ne dispose toutefois pas d'un rôle opérationnel dans la lutte contre la cybercriminalité, mais organise par exemple des exercices qui permettent d'évaluer la réponse des Etats travaillant ensemble contre les menaces sur les réseaux.

---

[22] http://www.enfsi.eu/

[23] C'est par exemple le cas en France avec la création d'un office central en 2000, l'OCLCTIC, et la formation de plusieurs centaines d'enquêteurs spécialisés (ESCI puis ICC en police nationale, NTECH en gendarmerie)

[24] http://www.ecteg.eu/

Le projet le plus récent est la création d'un réseau de centres d'excellence pour la recherche et la formation à la lutte contre la cybercriminalité. Financé avec le soutien de la commission européenne, ce projet 2CENTRE[25] vise à promouvoir la création de tels centres dans tous les pays européens (ou au niveau régional). Ces centres doivent rassembler les forces des services de police, et des milieux académiques et industriels pour animer la recherche scientifique encore balbutiante en Europe dans le domaine de la preuve numérique, développer et délivrer des formations. Les deux premiers centres créés sont en France et en Irlande, avec déjà un projet initié en Belgique et des contacts établis dans d'autres régions d'Europe et du Monde.

# 3 Les perspectives – une nouvelle étape dans la lutte contre la cybercriminalité

Le constat réalisé et l'observation détaillée des solutions apportées nous montrent qu'une réelle prise de conscience de tous les acteurs s'est concrétisée, mais il manque aujourd'hui une certaine cohérence dans le dispositif et d'importantes disparités subsistent selon les territoires. La perspective de la création d'un centre Européen de lutte contre la cybercriminalité, voulu par les responsables politiques européens doit être saisie pour répondre à ces enjeux, dans un contexte socio-économique qui n'est pas des plus favorables.

Pour des raisons juridiques et souvent d'efficacité, les services de police sont en général réticents à une posture trop directive et centralisatrice – et donc potentiellement bloquante – des organes de coopération internationale. Pourtant ils ont besoin au quotidien – et plus encore dans le domaine de la lutte contre cybercriminalité – d'un soutien efficace et réellement opérationnel de telles instances. Comme nous venons de le voir, de nombreux projets et initiatives ont vu le jour au cours des dernières années qu'il faut intégrer dans cette réflexion et profiter de cette dynamique, ne surtout pas la freiner.

La définition du périmètre d'un nouveau centre Européen de lutte contre la cybercriminalité doit résoudre cette équation. La réponse est très certainement dans une recherche permanente de solutions, d'outils qui soient au service de l'ensemble des partenaires nationaux qui luttent contre les délinquances numériques.

## 3.1 Périmètre du futur Centre Européen de lutte contre la cybercriminalité

### 3.1.1 Champ infractionnel

La question de la typologie d'infractions à couvrir est de plus en plus complexe. Autant, il est assez simple de lister les infractions très spécifiques au domaine numérique, autant le champ d'intervention des services spécialisés recouvre-t-il très souvent au plan national l'action d'autres services, par exemple lorsqu'il s'agit d'assurer des patrouilles sur Internet ou examiner des supports de preuve.

Ainsi, comme le démontre l'analyse de la situation dans les pages précédentes, le futur centre devra évidemment traiter des infractions d'attaques informatiques (atteintes aux systèmes de traitement automatisé de données), d'atteintes à la protection des données à caractère personnel et de l'identité numérique. Il devra aussi exercer son action dans l'ensemble des domaines où l'aspect numérique ou l'utilisation d'Internet sont primordiaux aujourd'hui (comme les escroqueries sur Internet, la contrefaçon de carte bancaire, les atteintes aux mineurs facilitées par Internet, etc.). Il devra aussi apporter son analyse

[25] http://www.2centre.eu/ - *Cybercrime centres of excellence network for training, research and education*.

et son expertise dans tous les domaines où l'usage de ces outils peut jouer un rôle, notamment en matière de veille judiciaire de l'Internet et de preuve numérique.

### 3.1.2 Angles d'approche et partenaires

La **coopération policière** est évidemment au cœur des préoccupations, et Europol doit donc jouer un rôle essentiel dans la création du centre Européen. Il serait d'ailleurs difficile, dans le contexte économique actuel d'envisager de répéter complètement les outils et l'infrastructure d'Europol pour un champ infractionnel donné, d'autant plus qu'on vient de voir qu'il était crucial de coopérer avec des spécialistes dans d'autres domaines. Même si l'étude commandée par la commission européenne n'en est qu'à ses premières étapes, il serait surprenant qu'elle conclue différemment.

Dans un environnement mondial, il faut aussi se poser la question des relations avec d'autres acteurs représentant d'autres régions du Monde, qu'il faudra très certainement renforcer. Interpol bien évidemment, mais aussi peut-être des partenariats privilégiés à développer ou renforcer avec certaines régions du Monde ou des pays (Afrique, Extrême-Orient, États-Unis,...). La question de la synthèse des réseaux de points de contact mis en place par Interpol, le G8 et le Conseil de l'Europe doit aussi être posée.

Les États-membres eux-mêmes doivent devenir des partenaires à part entière. Ainsi, le groupe de coordination des chefs d'unité de lutte contre la cybercriminalité réunie chaque année par Europol (European Cybercrime Task Force – EUCTF) peut être l'occasion d'identifier des acteurs efficaces pour représenter la communauté européenne dans telle ou telle conférence, réunion ou initiative, avec un véritable mandat, voire un soutien financier si nécessaire, du Centre Européen.

L'**approche judiciaire et juridique** sont tout aussi primordiales. C'est un rôle auquel contribuera évidemment Eurojust ou l'un de ses représentants, dans le dispositif à créer. L'accès rapide à la preuve, la garantie d'une mise en œuvre de l'action publique dans l'État où se trouve le suspect, nécessitent une bonne connaissance des contraintes juridiques propres aux différents pays (en Europe et au-delà). Ces informations doivent être disponibles pour l'efficacité des enquêtes menées en Europe.

L'**approche technique** est évidemment centrale, que ce soit en matière de connaissance de la menace que pour le développement ou l'identification d'outils et de méthodes efficaces de veille ou d'accès à la preuve. Les partenaires ici sont nombreux : l'ENISA qui fait le lien avec le centre d'alerte nationaux et les industries de la sécurité et les opérateurs, les groupes de spécialistes tels que ceux réunis par l'ENFSI, Interpol ou l'IOCE[26], la communauté en charge de la **formation et de la recherche**, notamment au travers de l'ECTEG et du projet 2CENTRE évoqués plus haut et bien évidemment le CEPOL.

Parmi ces acteurs, les sociétés ou les groupes de spécialistes qui font de la veille et collectent de l'information sur les actions illégales menées sur les réseaux (par exemple les sociétés antivirus, les sociétés de conseil en sécurité ou les associations internationales de spécialistes sur la sécurité des réseaux), sont une source intéressante d'information sur l'action à mener et posent la question de la prise en compte dans le cadre d'enquêtes judiciaires des informations qu'elles collectent. Il est important que le futur Centre Européen puisse avoir un échange direct avec eux.

Les modalités des interactions décrites ci-dessous pourront prendre des formes variées : accords de coopération, plateformes d'échange d'informations, échange d'officiers de liaison et devront bien évidemment utiliser au maximum les technologies avancées de communication et de travail collaboratif.

[26] Organisation internationale sur la preuve informatique – http://www.ioce.org/

## 3.2 Missions possibles et outils nécessaires

De cette synthèse, il en découle tout naturellement les composantes ci-dessous :

- des ressources et des outils de coopération policière et judiciaire, éventuellement en envisageant des procédures accélérées ou de gestion de l'urgence ;
- des capacités d'analyse dédiées, facilement mobilisables au service des enquêtes nationales ou conjointes (notamment lorsque des équipes communes d'enquête sont mises en place) ; cette structure devra pouvoir prendre en compte de façon légale des sources d'information alternatives professionnelles ;
- des outils opérationnels communs : salles de réunion virtuelles facilement et rapidement mobilisables, espaces de dialogue entre les différentes communautés, référentiel de spécialistes dans les différents domaines d'intérêt, outils et infrastructures de formation communs, outils de sensibilisation,...
- des instances permettant de développer une stratégie commune, notamment sur les questions de formation, de recherche et d'analyse de la situation, de réflexion sur les évolutions juridiques nécessaires, mais aussi ayant la capacité de répartir efficacement les tâches identifiées ensemble entre les différents partenaires ;
- des capacités techniques propres, au service des États partenaires, par exemple des capacités criminalistiques avancées et projetables (notamment en constituant des bases de référence) ou des capacités de veille de l'Internet (notamment en gérant des alertes aux services chargés de cette veille au niveau national, et en relayant les signalements provenant des internautes dans les différents pays) ;
- enfin, un véritable suivi des politiques et des instances de coopération.

# 4 Conclusion

Il est primordial, non seulement pour leur développement économique, mais aussi pour l'équilibre social, le développement de la démocratie numérique, l'accès à la culture et peut-être surtout la sécurité de leurs citoyens, que les pays européens abordent les années 2010 avec un outil rénové de prévention et de lutte contre la cybercriminalité.

L'expérience accumulée par les différents partenaires est très riche, l'analyse de la situation est donc facilement et rapidement réalisable. Souhaitons que le futur Centre Européen contre la Cybercriminalité voit effectivement le jour dès 2013 et soit tout de suite au service de cette lutte, au côté des acteurs nationaux et donne enfin une vision claire et déterminée.