Cybercriminalité (br, cn, es, us, nl, uk)

Date : 5 septembre 2013

Définie dans plusieurs des pays étudiés par la doctrine comme « l'utilisation des technologies d'information et de communication en vue d'une activité criminelle », la cybercriminalité a fait l'objet d'une définition globale et légale aux Etats-Unis et au Royaume-Uni où elle est définie comme « l'accès non autorisé à un ordinateur, à un réseau ou à des fichiers à données électroniques ». Dans tous les cas, la notion de cybercriminalité s'est traduite en droit pénal par la création d'incriminations spécifiques mais la lutte contre cette délinquance peut également être poursuivie sur le fondement d'incriminations plus générales et relatives à la protection des personnes ou des biens.

Dans l'ensemble des pays étudiés, face à l'émergence et l'importance de ce phénomène criminel, des services de police spécialisés disposant d'outils et de procédures adaptés ont été créés. De nombreux organismes spécialisés ont été institués souvent au rang de « haute autorité nationale ». Les politiques de prévention mises en œuvre s'efforcent d'associer l'ensemble des acteurs concernés (justice, police, douanes, entreprises privées, secteur bancaire, université et chercheurs) et sont considérées comme des « priorités nationales ».

Malgré le caractère transfrontalier de la cybercriminalité, la coopération internationale peine à se mettre en place. L'harmonisation des règles en matière de captation et conservation des données électroniques semblent en la matière être le principal enjeu pour parvenir à la mise en œuvre d'une entraide pénale efficace.

1 - Droit matériel et cybercriminalité

1-1 Nature et étendue des faits incriminés

Au Brésil, en Espagne, aux Pays-Bas et au Royaume-Uni, existent des incriminations relatives à « l'intrusion d'un système informatique, en vue de porter atteinte à son fonctionnement, ou d'y commettre des actes illicites ». Ainsi, les technologies d´information et de communication, lorsqu'elles sont objet du délit (le système informatique lui-même est attaqué) ou moyen de l'infraction, peuvent entraîner des poursuites pénales.

Aux Pays-Bas, la législation en vigueur donne des définitions partielles de la cybercriminalité. Par exemple, la loi sur la criminalité définit les « données », « le piratage », ainsi que « l'ordinateur ». Il existe plusieurs catégories de délits : les délits d'atteinte à la confidentialité, à l'intégrité et à la disponibilité des systèmes informatiques, les délits traditionnels en lien avec un système informatique, les violations de droits d'auteur et de droits assimilés, les délits d'atteinte à la vie privée ou à la protection des données.

Au Royaume-Uni, en vertu du Computer Misuse Act 1990, la cybercriminalité est strictement définie comme « l'accès sans autorisation à un ordinateur ou à des fichiers à données électroniques, pour y commettre des infractions telles que la fraude, le vol d'identité, la contrefaçon, toutes les atteintes à la propriété intellectuelle, etc ». Sont exactement incriminés « l'intrusion d'un système informatique pour y commettre des infractions (fraude, vol par identité, contrefaçon …) et les infections de systèmes par

virus ». En effet, la cybercriminalité repose principalement sur les infractions de « hacking » - intrusion - et « spamming » ou « malware » - infection par virus.

En Allemagne, il n'existe pas de définition légale de la cybercriminalité mais l'Office fédéral de Police judiciaire[ref] Le BKA, basé à Wiesbaden, publie un rapport annuel sur la cybercriminalité dont sont issues ces définitions[/ref] (« Bundeskriminalamt, BKA ») utilise deux définitions de ce phénomène : une définition étroite limitée à quelques infractions spécifiques et une définition élargie qui s'étend à tous les crimes et délits pour la commission desquels l'Internet a été utilisé (phishing, attaque par déni de service contre des sites internet, extorsion de fonds, commerce illégal, fabrication et diffusion d'outils logiciels destinés à des activités illégales, en particulier celles relevant de la cybercriminalité au sens étroit du terme).

Cette définition élargie est dépourvue de portée juridique ou statistique, puisque seules les infractions relevant de la cybercriminalité au sens étroit du terme figurent dans les statistiques policières à la rubrique « cybercriminalité ». Le terme de cybercriminalité n'est donc pas une notion juridique et les infractions relevant de ce domaine relève du droit pénal général allemand. (« Strafgesetzbuch, StGB »).

En Chine, la cybercriminalité est prévue et sanctionnée par la loi chinoise. Au travers des articles 285 à 287 de la loi pénale, le législateur chinois distingue les infractions préjudiciant à la sécurité d'un système informatique (telles par exemple que les intrusions illégales dans un système informatique ou les atteintes à l'intégrité d'un système informatique), des autres infractions plus généralistes réalisées par le moyen d'Internet.

Aux Etats-Unis, la cybercriminalité est régie au niveau fédéral par la section 1030 du titre XVIII du Code des Etats-Unis (US Code) qui compile les dispositions de plusieurs lois : le Comprehensive Crime Control Act de 1984, qui sanctionne l'accès non autorisé à un ordinateur et/ou à un réseau et le Computer Fraud and Abuse Act (CFAA) de 1986, qui prévoit au niveau fédéral une dizaine d'infractions. Mais les Etats fédérés prévoient aussi un ensemble d'infractions pénales relatives à la Cybercriminalité. On peut ainsi établir trois catégories de « cyber-crimes » en droit américain : les incriminations pour lesquelles le matériel ou le réseau informatique est la cible de l'infraction, les infractions pour lesquelles le matériel ou le réseau informatique est un outil pour commettre l'infraction, les infractions de contenu.

1-2 Qualifications pénales

En Allemagne, les 9 infractions suivantes sont spécifiquement prévues par le Code pénal :

- l'espionnage de données (« Ausspähen von Daten, article 202a du code pénal StGB) ;
- la capture de données (« Abfangen von Daten, article 202b StGB ») ;
- la préparation de l'espionnage ou de la capture de données (« Vorbereiten des Ausspähens und Abfangens von Daten, article 202c StGB ») ;
- l'escroquerie commise au moyen de la manipulation de données informatiques (« Computerbetrug, article 263a StGB ») ;
- la falsification d'enregistrements techniques (« Fälschung technischer Aufzeichnungen, article 268 StGB ») ;
- la falsification de données pouvant servir de preuve (« Fälschung beweiserheblicher Daten, article 269 StGB»);

- la tromperie par la falsification d'un traitement de données (« Täuschung im Rechtsverkehr bei Datenverarbeitung, article 270 StGB »);
- la modification de données (« Datenveränderung, article 303a StGB ») ;
- la modification frauduleuse de données et le sabotage informatique (« Computersabotage, article 303b StGB»).

En Chine, l'article 286 vise quatre catégories d'agissements dont la répression est proportionnée aux conséquences engendrées :

- suppression, modification, ajout ou interférence avec un système informatique, provoquant ainsi des perturbations anormales : maximal légal encouru 5 ans ; si les perturbations sont particulièrement sérieuses, ce maximum est porté à 7 ans ;
- Intrusion dans un système informatique dans le but d'obtenir les données stockées, traitées ou transmises dans l'ordinateur, ou dans le but d'exercer un contrôle illégal sur le système informatique de cet ordinateur ; provoquant un préjudice sérieux : maximal légal encouru 3 ans et/ou une amende; provoquant un préjudice particulièrement sérieux, ce maximum est porté à 7 ans et/ou une amende ;
- fourniture de programmes ou d'outils spécialement utilisés pour s'introduire insidieusement ou contrôler de manière illégale un système informatique provoquant un préjudice sérieux : maximum de 3 ans et/ou une amende, si le préjudice est particulièrement sérieux, ce maximum est porté à 7 ans et/ou une amende ;
- toute personne qui en connaissance de cause fournira au délinquant des programmes ou des outils permettant l'intrusion ou le contrôle illégal d'un ordinateur provoquant un préjudice sérieux : maximum encouru de 3 ans et/ou une amende ; si le préjudice est particulièrement sérieux, maximum légal encouru de 7 ans et/ou une amende.

A travers cet article sont donc incriminés les faits d'intrusion dans un système informatique portant sur des affaires d'Etat, la construction d'équipements de défense, ou des éléments de science et de technologie d'une très grande valeur.

Par ailleurs, l'article 287 incrimine d'une part l'utilisation d'un ordinateur afin de commettre une fraude financière, un vol, une corruption, un détournement des deniers publics, un vol de secrets d'Etat, et d'autre part les crimes de droit commun effectués au moyen de l'informatique et d'internet. Les sanctions sont celles édictées par les textes de droit commun pour les infractions concernées.

Aux Etats-Unis, au niveau fédéral, les infraction spécifiques sont les suivantes :

- l'obtention d'informations relatives à la sécurité nationale, punie de 10 à 20 ans d'emprisonnement ;
- l'accès à un ordinateur et l'obtention d'informations sans autorisation, puni de 1 à 5 ans d'emprisonnement ;
- le fait d'accéder illégalement à un ordinateur du gouvernement, puni d'un an d'emprisonnement ;
- l'accès à un ordinateur en vue de commettre une escroquerie et d'acquérir des informations, puni de 5 ans d'emprisonnement ;
- endommager intentionnellement un ordinateur en transmettant une donnée, puni de 1 à 10 ans d'emprisonnement ;

- endommager par négligence ou imprudence après avoir eu accès intentionnellement à un ordinateur, puni de 1 à 5 ans ;
- causer par négligence des dommages et des pertes après avoir accédé intentionnellement à un ordinateur, puni de 1 an ;
- trafiquer les mots de passe, puni de 1 an ;
- extorsion par l'intermédiaire d'un ordinateur, puni de 5 ans d'emprisonnement.

S'agissant des Etats fédérés, il existe trois catégories de « cyber-crimes » :

- les incriminations pour lesquelles le matériel où le réseau informatique est la cible de l'infraction (le « hacking[ref] Certaines législations étatiques distinguent « l'*outsider hacking* » de « l'*insider hacking* » :[/ref] » ou piratage informatique, le malware ou vandalisme, le Denial of Service (DdoS), qui correspond à une « attaque » simultanée de multiples ordinateurs),
- les infractions pour lesquelles le matériel où le réseau informatique est un outil pour commettre l'infraction. Cette seconde catégorie regroupe des infractions contre les personnes : le « grooming »[ref] Le « *grooming* » ou prédation sexuelle est une infraction particulière : Elle consiste dans le fait d'inciter une personne à se prostituer ou à avoir des relations sexuelles avec autrui. La circonstance de l'utilisation de réseaux de télécommunication est spécifiquement visée.[/ref] ou prédation sexuelle et le « voyeurisme[ref] Le « voyeurisme » ou atteinte à la vie privée est également pénalement réprimé. Il consiste dans l'action de capturer des images ou films de parties « privées » de la victime à son insu.[/ref] » ou atteinte à la vie privée, les violences psychologiques, le harcèlement, les menaces, l'incitation au suicide ou des infractions contre les biens (certaines infractions sont spécifiques à l'utilisation des réseaux informatiques, c'est le cas de « l'extorsion en ligne », ainsi, accéder à un ordinateur pour commettre une escroquerie ou une extorsion est spécifiquement incriminé, l'accès à un système automatisée de données en sachant que l'on ne détient pas l'autorisation pour commettre une escroquerie).

Les procureurs utilisent également la qualification de vol, de fraude et d'usurpation d'identité. Certaines qualifications pénales se sont parfois avérées inadaptées au monde virtuel. Mais d'autres qualifications de droit commun s'appliquent sur internet : c'est le cas de l'usurpation d'identité. L'ordinateur n'étant pas la cible mais l'outil des auteurs, un grand nombre de qualifications pénales de droit commun trouvent à s'appliquer, souvent sans avoir besoin d'incriminations.

- les infractions de contenu où peut distinguer deux types d'infractions: la diffusion volontaire de contenu illicite (pédopornographie[ref] Dès 1986, une commission sur la pornographie avait identifié la nécessité d'établir des qualifications spécifiques pour réprimer les échanges de documents ou l'incitation à la pédophilie sur les réseaux informatiques. Cette catégorie regroupe essentiellement la détention et l'échanges de fichiers pédopornographiques, réprimés à la section 2256 du titre XVIII de l'US *Code*5.[/ref]) et la diffusion volontaire de contenu non souhaité (les spams[ref] Cette catégorie correspond à l'envoi de courriels non sollicités définis à la section 7704 du titre XVIII du *US Code6*. L'objectif de ces dispositions est de protéger le consommateur contre certain type de publicité. L'envoi de multiples messages commerciaux non désirés est ainsi sanctionné si plus de 100 messages sont envoyés en 24 heures, plus de 1.000 messages sont envoyés en 30 jours, ou plus de 10.000 messages sont envoyés en une année.[/ref]).

Au Royaume-Uni, quatre infractions, d'importance graduée, sont définies dans les articles 1, 2, 3 et 3A

du Computer Misuse Act de 1990 :

- le simple accès non-autorisé à des fichiers informatiques privés à partir d'un autre système (computer material) ;
- l'accès non-autorisé avec l'intention de commettre ou de faciliter la commission d'infractions ;
- les actes non autorisés avec l'intention de nuire ou l'imprudence délibérée dans l'exploitation d'un ordinateur.
- créer, fournir ou obtenir des informations afin de les utiliser pour commettre les infractions citées dans les articles 1 à 3 ci-dessus.

Lorsque ces infractions sont poursuivies de manière sommaire on summary conviction, elles sont punies en Angleterre et au Pays de Galles d'une peine d'emprisonnement de 12 mois maximum et/ou d'une amende de £5000. En Ecosse, on summary conviction, ces infractions sont punies par une peine d'emprisonnement de 6 mois maximum et/ou une amende de £5000.

Lorsqu'elles sont poursuivies après mise en accusation, on indictment, la personne mise en cause risque une peine d'emprisonnement de 2 ans maximum et/ou une amende de £5000.

En Espagne, la loi espagnole du 22 juin 2010 incrimine certains comportements criminels en relation avec la cybercriminalité. On trouve ainsi dans le Code pénal des dispositions relatives aux actes d'intrusion, à l'usage des NTIC et à certains délits complexes.

Trois catégories de délits sont précisément incriminées :

- Les délits relatifs à l´intrusion dans les systèmes informatiques comme le sabotage informatique (article 264 du Code pénal) ou la révélation de secrets d´entreprises faisant l´objet de transcription informatique (article 278 du Code pénal).
- Les délits relatifs à l´usage des NTIC pour atteindre un comportement infractionnel comme le délit de corruption de mineur article de l'article 189 Code pénal.
- Les délits pour lesquels le comportement infractionnel nécessite une connaissance accrue des NTIC et engendre des investigations complexes comme le délit de falsification de documents des articles 390 et suivants du Code pénal.

Au Brésil, la loi incrimine la simple intrusion ou invasion des dispositifs informatiques aux fins de commettre des actes illicites (destructions de données, obtention d'avantages illicites) ainsi que l'atteinte aux systèmes informatiques.

2 - Droit processuel

2-1 Les polices spécialisées

Au Brésil, en Espagne, aux pays-Bas et au Royaume-Uni, il existe une police spécialisée dans le traitement de la délinquance cybercriminelle. Cette sépcialisation policière est assez développée au Brésil, aux pays-Bas et au Royaume-Uni. Au Brésil, la police judiciaire est chargée de coordonner les actions en matière de lutte contre la cybercriminalité. Des commissariats spécialisés ont été créés dans certains États.

Il existe également d'autres initiatives telles que la spécialisation d'agents de la Police Fédérale ou encore le renforcement de la sécurité du système financier. Aux Pays-Bas, c'est le THTC (Team High Tech crime) qui est en charge de la lutte contre la cybercriminalité. Au Royaume-Uni, il existe des services de police spécialisés à compétence nationale, tels que la MET, Metropolitan Police ou les services de renseignement. En Allemagne, les investigations de police judiciaire sont menées par les Offices de police judiciaire des différents Länder (« Landeskriminalämter, LKA ») ou, quand l'importance de l'affaire le justifie, par l'Office fédéral de Police judiciaire (« Bundeskriminalamt, BKA »).

La Chine s'est dotée de moyens d'enquête spécifiques (département cyber du Ministère de la Sécurité Publique (MSP) avec 30 000 agents annoncés lors du Groupe de Haut Niveau de 2010. Cela reste toutefois relativement opaque et hormis lors d'échanges bilatéraux institutionnels où le sujet est mentionné, il est particulièrement difficile d'en évaluer les moyens et missions. La structuration de ces services au sein de la police chinoise est déconcentrée avec des pouvoirs et des moyens d'actions donnés aux échelons provinciaux. Enfin, la qualité de l'auteur ou de la victime conditionnent également le service compétent car les administrations centrales chinoises disposent de pouvoirs d'enquête et de moyens pour les mener à bien.

Brésil : la législation prévoit la création au sein de la Police Judiciaire brésilienne de services et secteurs spécialisés dans le domaine de la lutte contre les crimes cybernétiques. Des commissariats spécialisés ont été créés dans de nombreux Etats[ref] Rio Grande do Sul, (Commissariat de répression des crimes informatiques).[/ref]. Il existe également d'autres initiatives telles que la spécialisation d'agents de la Police Fédérale ou encore le renforcement de la sécurité du système financier .

En Septembre 2012 un centre de défense cybernétique a également été mis en place. Des séminaires de défense cybernétiques sont également organisés par le Ministère de la Défense pour traiter de ce sujet.

Au Royaume-Uni , au sein de la Metropolitan Police existe The Police Central e-Crime Unit (PceU): Il s'agit d'une unité de police spécialisée -qui a une compétence sur tout le territoire-, chargée de mener des enquêtes nationales contre les cyber crimes les plus importants. A ce titre le PceU's Internet Governance Team a bloqué plus de 15 000 sites internet. Une unité spéciale doit être créée au sein de la future NCA, la National Cyber Crime Unit, qui devrait intégrer la Police Central e-Crime Unit. Les unités de police spécialisées comprennent des Hackers qui travaillent de façon anonyme et sont susceptibles d'infiltrer les systèmes potentiellement dangereux[ref] Il y a également des analystes recrutés en fonction de leurs diplômes en informatique et enfin des enquêteurs ayant reçu une formation de base en la matière. Les services de police préfèrent recruter du personnel déjà formé plutôt que de devoir investir dans leur formation. On doit ajouter que la conception du recrutement des officiers de police permet d'intégrer traditionnellement des personnalités venant d'horizons universitaires et professionnels variés.[/ref].

Il existe une unité spéciale établie au sein de la police et sponsorisée par l'industrie bancaire pour lutter contre la criminalité organisée relative aux fraudes liées aux cartes bleues et aux chèques. Il s'agit de la Dedicated Cheque and Plastic Crime Unit (DCPCU). Elle est composée d'officiers de la Metropolitan Police qui travaillent étroitement avec des enquêteurs spécialisés en matière de fraude dans l'industrie bancaire. L'objectif de la DCPCU est d'enquêter, d'arrêter et de poursuivre les délinquants responsables de fraude aux cartes bancaires et aux chèques.

En Allemagne, dans la plupart des lander, des unités – de taille extrêmement variable - spécialisées dans

la lutte contre les formes de criminalité utilisant l'Internet ont été créées dans les office de police judiciaire (L.K.A). Le LKA de Baden-Württemberg, qui veut visiblement occuper une place éminente dans ce domaine, publie un rapport annuel très détaillé (58 pages) accessible sur internet à l'adresse suivante :

http://www.lkabw.de/LKA/statistiken/Documents/2012_Cyberkriminalitaet_Digitale_Spuren.pdf

Au niveau de l'Office fédéral de Police judiciaire (BKA), il existe deux services compétents en la matière. Un service technique de soutien aux investigations, et un service de veille et de recherches permanentes.

Le premier, dénommé « centre de service technique pour les technologies de l'information et de la communication» (Technisches Servicezentrum Informations- und communikationstechnologien, en abrégé TeSIT) qui a pour mission, selon le ministère de l'intérieur dont dépend le BKA, de fournir aux enquêteurs des LKA ou du BKA « un soutien technique pour les mesures et les investigations dans les réseaux de données ». Il s'agit d'une équipe interdisciplinaire de l'institut de criminalistique du BKA composée de scientifiques, de techniciens informatiques, d'ingénieurs et de fonctionnaires de police, chargée en particulier de la recherche et de la conservation des preuves dans le cadre des enquêtes pénales.

Le second, rattaché au TeSIT, est un « service central de recherches permanentes dans les réseaux de données » (Zentralstelle für anlassunabhängige Recherchen in Datennetzen, en abrégé ZaRD) qui réalise une veille et surveillance des sites et forums Internet, en particulier de ceux susceptibles d'abriter de la pornographie infantile.

Aux Etats-Unis, la lutte contre la cybercriminalité ne fait pas l'objet d'une centralisation des réponses au sein d'un service de police ou d'une juridiction unique, un nombre important de services d'enquête sont ainsi chargés de mission de lutte contre différents aspects de la cybercriminalité. Si les Etats fédérés jouent un rôle non négligeable du fait de leur proximité avec les victimes, à travers les services de police qui reçoivent les plaintes, ce sont surtout les services fédéraux qui sont concernés. Ainsi le FBI, le Department of Homeland Security et l'une de ses composantes, le Secret Service jouent un rôle de premier plan, du fait de la spécialisation de certaines unités.

Le FBI est le plus important service de police judiciaire et de contre-espionnage aux Etats-Unis et le service le plus important en matière de lutte contre la cybercriminalité.

Ses trois priorités en matière d'enquête dans ce domaine sont : l'intrusion dans les réseaux informatiques, en particulier les réseaux de l'administration américaine, l'usurpation d'identité et les fraudes. Pour répondre au mieux aux spécificités de ce type de délinquance, le FBI a mis en place plusieurs structures administratives spécifiques, répondant à différents objectifs :

- La « Cyber Division » réorganisée en 2012, elle se concentre désormais principalement sur la sécurité des réseaux. Les investigations concernant les infractions de contenu sont désormais de la compétence de la Criminal Division du FBI, ce qui montre une forme de « normalisation » de la cybercriminalité.
- ?La « National Cyber Investigative Joint Task Force », créée en 2008, cette Task Force a pour

objectif de détecter et empêcher les intrusions informatiques et tentatives de piratage des données, principalement de l'administration américaine. Elle travaille en collaboration étroite avec le secteur privé, à la fois pour que les entreprises informent les services d'enquête des attaques dont elles font l'objet, mais aussi pour développer une politique de prévention vis-à-vis des entreprises et du consommateur.

- ?IC3 : Internet Crime Complaint Center est un centre de gestion des plaintes des victimes d'infractions liées à internet. Il centralise les plaintes en lignes pour différentes infractions, notamment usurpation d'identité, intrusion informatique, violations des droits de propriété intellectuelle, ou encore extorsion en ligne. Il s'agit de l'équivalent de Pharos en France.

La plainte en ligne est effectuée par l'intermédiaire d'un formulaire type renseigné par les victimes. Il joue ainsi un rôle de prévention important par rapport au consommateur et il permet aux internautes de signaler des contenus illicites ou des comportements dangereux.

- ?La « National Cyber Forensics Training Alliance » (NCFTA). Créée en 1997, elle est à l'origine un centre d'analyse des menaces sur internet. Elle rassemble des services de police, des entreprises concernées par la sécurité informatique, ainsi que des universités. Si NCFTA a un statut d'association, elle reste très liée aux pouvoirs publics et aux services de police notamment. Son rôle est de faire remonter les menaces et de diffuser les risques identifiés à l'ensemble du secteur privé. Ainsi, si un virus informatique est détecté, il est analysé et l'ensemble des acteurs est informé des risques et des éventuelles mesures à prendre pour se prémunir contre le danger identifié. NCFTA a également un rôle en matière d'enquête, et a mené plusieurs investigations contre des réseaux de pirates informatiques.

En collaboration avec IC3, NCFTA a mis en place une « Cyber Initiative and Resource Fusion Unit » (CIRFU), qui est une plate-forme de dialogue entre les pouvoirs publics et le secteur privé. CIRFU a un rôle de recherche concernant les menaces, d'orientation des enquêtes vers les services les plus appropriés, et d'échange entre les acteurs privés.

Le Department of Homeland Security est une création récente. Construit en réaction aux attentats du 11 septembre 2001 dans un objectif de coordination des agences fédérales, il rassemble des services qui auparavant étaient sous l'égide du ministère de la justice, du Trésor ou indépendants. Le DHS a essentiellement une mission de protection des frontières. A ce titre, il a développé une compétence en matière de cybercriminalité à travers le Cyber Crimes Center composé de trois unités, qui reflètent trois objectifs du DHS en matière de lutte contre la cybercriminalité.

- ?Computer Forensics Unit : regroupe une unité de police scientifique dont l'objectif est de pouvoir procéder à l'analyse du matériel informatique (ordinateurs, téléphones…) saisi lors des enquêtes. Cette unité comporte du personnel spécialisé, un réseau de techniciens judiciaires spécialisés ayant un rôle de conseil pour les services de terrain et d'assistance dans certaines opérations d'extraction de données.
- ?Cyber Crimes Unit : est un service d'enquête spécialisé. Il réalise des opérations d'infiltration, principalement pour identifier des infractions de fraude, de contrefaçon ou de contrebande douanière. Il dispose de pouvoir de réquisition administrative pour obtenir des informations rapidement de la part des opérateurs téléphoniques et des fournisseurs d'accès à internet, notamment en matière d'import/export de marchandises prohibées ou de contrebande.

- ?Child Exploitation Unit : est une unité exclusivement chargée de la pédopornographie et des atteintes sexuelles sur mineurs commises ou identifiées grâce à internet. Ce service gère une base de données de toutes les adresses IP qui ont été ciblées, afin de déterminer des objectifs à partir des informations transmises. Le service conduit des investigations en matière d'image pédopornographiques, mais aussi en ce qui concerne le tourisme sexuel ou les tentatives d'atteintes sexuelles commises en contactant des mineurs sur les réseaux sociaux.

2-2 La coordination des enquêtes

La coordination des enquêtes réalisées par les autorités de police est effectuée en Espagne, par un parquet spécialisé et au Royaume-Uni par une agence spécialisée, la SOCA (Serious Organised Crime Agency) qui sera remplacée en octobre 2013 par la National Crime Agency. Dans ce dernier pays, existe aussi une spécialisation des agents au sein du Crown Prosecution Service, service des poursuites. Des prosecutors sont formés pour devenir des national specialists prosecutors, spécialisés dans la poursuite des cyber crimes[ref] Ils participent à des stages de formation appelés High-Tech Crime Training qui leur permettent ensuite de travailler avec les services de police et de mener des poursuites de façon plus efficaces.[/ref]. Le HMRC (Her Majesty's Revenue and Customs), administration fiscale et douanière, a en outre mis en place une équipe spécialisée en matière de cybercriminalité pour lutter contre les fraudes fiscales par internet. Aux Pays-Bas, de façon originale, il existe un regroupement des organes (police, parquet, banques) sous la forme d'une task force.

Au Brésil, la lutte contre la cybercriminalité est inclue dans la stratégie nationale de défense, c'est l'armée qui est responsable de la coordination des actions de défense cybernétique, sans qu'il existe de réelle coopération judiciaire, policière ou douanière[ref] Au plan international il convient de souligner que le Brésil n'est pas signataire de la Convention du Conseil de l'Europe sur la Cybercriminalité.[/ref].

En Espagne, depuis 2010, un procureur Général en charge de la cybercriminalité, directement placé auprès du Procureur Général de l'Etat, coordonne pour toute l'Espagne la lutte contre la cybercriminalité. Il existe aussi, en application de la loi organique 24/ 2007 du 9 octobre, relative à la spécialisation du ministère public, un parquet spécifique en matière de criminalité informatique (70 parquetiers) qui travaille en collaboration avec des services de police et de garde civile spécialisés dans la cybercriminalité. Ont été créées dans les années 90 des unités spéciales : la BIT (Brigade d´ investigation technologiques) pour la police et le GDT pour la Guardia civil. En Catalogne, los mossos d'escuadra et au Pays Basque la Ertzaintza disposent également d'unités spécialisés dans le cybercrime[ref] Les agents qui officient au sein du Parquet Cybercriminalité bénéficient d´une formation particulière et d'une spécialisation.[/ref]. L´unification des services d´enquêtes dédiés à la cybercriminalité (policia y guardia civil) est prévue pour 2014.

Aux Pays-Bas, si en principe, l'ensemble des services de police répartis sur le territoire national peuvent être amenés à traiter de la cybercriminalité, c'est la police judiciaire au niveau national (Dienst nationale Recherche) et plus précisément le THTC (Team High Tech crime) qui est en charge de la lutte contre la cybercriminalité. Il existe une task force (ECTF) regroupant les services de police, le Parquet National, les banques et le CPNI (Centre néerlandais de protection des infrastructures nationales).

Au niveau policier, il convient de noter l'existence du Centre National de recensement de la cybercriminalité (Meldpunt) qui est en charge de la lutte contre la cybercriminalité en général et qui est

organisé autour de deux unités centrales implantées à Zoetermeer: Unité des homicides et crimes sexuels et unité de surveillance des sites Internet composée de cyber patrouilleurs effectuant des vérifications et préparant des dossiers qui sont envoyés aux unités régionales d'enquête :

-l'Unité crimes sexuels et auteurs d'infractions sexuelles en lien ou non avec Internet composée d'environ 45 personnes et qui alimente le fichier VICLAS (violent crime linkage analysis system) qui contient, à ce jour, 36.000 noms de personnes (enregistrement des noms et des modes opératoires).

Par ailleurs, s'intéressant à la pédopornographie et au tourisme sexuel, l'Unité gère un autre fichier ECLIPS de 27 .000 individus concernés par ces infractions.

-L'Unité de surveillance des sites Internet, composée de techniciens et de cyber patrouilleurs, est chargée de détecter toutes les menaces à l'ordre public et à la sûreté de l'Etat à titre principal sur les réseaux sociaux tels que Facebook, Twitter etc. (Surveillance par mots clés).

La surveillance concerne aussi bien la menace terroriste que les menaces à l'ordre public ou les menaces économiques (hacking).

Au Royaume-Uni, la SOCA, agence publique qui a pour mission générale de lutter contre la criminalité organisée, coordonne les enquêtes au plan national et conseille les 43 services de police locaux qui couvrent le territoire de l'Angleterre et du Pays de Galles pour leurs enquêtes. Au niveau international, elle a des représentants dans différents pays. Ils œuvrent, à la fois dans le cadre de la coopération pénale internationale et aussi à la mise en place de politiques ou d'aide à la rédaction de lois permettant de lutter contre la cybercriminalité. A partir d'octobre 2013, la SOCA sera remplacée par une nouvelle agence : la National Crime Agency qui reprendra en grande partie ses attributions, et disposera d'une organisation et d'une définition de ses fonctions plus lisibles dans l'organisation de la lutte contre la criminalité organisée. Elle devra lutter contre les cybers crimes les plus graves en initiant des enquêtes au niveau national contre la criminalité organisée.

Aux Etats-Unis, en matière judiciaire, il existe un bureau spécialisé au ministère de la justice, mais qui est loin de concentrer l'ensemble des poursuites contre la cybercriminalité.

2-3 Techniques d'enquêtes

Aux Pays-Bas, des mesures de réquisitions sont prévues, ainsi que des obligations de conserver les données. Le Royaume-Uni préfère concentrer ses efforts sur la prévention plutôt que sur la répression de la cybercriminalité[ref] Le Royaume-Uni fait partie de la Convention de Budapest relative à la cybercriminalité qui permet de lutter contre la criminalité internationale sur internet. Le gouvernement a annoncé une contribution à hauteur de 100 000 livres pour le projet The Council of Europe Global Project on Cybercrime.[/ref]. Surtout, l'efficacité des enquêtes demeure limitée. Les Etats-Unis disposent d'agents infiltrés et ont mis en place un système de veille permanent des données à grande échelle sur internet. Enfin, l'Allemagne ne dispose d'aucun cadre juridique permettant l'enregistrement préventif, par les fournisseurs d'accès téléphonique ou internet, des données de communication ("Vorratdatenspeicherung")[ref] A la suite de la décision du 2 mars 2010 de la Cour constitutionnelle Fédérale ayant annulé la législation existant sur ce point, considérée comme permettant des atteintes injustifiées au secret des correspondances garanti par l'article 10 de la Loi fondamentale allemande, les

dissensions au sein de la coalition gouvernementale n'ont pas permis à l'Allemagne de se doter d'un nouveau cadre juridique.[/ref].

En Espagne, une loi sur la conservation des preuves met à la charge des opérateurs de téléphonie une obligation de conservation des informations relatives aux trafics de données au profit des autorités d'enquête. Certains projets de modernisation sont en cours d'examen. la loi 25/2007 de conservation des données relatives aux communications électroniques et aux réseaux publics de communication transpose la directive Européenne 2006/24/CE. Elle oblige les opérateurs publics de communication à conserver toutes les informations relatives aux trafics de données (téléphonie, internet) pendant 1 an, et ce, afin de les mettre à disposition de l´autorité judiciaire qui enquête sur des délits graves. La notion de délit grave pose de sérieuses difficultés en pratique car elle revient à fermer la voie à des investigations qui ne porteraient pas sur un délit puni de 5 ans d'emprisonnement. Des projets sont en cours d'examen avec pour objectif de moderniser les enquêtes, notamment : la possibilité pour le juge d'instruction d'ordonner la fermeture de sites de pornographie infantile ou le blocage de leur accès en Espagne, quand ils sont situés dans un autre pays ; l'introduction d'agents infiltrés en matière de cybercrime. Les enquêteurs pourraient utiliser de fausses identités et s'introduire dans des systèmes informatiques en se faisant passer pour un mineur pour par exemple déceler des pédophiles.

Aux Pays-Bas, la loi sur la criminalité informatique a introduit dans le Code de procédure pénale l'article 125 i permettant au juge de l'instruction (rechter commissaris) de réquisitionner une personne qui a probablement accès aux données recherchées afin que celle-ci fournisse des données ou donne au juge les conditions d'accès si ces données avaient une relation avec le délit, le suspect ou l'enregistrement des données. Ces pouvoirs ont été renforcés en janvier 2006 par la loi sur la production des données (wet bevoegdheden vorderen gegevens). Les réquisitions peuvent être délivrées aux personnes qui traitent les données dans un cadre professionnel, une réquisition pour autres données entreposées ou données sensibles peut toutefois être adressée aux personnes qui traitent des données pour un usage personnel. La loi sur la criminalité informatique II a introduit la possibilité d'ordonner la préservation des données. Le CPP autorise le ministère public, en cas de délits où la détention provisoire est possible, d'ordonner la préservation des données conservées dans un ordinateur et qui peuvent disparaitre ou être modifiées. Cette conservation peut être ordonnée pour une période de 90 jours (renouvelable une fois).

Au Royaume-Uni, s'agissant des services de police, en dehors de la Metropolitan Police à Londres et de la SOCA, agence spécialisée, peu d'entre eux ont une expertise suffisante pour lutter contre la cybercriminalité[ref] Il existe plusieurs autorités d'information.[/ref]. Certaines difficultés sont liées à la preuve numérique: les fichiers supprimés peuvent difficilement être utilisés comme moyens de preuve et les sociétés de télécommunication ne sont pas obligées de révéler ces informations ou de les conserver. En Grande-Bretagne et au Pays de Galles, les 43 services de police qui couvrent l'ensemble du territoire sont indépendants du Home Office, Ministère de l'Intérieur. Depuis novembre 2012, leurs chefs sont élus au suffrage universel sur les bases d'un programme électoral. Dans ces conditions, il est peu probable que la cybercriminalité figure parmi leurs priorités, celles-ci étant principalement tournées vers la répression de la petite délinquance.

Le système britannique en matière de cybercriminalité présente ainsi certaines limites :

Il est fondé en grande partie sur la prévention de la fraude et le signalement rapide des fraudes pour en limiter les conséquences. Le manque de cohésion entre les différents organes en charge de la

cybercriminalité au Royaume Uni est aussi très souvent critiqué. La création de la NCA a pour but de répondre à ces critiques.

En Allemagne, la collecte des données de communication a lieu dans les conditions prévues par l'article 100g du code de procédure pénale (StPO) qui sont semblables à celles posées par l'article 100b[ref] **Art. l00b StPO**[/ref], pour l'interception des communications téléphoniques, et nécessitent une autorisation judiciaire. L'infraction à l'origine de l'enquête doit avoir été commise au moyen de l'utilisation d'une technologie de communication (ce qui est toujours le cas des 9 infractions spécifiques relevant de la cybercriminalité au sens étroit utilisé par le BKA), ou bien figurer dans la liste limitative de l'article 100a StPO[ref] **Art. l00a StPO** (1) La surveillance et la transcription des télécommunications peuvent être ordonnées lorsque (conditions cumulatives) :[/ref].

Aux Etats-Unis, le Secret Service est une des agences du Department of Homeland Security qui a développé une compétence autonome en matière de cybercriminalité. Contrairement à ce que le vocable peut laisser entendre en français, le Secret Service n'est pas chargé d'une mission de renseignement ou d'action extérieure mais de deux fonctions principales, la sécurité du système bancaire et financier américain, ce qui inclut une mission de police judiciaire en matière économique et financière, et la protection rapprochée du Président des Etats-Unis, du Vice-président, des officiels étrangers en visite aux Etats-Unis et des représentations diplomatiques. Le Secret Service a mis en place 31 Electronic Crime Task Forces locales sur tout le territoire, qui regroupent non seulement différents services de police, fédéraux et locaux, mais aussi des procureurs, le secteur privé et les universités. Il ne s'agit pas d'une organisation administrative spécifique à la cybercriminalité, mais d'une pratique assez fréquente aujourd'hui, à travers les « Fusion Center », visant à éviter les doublons et coordonner l'action des différents services. L'objectif de cette nouvelle structure n'est pas de répondre à chaque dénonciation d'infraction, mais de rassembler un maximum d'information afin de déterminer des cibles et ainsi mener des enquêtes sur des réseaux importants. Ils utilisent ainsi des agents infiltrés et font appel à des informateurs. Le Secret Service a également mis en place des groupes de travail privilégiés avec certains autres pays. C'est notamment le cas avec les pays baltes, l'Ukraine et les Pays-Bas. Deux International Electronic Crime Task Forces ont également été mises en place avec le Royaume-Uni et l'Italie, basées à Londres et à Rome. Des agents de liaisons sont également en poste à Interpol et Europol.

Plus récemment, le Secret Service a développé une compétence en matière de cybercriminalité en ce qui concerne sa deuxième mission fondamentale, la protection du Président et des hautes personnalités : une « Protective Intelligence and Assessment Division » a ainsi été mise en place. Son but est de réaliser une veille des risques pesant sur la sécurité des personnalités ou de certains lieux, à travers un suivi des réseaux sociaux. Ils utilisent pour cela un certain nombre d'outils informatiques. Il ne s'agit pas en l'espèce d'obtenir des informations non disponibles, mais de rassembler une multitude de données librement accessibles sur internet (Twitter, Facebook, Flickr, Instagram…). Ils utilisent aussi des informations des services locaux et dialoguent régulièrement avec les autres agences fédérales pour affiner certaines menaces. L'objectif du service est de réaliser des « Vulnerability Assessment » (évaluation de la vulnérabilité) concernant certaines personnalités ou certains évènements, afin d'adapter au mieux la protection déployée sur le terrain. Il s'agit donc d'un outil de gestion des effectifs et du déploiement des moyens en même temps qu'un outil de prévision de la menace. Cette division assure également une veille 24/7 en cas de grands évènements internationaux (G8, G20, sommets internationaux), afin de faire remonter certaines informations. Il s'agit donc d'une mission qui sur le fond s'apparente plus à la mission traditionnelle de la DCRI et de la sécurité publique en France. Pour

assurer leurs missions en matière de cyber surveillance, le Secret Service dispose d'un ensemble de formations pour son personnel assurées par un établissement dédié, le « National Computer Forensics Institute ».

3 - Les stratégies de lutte contre la Cybercriminalité

3-1 Les politiques de prévention

Les Pays-Bas ont inauguré le 1er janvier 2012 à La Haye, le « Centre National de cyber sécurité néerlandais (NCSC) » , structure publique mixte associant notamment le ministère de la défense et le ministère public. Son ambition est de développer la «cyber résilience de la société néerlandaise » (sic) en effectuant un suivi des tendances en matière de cybercriminalité, de menaces, d'incidents et de vulnérabilités. Il regroupe une soixantaine de personnes en provenance du ministère de la défense, des services de police, du ministère public et du NFI (Laboratoire central en médecine légale).

En Allemagne, la loi du 19 août 2009 pour le renforcement de la sécurité dans l'usage des techniques d'information par l'État fédéral «Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes » a renforcé la compétence de l'Office fédéral pour la sécurité des techniques d'information («Bundesamt für Sicherheit in der Informationstechnik, BSI»), créé en 1991, et dont le rôle principal est de mettre au point et de surveiller la mise en oeuvre des protocoles et standards de sécurité informatique par l'administration fédérale. Cet office, rattaché au ministère de l'intérieur, est désormais compétent également pour informer le public sur les éventuelles failles de sécurité existant dans les logiciels ou systèmes informatiques, et mener des actions de sensibilisation auprès des milieux économiques ou scientifiques. Basé à Bonn, il dispose d'un effectif de 550 personnes environ (informaticiens, physiciens, mathématiciens, personnel administratif).

En février 2011, le gouvernement fédéral allemand a adopté une « stratégie de cyber sécurité » élaborée essentiellement par le ministère de l'intérieur, dont les 10 axes principaux sont les suivants :

- la protection des infrastructures de communication allemandes
- la sécurisation des systèmes de communication en Allemagne
- le renforcement de la sécurité informatique dans l'administration publique
- la création d'un centre national de cyber protection
- la création d'un conseil national de cyber sécurité
- le renforcement du contrôle de la criminalité dans le cyber espace
- le développement de la coopération européenne et internationale dans ce domaine
- l'usage de technologies fiables
- le renforcement et la sensibilisation du personnel des autorités fédérales
- le développement d'outils permettant de répondre aux cyber attaques.
- La version en langue anglaise de cette stratégie gouvernementale est jointe à la présente note.

On relèvera en particulier que le centre national de cyber protection, chargé d'assister l'Office fédéral pour la sécurité des techniques d'information (BSI), coopère directement avec l'Office fédéral pour la protection de la Constitution (BfV) et l'Office fédéral pour la protection civile (BBK), sur la base d'accords de coopération conclus entre ces organismes. L'Office fédéral de police judiciaire (BKA), la

direction de la police fédérale (BPOL), l'Office de police des douanes (ZKA), les services de renseignements fédéraux, l'armée, et les autres autorités supervisant les infrastructures critiques sont représentées au sein du centre national de cyber protection.

Ce centre est aujourd'hui opérationnel, et joue un rôle essentiel dans la circulation de l'information entre les autorités concernées. C'est lui qui, concrètement, assure la coopération des autorités policières et douanières. Les autorités judiciaires n'y participent pas directement, même si le BKA joue un rôle d'interface à leur égard. Dans le laps de temps écoulé depuis sa fondation en avril 2011 jusqu'en mars 2013, il a traité 900 dossiers concernant la sécurité nationale et internationale des technologies de l'information, dont la grande majorité relevait d'une délinquance spécialisée motivée par l'appât du gain, une fraction moins importante relevant de l'activité de « Hackers » ne recherchant pas de profit personnel direct.

Le conseil national de cyber sécurité a également été instauré. Il comprend des représentants de la chancellerie fédérale, et les secrétaires d'État des ministères suivants : ministère des affaires étrangères, ministère fédéral de l'intérieur, ministère fédéral de la défense, ministère fédéral de l'économie, ministère fédéral de la justice, ministère fédéral des finances, ministère fédéral de l'éducation et de la recherche, ainsi que des représentants des Länder.

Des représentants des milieux économiques sont invités, le cas échéant, en qualité de « membres associés », de même que des universitaires sur les sujets relevant de leur compétence.

Il existe également un conseil de cyber sécurité –distinct du conseil national mentionné ci-dessus - établi sous la forme d'une association composée de personnalités des milieux politiques, économiques, et universitaires, qui organise des recherches, conférences et débats de haut niveau sur le sujet.

Le Royaume-Uni a créé bon nombre d’organisations publiques ou parapubliques dont l’objet est d’assurer une meilleure protection contre la cybercriminalité, principalement pour assurer la protection des intérêts industriels et financiers du pays. Il s’agit également d’assurer un meilleur partage de l’information.

En matière de politique de prévention différentes actions sont menées par la Serious Organised Crime Organisation (SOCA), Cybercrime Reduction Partnership et Cyber Security Information Sharing Partnership, Defence Cyber Protection Partnership, et la National Fraud Authority.

-La Serious Organised Crime Organisation (SOCA), agence chargée de certaines des investigations sur la criminalité organisée a, en 2011, publié un rapport intitulé « The UK Cyber Security Strategy : protecting and promoting the UK in a digital world ». Ce rapport identifie les problèmes liés au développement rapide du monde digital et a établi plusieurs priorités pour le Royaume-Uni notamment la mise en place d’une nouvelle stratégie pour la lutte contre la cybercriminalité pour 2015. Cette lutte est principalement axée sur la protection des intérêts commerciaux du pays:

- Contrer la cybercriminalité pour devenir un des espaces les plus sécurisés du monde afin de faciliter les transactions commerciales en ligne ;
- Réagir rapidement et vigoureusement contre les attaques en ligne et être plus apte à protéger les intérêts de tous au sein du cyber espace ;

- Aider à créer un cyber espace ouvert, stable et vivant, dans lequel les britanniques puissent naviguer en toute sécurité.
- Cybercrime Reduction Partnership et Cyber Security Information Sharing Partnership: lancé par le Security Minister James Brockenshire en mars 2013, le Cybercrime Reduction Partnership a établi un forum dans lequel le gouvernement, les autorités judiciaires, les principales industries - pharmaceutiques, défense, finances, énergie et télécommunications- et les universités peuvent régulièrement communiquer sur la cybercriminalité. Le Cyber Security Information Sharing Partnership (CISP) permet également au gouvernement et aux industriels de partager des informations sur les menaces actuelles présentes dans l'espace cyber et ainsi de mieux gérer les incidents. Suite à un programme pilote testé sur 160 entreprises dans ces 5 secteurs (défense, finance, pharmaceutiques, énergie et télécommunications), le CISP est à présent accessible aux entreprises appartenant aux secteurs économiques essentiels[ref]A terme le Cybercrime Reduction Partnership et le Cyber Security Information Sharing Partnership doivent fusionner car le gouvernement projette d'établir un National Computer Emergency Response Team qui regrouperait ces deux activités pour apporter une réponse plus rapide et plus efficace aux menaces cybercriminelles contre les grandes entreprises.[/ref].
  Defence Cyber Protection Partnership : mis en place en juillet 2013, ce Partnership entre le gouvernement et les industriels de l'armement tend à améliorer par le partage de renseignements, la détermination des menaces en matière de cyber criminalité.
- Dans le cadre de son action globale de prévention, le gouvernement a alloué plus de £650m pour la mise en place d'un National Cyber Security Programme.
- La National Fraud Authority : cette agence publique dépendante du Home Office qui comprend des représentants de l'administration et de la société civile, a pour objet de prévenir et de lutter contre la fraude en général, en partenariat avec des industriels. Elle a mis en place des campagnes publicitaires pour la lutte contre les comportements cybercriminels et contre la fraude on line telle que celle intitulée « the devils in your details » qui informe les particuliers sur les précautions à prendre pour assurer la protection de leurs données personnelles[ref] On peut encore citer :[/ref].

Le Brésil envisage de réaliser, sous la direction du gouvernement fédéral, une campagne nationale d'éducation sur la sécurité et la défense cybernétique pour élever le niveau de prise de conscience de la société brésilienne sur ce sujet. Il existe des organes spécialisés dans la sécurité cybernétique placés auprès des hautes institutions étatiques : la Présidence de la République et la Casa Civil (équivalent du premier ministre).

Auprès de la Présidence de la république :

Le Cabinet de sécurité institutionnel de la Présidence de la République (Gabinete de segurança institucional da presidência da - GSI-PR).

Le GSI-PR est l'organe de la présidence de la république chargé de la coordination dans le cadre des sujets stratégiques qui affectent la sécurité de la société et de l'État. Sous son égide a été élaboré un livre vert sur la sécurité cybernétique visant à effectuer un certain nombre de propositions de mesures à adopter dans ce domaine.

Pour effectuer cette coordination, le GSI-PR a dans sa structure organisationnelle trois organes subordonnés, listés ci-dessous :

- Le Département de sécurité des informations et communications (Departamento de segurança da informação e comunicações - DSIC).
- L'Agence brésilienne d'intelligence (Agência brasileira de inteligência - Abin).
  Cette agence a comme objectif stratégique le développement des activités d'intelligence pour la défense de l'Etat. S'agissant de cybernétique sa mission est d'évaluer les menaces internes et externes.
- Le Centre de recherche et de développement qui cherche à promouvoir la recherche scientifique et technologique appliquées aux projets de sécurité et de communication.

Auprès de la Casa Civil :

Fonctionne l'institut National de Technologie et d'Information (ITI), qui est chargé de depuis 2001, de développer au Brésil un système national de certification digitale et de dématérialisation des procédures administratives (tel que le processus en cours de développement auprès du pouvoir judiciaire Brésilien).

Aux Etats-Unis, la prise en compte des enjeux de la cybercriminalité a amené la maison blanche à tenter de mettre en place une politique publique interministérielle fondée sur la prévention et une meilleure collaboration public/privé. Ces politiques publiques se heurtent cependant à deux défis : l'internationalisation croissante du phénomène et la question de la cyber preuve. La politique de prévention de la cybercriminalité est une priorité politique de l'administration Obama qui focalise son programme sur les 3 axes suivants : réduction du risque, réduction de la vulnérabilité, réponse aux intrusions.

- La réduction du risque passe par le développement de campagnes de sensibilisation du public qui implique la formation des citoyens américains en matière de cybersécurité, la mise en place d'un partenariat avec le secteur privé et la coopération internationale en ce domaine.
- La réduction de la vulnérabilité passe par la protection du « cyber espace[ref] Le cyberespace a été défini dans la *National Security Presidential Directive* n°54 comme le réseau interdépendant d'infrastructures technologiques de l'information, réseau qui comprend Internet, les réseaux de télécommunication, les systèmes informatiques ainsi que les processeurs intégrés et les régulateurs dans les industries concernées.[/ref] ». Les Etats-Unis ont connu plusieurs échecs dans leur lutte contre la cybercriminalité (arrêt d'usines électriques, coupures électriques dans les villes, processeurs de paiement compromis et transactions bancaires frauduleuses depuis 130 automates dans 49 villes pendant 30 secondes, pertes systémiques, touchant la propriété intellectuelle) engendrant des milliards de dollars de perte. La « cybersécurité » est ainsi devenue une priorité nationale.
- La réponse aux intrusions est une compétence des services d'enquête mais suppose de développer des liens importants avec le secteur privé notamment dans le rapport des infractions dont ils ont été victimes et dans l'assistance des agents de police judiciaire. Les victimes commerciales ont un intérêt réel à rapporter aux services de police judiciaire les infractions liées à la cybercriminalité dont elles ont été victimes mais elles se montrent souvent réticentes à le faire en raison de la répercussion de cette publicité sur leur clientèle.

3-2 L'aide aux victimes

En Espagne et au Royaume-Uni, un effort particulier porte sur l'information des victimes et de

nombreuses campagnes de sensibilisation sont menées, notamment auprès des entreprises, lesquelles sont le plus souvent réticentes à poter plainte. Ces opérations de sensibilisation sont menées en Espagne par les autorités de police et au Royaume-Uni par le National Fraud Authority's Action Fraud. Au Royaume-Uni, le système judiciaire dans son ensemble (juges, jury, avocats) n'apporte pas une aide précieuse aux victimes, en raison de certains particularismes liés à la cybercriminalité, en particulier la complexité des procédures. Aux Pays-Bas, un site Internet interactif permet au public de signaler tous les faits en rapport avec les domaines cités, en complément d'une ligne téléphonique (ligne verte).

Espagne : La sensibilisation des citoyens espagnols à la cybercriminalité s'est faite sur plusieurs fronts. Sont particulièrement visés par les politiques de sensibilisation les mineurs et les entreprises.

D´abord, la police espagnole mène des campagnes de sensibilisation dans les établissements scolaires. D´après le rapport 2011 du Parquet général de l´Etat, 12 % des procès qui ont eu lieu en rapport avec l´usage des NTIC ont eu pour objet la pornographie infantile.

Ensuite, les entreprises espagnoles et notamment les banques sont des destinataires privilégiés des campagnes de sensibilisation contre la cybercriminalité. Peu enclins à dénoncer les cyber-attaques dont elles sont victimes pour raison de prestige.

Royaume-Uni : Le National Fraud Authority's Action Fraud permet aux victimes de porter plainte pour les cyber crimes qu'elles ont subis. La victime d'un cyber crime devra introduire une action au civil si elle souhaite obtenir réparation. On constate une certaine réticence des entreprises à poter plainte contre des faits de cybercrimalité prévus par le Computer Misuse Act en raison de la mauvaise publicité qui en résulterait quant à la fiabilité de leur système de sécurité en matière informatique. En outre les juges et avocats méconnaissent souvent les spécificités de l'informatique et le jury a tendance, pour les infractions jugées par indictment, à considérer les Hackers comme des « Robin des bois » luttant contre un système de communication vécu comme intrusif et donc attentatoire aux libertés fondamentales.

Allemagne : L'aide aux victimes est de manière générale peu développée en Allemagne, et il n'y a pas de politique particulière d'aide aux victimes de la cybercriminalité. Le puissant syndicat professionnel BITKOM, regroupant les entreprises exerçant dans le secteur des télécommunications, de l'internet et des médias, se consacre notamment à la sécurité informatique.

Chine : La politique d'aide aux victimes en Chine n'est pas aisée en général. Cependant, en matière de cybercriminalité, dès lors qu'elle porte atteinte aux intérêts de l'économie et du consommateur, la victime peut y trouver sa place. Nous avons vu ainsi récemment de grandes campagnes d'indemnisation des victimes d'escroqueries commises en ligne (protection de l'e-commerce).

3-3 Les stratégies à l'international

Allemagne : Bien que la cybercriminalité soit un dossier interministériel, c'est le ministère fédéral de l'intérieur qui joue le rôle principal dans les négociations européennes et internationales. On relèvera que l'impossibilité de rechercher des données de communication antérieures à la date d'une mesure ordonnée par l'autorité judiciaire se traduit par la non-transposition de la directive européenne 2006/24/CE du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications. Cette

situation a conduit la Commission européenne à engager fin mai 2012 contre l'Allemagne une procédure en manquement devant la Cour de Justice de l'Union Européenne. Le cadre juridique allemand peut donc être considéré comme plus restrictif que celui existant en France, et moins favorable à l'efficacité des enquêtes, ce qui est parfois source de difficultés dans l'exécution des demandes d'entraide ou CRI émanant de magistrats français.

Espagne : L´unification des services d´enquêtes dédiés à la cybercriminalité (policia y guardia civil) est prévue pour 2014. La Convention de BUDAPEST sur la cybercriminalité a été ratifiée par l´Espagne en 2010. Elle contient des dispositions importantes (article 16) sur la transmission à la justice des données informatiques ou téléphoniques par les opérateurs privés (facebook, google). A l'heure actuelle et contrairement au Portugal, l'article 16 de cette convention n'a pas fait l'objet de transposition dans la législation interne espagnole. Pourtant, aux dires de la Procureure Générale, la lutte contre la cybercriminalité y gagnerait en puissance.

Royaume-Uni : Au niveau international, la SOCA (Serious Organised Crime Agency) a des représentants dans différents pays qui œuvrent dans le cadre de la coopération pénale internationale. De plus, la SOCA coopère avec l'ICANN (The Internet Corporation for Assigned Names and Numbers) et participe au Commonwealth Cybercrime Initiative ainsi qu'à différents forums internationaux tels que The UN Group of Government Experts, the World Economic forum ou encore l' OSCE (Organization for Security and Co-operation in Europe) Le Royaume-Uni fait partie de la Convention de Budapest relative à la cybercriminalité qui permet de lutter contre la criminalité internationale sur internet.

Pays-Bas : Il convient de noter que, dans le domaine international, les Pays-Bas soutiennent et contribuent activement aux efforts suivants: calendrier numérique de l'UE pour la Sécurité stratégique, politique de cyber défense de l'OTAN, Forum sur la gouvernance Internet. Les Pays-Bas plaident, en outre, pour une large ratification de la Convention du Conseil de l'Europe sur la cybercriminalité. Les pouvoirs publics néerlandais entendent se concentrer sur le renforcement de la coopération dans le cadre de réponses opérationnelles entre membres du CERT, renforcer le IWWN (international watch and Warning network) qui fonctionne comme un forum informel pour les incidents globaux. Le gouvernement entend aussi encourager davantage les enquêtes transnationales avec une implication des autres agences européennes et des partenaires internationaux.

Chine : L'entraide pénale en matière judiciaire n'est pas fluide avec la Chine même si les échanges et la communication sont de meilleure qualité qu'avant. La prise en compte des dossiers par la partie chinoise (ministère de la justice et ensuite ministère de la sécurité publique) reste globalement assez lente et il faut souvent adresser des relances. Dans ce contexte, les « cyber crimes » ou les infractions commises par la voie de l'internet, qui nécessitent par excellence un traitement rapide, ne bénéficient pas de la toute la réactivité qui devrait être de mise. La majorité des dossiers en lien avec la cybercriminalité sont des affaires où l'internet est l'instrument qui a facilité la perpétration d'infractions de droit commun (par exemple les escroqueries par faux ordres de virement au préjudice de sociétés françaises). Des sommes illégalement détournées ont pu néanmoins être saisies dans plusieurs dossiers, témoignant d'une meilleure compréhension et d'une meilleure coopération.

Brésil : Au plan international, le Brésil n'est pas signataire de la Convention du Conseil de l'Europe sur la Cybercriminalité. Toutefois, il convient de relever qu'un partenariat a été initié avec les Etats-Unis dans ce domaine, dans le cadre du « International Strategy for Cyberspace »

(http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf).

Etats-Unis : Le défi de l'internationalisation des enquêtes et de la cyber-preuve font qu'un grand nombre d'infractions pénales ne sont aujourd'hui pas sanctionnées aux Etats-Unis du fait de la quasi impossibilité d'identifier ou de poursuivre les auteurs d'un cyber-crime. C'est très souvent le cas parce que l'infraction a été commise depuis un Etat tiers, qui n'exécutera pas de demande d'entraide américaine, ou qui l'exécutera de manière incomplète et tardive. La coopération pénale internationale est donc une des clés pour identifier et lutter contre certains groupes criminels. Elle se heurte cependant aux réticences des Etats-Unis à mettre en place des équipes communes d'enquête : pour des raisons juridiques, aucune ECE n'a ainsi été mise en place entre les enquêteurs américains et leurs homologues étrangers. Mais l'enjeu de la coopération pénale est aussi celui des réponses des Etats-Unis aux requêtes des pays étrangers. En effet, au delà des infractions visant spécifiquement l'utilisation d'un matériel ou d'un réseau informatique, les enquêteurs de tous les pays sont, comme en France, de plus en plus confrontés au développement rapide des éléments de preuve stockés dans les réseaux informatiques. En effet, un grand nombre d'infractions sont commises sans aucun lien avec les réseaux informatiques. Mais l'utilisation des courriels et des réseaux sociaux est devenue tellement quotidienne que la plupart des enquêtes impliquent d'obtenir le contenu des courriels ou des échanges sur la plupart des sites d'échange, de Facebook à Twitter. Or, les critères pour obtenir ces messages sont très stricts en droit américain : il faut démontrer qu'il existe une « probable cause » que le média ou la boîte courriel contient des informations essentielles pour une enquête qui ne peuvent être obtenues par un autre moyen moins attentatoire aux libertés. Ces flux de demandes d'entraide produits par la « digitalisation » de la vie quotidienne sont aujourd'hui traités avec difficulté du fait de la masse à gérer par le ministère de la justice américain : le formalisme des demandes d'entraide et du recours au débat contradictoire devant un juge se heurte à un nombre croissant de requêtes étrangères. Des négociations internationales devront ainsi sans doute s'engager à moyen terme pour dépasser la convention de Budapest, signée par les Etats-Unis, et fluidifier l'accès des services d'enquêtes à des informations qui ont été enregistrées dans leur pays, par des ressortissants de leur nationalité. Mais une telle évolution impliquerait de prendre en compte non pas le lieu où les données sont stockées, mais le lieu où les données ont été transmises ab initio, ce qui n'est aujourd'hui pas possible dans l'Etat actuel des conventions internationales.