Incidence du web 3.0 et du web 4.0 sur la cybercriminalité

2012

Droit pénal spécial

Adam Lamzourhi & Nicolas Saïdi-Cottier

Université Paris Ouest Nanterre La Défense

Cours de Monsieur Joël Ferry

Master 2 Droit des NTSI Univ- Paris-X

master 2 pro droit des NT|SI

[Sujet : Incidence du Web 3.0 et du Web 4.0 sur la cybercriminalité]

Table des matières

Sujet de rapport : Incidence du Web 3.0 et du Web 4.0 sur la cybercriminalité

> *«L'internet des objets qui intègre l'intelligence dans les objets de tous les jours est le prochain grand événement qui nous attend. Je souhaite encourager un internet des objets au service de nos objectifs économiques et sociaux tout en préservant la sécurité, ainsi que le respect de la vie privée et des valeurs éthiques».*
>
> Madame Neelie Kroes, vice-présidente de la Commission européenne,
> Responsable de la stratégie numérique.

Introduction

La numérisation, la convergence et la mondialisation permanente des réseaux informatiques entrainent de profonds changements dans la société de l'information. A l'heure actuelle, une grande partie de la population est connectée à Internet et utilise au quotidien les outils informatiques. Les réseaux sociaux et les blogs permettent aux internautes de s'exprimer et de partager de l'information. Les moteurs de recherches permettent l'accès à une masse de données considérables allant du simple site de rencontres, au site de propagande de la terreur.

La cybercriminalité désigne l'ensemble des infractions pénales commises à partir des réseaux informatiques. Elle regroupe des infractions très diverses en lien avec les nouvelles technologies de l'information et de la communication ou avec les systèmes de traitement automatisé de données. Plus largement, ce terme désigne à la fois, différentes catégories d'activités criminelles allant de la criminalité « traditionnelle » adepte de l'escroquerie en ligne et de la falsification de documents jusqu'à la diffusion de contenus illicites, notamment des contenus pédopornographiques, ultraviolents ou protégés par le droit d'auteur, en passant par les infractions propres aux réseaux informatiques telles que le piratage, les cyberattaques et le déni de service. Les expressions Web 3.0 et web 4.0 ne sont pas clairement définies. Il s'agit de termes utilisés en futurologie à court et moyen termes pour désigner le développement futur du World Wide Web, les prochaines transformations majeures que connaitra Internet.

Ainsi, nous utilisons actuellement le Web 2.0. Au-delà de l'aspect marketing, ce terme désigne l'Internet liant les personnes (blogs, forums, réseaux sociaux…) qui succède à la première version du Web 1.0, née il y a plus de 20 ans, celle liant les pages Web entres elles, à partir d'hyperliens. Donc, le Web 3.0 est la prochaine transformation majeure d'Internet. Bien que ce terme ne soit pas clairement défini, pour beaucoup il s'agit de l'Internet des objets (IdO), ou encore du web sémantique. Le Web 4.0 quant à lui, poursuit le développement d'Internet et pourrait, d'une certaine manière, être ce que certains utilisent déjà, le *Cloud Computing* ou l'informatique dans le nuage.

Néanmoins, il ne s'agit que de suppositions de spécialistes, l'avenir le dira. L'unique certitude est qu'une fois encore, cette nouvelle évolution d'Internet, ouvrira au passage, une brèche par laquelle certains délinquants seront tentés de passer.

Dans ce rapport, le web sémantique, l'Internet des objets et le *Cloud Computing* seront largement traités, il convient donc d'en donner leurs définitions et leurs sens. L'Internet des objets va permettre aux objets du quotidien de disposer d'une connexion sans fil à Internet à partir de puces (RFID) capables de collecter et transmettre un flux de données. Si, de nos jours, un internaute moyen dispose d'au moins deux objets[1] connectés à Internet, il pourrait en avoir sept en 2015. A l'échelle planétaire, cela reviendrait à près de 25 milliards de dispositifs avec une connexion sans fil, voir le double en 2020.

Les objets connectés pourraient être de toutes sortes, comme les voitures, les téléphones, les appareils électroménagers, les vêtements et même les aliments. Une fois de plus, l'aspect marketing sera important, les gens auront envie de bénéficier de nouveaux services sans pour autant que la sécurité soit garantie. Par exemple, la machine à café pourrait s'allumer le matin en fonction de l'heure où sonne le réveil. Une voiture connectée qui ferait un accident pourrait alerter les secours qui se rendraient sur place. Un cran au-dessus, un homme « connecté » à Internet pourrait être surveillé à distance. Dit comme cela, il est vrai que l'on pourrait penser aux bracelets électroniques des délinquants en liberté conditionnelle et se demander quel est l'intérêt pour le consommateur. Or, le concept attire, certains développent actuellement des puces pour les humains, munies d'accéléromètres elles pourraient alerter les secours en cas de chute à la maison ou d'arrêt cardiaque.

Le Web sémantique est l'Internet des machines qui formalisent, traitent et peuvent utiliser de manière autonome les données qu'elles hébergent grâce à un système de Métadonnées et à l'interconnexion des écosystèmes de données déjà existants et ceux à venir. Les applications devront s'affranchir des paramètres de supports, des différents systèmes d'exploitation (Windows, Linux…) et de tout matériel. Il s'agirait d'un web « intuitif » et pragmatique qui ne se limiterait plus à offrir des liens après une requête à partir de mots clés, mais il contextualiserait ces réponses en fonction du profil de l'internaute.

Le *Cloud Computing* ou informatique dans le nuage consiste à déporter sur des serveurs distants des stockages et des traitements informatiques habituellement localisés sur des serveurs locaux ou sur le poste de l'utilisateur. Elles sont ensuite stockées et accessibles depuis n'importe où, à la condition d'avoir une connexion internet. Il pourrait presque être qualifié de libre-service de données et de ressources informatiques.

Toutes ces nouvelles adaptations des services du World Wide Web risquent de s'accompagner d'une croissance du nombre de cyberdélinquants capables d'utiliser les outils mis à leur disposition par la société de l'information à des fins de profits.

[1] Souvent l'ordinateur et le Smartphone

Quelles seront les formes de la cybercriminalité qui risquent de sévir dans l'univers numérique et le Web de demain ? Comment la lutte contre cette cyberdélinquance pourrait-elle s'organiser face à une masse d'informations aussi imposante ?

Le développement du Web 3.0 et du Web 4.0 ou plutôt de l'Internet des objets et du web sémantique risque d'être accompagné de l'évolution de la criminalité. En effet, ce développement s'accompagne d'une modification du comportement du cybercriminel. Face à une société qui s'appuie sur les réseaux de l'information, les atteintes et les intrusions dans les STAD risquent d'être nombreuses (I), tout comme les infractions liées à l'usage de l'Internet des objets (II), ou encore celles qui s'appuient sur l'architecture du Cloud Computing (III). On risque également d'assister à l'apparition de nouvelles formes d'infractions sur les réseaux informatiques (IV). Afin de renforcer la confiance des utilisateurs dans ces transformations majeures d'Internet, ces dernières devront s'appuyer sur des moyens de prévention et de lutte contre la cybercriminalité renforcés (V).

I. Les atteintes aux STAD dans un monde de Métadonnées

Les métadonnées sont des informations structurées servant à décrire une ressource. Ces informations sur l'information peuvent faciliter l'échange de données structurées entre ordinateurs. Encore invisibles et inconnues pour les utilisateurs moyens, les technologies du web sémantique permettent à des milliers de bases de données dans le monde de s'interconnecter les unes aux autres et d'agréger ainsi une masse d'informations. Le web sémantique permet de donner du sens aux données accessibles à partir d'Internet afin de les partager plus efficacement. Ainsi, par exemple, dans le secteur médical, il permet une centralisation des données personnelles d'un patient. Dès lors ces grands systèmes de données risquent d'être la cible de l'activité cybercriminelle qui pourrait tenter de s'y introduire ou de les modifier afin de collecter un maximum d'informations sur leurs futures victimes, qu'ils s'agissent d'individus, de grands groupes industriels ou encore des gouvernements étatiques et de leurs différentes institutions. Cette nouvelle version d'Internet risque donc d'être succédée par des problèmes liés à la collecte de données sur Internet et d'intrusion dans les STAD (A), qui entraineront probablement une recrudescence des usurpations d'identité (B), des atteintes à la vie privée mais aussi des abus de confiance et des escroqueries en ligne de plus en plus sophistiqués (C).

A- La collecte de données à caractère personnel et la recherche frauduleuse d'informations

Internet ignore les frontières de l'État, c'est un espace d'expression difficile à réguler et à maîtriser. Étant un internet plus intuitif, le web sémantique s'appuiera sur des gigantesques bases de données et de métadonnées pour offrir aux internautes des réponses à leurs requêtes de plus en plus pertinentes.

Ces grandes bases de données pourraient être extrêmement vulnérables aux intrusions de cybers délinquants de plus en plus expérimentés, qui exploitent au maximum toutes les failles des systèmes informatiques.

Les cybercriminels seront tentés de s'introduire frauduleusement et à distance dans ces grands systèmes de traitements automatisés de données afin d'accéder frauduleusement à tout un tas d'informations. Cette collecte leur permettrait de s'organiser dans la préparation d'infractions en tout genre. La recherche du profit ou du pouvoir pourrait pousser certains individus à récolter frauduleusement des informations afin par exemple de connaître les faiblesses de différentes infrastructures.

Ainsi, si dans un avenir proche, beaucoup de sociétés risquent d'utiliser le web sémantique afin d'accélérer leur activité, il est probable que certains délinquants vont tenter de récolter les informations relatives aux données à caractère personnel des clients, ou sur leur système de sécurité afin de préparer des infractions assez complexes.

Prenons le cas d'une banque, ou bien encore d'une société de convoyeurs de fonds, imaginons que certains criminels accèdent aux informations relatives aux horaires du personnel, à leur adresse, au service de sécurité, ils pourraient préparer des infractions avec une longueur d'avance, avec une totale maîtrise des différents paramètres. Les cybercriminels pourront également perfectionner l'ingénierie sociale et l'on pourrait assister à l'avènement des problèmes d'usurpations d'identité, tant sur Internet que dans la société. Les escroqueries et abus de confiance en ligne risquent d'être de plus en plus sophistiqués et pourraient aboutir à une confusion totale des internautes.

B- Les problèmes d'utilisation des données personnelles, notamment l'usurpation d'identité

Le web sémantique et les réseaux sociaux offriront une véritable mine d'or d'informations relatives aux internautes pour les délinquants informatiques. Une analyse prospective dans ce domaine laisse imaginer une multitude d'atteintes possibles à l'identité numérique. Les principales données récupérées seraient, sûrement, en pole position, les données bancaires des internautes mais aussi tout une série d'informations relatives à la vie privée allant de la liste d'amis à l'historique de navigation ainsi qu'au dossier médical personnel de certains.

De plus si toutes ces bases de données sont interconnectées afin d'être compilées, il sera encore plus facile de venir puiser le flux d'informations à la source, dans sa globalité. Le web sémantique pourrait donc permettre des usurpations d'identité ultra perfectionnées. Les cybercriminels pourraient créer des faux profils mais aussi ouvrir des comptes en banques, obtenir des papiers d'identité voir frauder la sécurité sociale. Dès aujourd'hui, des millions de coordonnées bancaires sont en ventes sur Internet. Les échanges sur Internet se multiplient, les outils d'information et de communication sont au centre de toutes les attentions.

Ces recherches sur les données à caractère personnel des internautes permettraient aux criminels d'exploiter les faiblesses humaines des internautes en faisant régner une confusion générale. Le spamming, le phishing et autres attaques ciblées pourraient être encore plus précises et cela pourrait aboutir au triomphe de l'escroquerie numérique et de l'abus de confiance.

C- Les problèmes d'escroquerie et d'abus de confiance en ligne

Le web sémantique permet d'innombrables possibilités d'usages abusifs et illicites des données personnelles des internautes pour les cybercriminels. Parmi ces usages abusifs, on retrouve un phénomène fréquent qui est l'escroquerie en ligne. Ces pratiques risquent d'être facilitées par la collecte d'informations. Face à des systèmes informatiques de plus en plus sécurisés, les pirates risquent de se tourner vers les faiblesses « humaines ». Ainsi, l'utilisation massive des courriels comme mode de correspondance risque d'être accompagnée de nombreux spam et *phishing* ou hameçonnage. Le *phishing* par courriel risque d'être de plus en plus présent dans les cas d'escroquerie en ligne. Les cybercriminels seraient tentés de se servir de toutes les informations qu'ils pourraient collectées notamment des sites de vente en ligne et des réseaux sociaux. Ces courriels seraient de plus en plus crédibles et pourraient pousser les individus à tomber dans un « panneau ultra-réaliste » et les transformer en victimes d'escroquerie.

La victime étant dans une confusion totale, elle pourrait ne plus savoir discerner le courriel authentique du courriel vicié. La centralisation des données et leur accessibilité permettraient également d'adapter l'escroquerie au comportement des individus. Par exemple, en cas de création de sociétés ou d'associations, les cybercriminels pourraient adresser des factures et imposer des taxes factices directement au domicile des gérants qui pourraient penser avoir affaire à un document officiel.

Le cas de l'internaute qui recevrait un mail d'un de ses proches pour lui demander de l'argent car il se trouve dans une situation particulière est également envisageable. C'est par exemple la création d'un faux profil totalement identique à l'original sur les réseaux sociaux ou l'atteinte à la vie privée. Les cybercriminels qui auraient récolté des données sensibles dans ce web sémantique seraient également tentés de faire chanter leurs victimes afin de leur soutirer un maximum d'argent voir d'autres informations. Le web sémantique n'est qu'une facette du web 3.0 et du web 4.0, l'Internet des objets y tient aussi une place importante et risque donc d'attirer l'activité criminelle.

II. La cybercriminalité et l'Internet des Objets

Comme évoqué plus haut, l'Internet des Objets est la prochaine évolution majeure d'Internet, beaucoup l'assimilent au Web 3.0. Le terme Internet des objets permet de désigner la situation où une multitude d'objets disposent de connexion sans fil à Internet. Tous les objets de la vie quotidienne pourraient être connectés ou connectables et permettre une convergence. Ainsi, d'ici à 2020, il pourrait y avoir près de 50 milliards d'appareils et machines connectés à Internet. Autant de portes ouvertes pour des futures tentatives d'intrusions ou d'attaques. Par exemple la voiture connectée pourrait contourner les embouteillages et les accidents sur Internet. Les Smartphones permettraient eux de gérer le contenu de son frigidaire, ses alarmes ou encore les volets de son domicile. L'avènement de l'Internet des objets s'accompagnera probablement d'une multitude d'infractions parfois nouvelles, ou tout simplement d'anciennes pratiques rendues plus efficaces en raison du nombre d'objets connectés. La géolocalisation de tous ces objets ne doit pas aboutir à des atteintes aux libertés fondamentales des individus.

A- L'avènement des réseaux *botnets* en raison d'un nombre de machines colossal

L'Internet des objets permettra à la quasi-totalité des objets du quotidien de disposer d'un accès à Internet à partir de puces intelligentes et de collecter et de transmettre un nombre important de données. Les réseaux Botnets pourraient lever une armée de PC « zombies » afin de préparer d'éventuelles cyberattaques allant du simple *spam* au contrôle total et distant de la machine infectée. En moins d'une semaine, un pirate informatique peut réussir à prendre discrètement le contrôle de milliers de PC « zombies » distribués à travers la toile planétaire, formant ce que l'on va appeler, un « *bottom network* » ou, « *Botnet* » prêt à être utilisé pour des cyberattaques en tout genre. Si l'on multiplie la menace par le nombre de machines qui seront connectées d'ici 2020, il est normal de s'inquiéter de ce qui pourrait se produire en cas de « cyber guerre » ou encore en cas de virus informatique planétaire (codes malicieux). La motivation des pirates pourrait être d'ordre économique. En effet, les services d'une armée « *Botnet* » peuvent se louer à la semaine moyennant finance[2]. Les cybercriminels peuvent conduire en toute impunité une campagne de spamming sans que l'on s'en rende compte bien souvent. Leur but est de paralyser les serveurs de messagerie des grandes entreprises par l'importance du trafic.

Au-delà de l'aspect financier, l'utilisation de ces armées de PC infectés peut également jouer un rôle politique afin de lutter contre la censure ou les atteintes à la liberté d'expressions[3] ou afin d'appuyer une propagande. Cette quantité de PC infectés permet des

[2] À partir de moins de 500 $ la semaine de location pour près de 150 000 PC « zombies » infectés.
[3] Comme ce fut le cas dans l'exemple du Printemps arabe en Égypte et en Tunisie.

résultats impressionnants lors des attaques par déni de service ou encore en force-brute pour déchiffrer des messages et des informations confidentielles et protégées.

B- L'apparition de nouveaux comportements et de nouvelles infractions en rapport avec l'Internet des objets

L'internet des objets permettra la mise en réseau de milliards d'appareils et de machines capables de dialoguer et d'interagir par le biais de technologies sans fil, combinées à des protocoles d'adressage logique et physique. On peut donc très bien imaginer que les cybercriminels arriveraient à contrôler à distance ces objets connectés au Web. Alors que se passerait-il si un individu arrivait à prendre le contrôle de mon véhicule à distance ? Et si le cyber délinquant parvenait à utiliser à distance mon Smartphone qui sert très souvent de moyen de paiement ?

Imaginons qu'il soit nécessaire de disposer d'une puce RFID pour pénétrer dans un lieu. Il ne fait aucun doute qu'une partie de la criminalité informatique s'intéresserait au contenu de ces puces et tenterait de le dupliquer. Encore plus inquiétante serait la possibilité de bloquer quelqu'un chez lui à distance ou encore de paralyser son système anti incendie. Avec l'Internet des Objets, il risque d'y avoir encore plus d'interférences entre le monde réel et le monde numérique d'Internet. Ainsi, s'il devenait possible de détourner l'itinéraire programmé d'un véhicule connecté, peut-être assisterions-nous à des nouveaux styles de guet-apens où le chauffeur serait dirigé directement dans la « gueule du loup » croyant échapper à des embouteillages.

Les cambriolages prendraient une nouvelle dimension : grâce à tous ces objets connectés, il sera possible de déduire si quelqu'un est présent dans le domicile. Mais il serait aussi plus facile de les réprimer si par exemple les objets volés contenaient des puces avec une balise GPS permettant de localiser et d'arrêter l'organisation criminelle à l'origine du délit.

C- Les intrusions dans ces objets

L'Internet des objets doit être capable de mettre en confiance l'utilisateur pour qu'il adhère à cette nouvelle adaptation du Web. Pourtant, beaucoup d'interrogations existent sur la gouvernance de l'Internet des Objets. Que deviennent toutes ces données collectées par nos objets de la vie quotidienne ? Est-ce que cela peut aboutir à un espionnage généralisé de la population ? Et si oui alors, à qui cela profite-t-il ?

La cybercriminalité est variée, elle peut prendre diverses formes et avec autant d'objets connectés, on risque bien de se retrouver espionné à son insu. La géolocalisation

permet de savoir où se situe géographiquement un individu à partir d'une balise GPS utilisée par son Smartphone par exemple. Il serait peut-être possible d'accéder au contenu des différents objets en créant différentes passerelles indétectables pour l'utilisateur. L'espionnage industriel pourrait s'appuyer sur l'IdO afin d'être plus efficace, les objets connectés pourraient rapidement devenir les nouvelles failles des grands groupes industriels en matière de confidentialité des données. Il est probable que les possibilités d'interception seront encore plus nombreuses.

Si l'IdO (Internet des Objets) et le Web sémantique sont des facteurs de développement de la cybercriminalité, il convient de rappeler que c'est aussi le cas du *Cloud Computing* ou informatique dans le nuage.

III. Les problématiques liées au *Cloud Computing*

Le concept d'informatique dans le nuage ou *Cloud Computing* est un nouveau service d'Internet. Il s'agit du concept qui consiste à déporter sur des serveurs distants des stockages et des traitements informatiques traditionnellement localisés sur des serveurs locaux ou sur le poste de l'utilisateur. Les utilisateurs et les entreprises ne sont plus gérants de leurs serveurs informatiques mais peuvent accéder à de nombreux services en ligne sans avoir à gérer l'infrastructure sous-jacente, souvent jugée trop complexe. Les applications et les données ne se trouvent plus sur l'ordinateur local mais dans un nuage composé d'un certain nombre de serveurs distants interconnectés au moyen d'une excellente bande passante indispensable à la fluidité du système. L'accès au service se fait à partir d'un navigateur Internet ou d'une application standard. Il est largement probable que les cybercriminels profiteront du développement de l'informatique dans le nuage et s'intéresseront au service d'informatique dématérialisé afin de réaliser des infractions sur les réseaux informatiques. En effet, il ne fait aucun doute que la cybercriminalité s'appuie largement sur les technologies émergentes telles que le *Cloud Computing*.

A- Les technologies émergentes de *Cloud* attirent la cybercriminalité

Grâce à l'informatique dans le nuage et ses infrastructures, les cybercriminels risquent d'exploiter les données hébergées et de faire des infractions informatiques à distance, en préservant un peu plus leur anonymat. Ainsi, les services de Cloud sont des très bons moyens d'émettre du spam à très grande échelle notamment par l'importance de la bande passante du service. L'informatique dans le nuage permettrait aussi aux cybercriminels de s'introduire au cœur des entreprises qui utilisent le *Cloud* mais à distance. Il serait possible de paralyser les services de Cloud afin d'affaiblir un concurrent dans le domaine des affaires qui utiliserait cette technologie pour sous-traiter une partie de son activité.

Le côté anonyme et distant du *Cloud* risque d'attirer l'activité criminelle, tout comme la confidentialité des données. Les fournisseurs de services de *Cloud* doivent mettre en place tous les moyens nécessaires pour s'assurer que les données qui leur ont été confiées restent

bien dans le nuage et que personne n'y accède à l'insu de leur propriétaire légitime. Étant donné que cette règle est valable, également pour les administrateurs du fournisseur de service de *Cloud,* il y a très peu de chance de pouvoir empêcher le stockage d'un fichier malicieux dans le nuage.

B- Un risque d'infractions informatiques en rapport avec le contenu diffusé

Les services de Cloud pourraient peu à peu remplacer les échanges de pair-à-pair sur Internet et permettre ainsi une large diffusion de contenus illicites, allant des œuvres protégées par le droit d'auteur et les droits voisins jusqu'à la diffusion de contenus ultraviolents, incitant à la haine ou encore de la diffusion de contenus pédopornographiques. L'exemple de *megaupload* illustre bien le problème de l'informatique dans le nuage. Comment garantir que les données hébergées respectent les différentes législations alors qu'en principe, il semble impossible de les contrôler. Il est donc logique que les cybercriminels se tournent vers ce nouveau système d'échanges pour partager leurs contenus illicites.

Les services de *Cloud Computing* pourraient également servir à la diffusion d'informations protégées et dont la révélation constituerait des atteintes à la sureté nationale, des violations et des atteintes au secret défense. Imaginons que l'entreprise *Wikileaks* ait eu un service de *Cloud Computing*, ces révélations auraient pu être accessibles depuis Internet et de façon beaucoup plus discrète en permettant ainsi d'éviter la révélation des sources.

C- Le déni de service transposé dans une société totalement dépendante d'Internet

Les services de l'informatique dans le nuage risquent aussi d'offrir aux cybercriminels les moyens de réaliser des attaques par déni de service ou des attaques par force brute.

Ainsi, pour paralyser les systèmes informatiques hébergés sur les services de Cloud, les cybers délinquants vont lancer des attaques par déni de service directement contre le service afin de le perturber au maximum et donc, de perturber par la même occasion les entreprises.

Avec le développement des solutions de virtualisation, on risque d'assister de plus en plus à l'émergence de réseaux de zombies (« botnet ») s'appuyant sur les techniques de virtualisation issues de l'informatique dans le nuage. Les « botnets » risquent d'évoluer de plus en plus et d'atteindre un fonctionnement modulable en fonction des attentes des cybercriminels.

Les attaques par force brute à partir des services de *Cloud Computing* sont assez intéressantes pour les cybercriminels. Ces plateformes disposent de capacités techniques (CPU) et de bandes passantes qui sont spécialement appropriées pour la force-brute. Cela

pourrait permettre la recherche d'identifiants de connexion à des comptes ou encore de prendre le contrôle de machines connectées mais insuffisamment sécurisés.

L'avantage de ce type d'attaques pour l'activité criminelle est qu'elles proviennent d'adresses IP valides et qu'il est donc très difficile de les bloquer.

IV. Vers des nouvelles formes d'infractions sur les réseaux

L'avènement des nouvelles technologies et d'Internet marque l'apparition d'une nouvelle forme de conflits qui a donné naissance à de nouveaux types de phénomènes tels la cyber guerre donnant lieu à des cyber conflits pouvant se manifester sous diverses formes, le cyber terrorisme, espionnage industriel (A) ou le blanchiment d'argent sur les réseaux informatiques (B).

A. Cyber guerre, cyber terrorisme et espionnage industriel

La brise de la cyber guerre soufflait déjà en mai 1996 lorsque le *General Accounting Office* avait rendu public un rapport intitulé *« Computer Attacks at Department of Defense Pose Increasing Risks »*. Ce rapport porte sur des problématiques sécuritaires qui sont toujours d'actualité en 2011 : les attaques contre les systèmes d'information du Département de la Défense américain, les menaces pesant sur les systèmes sensibles, la notion de menace grandissante, la dépendance du secteur de la défense, du gouvernement et du secteur privé par rapport à la technologie, les actions des h*ackers,* les atteintes à la sécurité nationale. Les termes utilisés en 1996 sont identiques aujourd'hui : risques, attaques, menaces, sécurité, *hackers*, complexité, rapidité, dépendance, croissance. Les cyberattaques récentes soulignent les anticipations et affirmations de l'époque, et rappellent également à quel point les problèmes demeurent, et ce en dépit des recommandations. Dès lors la sécurité parfaite n'existe pas, il faut dès lors impérativement assurer la sécurité de l'information et prendre conscience des vulnérabilités présentes, notamment des menaces constituées par les *hackers*, États étrangers, ainsi que des individus au sein même de nos organisations.

Au fil des années, les menaces se sont affirmées, les prédictions confirmées et les attaques concrétisées. Les États sont entrés dans une ère de conflits nouveaux, celle de la cyber guerre.

Aujourd'hui, la définition du cyber terrorisme n'est pas tout à fait claire. On peut considérer le cyber terrorisme comme du terrorisme appliqué au cyberespace. Néanmoins, d'après le dictionnaire et au sens courant, le terrorisme se réfère à l'emploi systématique de la violence pour atteindre un but politique.

Dès lors on peut se demander si l'arrêt éventuel de l'Internet ou d'une partie de l'Internet, suite notamment à des actes de malveillance, serait susceptible de provoquer la

terreur au sein de la communauté des internautes? De la population? Ne s'agirait-il pas le plus souvent, et jusqu'à présent de terrorisme économique visant à porter préjudice aux organisations qui réalisent des activités au travers de l'Internet?

Or, la cybercriminalité, peut revêtir une dimension terroriste, étant donné que les systèmes attaqués font partie d'infrastructures critiques. Autrement dit, les infrastructures nécessaires au bon fonctionnement des activités d'un État ou d'un pays telles que l'énergie ou les transports voient leur vulnérabilité augmentée par un recours de plus en plus fréquent des technologies sur Internet. Il faut souligner l'importance que revêtent les systèmes de production et de distribution d'électricité car ces derniers concourent au conditionnement du fonctionnement de la plupart des infrastructures. La prise de contrôle sur ces infrastructures critiques paraît être un des objectifs du cyberterrorisme.

Afin de déterminer si un acte cyber criminel relève du cyberterrorisme il faudrait dès lors étudier les revendications des cybercriminels et également être prudent quant à l'usage du terme "cyberterrorisme" qui s'est en effet répandu depuis le 11 septembre 2001. Dès lors, il faut se rappeler que les premiers dénis de services distribués (*distributed denial-of-service*) largement médiatisés furent le fait d'un adolescent de 15 ans surnommé Mafia Boy en date du 10 février 2000. Plusieurs mois plus tard, ce dernier fut appréhendé et identifié, malgré le fait qu'il n'ait pas expliqué publiquement la motivation de ces actes. Tout porte à croire que cette dernière n'était nullement politique. Si cette même attaque avait été réalisée postérieurement au 11 septembre 2001, aurait-elle également été qualifiée de cyberterroriste? De même, en l'absence d'éléments concrets, sans revendication ni auteur présumé d'une attaque, il paraît difficile de qualifier une attaque d'acte cyberterroriste. Il est souvent difficile d'opérer une distinction entre la fonction de la cible uniquement, et les motivations d'un attaquant. Ce dernier est-il une personne ou un groupe de personnes ? (Mercenaires, délinquants, escrocs etc…).

Le type d'agression informatique n'est pas suffisant pour déterminer avec certitude la motivation ou les objectifs d'un malveillant. Cela est une des difficultés de la lutte contre le crime informatique étant donné qu'il est nécessaire de disposer d'informations complémentaires pour caractériser l'intention criminelle.

Même si le cyberterrorisme paraît être un concept qui englobe une réalité assez imprécise dans le répertoire des nouvelles menaces, il n'en demeure pas moins pertinent et recouvre malheureusement une certaine réalité. La sécurité intérieure d'un pays doit aujourd'hui faire face à des formes d'expression de menaces criminelles en lien avec l'existence des technologies de l'information. Ces technologies de l'Information sont au coeur de la guerre de l'information (*infoguerre infowar*) dont les enjeux sont avant tout économiques et les impacts d'une grande importance pour le bon déroulement des activités. Internet concourt non seulement à la manipulation de l'information mais est également un outil privilégié pour répandre des rumeurs ou toute forme d'intoxication ou de campagne de déstabilisation.

Par ailleurs, les activités d'espionnage et de renseignement se retrouvent facilitées car il est désormais très aisé d'intercepter des informations qui ont été transférées sur Internet. Peu importe les moyens, que cela soit par des processus de déstabilisation économique, par la propagation d'idéologies, par de la manipulation d'information, ou par la mise en péril d'infrastructure critiques, le cyberterrorisme est véritablement une nouvelle forme de menace à ne pas sous-estimer. Au-delà de la dimension des systèmes informatiques symbolisés par

Internet, c'est la vie elle-même qui se retrouve menacée par l'atteinte directe à l'intégrité des personnes.

L'attaque et l'espionnage d'entreprises représentent une activité furtive, organisée et financée par des acteurs professionnels agissant davantage à l'image des entreprises légitimes qu'ils espèrent voler. Les *« abeilles ouvrières »* opèrent sans relâche avec du matériel informatique de pointe, plusieurs écrans et les volets bien fermés. Les patrons de ces dernières sont quant à eux, des personnes bien connectées, observant les faits et gestes de tous et gardant un œil constant sur leur objectif.

La raison de l'espionnage industriel est simple, elle est financière. Les « cyberespions » ciblent les données confidentielles des entreprises qu'ils peuvent par la suite revendre à l'enchérisseur le plus généreux. On peut distinguer deux catégories de « cyberespions »: la première catégorie se concentre sur le long terme avec des menaces avancées persistantes, alors que l'autre catégorie se concentre plus sur les gains financiers à court et moyen termes.

L'objet de ces opération est la menace avancée persistante notamment l'opération Aurora au courant des années 2009 et 2010 qui avait pris pour cible des géants américains du secteur des technologies de l'information, autrement dit Adobe et la firme de Mountain View (Google). Les « cyberespions » à l'origine de cette menace semblent être de nationalité Chinoise de nombreuses spéculations mentionnent une implication de l'État Chinois. L'Opération Aurora exploite une vulnérabilité nommé *zero-day* dans le navigateur Internet Explorer dans l'objectif de modifier le code source et de récupérer la ou les adresses IP des dites entreprises.

B. Le blanchiment d'argent sur les réseaux informatiques

Il a généralement lieu par le biais d'envoi d'emails dont l'objet est souvent « Travail dans une équipe internationale » ou « *Workathome* » ou « Nous avons besoin de représentants ». L'opportunité représentée par la possible embauche offerte dans ces courriers électroniques est très alléchante : travailler en tant qu'agent financier ou notamment chef de transaction financière, et ce pour seulement quelques heures par semaine, qui plus est de son domicile, contre un salaire élevé. Le travail de la « mule » est d'accepter des transferts d'argent en direction de son compte en banque personnel. La victime se servira par la suite des services de transfert de fonds comme *Western Union* pour envoyer l'argent vers une fausse adresse professionnelle, située en général en Europe de l'Est. La « mule » perçoit un pourcentage sur le montant du transfert, il représente entre 3% et 5% de la somme payée par la victime.

Le transfert d'argent entrant provient de fausses enchères en ligne ou des transactions effectuées de manière illégale par des attaques de phishing qui se sont concrétisées. Les cybercriminels utilisent la « mule » comme simple blanchisseur de l'argent transféré. Dès lors que l'argent est en cours d'acheminement vers le compte étranger, la victime escroquée au préalable n'a presque plus aucune chance de récupérer son argent. À partir du moment où la

fraude est démasquée, ce sont les « mules » insouciantes qui doivent rendre compte des lettres d'accusation ou des demandes de dommages et intérêts.

V. Les moyens de lutte contre la cybercriminalité renforcés

Malgré la cybercriminalité qui sévit, il existe de nombreux moyens de lutte contre cette dernière. Cette lutte est donc assurée par des moyens efficaces telle la cybersurveillance (A) La cyberpatrouille (B) mais elle est cependant freinée par une coopération internationale qui peine à se mettre en place et à gagner le consensus de tous les États (C).

A- La Cybersurveillance

On peut définir la cybersurveillance comme tout moyen de contrôle technique, sur une personne ou un processus, lié aux nouvelles technologies et plus particulièrement aux réseaux numériques de communication. Autrement dit, la cybersurveillance est composée des voies et des moyens qui aboutissent à l'accès des données ou signaux transmis par voie électronique, et le contrôle des moyens techniques permettant ces transmissions. La cybersurveillance agit techniquement, par le biais de logiciels de surveillance capables d'enregistrer tous les évènements ou messages survenus pendant un temps donné et à un endroit déterminé. Les écoutes téléphoniques font partie intégrante de la cybersurveillance, notamment le traçage d'internautes sur le web ou encore sur un réseau Intranet. Par exemple, La surveillance et l'interception de courriers électroniques sont des activités de cybersurveillance.

La cybersurveillance se révèle utile et nécessaire autant pour des motifs de sécurité et de bonne gestion d'un réseau informatique que pour des motifs de vérification de la bonne transmission de correspondances.

B- La Cyberpatrouille

Depuis le 5 mars 2007 avec la loi sur la prévention de la délinquance, la législation française prévoit la possibilité pour des enquêteurs, spécialement formés à cet effet, de contacter des personnes soupçonnées de commettre des infractions de traite des êtres humains, de proxénétisme ou d'atteintes aux mineurs sur Internet et dès lors de procéder à la collecte de preuves de ces infractions, sans qu'il soit possible que les actions des enquêteurs constituent de la provocation. Ces prérogatives de prise de contact des enquêteurs sont prévues par les articles 706-35-1 et 706-47-3 du code de procédure pénale. Un décret en date du mois de mai 2007 est venu apporter des précisions sur les conditions d'application de ce texte et a introduit les articles D47-8, D47-9 et D47-11 du code de procédure pénale encadrant strictement la

procédure, notamment l'action des cyberpatrouilleurs et les limites de leurs prérogatives dans les échanges de contenus illicites sur Internet.

Tout d'abord, les cyberpatrouilleurs sont des enquêteurs de la gendarmerie nationale et de la police nationale affectés dans des unités centrales relevant du service technique de recherches judiciaires et de documentation pour la police et de la division de lutte contre la cybercriminalité pour la gendarmerie. Ensuite dès que ces derniers ont évalué les conditions d'action, ils peuvent former d'autres enquêteurs dans les régions.

La cyberpatrouille se rend sur les mêmes forums, groupes d'échanges et de discussion que les pédophiles présumés et va même jusqu'à dialoguer avec eux. Auparavant il n'était pas concevable que des pédophiles puissent échanger impunément dans des forums spécialisés sur internet, en particulier concernant l'échange d'images et de vidéos pornographiques qui mettent en scène des personnes mineures et surtout prendre contact avec des mineurs comme c'est souvent le cas désormais.

Les cyber patrouilleurs agissent en utilisant un pseudonyme, et peuvent dès lors procéder à la collecte des preuves de ces infractions, en particulier celles manifestées par des sollicitations sexuelles à des mineurs de 15 ans, mais également toutes les infractions qui sont visées par les articles 706-35-1 et 706-47-3 du code de procédure pénale , et enfin concourir à l'interpellation des prétendus pédophiles avant que ces derniers ne puissent échanger des contenus illicites avec des enfants ou rencontrer des mineurs.

C- Une nécessaire coopération internationale

La coopération internationale est nécessaire car aujourd'hui elle est encore insuffisante. Pour tenter d'élaborer et de normaliser la législation, plusieurs initiatives régionales ont été mises en oeuvre. Dans un premier temps la *Commonwealth Model Law on Computer and Computer Related Crime* en date de 2002 porte sur des dispositions de droit pénal et procédural, ainsi que la coopération internationale. Néanmoins, seuls les pays du Commonwealth bénéficient des dispositions contenues dans ce texte.

L'Union européenne a adopté plusieurs approches, notamment la directive sur le commerce électronique de 2002, la directive relative à la conservation des données de 2005 ainsi que la modification de la décision-cadre du Conseil relative à la lutte contre le terrorisme en date de 2008. Tous les états membres de l'Union sont tenus de mettre ces instruments en œuvre.

Le Conseil de l'Europe a mis en œuvre trois instruments principaux dans l'objectif de l'harmonisation de la législation sur la cybercriminalité. Le plus connu est la Convention sur la cybercriminalité, élaborée puis adoptée en 2001. Cette convention est composée de dispositions sur le droit pénal matériel, le droit procédural et la coopération internationale. Le 28 janvier 2003, le comité de la prévention pour la cybercriminalité a ajouté le premier Protocole additionnel à la Convention sur la cybercriminalité. En 2007, la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels a été ouverte à la signature. Cette Convention vise des dispositions particulières sanctionnant l'échange de pornographie qui impliquent des mineurs à l'obtention d'un accès à cette forme de pornographie par le biais de technologies de l'information.

Plusieurs initiatives scientifiques telles que la *Stanford Draft International Convention* (CISAC), mise en oeuvre à titre de suivi d'une conférence en date de 1999 par l'université de Stanford aux Etats-Unis, et *Cybercrime Legislation Toolkit* de l'*International Telecommunication* Union (ITU) que nous avons évoqués précédemment, il s'agit d'une boîte à outils sur la législation sur la cybercriminalité, qui a été élaborée par l'*American Bar Association* et des experts.

Néanmoins, l'impact mondial de ces approches se révèle limité étant donné qu'elles ne sont applicables qu'à leurs états membres. Signée par 46 états et ratifiée par 26 états, la Convention sur la cybercriminalité du Conseil de l'Europe apparaît comme celle disposant de la plus grande portée juridique.

En définitive, les incidences du web 3.0 et 4.0 sur la cybercriminalité sont nombreuses. Les cyberdélinquants apparaissent comme des personnes disposant de plus en plus d'outils et de failles ainsi qu'un champ décuplé pour pratiquer leurs activités. Certes la lutte est engagée mais elle doit davantage être renforcée. Avec l'avènement du nouveau phénomène de sécurité publique illustré par l'utilisation de l'outil internet par les terroristes à des fins de propagande, le financement du terrorisme par le biais de paiements liés à l'internet ainsi que la collecte de renseignements portant sur une cible potentielle, il s'avère plus urgent que jamais que les États agissent collectivement.