LA CYBERCRIMINALITE

Cet article est une synthèse pédagogique à considérer comme une introduction au monde du cyberespace, ses problématiques et enjeux. Il servira notamment de support au café-débat *Summer School Crim'HALT* du 18 juillet sur la cybercriminalité et ses enjeux. Pour le lecteur souhaitant de plus amples informations, nous vous invitons à vous référer à la bibliographie proposée par les auteurs de cet article, ou bien à prendre directement contact avec notre équipe.

UN BREF HISTORIQUE DE L'USAGE CRIMINEL DE L'ESPACE CYBER

Le Dessous des cartes propose une infographie instructive[1] quant au développement exponentiel du cyberespace :

> *« Depuis la mise en place de l'Internet grand public, à peu près en 1988, le nombre d'internautes double chaque année.[...] Internet permet aujourd'hui à 22% de la population mondiale d'échanger des données, de discuter dans les forums, de s'informer, de jouer et de faire des achats. Et en construisant des liens entre eux, les internautes ont façonné peu à peu des communautés, puis un cyberespace, qui est certes virtuel, mais indispensable à beaucoup d'entre eux. Pas de structure hiérarchique, ni pyramidale, c'est un réseau qui fonctionne comme on dit "de pair à pair", et c'est peut-être ce qui explique son développement exponentiel. Le réseau est mondial et sans frontières. »*

La notion de cyberespace est apparue sous la plume du romancier William Gibson dans les années 1980, mais ne commencera à prendre sa forme politique et géopolitique qu'à partir de la fin des années 1990. Son statut reste une question très polémique, la réponse dérivant souvent de la nature l'émetteur. Ainsi les gouvernements et théoriciens des sciences politiques et relations internationales voient le cyberespace comme un espace soumis aux mêmes principes que les quatre autres (air, terre, mer, espace), là ou des acteurs indépendants comme le magazine Wired conçoivent le cyberespace comme un espace sans frontières et totalement « libre ».

Si les premiers « hackers » tels que Kevin Mitnick employaient les connexions téléphoniques et premières connexions internet de manière détournée bien avant tout le monde, le premier « hack » remonte lui aux années 1960[2] ! Néanmoins, l'emploi massif du cyberespace à des fins détournées reste corrélé à l'arrivée massive d'ordinateurs disposant d'une connexion internet dans les foyers dans les années 1990 et sera par la suite exponentiel, le nombre de cyber attaques et emplois détournés du cyberespace n'ayant cessé de croitre depuis.

[1] http://ddc.arte.tv/nos-cartes/le-cyberespace
[2] Voir à ce sujet l'interview de John Draper (en anglais) : http://www.computerworld.com/article/2470109/endpoint-security/interview-with-iconic-hacker-captain-crunch.html

PRINCIPALES NOTIONS

Cyberespace

Si le terme reste souvent approché comme un synonyme d'Internet, il existe toute une littérature propre à la notion plus « globale » de Cyberespace et notamment en lien avec les idéaux qui lui sont couramment associés, notamment la liberté de l'information et de l'expression[3].

Cybersécurité

Ensemble des normes, outils, institutions et autres politiques associés à la régulation d'Internet et et à la notion de confiance numérique. Elle concerne au premier lieu les entreprises victimes d'attaques informatiques.

Cyberguerre

Utilisation dérivée du cyberespace dans un but offensif dans le domaine étatique, souvent par le biais d'attaques cybernétiques visant à endommager ou paralyser un réseau informatique ou autre structure disposant de programmes informatiques.

Cybercriminalité

Utilisation dérivée du cyberespace, regroupant toutes les infractions pénales commises à l'encontre ou au moyen d'un système informatique. Les méthodes et fins de ces attaques peuvent varier considérablement en fonction de leur auteur (voir ci-dessous) et de leur objectif. Ainsi, la récente attaque contre la banque du Bangladesh demande un niveau de technicité et d'expertise bien au-delà de la simple tentative de « phishing » par email que l'internaute chevronné saura identifier immédiatement.

Deep Web et Dark Web

Si nombre de ces infractions transitent par le biais de l'internet « référencé », c'est-à-dire accessible par moteur de recherche comme Google, il existe une autre facette d'internet beaucoup moins connue du grand public et communément appelée « Deep Web » (« Web invisible » en français). Cet internet immergé n'est pas clairement défini ni délimité et correspond à un espace infiniment plus « volumineux » que le web référencé : de 15 à 500 fois plus grand selon les sources. A ce titre, le Deep Web constitue donc un outil privilégié pour de nombreux acteurs de l'économie illégale aussi bien que pour des activistes et communautés privées (cf la récente apparition des bibliothèques numériques « privées » sur le Deep Web).

La cybercriminalité exercée par l'intermédiaire du Deep Web est appelée « Dark Web » et attire de façon grandissante l'attention des médias, institutions et particuliers. Des affaires ont ainsi été largement médiatisées, telle que celle du site internet « Silk Road » (« Route de la Soie », en référence à la route empruntée par les vendeurs d'héroïne pour passer de l'Afghanistan à l'Europe) où sont proposés à l'achat divers produits et services illégaux : drogues, armes, brouilleurs d'ondes, coordonnées bancaires, attaques informatiques… Par deux fois, le site a été fermé par les autorités puis rouvert par les internautes. Les transactions, légales et illégales sont réalisées en bitcoins, une monnaie électronique non régulée par les États.

[3] Voir à ce sujet l'article d'Alix Desforges : http://ceriscope.sciences-po.fr/node/419

PRINCIPAUX ACTEURS

Hackers et pirates

Les deux termes sont à distinguer. Le hacker vise, par une utilisation astucieuse d'Internet, à y apporter sa contribution, selon une certaine éthique. Le pirate est quant à lui un criminel, qui tire profit des vulnérabilités[4]. Certaines entreprises américaines ont appris à tourner à leur avantage les capacités des hackers en les mettant au défi d'attaquer leur site, avec une promesse d'embauche en cas de réussite.

Gouvernements

Les gouvernements sont des acteurs importants d'Internet de par leur capacité de régulation. Leur action en matière de réglementation influe sur le comportement des internautes. Plus l'accès à Internet est contrôlé, plus ces derniers auront tendance à utiliser le Deep Web pour accéder à une information non censurée. Les États sont par ailleurs des acteurs de la cyberguerre, en tant que commanditaires et cibles d'attaques informatiques[5].

Collectifs autonomes et société civile

Des groupes se sont formés sur Internet, rassemblant des individus revendiquant une même cause par des moyens informatiques, des « hacktivistes » (contraction de « hacker » et « activiste »). Des groupes comme Anonymous et le Chaos Computer Club œuvrent ainsi à la défense de la liberté d'expression et d'information.

La société civile s'est par ailleurs appropriée l'espace cyber pour s'organiser politiquement, en particulier dans des contextes de contrôle strict de l'information et de contestation politique.

Sociétés privées

Les entreprises privées sont également des cibles privilégiées des attaques informatiques. De nombreux motifs (vol de données sensibles, chantage…) font d'elles des cibles spécifiques. Elles sont de surcroît des acteurs de la lutte contre la cybercriminalité, le marché de la cybersécurité connaissant une forte croissance.

Internautes

Les internautes peuvent être coupables et victimes dans le cyberespace, parfois les deux. Nombre d'entre eux ont ainsi déjà téléchargé du contenu illégalement ; nombreux sont également ceux qui ont été victime d'un piratage informatique quelconque. Souvent, les données permettant le piratage (email, mot de passe, codes bancaires) sont données volontairement par l'internaute dupé par une fausse page internet, ce qui souligne le besoin de sensibilisation en ce sens.

---

[4] Voir sur cette distinction l'entretien avec Damien Bancal sur 01net : http://www.01net.com/actualites/hackers-et-pirates-sur-internet-161741.html

[5] La carte de Norse Corporation, supposée refléter les attaques en temps réel de par le monde, montre des coïncidences entre les pays victimes de nombreuses attaques et ceux traversant des guerres ou de fortes tensions diplomatiques. http://map.norsecorp.com/#/

LE CADRE JURIDIQUE DE LA LUTTE CONTRE LA CYBERCRIMINALITE

Infractions traditionnelles et infractions spécifiques au cyberespace

On peut distinguer cinq catégories d'infractions dans le cyberespace : les infractions au droit de la presse, la pédopornographie, le piratage, l'escroquerie et la contrefaçon[6]. Certaines infractions ont de longue date été adressés par le droit. C'est le cas de l'escroquerie, de la fraude, l'usurpation d'identité, ou encore des infractions de contenu (droit d'auteur, vie privée, mineurs…). En règle générale, la dimension cyber constitue une circonstance aggravante de ces délits[7]. La réponse juridique à ces infractions est détaillée par différents code (pénal, presse, propriété intellectuelle…).

Des délits spécifiques au cyberespace ont parallèlement émergé. Il s'agit notamment de la collecte, du traitement non autorisé ou la divulgation des données personnelles, ou encore des violations de correspondance électronique. Les atteintes aux systèmes de données à caractère personnel mis en œuvre par l'État sont aggravées lorsqu'elles sont commises en bande organisée. Afin de lutter contre la radicalisation sur Internet, des dispositions concernent spécifiquement l'apologie du terrorisme sur Internet et la consultation régulière de certains sites.

Un cadre juridique et des moyens d'investigation évolutifs

Le cadre juridique connaît des évolutions régulières, renforçant les moyens de la lutte contre la cybercriminalité. La caractérisation de certains délits a ainsi évolué. C'est par exemple le cas du vol de données immatérielles, qui a vu sa définition élargie à l'extraction, la détention, la reproduction, et la transmission de données en 2014[8]. Il prend ainsi acte des évolutions techniques constantes, dans une certaine mesure, des exigences de garanties en matière de libertés publiques.

Les moyens d'investigation ont évolué afin de s'adapter aux particularités cyberespace, dans lequel les horaires habituels de perquisition ne font pas sens, et où les preuves sont extrêmement volatiles. Les moyens d'investigation peuvent notamment consister en la mise en place de dispositifs de captation des données ou en l'infiltration de réseaux sous pseudonyme. Les moyens de police ne sont pas seuls mis à contribution. Les obligations pesant sur les fournisseurs d'accès Internet (FAI) se sont progressivement renforcées. Si en principe il ne leur revient pas d'opérer des activités de surveillance et de recherche des activités illicites, ils ont cependant pour obligation d'agir afin de bloquer, sur demande du juge, des sites pour des faits d'apologie du terrorisme, de traite des êtres humains, de proxénétisme ou de prostitution de mineurs[9]. Une plateforme a également été mise en place, invitant les internautes à signaler les différents contenus illicites.

---

[6] Frédérique Chopin, « Les politiques publiques de lutte contre la cybercriminalité », AJ Pénal, 2009, p.101.
[7] Loi LEN du 21 juin 2004
[8] Loi du 13 novembre 2014 relative au terrorisme.
[9] Voir notamment Myriam Quéméner, « Les nouvelles dipositions de lutte ocntre la cybercriminalité issues de la loi du 13 novembre 2014 renforçant la lutte contre le terrorisme », AJ Pénal 2015, p. 32.

LES ECUEILS DE LA LUTTE CONTRE LA CYBERCRIMINALITE

Le caractère transnational d'Internet

Tandis que le droit pénal relatif au cyber est propre à chaque État, les infractions ont généralement un caractère transnational. Le manque de coordination des législations fait ressortir des différences législatives entre les pays, dont les cybercriminels tirent parti pour mieux dissimuler leurs actions et se protéger.

Des criminels anonymes qui agissent à différentes échelles

Les cybercriminels maximisent leur anonymat par l'usage de moyens de cryptage et d'anonymisation. Leur identification est incertaine, ce qui tend à accroître leur sentiment d'impunité. Il est d'autant plus complexe de contrer leurs attaques que celles-ci peuvent être de divers type, s'appuyer sur des failles non identifiées et toucher des cibles ayant un usage et une connaissance différente d'Internet. Le cyber fait ainsi coexister des infractions de grande ampleur touchant de grandes entreprises ou des structures étatiques (piratage de Sony, virus Stuxnet dans une centrale nucléaire iranienne) avec des attaques limitées touchant des particuliers.

Dans ce contexte, la réponse pénale s'avère difficile

Les victimes étant insuffisamment protégées et informées, les actes sont souvent identifiés longtemps après qu'ils aient été commis. Les investigations sont longues et les preuves difficiles à rassembler car souvent volatiles et peu faciles d'accès. Ces dernières, comme les suspects, sont d'ailleurs rarement physiquement accessibles. Le volume de données échangées sur Internet étant massif, la surveillance des actes frauduleux requiert ainsi des moyens considérables.[10]

Un cadre juridique controversé

La lutte contre la cybercriminalité peut impliquer une action légale susceptible de toucher les criminels comme les citoyens ayant un usage non répréhensible d'Internet. Les outils visant à garantir l'anonymat des internautes, le cryptage des communication mais également le Deep Web et le bitcoin sont utilisés tant par des criminels que des citoyens aux motivations non répréhensibles. Dès lors l'interdiction de ces outils, outre le fait qu'elle semble techniquement difficile, risquerait d'avoir pour principal effet d'en restreindre l'accès pour les citoyens, sans pour autant empêcher les criminels de les utiliser.

De surcroît, certaines mesures d'investigation dans le cyberespace sont critiquées comme contrevenant aux libertés fondamentales. Si le bien-fondé de des objectifs, tels que la lutte contre la cybercriminalité et le terrorisme, n'est pas discuté, la crainte est que des dérives ne naissent en pratique. Ainsi des organismes tels que la Quadrature du Net, Amnesty International et l'Observatoire des Libertés et du Numérique[11] ont vivement critiqué la loi relative au renseignement du 24 juillet 2015[12].

---

[10] Voir sur les difficultés de la réponse pénale à la cybercriminalité le rapport de l'INHESJ *Enjeux et difficultés de la lutte contre la cybercriminalité*: http://www.inhesj.fr/sites/default/files/files/formation/gds6.pdf

[11] Voir au sujet des recours déposés devant le Conseil d'État : https://www.laquadrature.net/fr/loi-renseignement-attaquee-devant-conseil-detat

[12] Voir au sujet des opposants à la loi travail l'article de Benjamin Ferran et Lucie Ronfaut sur LeFigaro.fr : https://www.laquadrature.net/fr/loi-renseignement-attaquee-devant-conseil-detat

POUR ALLER PLUS LOIN

- Master ECS Paris, « Deep Web, la face cachée d'Internet… Ou comment recevoir un kilo de cocaïne par la Poste » : http://ecs-digital.com/culture/deep-web-la-face-cachee-dinternet-ou-comment-recevoir-un-kilo-de-cocaine-par-la-poste/
- Michael K. Bergman, « The Deep Web, surfacing hidden values », *The Journal of Electronic Publishing* : http://quod.lib.umich.edu/cgi/t/text/idx/j/jep/3336451.0007.104/--white-paper-the-deep-websurfacing-hidden-value?rgn=main;view=fulltext
- Alix DESFORGES, « Cyberespace et Internet : un réseau sans frontières ? », *CERISCOPE Frontières*, 2011 : http://ceriscope.sciences-po.fr/node/419
- Olivier Kemps, « Stratégie du Cyberespace », *Diploweb.com* : http://www.diploweb.com/Strategie-du-cyberespace.html
- Yann Padova, « Un aperçu de la lutte contre la cybercriminalité en France », *RSC 2002*, p. 765.
- Frédérique Chopin, « Les politiques publiques de lutte contre la cybercriminalité », *AJ Pénal*, 2009, p.101.
- Marine Valzer, « La cybercriminalité et les infractions liés à l'utilisation frauduleuse d'internet : éléments de mesure et d'analyse pour l'année 2014 », *Rapport annuel 2015 de l'ONDRP* : http://www.inhesj.fr/sites/default/files/files/ondrp_autes_pub/cyber_cr.pdf
- INHESJ, *Rapport du Groupe de diagnostique stratégique n°6 : Enjeux et difficultés de la lutte contre la cybercriminalité*, juillet 2015 : http://www.inhesj.fr/sites/default/files/files/formation/gds6.pdf
- Groupe de travail interministériel sur la lutte contre la cybercriminalité, *Protéger les internautes : Rapport sur la cybercriminalité*, février 2014 : http://www.cil.cnrs.fr/CIL/IMG/pdf/rap_cybercriminalite.pdf
- CLUSIF, *Les synthèses du CLUSIF : Panorama de la cybercriminalité, année 2015 – Conférence thématique du CLUSIF du 14 janvier 2016* : http://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-2016-Synthese-Panocrim-annee-2015.pdf
- Myriam Quéméner, « Concilier la lutte contre la cybercriminalité et l'éthique de liberté », *Sécurité et stratégie 1/2011 (5)* , p. 56-67 : www.cairn.info/revue-securite-et-strategie-2011-1-page-56.htm.