CrimRxiv

La cybercriminalité

David Décary-Héту

Published on: Jul 08, 2020

DOI: 10.21428/cb6ab371.9e0bdd09

License: [Creative Commons Attribution 4.0 International License \(CC-BY 4.0\)](https://creativecommons.org/licenses/by/4.0/)

Définitions

Le terme *cybercriminalité* est un terme journalistique qui n'a toujours pas, dans la plupart des pays, de définition légale. Plusieurs traités internationaux (United Nations Manual On The Prevention And Control Of Computer-Related Crime, Cybercrime Treaty) n'offrent eux non plus aucune définition officielle optant plutôt pour des définitions fonctionnelles. Les définitions du terme *cybercriminalité* viennent donc du monde scientifique. Le terme est défini de manière très large par Schell & Martin (2004) pour qui la cybercriminalité inclut tous les crimes reliés à la technologie, aux ordinateurs et à l'internet. D'autres définitions sont plus restrictives et se limitent aux activités criminelles et nocives qui mènent à l'acquisition ou la manipulation d'information pour des gains personnels (Wall, 2007). La tendance actuelle pointe vers des définitions larges qui incluent tous les crimes facilités ou commis par des appareils électroniques ou des réseaux informatiques. Cette dernière définition de Gordon & Ford (2006) sera celle que nous retiendrons pour le présent article en raison de sa simplicité.

Il existe une certaine confusion entre les différents groupes d'individus qui commettent des cybercrimes. Un premier groupe, les *white hat hackers*, travaillent pour des firmes de sécurité ou encore dans le milieu académique. Leur objectif est de tester la sécurité de logiciels et d'équipements avec l'autorisation de leurs propriétaires. Ils n'ont donc aucune intention malicieuse, bien au contraire. Ils utilisent les mêmes outils que les cybercriminels aussi connus sous le nom de *black hat hackers* ou encore de *crackers*. Les black hat hackers sont les individus qui commettent des crimes pour leur gain personnel ou pour leur plaisir. Le troisième et dernier groupe d'individus forme un hybride et est connu sous le nom de *grey hat hackers*. Ces derniers cherchent aussi à tester la sécurité des logiciels et d'équipements, mais sans l'autorisation de leurs propriétaires. Ils utilisent leur sens éthique pour défendre leurs crimes en affirmant agir avant tout pour avertir les individus et compagnies des problèmes dans leur sécurité.

Historique

Les comportements délinquants impliquant des systèmes informatiques remontent aux années 1960 et 1970 alors que des académiciens de grandes universités comme le Massachusetts Institute of Technology (MIT) cherchaient à explorer l'univers du virtuel même si cela impliquait de transgresser certaines normes sociales ou lois (Schell & Martin, 2004). Ce désir d'explorer et cette curiosité sont à la base du

comportement de bien des délinquants qui les ont suivis dans les années 1980 et 1990. C'est en cherchant à évaluer la taille de l'internet que Robert Morris a conçu le premier ver informatique en 1988 qui a eu pour effet de mettre hors service plus de 6,000 ordinateurs. Quelques années plus tard, Kevin Mitnick, un jeune pirate informatique s'intéressant au fonctionnement du système de téléphones aux États-Unis a infiltré bon nombre de compagnies téléphoniques américaines ainsi que les compagnies leur fournissant des logiciels. Mitnick affirme qu'il était en mesure de faire des appels que même les ingénieurs des compagnies de téléphone ne pouvaient retracer.

Ces deux cas illustrent bien une forme de cybercriminalité qui se veut avant tout une quête de savoir et de curiosité et où les délinquants cherchent surtout à avoir accès à des ressources ou des informations auxquelles ils n'ont pas de droit légitime. En ce sens, ils sont beaucoup plus proches des grey hat hackers que des blacks hat hackers. Les comportements des grey hat hackers sont très différents des comportements des cyberdélinquants ayant vu le jour à la fin des années 1980 et qui ont été particulièrement actifs au cours des années 1990. Ceux-ci avaient pour objectif de créer des virus aux capacités destructrices importantes. Des virus comme *Jérusalem* effaçaient par exemple tous les programmes activés les vendredis 13; d'autres comme *Michelangelo* effaçaient tous les fichiers d'un ordinateur le jour de l'anniversaire de l'artiste.

Sous sa plus récente forme, la cybercriminalité s'est grandement transformée suite à une commercialisation des comportements délinquants et une mise en réseau des délinquants. Cette transformation a été permise par les outils de communication qui ont été développés sur internet. Une transformation similaire s'est opérée dans le monde légitime avec le développement de compagnies offrant des logiciels comme service; les délinquants n'ont en quelque sorte qu'adapté les mêmes technologies à leur besoin. Dans ce nouveau contexte, les délinquants se sont grandement spécialisés et offrent sur des forums de discussion, des sites de revente ou encore des salles de clavardage, leurs services de conception de virus, d'envoi de pourriel, d'infection d'ordinateur ou encore de fraude de données personnelles et financières. Chaque offre de service est complémentaire et un délinquant ou un groupe du crime organisé peut alors faire appel au professionnel dont il a besoin au moment où ses services sont requis. Chaque morceau du script criminel peut ainsi être loué. Cela permet aux délinquants qui achètent ces services de ne pas avoir à se perfectionner dans un domaine en particulier et aux fournisseurs de service de limiter leurs risques en commettant par directement un délit, mais en fournissant à d'autres les moyens de les

commettre. La cybercriminalité a ainsi pris un tournant de nature acquisitive avec cette commercialisation des services qui a mené à la création de plusieurs formes de délinquance comme les botnets, le carding et les ransomware (voir définitions plus bas).

Le cybercrime comme un service

Les fournisseurs de services illicites

Dans le contexte du crime comme un service, peu de délinquants ont les connaissances et/ou les capacités nécessaires à la création de logiciels malveillants. Cette spécialisation est plutôt réservée à une élite de programmeurs qui produisent de leur propre chef ou sur demande des logiciels aux multiples fonctionnalités. Celles-ci incluent le contrôle à distance d'ordinateurs et/ou l'exfiltration de données personnelles et financières. Les concepteurs de logiciels malveillants ne lancent pas eux-mêmes leurs créations dans la nature, mais rendent disponibles ces logiciels sur internet, offrant même à l'occasion un service de soutien technique.

Les délinquants ont besoin d'avantage que de logiciels malveillants pour mener à terme leurs activités criminelles. Ils doivent aussi louer des serveurs d'où lancer leur attaque, trouver des individus prêts à servir de mule pour blanchir leurs profits, trouver des experts en fraude pour monter leurs arnaques ainsi que des experts en télécommunication pour sécuriser leurs opérations. Tous ces services sont disponibles de manière indépendante et sont offerts aux délinquants qui auraient des besoins dans l'un ou l'autre de ces domaines.

Plutôt que de faire affaire avec de multiples fournisseurs, il est aussi possible pour les délinquants de se tourner vers des *botmasters*, les délinquants contrôlant des *botnets*. Les botnets sont des réseaux d'ordinateurs personnels, appartenant à des compagnies ou des gouvernements, qui ont été infectés par un virus. Ce virus sert de contrôleur à distance et permet au botmaster d'avoir un contrôle total des ordinateurs dans son botnet, comme s'il était devant le clavier de chaque ordinateur. Les botnets modernes comptent plusieurs milliers voire plusieurs centaines de milliers d'ordinateurs. En faisant affaire avec un botmaster, les délinquants peuvent obtenir plusieurs services à la fois comme l'envoi de pourriel, l'hébergement de faux sites bancaires et l'entreposage de mots de passe dans le cas d'un délinquant intéressé par la fraude d'identité. Toutes les données enregistrées sur les ordinateurs piratés, toutes les données qui transigent par ces ordinateurs, la bande passante et les ressources computationnelles sont à la disposition des botmasters.

Les marchés criminels en ligne

Il existe un besoin naturel pour les délinquants et les fournisseurs de services illicites de se retrouver pour acheter et vendre des services. Ceux-ci se retrouvent habituellement dans des salles de clavardage sur IRC ou encore sur des forums de discussion. Une nouvelle tendance est d'utiliser des cryptomarchés. Ceux-ci ressemblent, du point de vue de leur utilisation, à des sites de marchands en ligne comme Amazon ou eBay où les fournisseurs peuvent offrir leurs services et où les délinquants peuvent laisser des commentaires sur leurs interactions passées avec les fournisseurs. L'identité des participants à ces marchés est protégée par le service *The Onion Router* (TOR) et les paiements se font en *bitcoins*, une monnaie virtuelle anonyme.

Types et typologies de cybercriminalité

Wall (2007) distingue trois types de cybercriminalité. La première est composée des délits qui menacent l'intégrité des ordinateurs et inclut le piratage, le contournement des mesures de protection et les dénis de service. La deuxième est composée des délits assistés par les ordinateurs et inclut les fraudes et les vols. Finalement, la troisième est composée des délits basés sur le contenu des ordinateurs et inclut la pornographie, la violence et les communications offensantes.

Cette classification de Wall (2007) est l'une des plus utilisées bien qu'il en existe de nombreuses autres. Parmi celles-ci, plusieurs classent les activités des délinquants en deux groupes soit les délits assistés par ordinateur – soit les délits qui existaient avant l'internet et qui prennent maintenant une nouvelle couleur (fraude, blanchiment d'argent, harcèlement sexuel, crimes haineux) – et les délits centrés sur les ordinateurs – soit les délits qui sont apparus suite à l'internet (piratage informatique, déni de service, vandalisme de sites web) (Furnell, 2002).

Leman-Langlois (2006) propose une troisième voie qui met en commun certains des éléments des typologies décrites ci-dessus. Son modèle fait la distinction entre les crimes dits traditionnels qui existaient avant l'internet et les crimes émergents qui sont apparus suite à l'adoption importante de l'internet. Dans chaque cas, les crimes sont classés en fonction du rôle que les réseaux informatiques ont joué. Les crimes *émergents* qui ont été *déclenchés* par l'arrivée des réseaux informatiques incluent les attaques de déni de service et le vandalisme virtuels, des crimes qui ne pourraient exister sans ces réseaux. Les crimes *traditionnels* qui ont vu leur impact se *multiplier* suite à l'arrivée des réseaux incluent la pornographie juvénile et la fraude tant d'identité que financière. Ces crimes existaient avant, mais l'apparition de marchés en

ligne a grandement augmenté leur fluidité et l'efficacité des délinquants. Les crimes *émergents* ont aussi profité de l'effet *multiplicateur* des réseaux comme en fait foi l'explosion du nombre de fraudes de propriété intellectuelle sur internet et les réseaux poste-à-poste. L'aspect cyber a finalement eu un rôle *accessoire* dans le cas de crimes traditionnels comme le leurre. Il est vrai que les délinquants peuvent trouver des victimes dans les salles de clavardage, mais cela ne réduit pas les efforts nécessaires à attirer une victime. Ce rôle *accessoire* s'observe aussi dans les crimes *émergents* comme le terrorisme où les réseaux de support peuvent s'organiser grâce aux réseaux. Cette structure et les communications qui en découlent ne sont pas transformées cependant par l'arrivée des réseaux.

Ces typologies incluent un nombre important de comportements criminels très variés. Parmi ceux-ci, quelques-uns se démarquent de par leur prévalence et de leur impact social.

- *Le piratage informatique* : le piratage informatique est un accès non autorisé à un ordinateur. Ce crime permet d'accéder aux données contenues sur un système informatique, aux données qui transigent à travers le système et d'utiliser les ressources (computationnelle, bande passante) du système. Le piratage informatique est la première étape qui donne les ressources nécessaires à la commission de plusieurs autres crimes.
- *Les pourriels* : les pourriels sont des courriels non sollicités. Ils sont utilisés pour vendre des produits illicites ou contrefaits ou pour collecter des informations personnelles, financières et des comptes d'utilisateurs. Les pourriels copient souvent les courriels officiels et tenter d'attirer leurs victimes vers de faux sites qui copient eux aussi les véritables sites web.
- *La prise en otage* : certains virus prennent en otage les fichiers de leurs victimes en chiffrant leur contenu puis en exigeant une rançon pour obtenir les clés de décryptage. D'autres virus se font passer pour des logiciels antivirus et exigent un paiement afin de retirer un virus qui, dans les faits, n'existe pas. Finalement, certains virus prennent le contrôle du micro et/ou de la caméra d'un ordinateur et surveillent à leur insu leurs victimes. Le délinquant peut ensuite exiger une rançon sous la menace de diffuser le contenu capturé par le micro et la caméra sur internet.
- *Les botnets* : tel que décrit ci-dessus, les botnets sont de vastes réseaux d'ordinateurs infectés et contrôlés à distance par un botmaster. Les botnets sont utilisés pour copier des informations personnelles et financières, lancer des attaques de déni de service, envoyer des pourriels et générer artificiellement du trafic vers certains sites afin d'en augmenter les revenus publicitaires.

- *Le carding* : le carding englobe toutes les fraudes de cartes de débit et de crédit en ligne. Cette fraude se distingue des autres types de fraude de par son ampleur et de par le nombre d'individus qui y participe. Cette fraude s'est perfectionnée à un point tel qu'il est maintenant possible d'acheter sur certains sites des cartes de crédit d'institutions bancaires spécifiques ainsi que toutes les informations personnelles des détenteurs de ces cartes.

Les coûts de la cybercriminalité

Évaluer les coûts d'une forme de criminalité aussi large et internationale que la cybercriminalité est un exercice périlleux. L'effort le plus sérieux nous vient d'un groupe de chercheurs anglais (Anderson et al., 2012) qui se sont intéressés aux coûts de la cybercriminalité en Grande-Bretagne et dans le monde. Les deux conclusions les plus intéressantes de leur rapport sont tout d'abord que les délits dits traditionnels et qui ont migré vers l'internet comme la fraude fiscale ont des impacts nettement plus élevés que les nouvelles formes de délits. La deuxième conclusion est que les coûts associés à la protection des infrastructures et des services sont beaucoup plus importants que les profits retirés par les délinquants. Ainsi, les banques investissent des milliards de dollars dans la sécurité de leurs réseaux informatiques, mais perdraient bien moins en fraude directe. Cela crée un déséquilibre qui risque d'être difficile à soutenir à moyen ou long terme.

Les controverses

Deux controverses ont actuellement cours en lien avec la cybercriminalité. La première est en lien avec la spécificité même de la cybercriminalité. Des auteurs affirment qu'il n'existe pas de différence significative entre les mondes réels et virtuels. Rien, dans la nature de la cybercriminalité, ne la distinguerait des crimes dits traditionnels. Cette position est renforcée par l'étude d'autres révolutions technologiques comme le téléphone et l'automobile. Bien qu'importantes, ces innovations n'ont pas amené la création de nouvelles catégories de crimes, et ce, malgré le fait que l'automobile ait permis aux délinquants de modifier plusieurs de leurs scripts criminels tels que les vols de banque. En suivant cette logique, la cybercriminalité ne devrait donc pas en théorie former une catégorie distincte de crime, mais être étudiée avec toutes les autres formes de criminalité.

Un autre débat important tourne autour de la menace réelle que pose la cybercriminalité. Plusieurs acteurs comme les firmes de sécurité privée et les médias ont un certain avantage à maximiser la menace que pose la cybercriminalité afin

d'augmenter leurs revenus. D'autres acteurs issus du monde académique cherchent à mesurer beaucoup plus détachée et objective la réelle menace que pose la cybercriminalité. Les messages en provenance de ces différents acteurs sont souvent contradictoires et amènent une grande ambiguïté sur le niveau de menace que fait peser la cybercriminalité. D'autres études devront encore se pencher sur cette question pour trancher ce débat.

Références

Anderson, R. & C. Barton & R. Böhme & R. Clayton & M. van Eeten & M. Levi & S. Savage. "Measuring The Cost Of Cybercrime." DANS Böhme, R. (ed). *The Economics of Information Security and Privacy*. New York, États-Unis : Springer.

Furnell, S. (2002). *Cybercrime: Vandalizing the Information Society*. Boston, États-Unis: Addison-Wesley.

Gordon, S. & R. Ford. (2006). "On The Definition And Classification Of Cybercrime." *Journal In Computer Virology*. 2(1): 13-20.

Leman-Langlois, S. (2006). "Le crime comme moyen de contrôle du cyberspace commercial." *Criminologie*. 39 (1): 63-81.

Schell, B. H. & C. Martin. (2004). *Cybercrime: A Reference Handbook*. Santa Barbara, États-Unis : ABC-CLIO.

Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge, Grande-Bretagne: Polity.