**Zeitschrift:** Revue Militaire Suisse
**Herausgeber:** Association de la Revue Militaire Suisse
**Band:** - (2018)
**Heft:** [2]: Numéro Thématique 2

**Artikel:** La cybercriminalité : réalités et perspectives de lutte contre la cybercriminalité
**Autor:** Ghernaouti, Solange
**DOI:** https://doi.org/10.5169/seals-823451

*Int. / Strat.*

# La *cyber*criminalité : Réalités et perspectives de lutte contre la cybercriminalité

**Solange Ghernaouti**

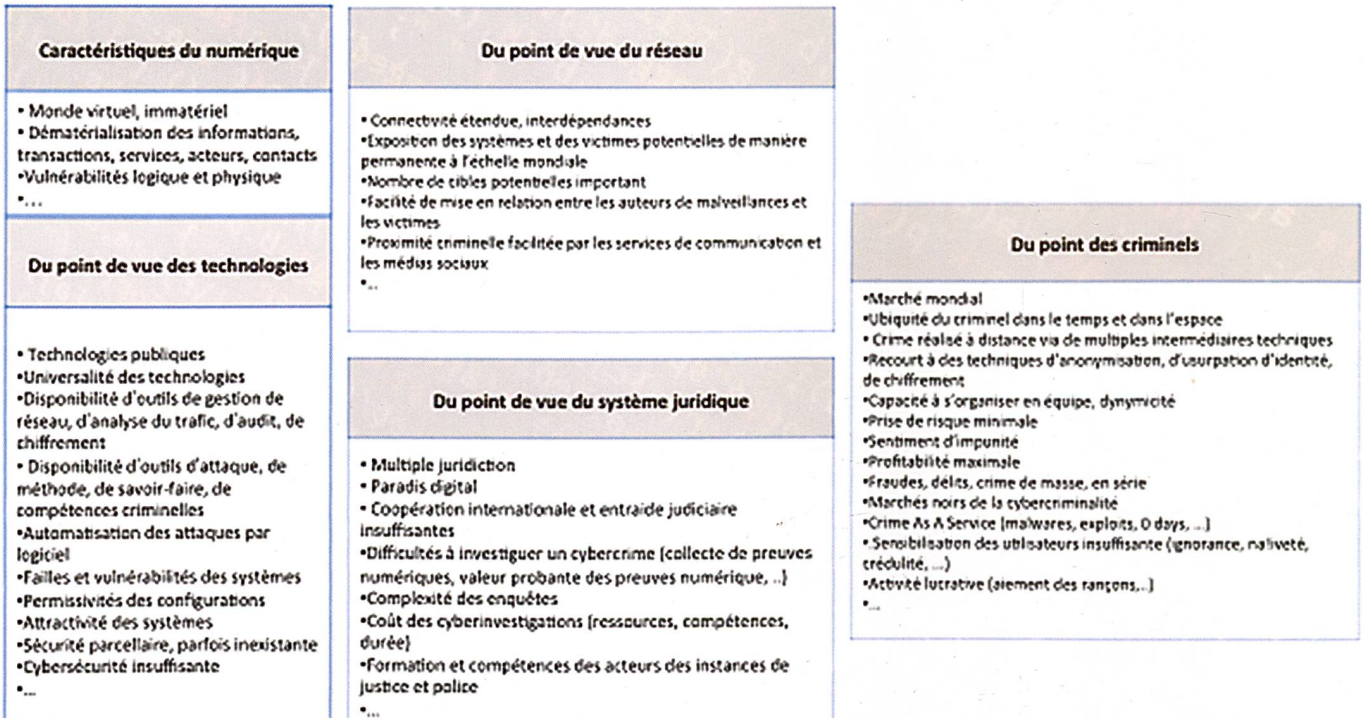
Professeure, Université de Lausanne. Directrice, Swiss Cybersecurity Advisory & Research Group (SCARG). Présidente, Fondation SGH - Institut de recherche Cybermonde. Associate Fellow, Geneva Center for Security Policy (GCSP). Board member, Global Initiative against Transnational Organized Crime (GITOC).

Le cyberespace constitue le prolongement technologique de notre environnement réel, induisant un *continuum* entre le monde cyber et le monde physique classique. Les cybermenaces sont des menaces bien réelles, leur réalisation peut affecter les individus, les organisations publiques et privées et donc la société.

Du fait de l'interconnexion, à l'échelle mondiale, des infrastructures numériques et des systèmes d'information, les risques induits par des cyberattaques ne sont pas conjoncturels et isolés. Ce sont des risques structurels, permanents et systémiques ayant des effets en cascade. Ils peuvent avoir des impacts directs et indirects loin de leur origine.

Le cyberespace contribue à un écosystème numérique régit par la loi du marché et les acteurs les plus forts. Ni pire ni meilleur, il reflète notre réalité sociale, économique et politique. Objet de conquêtes et de convoitises, c'est un moyen de développement économique et personnel, un moyen d'enrichissement licite et illicite, un lieu d'expression du pouvoir et aussi d'expression des crimes

Figure 1 – Internet, vecteur de cyberattaques mais aussi vecteur d'ac-tions, de modes opératoires criminels et caisse de résonnance de la criminalité.



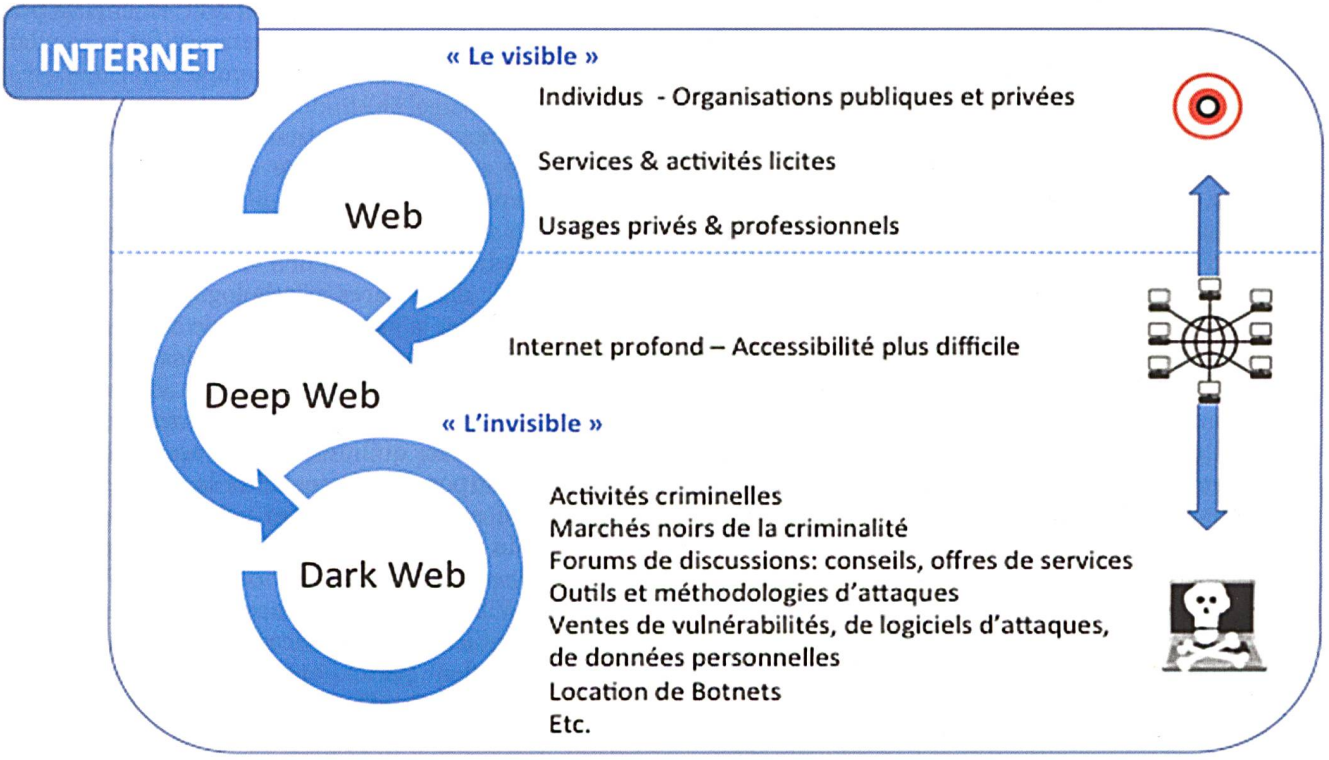



Figure 2 – Disponibilité des outils et des services de la cybercriminalité via Internet et le Dark Web.

et des conflits. Le cyberespace peut être considéré comme un champ de bataille économique et politique, à l'échelle mondiale, qui fait fi des frontières géographiques.

Le fort taux de pénétration d'Internet, l'évolution des usages, du développement d'objets connectés, qui augmentent potentiellement le nombre de victimes possibles et étendent la surface d'exposition aux cybermenaces, stimulent l'attractivité des cybercriminels.

Internet constitue désormais un vecteur de propagation de cyberattaques à des fins d'enrichissement criminel, d'influence, de déstabilisation, de coercition, de puissance ou encore par exemple de nuisance. Le nombre, la diversité des victimes, la relative impunité dont bénéficient délinquants et criminels, font que la cybercriminalité est une activité rentable au regard des investissements et moyens nécessaires pour la réaliser. La figure 1 résume les principales caractéristiques d'Internet qui favorisent la cybercriminalité.

Le mode de fonctionnement d'Internet, l'usage du chiffrement et des outils d'anonymisation par les criminels ainsi que le manque de moyens auxquels sont confrontés les instances de justice et de police pour poursuivre un crime transnational, les problèmes d'entraide judiciaire internationale et l'accès à la preuve numérique difficile profitent aux criminels. Ainsi, Internet leur offre une couche d'isolation protectrice et leur permet une activité intensive et permanente qui autorise une massification du crime.

**Des cybercriminels opportunistes avec une grande capacité d'adaptation**

Internet favorise à l'échelle planétaire la mise en relation de cibles et de prédateurs, escrocs et malveillants de toutes sortes qui peuvent agir à distance et cachés derrière un écran. Le crime est automatisé par des logiciels et tout système connecté à Internet peut devenir une cible de la cybercriminalité. Ce qui contribue à une ampleur importante de la criminalité qui devient accessible à tout un chacun disposant d'un ordinateur et d'une connexion Internet. En effet, nul besoin d'être un génie de l'informatique pour concevoir des programmes malveillants (virus, crypto-verrouilleur, cheval de Troie, ...), toute la panoplie du parfait cybermalfaiteur est accessible via Internet. Le réseau permet non seulement la diffusion des attaques mais aussi des outils du crime et des modes opératoires criminels notamment par les places de marché noir de la cybercriminalité situées dans le Dark Web (figure 2).

Chaque internaute peut être un criminel ou le devenir. Le passage à l'acte est facilité, y compris pour les plus jeunes, par la disponibilité et la dématérialisation des moyens et la proximité des victimes via les outils de mise en relation et de communication d'Internet (messageries, médias sociaux, ...) accessibles également en permanence depuis un smartphone.

Les criminels savent tirer parti des opportunités que leur offre Internet pour innover et être performants dans leurs activités classiques (trafics d'êtres humains, d'armes, de drogue, d'animaux, escroqueries, extorsion, crime économique, blanchiment d'argent, etc).

Industrie et marché noir des outils de la cybercriminalité sont structurés autour de la mise à disposition des

moyens (infrastructures d'attaques) et des compétences qui sont disponibles, notamment sur le Dark Web, à qui souhaite les trouver (notion de « *crime as a service* »). De la délinquance informatique au crime économique d'envergure, en passant par le harcèlement, la manipulation d'information, la surveillance ou l'espionnage, le vol de données de personnelles, des identités usurpées, etc. tout se vend et tout s'achète sur Internet. En termes de cybercriminalité, les limites semblent être celles de l'imagination créative des auteurs, qui selon leurs motivations peuvent agir isolément ou être en bande, ce qui peut relever du crime organisé. Impossible d'être exhaustif quant à la nature et le type de malveillance, de délits ou de crimes possibles, en revanche, il est certain que les forums de discussions, les plateformes de mise en relation ainsi que les cryptomonnaies favorisent les activités criminelles et les trafics illicites. Parmi ces derniers, citons la vente de produits pharmaceutiques contrefaits ou encore celle de produits alimentaires ne répondant pas aux normes du marché, de « kits de suicide », de « kits de viol » ou encore de « kits de piratage ».

Les cybercriminels s'intéressent aux cryptomonnaies notamment du fait des possibilités d'anonymisation et de fraudes sur des levées de fond (ICO – *Initial Coin Offering*) qu'elles procurent ( vol de 70 millions de KickCoins pour une valeur d'environ 7.7 millions de dollars américains sur 'ICO KICKICO en juillet 2018). De plus les vols de portemonnaies électroniques, les botnets de minage et des cyberattaques sur des plateformes d'échanges, la vente de « kit de logiciels malveillants de minage de cryptomonnaies » constituent de nouvelles activités criminelles profitables.

**La cybercriminalité, des activités protéiformes, des victimes bien réelles**

Parmi les escroqueries les plus classiques citons celles aux faux ordres de virement bancaires (remise volontaire de fonds par virement), aux faux investissements (trading à partir de faux sites), à la fausse amitié (*Scam romance*), aux faux supports techniques ou encore à la charité.

Par ailleurs, l'espionnage et la surveillance numérique sont omniprésentes et les cyberattaques peuvent être au service de l'ingérence économique (collecte d'informations stratégiques, de savoirs-faire, chantages, destabilisation, ...) pouvant conduire entre autre, à des pertes de productivité, d'avantages concurrentiels, d'altération du mode de fonctionnement des organisations ou encore par exemple à des atteintes au potentiel éconmique, industriel, technique ou scientifique du pays.

L'ingénierie sociale est souvent un point de départ pour la réalisation de fraudes, d'escroqueries, de crimes ou la réalisation de cyberattaques plus ou moins sophistiquées. Ces dernières peuvent être massives comme ce fut le cas en mai 2017 de la diffusion du rançongiciel *WannaCry* qui toucha des systèmes informatiques de différents domaines d'activité (transport, santé, finance, ...) dans 150 pays environ. Mais il peut s'agir de cyberattaques ciblées ou encore être des attaques en profondeur parfois également dénommées furtives (ou ATP en anglais pour *Advanced Persitent Threats*), comme ce fut le cas dans l'affaire RUAG (2016-2017) par exemple.

La pédopornographie continue de croître, comme d'ailleurs le nombre d'atteinte aux mineurs avec un nombre d'enfants victimes de plus en plus jeunes (y compris des nourrissons), ayant subis des abus sexuels, des violences, des exploitations sexuelles en ligne (*live streamming*), des sévices psychologiques et corporels pouvant entrainer la mort. Force est de constater que les images et vidéos illicites proviennent des abuseurs eux-mêmes souvent liés à l'entourage de la victime, ou des victimes soumises à des chantages (*sextorsion*). S'il est courant de rappeler qu'Internet est à usage dual, civil et militaire, il est possible de constater la dualité des outils de communication couramment usités. Ils peuvent être au service du meilleur et du pire. En effet, les pédophiles utilisent par exemple Skype, Yahoo messenger, Whatsapp, Snapchat, Viber, Instagram, accèdent à des services payants en utilisant des services de Western Union ou de Paypal, règlent parfois en Bitcoin. Ils sont capable d'utiliser des services d'anonymisation (VPN , proxy) et de réaliser des transaction dans le Dark Web, d'utiliser des réseaux pair à pair (E-Donkey, E- Mule, Giga Tribe, ...)) ou encore toujours par exemple des réseaux TOR. C'est essentiellement via des réseaux sociaux des sites ou des forums pour adolescents, des jeux en lignes, que les prédateurs sexuels trouvent les moyens de rencontrer et de contacter des victimes potentielles.

Les objets connectés facilitent la création de réseaux d'ordinateurs « zombies » (Botnets), contrôlés à distance pour être activés et servir de relais dans des cyberattaques. C'est en 2016, que des caméras de vidéosurveillance furent intégrées dans des botnets (de nom Mirai) pour notamment réaliser des attaques par déni de service.

Les botnets impliquant des ordinateurs d'individus ou parfois d'organisations publiques ou privées sont largement mis en œuvre par des hacktivistes pour revendiquer les causes qu'ils soutiennent par des groupes tels que Anonymous, AnonPlus ou Ghostshell par exemple. Toutefois, certains perturbateurs du Net ne possèdent pas de motivation financière ou idéologique. Des groupes politiques extrémistes peuvent être très actifs et manifester leurs opinions via des cyberattaques ou des actions de manipulation psychologique, de désinformation et d'influence pouvant conduire à des instabilités politique et sociale, voire à des atteintes à la démocratie.

Internet est également au cœur de la communication à des fins terroristes (propagande, radicalisation, influence, intimidation, déstabilisation, recrutement, formation). Le retrait de contenus « terroriste », les contre-discours sont des enjeux majeurs pour renforcer la lutte contre le terrorisme et prévenir la radicalisation des personnes. Il existe une certaine convergence des mondes de la cybercriminalité et du terrorisme par la mise à disposition des ressources nécessaires pour cyberattaques relevant d'actions terroristes mais par les circuits financiers.

La délinquance, les infractions économiques et financières sont facilitées par le vol et recel de données de cartes bancaires, les trafics de fausses monnaies, de faux documents, et par la disponibilité de logiciels malveillants (rançongiciels, guides méthodologiques, ...). Cela autorise une dissémination des modes opératoires et constitue une industrialisation des outils de la cybercriminalité. La délinquance de masse est désormais une réalité qui s'appuie sur le transfert d'infractions traditionnelles vers la « criminalité dématérialisée » dont les conséquences est une augmentation exponentielle des préjudices et dommages. Internet est un vecteur amplificateur et de globalisation de la criminalité. Le risque informatique d'origine criminelle est ainsi devenu un risque structurel dont le coût est porté par la société. Il est estimé à environ 1% du PIB, soit pour la Suisse d'environ CHF 6 milliards. L'évaluation du coût de la cybercriminalité reste un exercice complexe et difficile du fait que le taux de de dépôt de plaintes reste faible au regard de l'importance des faits. Les secteurs bancaire, financier et de la santé sont particulièrement la cible de vols de données sensibles. Des cyberattaques visant des chaines de traitement logistique peuvent entraîner des dysfonctionnements considérables. Qu'il s'agisse d'appât du gain, de sabotage, d'espionnage, d'ingérence économique, d'expression de revendication, les impacts de la cybercriminalité peuvent être d'ordre financiers ou réputationnel mais peuvent aussi engendrer des pertes de vie humaines, des dégâts écologiques et environnementaux notamment lors de cyberattaques visant des infrastructures vitales.

Les coûts indirects de la cybercriminalité s'expriment en perte de compétitivité, de propriété intellectuelle, de données sensibles, de réputation mais aussi d'emplois et d'attractivité de la place économique, financière ou internationale de la Suisse. Sans compter les préjudices portés par les citoyens et les entreprises victimes, c'est à dire par la société. De plus les gains issus de la cybercriminalité – qui ne sont pas soumis à l'impôts – dont sont victimes les suisses, profitent rarement au développement économique de la région! Par contre, la société doit investir dans des mesures de prévention et de protection, dans des mécanismes assurantiels, de sensibilisation du public, mais aussi dans des services de renseignement, d'aide au victimes, de détection, d'alertes, d'échange d'information ou encore par exemple dans les services de police et justice. Les coûts des enquêtes, des poursuites et des procès sont aussi à la charge de la société et font également partis des coûts directs engendrés par la cybercrimnalité.

Bien que des actions de police soient parfois spectaculaires comme celles ayant abouti à la fermeture de site de vente de stupéfiants *Silk Road* en 2014 et Alphabay et Hansa Market en 2017, malgré des arrestations de cybercriminels, la communauté de la cybercriminalité se porte bien. Très dynamique, elle sait s'adapter aux opportunités criminelles et aux nouvelles technologies.

**Lutter contre la cybercriminalité, un enjeu majeur**

Dans la mesure où la lutte contre la cybercriminalité fait partie de la lutte contre les cybermenaces et d'une démarche globale de cyberdéfense des intérêts nationaux, il est important de développer une culture nationale et des actions concrètes favorisant la sécurité des systèmes d'information, la protection, la robustesse et la résilience des infrastructures numériques. La lutte contre la cybercriminalité passe par la réduction des obstacles d'ordre technique, juridique, procédural, économique et politique ainsi que ceux qui sont un frein à la coopération de toutes les parties prenantes aux niveaux national et international, notamment pour ce qui concerne l'entraide juridique internationale

La cybercriminalité est une extension du champ et des moyens de la criminalité traditionnelle. Cette dernière est devenue plus performante grâce aux technologies de l'information. Le risque « Cyber » d'origine criminelle est complexe et multiforme, il accentue tous les risques traditionnels, en génère de nouveaux, tout en contribuant à la globalisation des risques. Il est devenu une urgence planétaire à prendre en considération.

Il appartient à l'Etat d'assurer la sureté et la sécurité de ses concitoyens y compris dans le cyberespace selon un cadre légal qui permet de satisfaire les besoins de sécurité tout en respectant les droits humains fondamentaux.

Le cyberespace modifie les frontières traditionnelles entre les actions de défense économique et celles relevant de la défense militaire. Il s'agit du même Internet, les cyberattaquants utilisent les mêmes technologies, les mêmes savoir-faire et la même boîte à outils pour réaliser des cyberattaques, qu'ils soient motivées par l'appât du gain ou par des besoins de déstabilisation, de terrorisme, de prise de pouvoir ou à des fins conflictuelles. La prolifération des capacités offensives Cyber dont la diffusion, l'acquisition, l'usage sont facilitées par Internet, constituent un enjeu tant pour la cybersécurité que pour la cyberdéfense. Dès lors, un *continuum* cybersécurité-cyberdéfense cohérent prend tout son sens du fait des interdépendances entre les besoins de lutte contre la criminalité, ceux de sécurité nationale et de défense. Quelles que soient les perspectives civiles ou militaires de la maitrise des cyberrisques, il en va de la souveraineté de la Suisse de pouvoir les mettre sous contrôle pour assurer sa sécurité et sa défense.

Disposer de moyens suffisants dans une démarche de lutte contre la cybercriminalité peut bénéficier aux mesures relevant de la cyberdéfense pour être en capacité de se défendre et éventuellement d'attaquer dans un contexte de cyberguerre. Mutualiser certaines ressources, partager des informations et des renseignements, pour globalement monter en puissance est pertinent. Il serait regrettable de privilégier une démarche de cybersécurité ou de cyberdéfense au détriment de l'autre, voire d'abandonner l'une ou l'autre.

Suite de l'article en page 23