الجمهورية الجزائرية الديمقراطية الشعبية
REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
وزارة المالية
MINISTERE DES FINANCES
CTRF
CELLULE DE TRAITEMENT DU RENSEIGNEMENT FINANCIER
خلية معالجة الإستعلام المالي
خ م إ م

LETTRE D'INFORMATION : BON A SAVOIR (N°32)

La Cybercriminalité

La cybercriminalité est le fléau à combattre issu de l'expansion d'internet, des réseaux sociaux et du e-commerce.

Ce combat est d'autant plus difficile qu'elle vise tous les domaines d'infractions...

Branche pénale de l'informatique, la cybercriminalité ou quelles infractions peuvent être commises via les réseaux informatiques ou de communication (télécommunication, radiodiffusion, smartphones….).

Elle n'est pas forcément le fait d'un seul homme, mais fait jouer de plus en plus des bandes de réseaux réalisés sur le plan international, sa preuve reste difficile

Après 40 000 nouveaux signalements en janvier, EDF a admis qu'elle avait fait les frais d'une attaque « phishing » depuis août 2012.

Il s'agit d'une notion largement définie.

Il n'y a pas de définition universelle de la cybercriminalité n'a été admise, si bien que chaque Etat l'a défini selon ses propres critères.

En France la notion est définie largement.

- La cybercriminalité touche diverses atteintes aux personnes : Diffamation, Injures, Pornographie et pédopornographie, diffusion de photos, Incitation à la haine raciale, Atteintes à la vie privée, Dénigrement, Usurpation d'identité,
- La cybercriminalité touche diverses atteintes aux biens : Téléchargement illégal, Hameçonnage ou phishing, Intrusions ou piratages des données, Différents types d'intrusions dans le système informatique par le biais de programmes malveillants :
    - Le ver : pour se propager entre ordinateurs avec des séries de codes informatiques
    - Le virus : pour infecter d'autres programmes
    - Le cheval de Troie : pour avoir un contrôle à distance de l'ordinateur infecté,
    - Les bombes logiques : pour détruire de façon différé.
    - L'attaque en déni de service : pour empêcher d'utiliser un service par saturation d'exécution de programmes
    - Le spam : communication électronique, expédiée en masse à des fins publicitaires ou autres,
    - L'adware : pour afficher des bannières publicitaires,
    - Le spyware: pour installer un logiciel espion et imposer régulièrement des informations statistiques sur les habitudes de l'utilisateur

-l'entrave au fonctionnement d'un système automatisé de données est réprimé par l'article 323-2 du code pénal: « Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende ».

- La contrefaçon (vol de propriété intellectuelle).
- La destruction de données,
- Le cybersquatting pourra être de la contrefaçon en présence d'un nom de domaine similaire ou identique à une marque.
-Toutes sortes d'escroqueries commises via les réseaux (ex aux enchères sur le net, fraude à la carte bleue, vente en ligne avec encaissement sans livraison de la marchandise…)
L'Article L 313-1 du Code Pénal définit l'escroquerie : "le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge. L'escroquerie est punie de cinq ans d'emprisonnement et de 375 000 euros d'amende".

"L'Economie de la cybercriminalité"

Dès lors qu'un petit cyber-escroc peut empocher plusieurs milliers de dollars par jour sans être inquiété ou repéré par l'administration ou les autorités judiciaires de son pays, est-il vraiment surprenant que les grandes bandes organisées soient si difficiles à neutraliser ? En l'absence de cyber-frontières entre les pays, les organisations internationales ont-elles vraiment les moyens de lutter contre la cybercriminalité ?
Pour l'heure, les cybercriminels n'ont d'autre objectif que de gagner de l'argent - et beaucoup d'argent. Virus, spams et autres « botnets » ont beau drainer plusieurs centaines de millions de dollars chaque année à travers le monde, l'existence d'un véritable cadre politique international permettant la définition de mesures efficaces de lutte contre la cybercriminalité continue de manquer
Dans le monde réel, toute entreprise criminelle ne peut réussir qu'à condition de savoir par quels moyens « blanchir » l'argent mal acquis - qu'il s'agisse de billets de banque volés ou d'argent sale de la drogue. Mais législation contre le blanchiment de l'argent sale oblige, la démarche est logiquement chronophage et complexe. Pour les cybercriminels, la tâche s'avère beaucoup moins compliquée : pour l'essentiel virtuel, le processus peut s'opérer en n'importe quel point du globe - et de préférence là où la législation en la matière est lacunaire.
S'il est donc presque impossible de tracer les cybercriminels par Internet, suivre la trace de leurs gains financiers peut apparaître comme la solution la plus efficace. Mais là encore, la démarche nécessite une coopération internationale qui n'est pas simple à mettre en œuvre.
En effet, les cybercriminels et autres professionnels du blanchiment d'argent ont tendance à recycler les sommes d'argent volé en de multiples micro-transactions, généralement assurées par un grand nombre de personnes au sein d'un vaste réseau aux multiples ramifications internationales.
En outre, les cybercriminels connaissent bien la liste des paradis juridiques où il fait bon se réfugier. À l'instar des paradis fiscaux, ces pays se caractérisent en effet par leurs dispositifs réglementaires particulièrement laxistes en matière de lutte contre la cybercriminalité.
Enfin, chaque pays a beau être doté d'un solide arsenal juridique pour combattre les cybercriminels opérant sur leur territoire, il est facile pour ces derniers - et pour leurs

avocats - d'exploiter l'absence de véritable coopération internationale entre les gouvernements.
Quel que soit l'objet de la discussion, amener des gouvernements à coopérer et à trouver un accord est toujours difficile - même lorsque les relations entre les nations concernées sont au beau fixe.
Certes, on a pu observer quelques avancées permettant de combler un tant soit peu les lacunes en matière de coopération et de réglementation internationale mais ces efforts demeurent largement insuffisants. Et à l'heure où bon nombre d'instances gouvernementales se perdent dans la quête impossible d'une formule magique, plusieurs centaines de millions d'euros continuent d'être tranquillement blanchis, à l'insu du plus grand nombre et en toute impunité.
L'idée de créer une police supranationale ou de refonder l'Internet n'est que pure fantaisie. Quant aux tentatives de solutions envisagées par l'OCDE et le G8, elles sont vite retombées comme un soufflet. Il existe toutefois certaines pistes intéressantes qui ont le mérite de rendre moins vaine la lutte contre la cybercriminalité.
Sans aucun doute, la Convention de la Cybercriminalité du Conseil de l'Europe constitue l'initiative à ce jour la plus constructive pour développer un cadre juridique efficace. En dépit de son nom, cette convention est soutenue par une vaste coalition internationale et ouverte à tous les pays. Aussi prometteuse puisse-t-elle paraître, il reste encore beaucoup de chemin à faire puisque sur les 46 pays ayant signé le traité, seulement la moitié l'a ratifié et parmi ceux-là, seulement quatre pays ont effectivement utilisé les outils que leur fournit la Convention.
Une large ratification de la Convention par tous les pays signataires constituerait certes une avancée majeure - rappelons-nous que la Déclaration Universelle des Droits de l'Homme a plus de 60 ans et que certains pays ne l'ont toujours pas approuvée à ce jour - mais ne saurait pour autant apporter une solution complète aux problèmes en jeu. Pour y parvenir, toute ratification ou mise en œuvre de la Convention doit être accompagnée d'une volonté politique forte et s'appuyer sur un solide système de gouvernance.
Trouver une solution efficace de lutte contre le cybercrime est une démarche certes ambitieuse mais pas impossible. Au-delà des dispositifs réglementaires déjà à l'étude, la consolidation des données criminelles internationales dans une base de données mondiale - du type de ce qu'INTERPOL fournit aux autorités judiciaires - pourrait offrir une solution prometteuse.
Il est encore trop tôt pour savoir si les bases de données d'INTERPOL sont adaptées ou non à la lutte contre la cybercriminalité organisée à l'échelle internationale. Mais l'implication croissante de cette organisation intergouvernementale offre sans aucun doute de bonnes perspectives.
La décision appartient in fine aux gouvernements et aux institutions internationales. À l'heure où l'impact de la cybercriminalité sur l'économie mondiale ne cesse de s'accroître, la coopération internationale bouscule l'agenda mais il faudra se montrer encore un peu patient avant de voir s'il en ressortira vraiment quelque chose.

Combattre l’industrialisation de la cybercriminalité

Dans le domaine de la cybercriminalité, cinq ans est une période très longue qui a vu se développer rapidement l’économie numérique clandestine, le hacktivisme et les réseaux d’ordinateurs zombies.

Lorsqu'on parle de l'économie numérique clandestine, on entend les réseaux autonomes qui fonctionnent principalement dans des forums Internet fermés et facilitent divers actes de cybercriminalité, y compris les attaques bancaires, les fraudes sur les cartes bancaires le vol d'identité et d'autres intrusions en ligne. Les données personnelles et financières volées sont vendues sur Internet.

La sophistication de ce modèle commercial criminel est telle que les membres de ces réseaux sont capables de réaliser des tâches spécifiques comme fournir un code malveillant ou des mécanismes pour déclencher des attaques. Certains spécialistes sont même spécialement chargés de créer des chiffres d'authentification de cartes bancaires et de recruter des mules, des personnes chargées de transformer l'argent virtuel en argent réel – sans savoir nécessairement qu'ils se livrent à une activité criminelle.

Les cybercriminels innovent constamment. Non seulement ils font un usage intense des médias sociaux pour escroquer les utilisateurs et distribuer des liens à des logiciels malveillants, mais ils parcourent aussi l'environnement pour identifier les nouvelles vulnérabilités, les nouveaux environnements populaires auprès des internautes et les nouveaux vecteurs d'attaques.

Parmi les formes d'escroquerie les plus ingénieuses de ces dernières années figurent le rançongiciel. Ce logiciel malveillant bloque l'ordinateur de l'utilisateur jusqu'à ce que celui-ci paie une amende sur un compte bancaire.

Avec l'appui du Centre européen de lutte contre la cybercriminalité (EC3) à Europol et à Interpol, les services chargés de l'application de la loi accomplissent des progrès contre les groupes criminels engagés dans la diffusion de rançongiciels.

En février 2013, l'Opération Rançon, menée par la police espagnole, a conduit à l'arrestation de 11 personnes responsables de la création, du développement et de la diffusion de ce type de logiciels malveillants ainsi qu'à l'arrestation de 10 autres personnes responsables de transactions financières frauduleuses. Des enquêtes sont en cours.

Regroupant des milliers d'ordinateurs infectés qui servent essentiellement de zombies pour mener des attaques sur d'autres systèmes, les réseaux d'ordinateurs zombies ont accéléré l'industrialisation de la cybercriminalité plus que tout autre outil. Avant l'essor de ces réseaux, les victimes de la cybercriminalité étaient attaquées une par une, ce qui nécessitait plus de temps et d'effort de la part des criminels. Aujourd'hui, les courriels poubelles et les attaques par déni de service distribué qui rendent indisponibles les sites Web des gouvernements et les sites Web commerciaux en les saturant dépendent particulièrement des réseaux zombies pour leur puissance de traitement. Votre ordinateur personnel, votre ordinateur portable ou votre smartphone ont pu être exploités à cette fin.

Les réseaux d'ordinateurs zombies sont non seulement puissants, mais aussi très efficaces. Tout comme les entreprises légitimes mettent leurs ordinateurs dans le nuage, nous pouvons nous attendre à y voir aussi bientôt des réseaux d'ordinateurs zombies, des entités très dynamiques qui changent rapidement de lieu, ce qui exigera une coopération internationale opportune et concertée pour les démanteler.

En attendant, l'Internet est de plus en plus désigné comme une infrastructure essentielle. C'est aussi une technologie dont dépend la vaste majorité des infrastructures essentielles, y compris les sources d'alimentation en électricité, la fourniture de soins de santé et les communications d'urgence.

En tant que citoyen du monde, vous pensez peut-être que la menace liée à la cybercriminalité n'est pas réelle, ou qu'elle est exagérée. Alors que les statistiques citées dans les grands médias parlent régulièrement des millions d'ordinateurs infectés

et des milliards de dollars US perdus par les intrusions ou les fraudes en ligne, il est rare que l'impact immédiat soit ressenti par l'internaute moyen, lequel sera remboursé par son fournisseur de services financiers et ne jugera pas nécessaire de signaler cette activité criminelle à la police. Contrairement à l'exploitation sexuelle des enfants en ligne, à ce jour, la cybercriminalité n'a généralement pas un effet dévastateur sur ses victimes.

Cela fait plus d'une décennie que la police est consciente de la menace posée par la cybercriminalité, mais il a fallu du temps pour que ce domaine soit reconnu une priorité et doté de ressources. Les capacités de lutte contre la cybercriminalité dans le monde se développent à un rythme différent.

En janvier 2013, EC3 a vu le jour. Basé à Europol à La Haye, le centre fournit un appui opérationnel et une coordination du renseignement aux enquêtes sur la cybercriminalité dans 27 États membres de l'Union européenne qui, de leur côté, mobilisent leurs capacités et leur savoir-faire pour apporter des réponses plus globales et ciblées aux menaces en ligne.

En 2014, le nouveau Centre Interpol de lutte contre la criminalité numérique sera opérationnel au Complexe mondial Interpol pour l'innovation à Singapour. Dans ces deux centres, l'accent est mis sur les initiatives collectives qui mettent à profit l'expérience de toutes les parties prenantes concernées par la cybersécurité, y compris l'industrie, le milieu universitaire, les organisations de la société civile et les autorités gouvernementales.

Cela continuera à attirer les cybercriminels, ce qui exigera une plus grande protection de la part des fournisseurs de services ainsi qu'un renforcement des niveaux de coopération internationale par ceux qui sont chargés d'enquêter sur les violations et de faire porter la responsabilité aux cybercriminels.

Partout dans le monde, la législation devra non seulement rattraper son retard par rapport à l'usage criminel des technologies émergentes, mais aussi ne pas se laisser distancer. Il existe aujourd'hui un risque réel que, sans harmonisation dans ce domaine, les pays qui ont de faibles niveaux de cybersécurité, une législation faible en matière de cybercriminalité et des capacités réduites dans le domaine de l'application de la loi deviennent des refuges pour les cybercriminels durant de nombreuses années à venir.

Déjà, la coopération internationale est essentielle pour mener des enquêtes efficaces et traduire les cybercriminels en justice.

Toutefois, nous devons aussi substituer aux pratiques traditionnelles de justice pénale des pratiques d'arrestation, de poursuites et de condamnation plus intelligentes. Des mesures de prévention efficaces sont, et continueront d'être, possibles. Des organisations internationales comme Europol, Interpol et les Nations Unies sont des multiplicateurs de force dans la fourniture d'initiatives multisectorielles efficaces visant à démanteler les réseaux d'ordinateurs zombies, réduire les profits générés par l'économie numérique clandestine et faire activement participer les citoyens à la protection contre les attaques.

La lutte contre la cybercriminalité requiert également la création de centres de spécialistes de l'information et de la coordination du renseignement. Très souvent, ce n'est qu'au niveau international que les analystes peuvent avoir une idée précise de la portée des activités des groupes cybercriminels et du tort qu'elles causent. Les autorités chargées de l'application de la loi et de la sécurité, par exemple, ont besoin d'organisations comme Europol, Interpol, l'Institut interrégional de recherche des Nations Unies sur la criminalité et la justice pour les aider à évaluer la menace et

établir des liens cruciaux entre les délits dans des parties du monde souvent très diverses.
Pendant des années, la communauté internationale a décrit la cybercriminalité comme un problème sans frontières. Il nous faut passer à l'action et apporter des réponses coordonnées qui ne soient pas seulement ponctuelles, mais adaptées à l'évolution des technologies d'Internet. En travaillant ensemble avec l'objectif commun de garantir un Internet plus sûr, nous parviendrons non seulement à répondre aux menaces actuelles aussi efficacement que possible, mais aussi à être préparés pour l'avenir.
https://unchronicle.un.org/fr/article/combattre-l-industrialisation-de-la-cybercriminalit

Comment s'organiser contre la cybercriminalité

Avec le développement des nouvelles technologies, la criminalité informatique ne cesse d'augmenter. Les entreprises doivent désormais être capables d'identifier précisément le risque.
La lutte contre la cybercriminalité constitue un enjeu juridique et économique considérable pour les entreprises. Le développement des nouvelles technologies et la révolution numérique n'ont fait qu'accentuer ce risque. Si au départ cette forme de criminalité fut l'œuvre d'individus isolés, elle est désormais le fruit d'organisations criminelles internationales. Le cybercrime s'est ainsi professionnalisé avec la création, notamment, de réseaux de plus en plus structurés, spécialisés dans le trafic de drogue, la prostitution, le blanchiment d'argent ou l'espionnage industriel. La cybercriminalité est l'une des formes de criminalité qui connaît la plus forte croissance tant au niveau national qu'international.

Sous de multiples formes

La cybercriminalité revêt de multiples formes que les entreprises doivent appréhender en fonction de leur domaine d'activité. Au nombre des infractions rencontrées, on compte les fraudes informatiques ou atteintes aux systèmes de traitement automatisé de données, les violations de données personnelles, les atteintes à l'e-réputation, la diffusion de contenus illicites, la contrefaçon de marques, d'œuvres et de logiciels, ou les infractions de droit commun commises via l'utilisation des nouvelles technologies, notamment par internet.
Diversifié, complexe, ce type de délinquance se caractérise aussi par des motivations très variées (gain financier, défi technique, espionnage industriel…). Plus grave encore, la majorité des cyberattaques serait interne aux entreprises.
Les entreprises doivent donc bien connaître les risques qu'elles encourent en cas d'attaques. Celles-ci ont souvent d'importantes répercussions financières, du fait, par exemple, de l'arrêt – même temporaire – d'un service informatique. De même, la fuite de secrets industriels et la perte d'actifs incorporels stratégiques peuvent s'avérer gravement préjudiciables. La cybercriminalité fait également peser un « risque de réputation » significatif sur les entreprises. En cas d'attaque, leurs données personnelles, celles de leurs partenaires commerciaux ou de leurs clients peuvent être dérobées et divulguées. Les entreprises doivent donc prendre conscience du risque pénal que la cybercriminalité leur fait courir, si notamment elles se trouvaient associées – via leur réseau informatique – à toute sorte d'actions illégales tel que le « spamming » (l'envoi de messages publicitaires indésirables en grande quantité). Leur

responsabilité pourrait également être engagée en cas de non-respect de la réglementation relative à la sécurisation des systèmes d'information.

Une politique de défense

Des solutions pour faire barrage à la cybercriminalité se mettent en place. L'explosion du nombre de cyberattaques a ainsi contraint la France à adopter une politique de défense visant à protéger ses systèmes d'information. Elle s'est dotée de divers organes spécifiques pour lutter contre la cybercriminalité au niveau de la police, de la gendarmerie ou des douanes. Par ailleurs, le procureur de Paris, François Molins, a annoncé le 4 septembre la création d'un pôle au sein du parquet de Paris dédié à cette forme de délinquance. Enfin, le caractère transfrontalier de la criminalité impose aux États la mise en place d'actions concertées visant à établir des politiques de coopération internationale.

Un Centre européen de lutte contre la cybercriminalité (EC3) a été créé en janvier 2013, dont l'objectif est la protection des entreprises européennes contre les activités illicites en ligne et les attaques des systèmes d'information. C'est aussi dans ce cadre que la directive 2013/40/UE relative aux attaques contre les systèmes d'information a été adoptée le 12 août 2013 par le Parlement européen. Ce texte prévoit l'harmonisation des législations en vigueur en matière de lutte contre la cybercriminalité et l'instauration d'une coopération renforcée dans l'Union européenne par la mise en place d'un système coordonné de suivi des infractions.

Le cyber-risque constitue désormais une menace substantielle que les dirigeants d'entreprise doivent anticiper. Une vigilance renforcée s'avère nécessaire à tous les échelons de leur hiérarchie des entreprises, garantes du respect du contrôle interne et de la protection de leurs actifs.

À surveiller

- L'entreprise doit connaître les techniques employées par les cybercriminels pour appréhender ses éventuelles faiblesses.
- Elle doit évaluer l'impact d'une attaque sur son organisation et celle de ses partenaires.
- En cas d'attaque, l'entreprise doit pouvoir identifier quels services de police sont compétents et quelles sont les nouvelles réglementations qui peuvent la protéger.

Cybercriminalité : Un aperçu du monde des criminels virtuels

Avec l'apparition du cyberespace et de l'Internet, une nouvelle forme de criminalité a pu apparaître. Couramment désignée par« cybercriminalité », cette dernière constitue l'une des formes de crime augmentant actuellement le plus vite – sans que l'on n'y accorde une attention suffisante.

De l'autre côté de l'écran

La cybercriminalité renvoie aussi bien à des infractions propres aux nouvelles technologies (cyberchantage, piratage) qu'à des infractions commises au moyen des nouvelles technologies (vol d'identités bancaires, réseaux pédophiles ou de proxénétisme, blanchiment d'argent…). Elles peuvent toucher les individus tout comme les entreprises ou les Etats. Surtout, une attaque cybercriminelle peut aisément affecter un nombre considérable de cibles simultanément. Ses effets sont soit immédiats soit différés, ce qui rend leur impact d'autant plus incertain à appréhender.

Il est difficile de mesurer l'ampleur du phénomène au niveau international. En effet, les statistiques sont rares et proviennent majoritairement des pays anglo-saxons.
Aujourd'hui, ce sont plutôt des personnes isolées (par exemple les hackers) ou bien des personnes organisées en réseaux et appartenant à des groupes criminels qui vivent de leurs activités clandestines.
Les premiers sont souvent des amateurs cherchant une forme de reconnaissance sociale. Ils utilisent leurs compétences en informatique à des fins criminelles plus par défi que par réelle intention de nuire. Ils peuvent éventuellement se regrouper, comme les Anonymous, formant ainsi une sorte de communauté. Ce sont généralement des individus spécialisés dans un domaine, par exemple le « craquage » de sites protégés.
Leurs motivations ne sont pas majoritairement d'ordre politique. Beaucoup d'entre eux se révèlent au contraire très sensibles à l'appât du gain.
Quant aux groupes cybercriminels, ils sont restés pendant longtemps fragiles : pas de confiance entre les acteurs, peu de moyens financiers…Cependant, ils ont rapidement su percevoir les avantages présentés par le monde virtuel et s'y adapter, conduisant ainsi à une véritable professionnalisation du milieu. Parmi les membres de ces réseaux, on trouve beaucoup d'individus ayant déjà un casier judiciaire pour des crimes « mineurs » (vols, voies de faits…).

Un phénomène en pleine expansion

Depuis les années 2000, la cybercriminalité se développe fortement. Cela est favorisé notamment par l'accès croissant des individus à l'Internet (en particulier dans les pays du Sud) et la diversification des supports (principalement dans les pays du Nord) permettant de se connecter : ordinateurs, téléphones portables, tablettes, wi-fi…
Ainsi, le nombre de victimes potentielles augmente de façon exponentielle. Ces victimes potentielles sont souvent bien peu protégées par rapport aux dangers encourus. Cela provient à la fois des connaissances limitées des usagers, qui ont donc une maîtrise insuffisante de l'outil informatique (particulièrement les citoyens ordinaires) mais aussi du fait que les nouvelles inventions technologiques contiennent de nombreuses failles. Par exemple, la facilité déconcertante avec laquelle certains comptes en ligne, comme sur les réseaux sociaux, sont piratés, révèle bien une insuffisance d'efforts en amont alloués à la protection des données personnelles des utilisateurs. Le terme de cyberespionnage est par ailleurs apparu pour désigner l'ampleur de ces attaques visant les entreprises et les Etats.
Par ailleurs, le milieu même dans lequel s'inscrit la cybercriminalité explique en partie la hausse des actes cybercriminels. Le cyberespace présente en effet de grands avantages, dont celui de pouvoir agir activement dans l'ombre. Le piratage d'un compte bancaire est une attaque peu coûteuse (prix de la connexion à Internet), rapide, réalisable dans l'anonymat le plus complet et sans laisser de traces. Le responsable se trouve quelque part sur l'immensité de la Toile.
Les sociétés actuelles tendent à être de plus en plus dépendantes de l'informatique, ce qui se traduit notamment par l'immatérialisation croissante d'un nombre colossal de données (formulaires administratifs, circulation des capitaux…), alors que le système n'est pas davantage protégé. Le nombre de failles dans lesquelles les cybercriminels peuvent se glisser augmente en conséquence. Les possibilités d'attaques sont ainsi toujours plus grandes et les risques encourus très faibles. On devine que les profits générés par les groupes criminels en mesure désormais de s'internationaliser sont considérables. Plus facile à blanchir, une grande partie de cet argent est réinvestie dans l'activité criminelle ; si bien que le phénomène est auto-entretenu par ces acteurs non étatiques qui gagnent irrésistiblement en puissance.

Les réactions contrastées des autorités

Les Etats ont bien mesuré l'importance de la cybercriminalité. Cependant, du fait même de sa nature, cette dernière bouleverse les méthodes classiques d'appréhension du crime. Il devient très difficile de répondre à des questions aussi basiques et fondamentales que « qui m'attaque ? », « par quel moyen ? », « dans quel but ? », « quel dommage causé ? ». De même, l'anonymat des cybercriminels et l'impossibilité de tracer leurs actions rendent la collecte de preuves du crime quasiment impossible.

Le problème de la juridiction des Etats sur l'Internet, espace sans frontières définies, complexifie davantage le problème. Un nom de domaine comme « .fr » ne garantit pas une pleine et entière application de la législation française sur le site. Les cybercriminels savent tirer profit de cette situation. De plus, qui serait capable aujourd'hui de dire, pour un criminel de nationalité A ayant commis un crime dans la cyberjuridiction d'un Etat B, selon quelle législation il sera jugé ?

Cela implique la nécessité d'une coopération interétatique et d'un droit international pour l'Internet. Parce que la cybercriminalité prend place dans un cadre global, la réponse apportée doit être tout aussi internationale. La convention de Budapest adoptée par 32 Etats en 2001, texte à ce jour le plus significatif en la matière, va clairement dans ce sens.

Ainsi, les initiatives étatiques se multiplient pour lutter contre la cybercriminalité. Certains Etats font d'ailleurs preuve d'un zèle exceptionnel. La France, par exemple, a créé de nombreux services dans ses ministères, avec des équipes spécialisées en informatique. Les Etats-Unis, la Grande-Bretagne ou encore l'Allemagne disposent eux aussi d'unités spéciales, avec des effectifs variables : la National Security Agency emploie 3 000 personnes tandis que le Bundesamt für Sicherheit fonctionne avec 450 employés. En matière d'arrestations, leurs efforts sont mitigés. Le nombre d'arrestations, par rapport au nombre de cybercriminels identifiables, est en constante augmentation mais reste maigre.

Par ailleurs, une manière efficace de lutter contre la cybercriminalité serait de faire de la prévention du côté des victimes potentielles. Une meilleure éducation de la population quant aux risques encourus et aux protections existantes réduirait sans doute le nombre de comportements inconscients. Les cybercriminels tirent une grande partie de leur force du fait que leurs victimes ne se méfient pas d'eux. Il s'agit donc de mettre un terme à cette ignorance de l'existence de réseaux nuisibles.

Dans ce domaine et dans d'autres, l'Etat n'est pas le seul à pouvoir agir, bien qu'étant prépondérant en tant que détenteur de la puissance législative et judiciaire. L'action récente de l'ONG néerlandaise « Terre des hommes » est la preuve que d'autres acteurs peuvent jouer un rôle efficace. Cette ONG, spécialisée dans le combat contre la pédopornographie sur le web, a créé un personnage informatique, une petite fille appelée Sweetie. Prétendant être originaire des Philippines, elle s'est rendue sur divers sites consultés par des pédophiles, lesquels ont massivement cherché à entrer en contact avec elle. Le personnel de l'ONG a alors collecté des informations sur ces hommes, réussissant souvent à trouver leur localisation, leur nom, leur numéro de téléphone… Un imposant dossier regroupant ces données a ainsi pu être déposé chez Interpol. Reste à savoir si les arrestations suivront.

https://classe-internationale.com/2014/01/04/cybercriminalite-un-apercu-du-monde-des-criminels-virtuels/

Criminalité réelle dans le monde virtuel

Avant d'aller vous coucher, vous éteignez votre ordinateur – ou pas... Pendant votre sommeil, un pirate informatique prend le contrôle de votre appareil via le câble Ethernet ou le réseau sans fil. L'opération se répète cent fois aux quatre coins du monde pour créer une véritable armée d'ordinateurs «zombies». L'attaque pour saturer les serveurs informatiques peut commencer.

Cette histoire n'est pas le scénario d'un film de science-fiction. Mais il suffit de débrancher Internet durant la nuit pour éviter de devenir le complice bien involontaire de pirates informatiques. «Les citoyens doivent adopter une meilleure hygiène informatique : faire les mises à jour, utiliser un antivirus, faire des sauvegardes. Les terminaux informatiques – ordis, téléphones, tablettes – susceptibles d'être piratés se multiplient», souligne Hugo Loiseau, professeur à l'École de politique appliquée.

Avis aux adeptes du stockage dans le nuage (iCloud, Dropbox…) : si vous avez des photos compromettantes, enlevez-les! «L'Agence nationale de la sécurité américaine (NSA) navigue sans contrainte dans le nuage. Si elle le peut, des informaticiens ou ingénieurs aux intentions criminelles sont aussi capables de le faire», avertit Hugo Loiseau.

Du petit-fils emprisonné au «généreux» détenteur d'un fonds fiduciaire en Afrique, les nombreuses fraudes sur Internet s'ajoutent au piratage. «Il faut développer auprès des citoyens – surtout les jeunes – cette capacité à poser une réflexion critique devant tout ce qui leur est envoyé», croit Hugo Loiseau.

«L'augmentation importante du phénomène du cyberespace démultiplie les possibilités de diffusion, et les cybercriminels en profitent, explique-t-il. Les activités criminelles traditionnelles sont donc décuplées : fraude, méfaits, vol, pédopornographie, propagande haineuse…» À l'échelle planétaire, la cybercriminalité engendrerait des pertes d'environ 600 milliards de dollars. Un chiffre immense comparé aux revenus liés au trafic de cocaïne et de cannabis, précise le professeur Loiseau.

Un ennemi évanescent

Cette conscientisation citoyenne est essentielle, car lutter contre la cybercriminalité revient à traquer un ennemi évanescent. Difficile de traduire un fantôme en justice. Imaginons que des pirates volent des données de cartes de crédit à Montréal. Ils transfèrent ensuite l'information sur un serveur en Roumanie, par exemple. Les policiers canadiens doivent donc demander au corps de police roumain d'intervenir – si ladite information se trouve encore en Roumanie. «Il y a plusieurs couches de complexité. Tout est décentralisé : les serveurs sur lesquels sont entreposées les données changent. Ils sont situés dans d'autres pays et il n'y a pas la collaboration internationale automatique. Les lois d'un pays ne s'appliquent pas à un autre pays», résume le professeur Loiseau.

Certes, les pays tentent d'unir leurs forces pour lutter contre la cybercriminalité. Les États-Unis, le Canada, l'Australie et plusieurs pays d'Europe ont signé une convention internationale sur la question en 2001… que seulement 14 pays ont ratifiée. Celle-ci n'est donc pas entrée en vigueur. «Il y a beaucoup d'obstacles : liberté d'expression, changements de gouvernements, lenteur des parlements», précise Hugo Loiseau.

Le côté noir du Web

Comme si ce n'était pas suffisant, les pirates informatiques brassent leurs affaires dans le monde obscur et caché du cyberespace : le *dark net*. N'y entre pas qui veut. Seuls des logiciels spécifiques et des clés de cryptage permettent d'accéder à cet Internet sous-jacent.

Une fois sur le *dark net*, on accède, entre autres, à un marché de matières illégales à ciel ouvert. On y trouve de tout : numéros de carte crédit, armes, drogues, etc. Les criminels réalisent leurs transactions en bitcoins pour enlever la traçabilité et faciliter le blanchiment d'argent.

Évidemment, les policiers mènent des enquêtes sur le *dark net*, mais bâtir la preuve est extrêmement difficile : «Tout repose sur la confiance. Le vendeur a une cote de confiance, selon les expériences de vente et d'achat antérieures, comme sur Amazon. Pour enquêter sur ce sous-réseau et l'infiltrer, les corps policiers doivent donc établir leur propre cote de confiance, explique Hugo Loiseau. Par ailleurs, les risques d'atteinte à l'intégrité physique d'une personne sont éliminés sur le *dark net*, puisque les échanges se passent dans le monde virtuel. Si une transaction tourne mal, la conséquence est la perte de confiance.»

Ces multiples obstacles à la lutte aux cybercriminels illustrent toute l'importance d'adopter une bonne «hygiène informatique» pour leur compliquer la tâche. Mais qu'en est-il de nos données sur les serveurs gouvernementaux, sont-elles bien protégées? «Il n'y a pas de garanties à 100 %. Les systèmes gouvernementaux commencent à être vétustes. Mais en général on peut avoir confiance. Il y a des vérifications faites régulièrement sur les réseaux gouvernementaux, bien que des failles puissent toujours survenir», affirme le professeur Loiseau.

Comment les cybercriminels s'emparent-ils de vos informations bancaires ?

Depuis quelques années, l'activité des cybercriminels est de plus en plus effrénée. Et pour cause, Internet avance à pas de géant chaque jour et le nombre d'internautes ne cesse de grandir et les quantités de données personnelles avec. A cela, s'ajoute l'essor du e-commerce. Un cocktail explosif qui fait des heureux chez les pirates !

Deux méthodes sortent du lot et mérites d'être détaillées car elles sont massivement exploitées par les pirates informatiques : le phishing et les malwares. Ce sont en effet les **t**echniques les plus répandues et les plus efficaces actuellement. Pour finir, nous aborderont la carding « physique ».

I. Le phishing ou hameçonnage

C'est vieux mais toujours très en vogue car le taux de retour de personnes trop crédules reste élevé… Le principe est d'envoyer un mail en ce faisant passer pour une organisation connue et de confiance et de demander des renseignements confidentiels.

Bien souvent, les pirates auront recours à des faux sites, plus ou moins réussis, qu'ils mettent en place à l'aide de kits de phishing achetés ou téléchargés sur la Toile. Certains se spécialisent dans la création de ces derniers, afin de les rendre disponible sur le BlackMarket.

Certains de ces sites sont de simples espaces extorqués à des sites légitimes après les avoir piratés via une faille Web ou serveur. L'URL est alors facilement détectable pour un œil averti, et le taux de retour ne sera de ce fait pas très élevé. Un cybercriminel mieux organisé et plus doué tendra plutôt à monter un véritable piège,

avec un vrai nom de domaine ressemblant en tout point avec celui d'une institution réelle mais aussi en poussant plus loin encore, par exemple en mettant en place un faux certificat SSL, faisant croire à un maximum d'internautes qu'ils se trouvent sur un site sécurisé, le tout grâce au fameux petit cadenas présent dans le navigateur de la victime…

Vous l'aurez compris, il faut impérativement vérifier tous les éléments d'un site afin de savoir si l'on ai réellement sur le vrai ou une simple copie. Dans la mesure du possible, n'accédez jamais à un site bancaire en ligne via un lien présent dans un mail mais tapez toujours l'URL directement depuis votre navigateur.

II. Les malwares

Qui n'a jamais été victime d'un malware ? Peu d'internautes vraisemblablement… et cela est logique à la vue des chiffres concernant les malwares connus sur la Toile et les technologies avancées que les pirates utilisent pour affiner ses derniers.

De multiples types sont dangereux pour vos données confidentielles. Les chevaux de Troie ou trojans tout d'abord. Ils sont capable de prendre subrepticement le contrôle de votre machine sans que vous ne vous en rendez compte. Ensuite, le pirate ayant la main dessus pourra espionner votre vie numérique, et vous dérober des données critiques, telles que vos identifiants bancaires ou vos données de carte de crédit lors d'un paiement en ligne. Les trojans bancaires sont très puissants et permettent des solutions sur-mesure pour récupérer le plus de données possible : capture d'écran régulières sur les sites bancaires afin de voler les codes tapés sur les claviers virtuels, form grabber capturant les identifiants saisis au sein des formulaires Web ou encore vol de mots de passe enregistrés sur la machine.

Ensuite, les keyloggers font aussi des dégâts, bien que ces derniers soient de mieux en mieux détectés par les solutions de sécurités modernes. Ils permettent d'enregistrer en local chaque frappe au clavier en local puis de les envoyer sous diverses formes au pirate de manière régulière. Les keyloggers permettent de simplifier la tâche du vol en lui-même mais nécessite un gros travail de tri ensuite… c'est pourquoi les pirates préfèrent utiliser des « form grabbers », qui ne capture que les données les plus intéressantes : vos identifiants.

Pour cela, le procédé se greffe sur votre navigateur Web et sniffe le trafic des requêtes POST envoyées à la suite de la validation d'un formulaire en ligne. Des mots clés types sont alors utilisés pour filtrer et ne garder que ceux qui ont un intérêt.

Pour finir, les « password stealer » font aussi beaucoup de victimes. Ces malwares cibles tous les logiciels installés sur votre machine pouvant stockés en local des identifiants utilisateurs. Et ils sont nombreux ! Les navigateurs Web, clients de messagerie et les clients FTP font partis des cibles prioritaires.

Les identifiants utilisateurs y sont stockés de manière chiffrée, dont l'algorithme diffère selon les logiciels. Les passwords stealers sont capable, lors de leur exécution, de localiser ces identifiants puis de les isoler et de les déchiffrer à la volée. Ensuite, il n'aura plus qu'à les envoyer discrètement au pirate via divers moyens plus ou moins efficaces : fichier texte sur un FTP, texte dans un e-mail ou encore via des requêtes HTTP vers une interface Web qui stockera les données en base de données.

En résumé, les techniques sont nombreuses et tout internaute est une cible potentielle. Il est non seulement nécessaire de posséder une suite de sécurité installée et à jour sur son système mais aussi de savoir naviguer et télécharger de manière réfléchie et de na pas tomber dans les nombreux pièges tendus par les pirates du Web.

III. Le skimming

Les techniques citées précédemment sont purement virtuelles et ne nécessites aucune intervention physique. Ce n'est pas le cas du skimming.

Dans ce cas, le pirate va se munir de matériel spécifique afin de piéger un distributeur automatique de billets (DAB) en y insérant son skimmer. Le but ? Copier les données de la bande magnétique de toute carte de crédit insérée dans ce dernier, et ce, en sans que l'utilisateur s'en aperçoive. Afin d'intercepter le précieux code confidentiel à 4 chiffres, un clavier piégé peu aussi être mis en place.
Une fois les données enregistrées, le pirate va pouvoir à l'aide d'autre matériel, transférer les données dans des cartes vierges, prévues à cet effet. Et voila, le tour est joué ! Il va ensuite pouvoir l'utiliser un peu partout sans être inquiété.
https://www.pcsansvirus.com/pages/emsisoft-anti-malware/attention-aux-phishing-dis-hameconnage-et-vos-donnees-personnelles.html

« La cybercriminalité est la nouvelle menace du XXIe siècle »

Pour riposter aux cyberattaques, les forces de l'ordre sont contraintes de se mettre au niveau techniquement et de développer des outils transnationaux.
Aussi, le Complexe mondial pour l'innovation, une forteresse high-tech dédiée à la lutte contre les cybermenaces, vient-il de voir le jour à Singapour. Explications.
Commissaire de police depuis 1976, Mireille Ballestrazzi, également présidente du comité exécutif d'Interpol, le réseau international des polices, décrypte pour *La Tribune* comment les forces de l'ordre françaises, européennes et internationales luttent contre la cybercriminalité.
À l'heure où Internet s'immisce partout, y compris dans nos objets connectés du quotidien, et que le Dark Web monte en puissance, la cybercriminalité s'impose comme « la menace du XXIe siècle » et pose un défi d'une ampleur inégalée aux forces de police.
La Tribune - Avec la numérisation de la société et de l'économie et le développement des nouvelles technologies, les crimes et délits se multiplient dans le cyberespace. Comment les forces de police abordent-elles cette problématique?
M.B - La cybercriminalité est clairement la nouvelle menace du XXIe siècle. Elle force les polices à repenser leurs moyens d'action, à se mettre au niveau techniquement et à développer des outils transnationaux, car l'échelle devient mondiale. Le cybercrime est d'autant plus difficile à appréhender qu'il prend des formes diverses et n'a, par définition, pas de frontières. Il peut s'agir d'apologie du terrorisme, de réseaux de pédopornographie ou de proxénétisme, ou encore d'attaques contre des systèmes de données, comme celle qu'a connue récemment TV5 Monde. Internet donne aussi aux malfaiteurs un nouveau terrain de jeu pour mettre en place des escroqueries comme la fraude à l'e-paiement, le blanchiment d'argent ou le trafic de stupéfiants. Le cyberespace permet l'expression de menaces inédites par l'utilisation des nouvelles technologies, mais il étend aussi le périmètre des crimes « classiques ». Avec la démocratisation de l'accès à Internet et l'innovation constante autour des nouvelles technologies, la cybercriminalité devient un enjeu de société, à la fois pour les gouvernements, les entreprises et les citoyens. Et ce n'est que le début : toutes les études tablent sur une augmentation significative du nombre de crimes liés à Internet dans les années et décennies à venir. Il s'agit d'un vrai défi pour les États et les polices du monde entier.
En tant que présidente du comité exécutif d'Interpol, vous avez inauguré, en avril dernier, le Complexe mondial pour l'innovation, situé à Singapour et

spécialisé dans la lutte contre la cybercriminalité. C'est l'outil qui manquait pour être à la hauteur de l'enjeu ?

Il est essentiel que la police tente d'avoir une longueur d'avance sur les malfaiteurs. Lutter efficacement contre le crime en général et contre la cybercriminalité en particulier demande la mise en place d'outils globaux. Interpol, dont le siège est à Lyon, remplit déjà cette mission. Il dispose de bases de données massives, sur la pédopornographie par exemple, alimentées par l'ensemble des polices du monde. En revanche, les crimes sur Internet nécessitent une attention particulière. C'est pourquoi les 190 membres d'Interpol ont accepté à une quasi-unanimité l'ouverture de cette nouvelle structure à Singapour. Le Complexe mondial transcende le modèle traditionnel répressif en matière d'application de la loi, en utilisant toutes les possibilités de l'ère numérique.

Quelles sont ses missions ?

C'est un centre ultramoderne, doté d'ordinateurs de grande capacité. Le choix s'est porté sur Singapour, car Lyon n'avait pas la place pour l'accueillir. Il dispose d'experts et d'équipements à la pointe du progrès, au service de deux grandes missions. D'abord, la recherche autour du développement des nouvelles technologies par les criminels, de manière à fournir aux services de police des outils de riposte adaptés. Ensuite, le Complexe fournit une aide aux enquêteurs du monde entier, via des formations, des échanges d'informations et un renforcement des capacités d'intervention. Il travaille aussi avec d'autres organismes transnationaux comme Europol, le réseau des polices des pays de l'UE. Actuellement, le centre compte 95 personnes, mais l'effectif va monter en puissance pour atteindre 160 employés d'ici à 2018-2019.

Concrètement, comment se passe la collaboration internationale pour lutter contre une cybermenace ?

Prenons l'exemple de la pédopornographie, qui prospère sur Internet. Il existe des sites d'une horreur absolue. Grâce à sa base de données, Interpol peut découvrir un réseau. Mais souvent, l'initiative part d'un pays membre, qui identifie un certain nombre d'adresses IP problématiques et ouvre une enquête judiciaire. Internet étant mondial, les adresses IP concernent souvent plusieurs États. Interpol contacte alors le bureau central d'Interpol dans chaque pays concerné pour mettre en place une coopération internationale. Celle-ci permet de partager les informations et de mener des actions simultanées comme l'arrestation, au même moment et dans plusieurs pays, de plusieurs organisateurs d'un réseau pédopornographique. Il arrive très régulièrement que la police française ou la gendarmerie participe à ce genre d'opérations. De même, la police judiciaire est en lien direct avec Singapour via un commissaire de police qui y est détaché. Nous collaborons aussi avec EC3, la plateforme d'Europol vouée à la cybercriminalité. L'objectif de toutes ces structures est d'être plus efficace sur le terrain mais aussi d'éviter les doublons, car lutter contre la cybercriminalité coûte très cher. Pourquoi faire enquêter plusieurs équipes, séparément, dans différents pays, quand on peut avoir une vision d'ensemble ?

Comment prenez-vous en compte le Dark Web, les tréfonds d'Internet, véritable repère de cybercriminels ?

Nous sommes démunis face au Dark Web. La quasi-totalité de nos actions se concentrent sur le Web ouvert, qui est déjà très large. Le Dark Web est un vrai problème, car les malfaiteurs les plus pointus techniquement l'utilisent de plus en plus pour des actions liées au terrorisme, aux trafics de stupéfiants ou au blanchiment d'argent. Nous sommes démunis, car nous n'avons pas assez d'outils pour l'explorer. Par définition, on ignore ce qui se passe sur le Dark Web, donc il est très difficile de le combattre. Nous échangeons régulièrement avec le FBI pour mesurer la menace du

Dark Web et pour mettre au point des outils technologiques qui nous permettront d'identifier les malfaiteurs qui y opèrent.

Quels sont les pays les plus ciblés par les cyberattaques et ceux qui produisent le plus de cybercriminels ?

En volume, l'essentiel de notre action porte sur les escroqueries et les fraudes. Les pays les plus riches sont, logiquement, les plus ciblés par les cybercriminels. Ils en produisent aussi beaucoup, même si les malfaiteurs peuvent provenir de toutes les régions du monde, y compris de pays qui sont moins attaqués, comme l'Afrique de l'Ouest. La filière nigériane, notamment, fournit beaucoup de pirates numériques qui agissent partout.

Une harmonisation des lois et des pratiques au niveau européen est-elle possible?

Des discussions sont toujours en cours, cela avance doucement. Il est clair que l'échelle nationale n'est pas suffisante, il faut agir au niveau européen et mondial.

Nous souhaitons que la Convention de Budapest, rédigée par le Conseil de l'Europe en 2005, soit transposée au niveau mondial. Il s'agit du premier traité définissant les grands principes de la cybercriminalité. Il tente aussi d'harmoniser certaines lois nationales pour améliorer les techniques d'enquêtes en augmentant la coopération entre les nations. C'est un combat de longue haleine, car les pays n'ont pas tous la même vision de ce qu'est la cybercriminalité et comment il faut la traiter. Il est important de s'organiser, car ce n'est que le début. On entre dans un monde connecté.

Demain, il y aura des voitures sans conducteur, par exemple. Cela soulève des questions sur les moyens de prévention et de riposte contre les pirates numériques.

Nous sommes dans une course-poursuite permanente pour nous mettre au niveau des cybercriminels, anticiper leurs attaques et utiliser la technologie contre eux. Plus les nouvelles technologies entrent dans notre quotidien, plus les possibilités d'infractions sont grandes, et plus la lutte contre les attaques est complexe

Cybercriminalité et gouvernance dans les TIC, l'UA s'arme à Bamako

Pour combattre la cybercriminalité sur le continent africain déjà stipulé dans la Convention de l'UA sur la cybersécurité et la protection des données à caractère personnel ,il s'est tenu à Bamako le vendredi 16 septembre dernier, la première session extraordinaire du comité technique spécialisé de l'Union Africaine sur la communication et les TIC.

Cette rencontre a réuni les ministres de l'UA en charge des télécommunications et des TIC, le Directeur exécutif de Smart Africa Hamadoun I. Toure, le ministre de l'Economie Numérique et de la Communication du Mali, Me Mountaga Tall en présence de la commissaire chargée des infrastructures et de l'énergie de l'UA, Mme Ilham Ibrahim.

Les travaux concernaient l'adoption du projet de Déclaration de leur organisation sur la gouvernance de l'Internet et des échanges sur les corrélations entre TIC et les autres domaines de la vie économique et sociale des Etats, ont aussi étaient abordées.

Pour Mme Llham Ibrahim les TIC sont un catalyseur des relations et coopérations entre les Etats et un volet important pour le développement du continent**.** Mme Llham Ibrahim a aussi exhorté les Etats à ratifier la convention de l'UA sur la cybersécurité et la protection des données personnelles.

Rappelons également que la Convention de l'UA sur la cybersécurité et la protection des données à caractère personnel est divisée en 4 chapitres :

- Chapitre 1 : les transactions électroniques
- Chapitre 2 : la protection des données à caractère personnel
- Chapitre 3 : promotion de la cybersécurité et lutte contre la cybercriminalité
- Chapitre 4 : dispositions finales.

Au sein des travaux, une information de taille a été soulignée par le Ministre Me Mountaga Tall : L'apport des TIC au Mali a permis de relever le taux de croissance du PIB à 6% en 2015 et les enjeux pour pérenniser la politique de l'Etat du Mali en la matière sont cruciaux.

Au final, tout ces travaux seront soumis au prochain sommet des chefs d'Etat et de gouvernement de l'Union africaine prévu en janvier 2017 à Addis Abeba.

Adoption des Conventions de Budapest et de Malabo : Un pas important de la cybersécurité et de la cybercriminalité

L'information est tombée comme un couperet : au titre des textes législatifs et réglementaires, le conseil du 30 mars 2016 a adopté les projets de loi autorisant le Président de la République à ratifier la Convention de l'Union africaine sur la cyber sécurité et la protection des données à caractère personnel du 27 juin 2014 et la Convention de Budapest sur la cybercriminalité du 23 novembre 2001 et son protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques du 28 janvier 2013.

L'adoption gouvernementale des projets d'actes réglementaires autorisant la ratification de ces deux instruments de lutte contre la cybercriminalité au cours d'une même réunion du Conseil des ministres, au-delà de la volonté politique qu'elle traduit, révèle de la part des pouvoirs publics une approche claire de la coopération en matière de cybersécurité et de cybercriminalité**.**

En effet, le Sénégal a engagé, dès l'année 2008, un vaste chantier de réforme du cadre juridique des Technologies de l'Information et de la Communication (TIC), qui s'est traduit par l'adoption de la loi n° 2008-11 du 25 janvier 2008 portant sur la cybercriminalité. Notre pays a également mis en place, au niveau de la *Division des investigations criminelles du Ministère de l'Intérieur et de la Sécurité publique, une Brigade spéciale de lutte contre la cybercriminalité (BSLC), ayant une compétence nationale.*

Cependant, en dépit de l'existence de ce cadre législatif et institutionnel, il subsiste encore des *obstacles au traitement effectif de la cybercriminalité liés notamment à la nature planétaire du phénomène qui ignore les frontières des Etats, source de difficultés judiciaires dans la conduite des investigations*. Le Sénégal, n'aura pas besoin de transposer cette Directive, le dispositif juridique qu'elle prévoit étant en réalité inspiré de la loi sénégalaise n° 2008-11 du 25 janvier 2008.

Dans le cadre de l'Union africaine, les Chefs d'Etats et de Gouvernements, réunis les 26 et 27 juin 2014 à Malabo (Guinée Equatoriale) lors de la 23e session ordinaire du Sommet de l'UA, ont adopté la Convention africaine sur la cybersécurité et la protection des données à caractère personnel . La Convention de Malabo du 27 juin 2014 constitue une innovation majeure de la stratégie de lutte contre la cybercriminalité en Afrique ; elle retient une approche très large de la cybersécurité .

impliquant la lutte contre la cybercriminalité, la protection des données à caractère personnel et l'encadrement des transactions électroniques.
La convention de l'UA présente la particularité d'intégrer l'approche de cybersécurité dans la stratégie de lutte, impliquant notamment la promotion de la culture de la cybersécurité, l'élaboration d'une politique nationale de cybersécurité, la sensibilisation des populations, la formation des acteurs et la mise en place de structures de cybersécurité (CERT, structure d'investigation etc.).
Aussi, la ratification de la Convention de l'Union africaine favorisera-t-elle une consolidation des rapports de coopération entre le Sénégal et les Etats africains membres de l'UA.
Malgré, les vertus sont parées cette convention, les africains devraient, au risque de commettre un sacrilège, résister à la tentation de vouer un « culte panafricaniste » à ce traité au point de l'assimiler à l'unique outil de coopération contre le cybercrime. En réalité, la Convention de Malabo constitue un instrument continental de coopération, que seuls les Etats membres de l'Union africaine peuvent ratifier. Il s'agit d'une « convention fermée ». Or, la cybercriminalité n'est pas un phénomène criminel africain ou européen mais un fléau mondial.
Ainsi, malgré l'innovation que constitue ce traité, les Etats de l'Union africaine sont encore confrontés au défi de l'identification d'un instrument juridique international de lutte contre la cybercriminalité.
Mais, force est de constater qu'il n'existe pas encore, à l'échelle des Nations-Unies, un instrument juridique spécifique à la cybercriminalité.
Le seul instrument international de lutte contre la criminalité du cyberespace est la Convention de Budapest du 23 novembre 2001, entrée en vigueur 1e juillet 2004. Cet instrument juridique, s'il a été secrété dans le cadre du Conseil de l'Europe, n'en constitue pas moins le premier traité international visant à apporter des réponses pénales aux problèmes soulevés par la cybercriminalité. En effet, ouverte à la signature des Etats non membres du Conseil de l'Europe ayant participé à son élaboration, la Convention de Budapest est également ouverte aux autres Etats non membres, par l'adhésion (art. 37).
A cet égard, le Comité des Ministres du Conseil de l'Europe, lors de la réunion qui s'est tenue le 16 novembre 2011, prenant en compte le leadership du Sénégal en Afrique, a décidé de l'inviter à adhérer à la Convention de Budapest. Le Sénégal a donné une suite favorable à cette demande et c'est justement la procédure d'adhésion vient d'aboutir à l'adoption d'un projet de texte autorisation le Président de la République à ratifier (adhérer) cette convention.
La finalisation de la procédure d'adhésion présente le mérite d'arrimer notre pays à la lutte internationale contre la cyberdélinquance qui se joue des frontières des Etats. Ainsi, les autorités judiciaires et policières pourront obtenir l'assistance des Etats membres à la Convention de Budapest (USA, France, Afrique du ud, Japon etc.) ainsi que des acteurs globaux de l'Internet (Face book, You tube, Google, G mail etc.) dans leurs investigations ainsi que de l'assistance technique et opérationnelle du Conseil de l'Europe : obtenir le retrait d'une vidéo compromettante sur You tube, adresser une réquisition d'identification du titulaire d'un compte Yahoo impliqué dans la commission d'un délit, bloquer un compte Face book diffusant des contenus frauduleux etc.
L'option de la ratification de la Convention africaine de Malabo et de l'adhésion à la Convention européenne de Budapest révèle au grand jour que les autorités ont pris conscience des enjeux stratégiques qui s'attachent à la diversification des mécanismes de coopération en matière de cybercriminalité et de cybersécurité.

Au fond, face à la complexité du phénomène cybercriminel, tous les niveaux de coopération doivent être mis à contribution : le niveau sous régional (Directive de Abuja du 19 août 2011), l'échelle continentale (la Convention de Malabo) ainsi que l'ordre international (la Convention de Budapest).
En réalité, tous les chemins de la lutte contre l'impunité qui sévit dans cyberespace mènent Budapest, après des escales Abuja et Malabo.

Cybercriminalité
Retour sur les principales attaques informatiques en France et dans le monde

Selon a commission européenne, la cybercriminalité englobe 3 catégories d'activité criminelles :
1) Les atteintes directes à des systèmes informatiques (ou Système de traitement automatisé de données, ou encore S.T.A.D.) en perturbant leur fonctionnement, tels que les attaques par déni de services (appelé aussi denial of service attack ou aussi DOS) destinées à faire tomber un serveur (comprenez rendre inaccessible ou mettre en panne un serveur) à distance.
2) Réaliser des actes illicites en utilisant les outils numériques (escroqueries, vols de données bancaires ou personnelles, espionnage industriel, atteinte à la propriété intellectuelle, sabotage, accès frauduleux, fraudes, usurpation d'identité, phishing, création de PC zombies, contamination d'autres postes informatiques ou d'autres serveurs…)
3) Modifier le contenu d'un espace numérique pour y déposer ou diffuser des contenus illicites (pédopornographie**,** racisme, xénophobie**).**
Les cyberdélinquants n'ont d'autre objectif que de gagner beaucoup d'argent. Virus, spams, et autres botnets drainent plusieurs centaines de millions de dollars chaque année à travers le monde.
Sans nous étaler sur les 144 milliards de courriers électroniques qui transitent dans le monde chaque jour dont 70% ne sont que du spam, les 10 millions de français victimes d'actes cybercriminels et 75% de ces actes de cybercriminalité qui sont de grande envergure (Norton 2013) qui concernent les 3,2 milliards d'internautes dans le monde en 2014 (dont la moitié pour l'Asie),
https://www.lenetexpert.fr/cybercriminalite-retour-les-principales-attaques-informatiques-en-france-monde/

Chantage sur Facebook et autres cybercrimes: l'anonymat et le nomadisme en ligne de mire

Usurpation d'identité, "phishing", chantage à la photo dénudée... La cybercriminalité désigne les infractions pénales commises grâce à un système informatique, la plupart du temps connecté à un réseau.
Le 10 octobre 2012, le jeune Gauthier, 18 ans, mettait fin à ses jours à Brest, victime d'un chantage sur Facebook. Peu de temps auparavant, la jeune canadienne Amanda Todd, 15 ans, faisait de même ; victime de harcèlement sur les réseaux sociaux suite à la diffusion d'une photo dénudée d'elle. Ces deux tragiques faits-divers médiatisés ont

mis au jour, pour une grande partie du public, l'investissement d'Internet et surtout des réseaux sociaux par une certaine forme de criminalité, la cybercriminalité.
L'importance actuelle et future des réseaux sociaux va conduire à une prochaine prise de conscience massive de ce phénomène criminel. Pour être sereinement appréhendé, la cybercriminalité sur les réseaux sociaux doit faire l'objet d'une meilleure compréhension afin de pouvoir lutter contre efficacement.

La criminalité sur Internet est amenée à se développer

Le vecteur Internet est incontestablement un outil de développement de la criminalité et plus particulièrement les réseaux sociaux qui activent, subrepticement, une nouvelle fonctionnalité, celle de facilitateur du crime. Voilà donc ces gigantesques réseaux virtuels devenus le premier terrain de chasse pour le (cyber criminel. Car c'est tout naturellement l'utilisation de Facebook et des réseaux sociaux par des personnes mal intentionnées qui en font un instrument d'une criminalité plus classique.

Dès lors, cette forme de criminalité a de beaux jours devant elle. Le panel des infractions commises est aussi varié qu'étendu. Le réseau social peut ainsi être un instrument de préparation, de réalisation et de révélation de l'infraction. Il permet de préparer l'infraction en trouvant des victimes ou des co-auteurs. Il permet de réaliser l'infraction, comme c'est le cas pour des affaires de menaces, harcèlement, escroqueries, pédopornographies, etc. Il permet enfin de révéler l'infraction, comme la diffusion de contenus interdits ou protégés.

La cybercriminalité va se développer. Comment alors la combattre ? Cela suppose d'aborder le problème sous deux angles d'attaque, correspondant aux deux caractéristiques majeures de la cybercriminalité, qui expliquent à la fois son fabuleux développement et la difficulté pour les acteurs étatiques de s'y opposer. Elles tiennent en deux mots : le nomadisme et l'anonymat.

Lutter contre les paradis cybernétiques

Le levier du nomadisme est le plus difficile à combattre dans l'immédiat. Le nomadisme, ou l'ubiquité, est cette capacité des cybercriminels à s'affranchir des frontières. Frontières qui, elles, demeurent pour les forces et l'ordre et les magistrats dans le cadre de la coopération judiciaire internationale. Ainsi, à l'instar des paradis fiscaux, il existe des paradis cybernétiques.

Aussi, si l'exemple de la convention du Conseil de l'Europe sur la cybercriminalité signée en 2001 à Budapest doit être mis en valeur, force est de constater qu'elle demeure trop limitée à la fois dans son objet et dans le nombre de ses États signataires.

Dès lors, si le nomadisme nous empêche de lutter efficacement contre la cybercriminalité à court terme, nous devons concentrer nos efforts sur la question de l'anonymat.

Résoudre la question de l'anonymat

En effet, la coopération judiciaire ne pourra être efficace que si la question de l'anonymat et des délits sous-jacents, tels l'usurpation d'identité, est résolue préalablement. La lutte contre la cybercriminalité doit se faire dès à présent selon deux angles d'attaque : le juridique et les moyens humains.

D'un point de vue juridique, le corpus propre à chaque État doit orienter sa législation vers une plus grande responsabilisation des différents acteurs d'Internet – FAI, hébergeurs, éditeurs et autres – notamment dans leurs obligations légales en termes d'identification des internautes. A l'image du *know your customer* – KYC – dans les milieux financiers, un *know your customer Internet* – KYCI – renforcé permettrait une meilleure responsabilisation de tous les acteurs, y compris des internautes, afin de prévenir les comportements fautifs, sinon de les sanctionner.

Parallèlement, la question d'un allongement de la durée de conservation des données, actuellement fixée à un an, devrait être étudiée afin de permettre aux forces de l'ordre de pouvoir enquêter dans des délais de conservation des données compatibles avec la durée de prescription des délits. Enfin, il est urgent d'élargir à un plus grand nombre d'infractions la possibilité d'utiliser la procédure d'infiltration. Cette procédure, particulièrement efficace, permet de démasquer et de neutraliser les cybercriminels les plus actifs. C'est une demande forte des enquêteurs.

D'un point de vue humain**,** il conviendrait tout d'abord de renforcer les équipes qui doivent faire face à cette nouvelle menace. Il est en effet indispensable d'accroître le nombre d'enquêteurs spécialisés, à l'image des mesures proposées par le rapport Breton en 2005. Par ailleurs, une centralisation, par direction et au niveau national, de ces nouveaux effectifs serait porteuse d'efficacité, afin de créer suffisamment d'équipes d'enquêteurs aptes à prendre en compte les dossiers les plus complexes. Cette concentration d'enquêteurs devrait se faire au sein de la division lutte contre la cybercriminalité de la gendarmerie, de cyberdouane et de l'OCLCTIC.

Ces aspects répressifs doivent bien évidemment se faire concomitamment avec un développement des actions de prévention, d'éducation, de formation et de sensibilisation à l'utilisation et aux dangers d'Internet.

Internet doit demeurer un espace de liberté, mais également un espace de responsabilité pour tous les acteurs. Les réseaux sociaux, devenus incontournables, doivent être des acteurs dynamiques de la lutte contre la cybercriminalité aux côtés des pouvoirs publics.