Cybercriminalité : Enjeux et moyens d'action

« Quelles sont les enjeux, moyens d'action et les difficultés de la lutte contre la cybercriminalité dans une société "tout numérique" ? »

Sciences humaine économique juridique et sociales
2016-2017 / 3ème année STI

Par Pierre-Louis Palant, Charlotte Rambourg & Flavien Ronteix–jacquet

Professeur Pilote : Mr Bergeron

Résumé Ce dossier fait un éclairage sur la cybercriminalité, ces dangers, ces enjeux. En effet elle est une nouvelle menace que ce soit pour les entreprises, les institutions et surtout les populations. L'Etat et les entreprises se défendent, tout comme la population par l'éducation ou la sensibilisation. Malheureusement elle n'est pas parfaitement efficace, avec de nombreuses failles et des risques pour les libertés civiles.

Summary in English

Cybercrimes are becoming an even bigger threat than they ever were, thanks to the fast development of new technologies. There are many different forms of cybercriminality, from identity theft and international fraud, to cyberbullying and industrial espionage. To put it simply, a cybercrime is a crime committed using one or several computers and one or several networks, such as the Internet or TOR networks.

Anyone that has a computer and Internet access can be the target of a cybercrime. They are one of the fastest growing crime medium, mainly for one reason : It is low risk, but has the potential for high reward for the criminals who use available technologies appropriately, thanks to the anonymity the Internet procures.

People are individually vulnerable to such crimes. They are often not well or even not at all educated about new technologies and their risks, so they do not know how to protect themselves and are often unknowingly making mistakes that endangers them on the Internet. They are easy targets for scams, identity theft, and phishing (deceiving someone into giving their password willingly), and personal data theft.

Companies are less vulnerable, because the biggest of them have at least one employee in charge of cybersecurity. That does not mean that they are not targeted, but it is sometimes a bit more challenging for criminals. They are mostly victims of industrial espionage,spear phishing (highly personalised phishing attempt) and theft, particularly with ransom-wares, a type of malware that is being more and more used (+260% in 2015 according to Symantec).

Institutions such as government agencies or services are also at risk of being attacked by a cybercriminal. Even though they are probably the most protected, they have also the most reasons to be targeted. The whole infrastructure of a country could take a severe hit if critical services were compromised.

Such a threat must be countered. A large portion of cybercrimes could be avoided by educating people about them, to try and make them more responsible when using new technologies. Awareness campaigns could be particularly efficient, given that at the moment there are practically none.

Companies also need to be reminded of the risks. They often neglect cybersecurity, maybe because the people in charge are not well educated either. They have to upgrade their security

constantly, to inform their employees and to teach them the right behaviours. Investments in R&D in cybersecurity are also not sufficient enough.

Furthermore, governments can pass laws to protect their people and themselves against cybercrimes. The problem is, catching cybercriminals requires constant surveillance. This raises interrogations and worries about private life and about what the government knows of its people. Governments also have to protect the private life of their people, who has to be vigilant every time a surveillance law is proposed.

Cybercrimes will continue to grow unless structural changes are made. Networks know no borders, unlike law enforcement, making cybercriminals even harder to catch. They could be committing their crimes from the other side of the world, and extradition deals are a slow and uneasy process. There needs to be unification of the means of fighting cybercriminality.

But in the end, cybercriminality is just another form of criminality, which is as old as mankind. Some Humans are criminals, and to this day we have found no way of preventing that. For now we can only make technologies safer to use.

Remerciements

Nous remercions la documentaliste pour son aide durant la recherche documentaire ainsi que notre professeur pilote, mr Bergeron pour son accompagnement tout au long du projet.

Sommaire

Introduction **5**

1 La cybercriminalité, une nouvelle menace ? **7**
1.1 Pour l'économie 7
1.2 Pour les institutions 8
1.3 Pour les populations 9

2 ...Contre laquelle il faut lutter **11**
2.1 Par l'Éducation 11
2.2 Par l'auto-défense des entreprises 12
2.3 Par la législation et la question de la surveillance 13

3 ...tout en surmontant des difficultés **16**
3.1 Le respect de la vie privée 16
3.2 Les limites des législations 18
3.3 Le facteur humain 19

Conclusion **21**

Appendices **22**

Introduction

Fraude internationale sur internet, attaque informatique ou usurpation d'identité sur Facebook, **la cybercriminalité a de nombreux visages** et ne cesse de s'amplifier avec le développement des **nouvelles technologies**.

La cybercriminalité regroupe **l'ensemble des infractions pénales commises par le biais des réseaux informatiques**, notamment sur Internet. Les criminels sont de plus en plus ingénieux pour utiliser les technologies modernes afin de commettre diverses infractions. Ainsi certains criminels « traditionnels » se sont déplacés vers l'arnaque et le piratage informatique.

Du côté des particuliers, on compte de **nombreuses attaques comme** : le piratage des données et des systèmes informatiques, le vol d'identité, la diffusion d'images d'abus pédosexuels, l'escroquerie lors de vente via des annonces ou aux enchères sur Internet (vente d'objets volés ou marchandise non livrée) l'accès non autorisé à des services financiers en ligne, la propagation de virus, le déploiement de botnets, les escroqueries diverses et variées via email, tels que l'hameçonnage (« phishing »), etc...

C'est l'une des formes de criminalité qui connaît actuellement la croissance la plus forte : **le relative'anonymat que l'on a sur internet est un atout pour le cybercrime**.

Du côté des arnaques sur les réseaux sociaux, la France est le quatrième pays le plus touché dans le monde et le deuxième en Europe. Symantec a dénombré 300 000 cas de ce type l'an dernier. *Les arnaques qui passaient autrefois par les spams ont tendance à se répandre sur les réseaux sociaux*, indique Laurent Heslault, le directeur stratégie sécurité chez Symantec.

En 2015, **les failles de sécurité ont causé la perte ou le vol de 429 millions d'informations personnelles dans le monde**, dont un tiers de données médicales. En France, le vol de données a fait 2 millions de victimes l'année dernière, selon un rapport de Phishing Initiative. Un chiffre probablement en deçà de la réalité, car 85% des entreprises refusent de dévoiler la quantité de données perdues. *En dissimulant l'impact réel d'une attaque, il est difficile d'évaluer les risques encourus et de renforcer sa protection contre les attaques futures*, regrette Laurent Heslault.

Quant aux **programmes malveillants**, ils se multiplient et ont atteint le nombre de 430 millions en 2015, contre 22 000 dix ans plus tôt ! Les principales menaces sont les "ransom-

wares", en français «rançongiciels» qui sont aussi en plein essort, +260% selon symantec en 2015.

Difficile d'arrêter les cybercriminels, car il faut les prendre sur le fait. Il n'est pas toujours aisé pour les autorités compétentes de rassembler les preuves, en raison de la technicité et de la rapidité d'exécution des infractions.

Tout ceci démontre **l'urgence de la situation**, surtout qu'avec notre société "tout numérique" nous allons vivre dans les années à venir une recrudescence de plus en plus importante de ces attaques. **D'où les questions de la protection des individus**, des sociétés et des institutions ainsi que des limites de la protection avec notamment la surveillance généralisé.

Chapitre 1

La cybercriminalité, une nouvelle menace ?

Aujourd'hui, **plus d'un tiers de la population mondiale à accès a internet**. Cela met à disposition un espace avantageux pour toute activité criminelle. La cybercriminalité se développe de plus en plus rapidement et atteint tout le monde.

1.1 Pour l'économie

Alors qu'en 1980, les cybercriminels solitaires recherchaient l'exploit, aujourd'hui ils cherchent à prospérer. Les victimes principales sont les PME. En effet, elles possèdent des brevets et fournissent des services importants. Le nombre d'entreprises françaises touchées entre 2009 et 2016 a été plus que doublé aujourd'hui. Les **attaques ciblent principalement les données économiques de l'entreprise**. Ainsi, les entreprises sont confrontées aux **« ransomware »** [1] qui chiffrent les données de l'entreprise puis demande à leurs propriétaires d'envoyer de l'argent en échange de la clé qui permet de les déchiffrer.

Contrairement à ce que l'on pourrait penser, les grandes entreprises sont toute aussi vulnérables face aux cybercriminel. En effet, les cybercriminel utilisent une technique dite « par rebond ». Le cybercriminel va cibler un sous-traitant à qui il va ensuite soutirer des informations sensibles.

La cybercriminalité s'oriente désormais vers le vol de savoir-faire, de propriété intellectuelle ou brevet alors qu'historiquement, cela se concentrait sur le vol de coordonnées bancaires.

Selon une étude du CLUSIF les type d'attaques les plus fréquente sont : **les infections par virus , les fraude informatique et télécom, le chantage ou extorsion informatique** comme vu précédemment. Les pirates s'attaquent aussi aux finances de l'entreprise (fraude au président) et on recourt à l'espionnage économique ou encore au sabotage de réseau.

1. rançongiciel ou logiciel de rançon est un logiciel malveillant qui prend en otage des données personnelles en les cryptant

La France connait une grand majorité **d'attaque ciblées ou spear phishing** [2] qui visent en très grande majorité les PME (77,46%) avec comme secteur privilégié, les administrations, l'industrie, les banques et l'immobilier. Le spear phishing est une technique dite d'harponnage en collaboration avec de l'ingénierie social [3].Contrairement à l'hameçonnage classique qui consiste à envoyer le même message à un grand nombre de personne en attendant qu'une réponse, le spear phishing se focalise sur un nombre réduit d'utilisateur auxquels on envoie un message hautement personnalisé. Alors que la majorité des attaques sont jugées sans gravité par les entreprises, leurs récurrences et leur conséquence sont de plus en plus préoccupantes.

Jusqu'à présent, l'**impact économique de la cybercriminalité demeurait difficile à quantifier**. Avec la collaboration du CSIS [4], McAffee [5] a réalisé une enquête afin de révéler le réel impact économique de la cybercriminalité sur nos sociétés. Cette enquête classe **les actes malveillants** en 6 parties :

La perte de la propriété intellectuel
La cybercriminalité
La perte de données sensible d'une entreprise
Les coûts d'opportunité
Coût supplémentaire de sécurisation des réseaux
l'atteinte à la réputation de l'entreprise

Le coût annuel de la cybercriminalité sur **l'économie mondiale est de plus de 400 milliard de dollars**. Cependant, malgré l'ampleur des phénomènes liés à la cybercriminalité, certain pays, gouvernement et entreprise sous-estime la menace naissante alors que sa vitesse et sa technologie ne cesse d'augmenter.

Dans les pays développé, la cybercriminalité à de grave conséquence sur l'emploi. Au état unis, elle cause la perte de 200 000 emplois américain. **En Europe, cela monterai jusqu'à 150 000**. Le coût le plus important de la cybercriminalité est l'atteinte à la performance de l'entreprise et à l'économie nationale. Elle porte préjudice au commerce, à la compétitivité, à l'innovation et à la croissance économique mondiale. Elle constitue une taxe sur l'innovation et ralentie le rythme de l'innovation mondiale.

Aujourd'hui les **gouvernements doivent consentir à élargir leur cybersécurité afin de contrer ces attaques qui menacent l'économie et la sécurité nationale**. Ils doivent sensibiliser les entreprise au risque que cela engendrent.

1.2 Pour les institutions

Les gouvernements sont toute aussi vulnérables face aux cybercriminel. Une nouvelle guerre est déclaré et elle se situe sur internet : **pas de combattant ni de champ de bataille, l'ennemie est ainsi anonyme**. On voit se développer une course aux nouvelles technologies

2. Password harvesting fishing « pêche aux mots de passes »
3. Forme d'acquisition déloyale d'information et d'escorquerie afin d'obtenir un bien, un service ou des information clés.
4. Center for Strategic and International Studies
5. McAfee, est un éditeur de logiciel initialement connu pour son logiciel anti-virus McAfee VirusScan

afin d'être mieux équiper en cas d'attaque. Le Livre blanc sur la défense et la sécurité national publié en 2008 **met en évidence les nouveaux risques et nouvelles menaces**. En effet : "*Dans les quinze ans à venir, la multiplication des tentatives d'attaques menées par des acteurs non étatiques, pirates informatiques, activistes ou organisations criminelles, est une certitude. Certaines d'entre elles pourront être de grande ampleur.*"

Les **attaques informatique massives qui ont frappé l'Estonie** [6] en 2007, sont bien une démonstration concrète de ce que peut être l'arme informatique. Les **attaques par « déni de services »** [7] perturbent et paralysent des systèmes essentiels à la vie quotidienne et permette de contrôler ces derniers à distance grâce aux « botnets ». Cela permet ainsi aux cybercriminels d'entrer dans des réseaux gouvernementaux sensibles discrètement. Une attaque aurait un impact majeur car les systèmes d'information dirigent la société d'aujourd'hui particulièrement pour les systèmes de gestion (par exemple le fichier centrale de la république française qui contient les identités de tout les citoyens). Les états, tout comme les entreprises, sont dépendant des systèmes d'information pour fonctionner convenablement. Ainsi, une attaque majeur sur ces système déréglerai l'équilibre instauré et aurai un impact économique important.

La vulnérabilité des réseaux informatiques n'est **pas uniquement un souci d'ordre technique mais de sécurité national**.

Ainsi, il y a peu de temps des **pirates informatiques russes ont lancé une cyberattaque contre le pentagone**. Cette attaque visait particulièrement la messagerie non confidentiel de l'état-major inter armées. Elle visait environ 4000 civils et militaire travaillant pour l'etat-major. Selon les retours sur l'attaque, **elle aurait été automatisée et à réussi, en moins de une minute, à récolter et diffuser des informations sur internet**. La cyberattaque a été coordonnée via des comptes cryptés et de réseaux sociaux. La provenance n'a toujours pas été déterminée par le gouvernement américain même si **sa sophistication et sa rapidité laisse penser qu'il s'agirait d'une agence gouvernementale**.

1.3 Pour les populations

La population est la plus touchée quotidiennement sur internet. On dénombre énormément d'arnaque qui touche chaque membre de la société. Le marché de la cybercriminalité est très rentable et arnaquer le premier venu est très simple. Le vol d'identité par exemple rapporte à lui seul 1 milliard de dollars par an.

Les moins de 30 ans sont plus exposés aux pirates informatiques que leurs ainés (Etude de Symatec). En effet, bien que l'on pourrait penser le contraire les jeunes née depuis les années 1980 sont les plus touché par ce type d'attaque. Il ressort qu'en Europe **plus de un quart des jeunes a déjà été exposé à la cybercriminalité**. Cela provient du fait que cette nouvelle génération est beaucoup plus « connectée » grâce aux nouvelles technologies. De plus, elle serait également moins vigilante (38% de cette génération avoue partager ses mots

6. Un des pays du monde le plus connecté, toutes les démarches administrative, les paiements et les contrats sont réalisés par internet

7. Demande de requête réalisé par des milliers d'ordinateur pour suspendre l'activité d'un serveur

de passe). L'étude menée par Symatec souligne que **près de la moitié des français 47% a déjà été confronté à la cybercriminalité** ! Parmis ce pourcentage, certain on déjà été attaqué par le biais de ransomware ou se se déjà fait voler leur coordonéee bancaire par des site marchand frauduleux par exemple. (Voir Annexe A & B)

On peut remarquer également que 25% des français n'utilise pas de mot de passe pour leur téléphone mobile qui contient des informations très importantes.

Le **cyberharcèlement** est également considéré comme un cybercrime. Bien que sous-estimer, il peut entrainer de grave conséquence particulièrement chez les enfants ou adolescent qui manquent encore de confiance. Le cyberharcèlement est une forme récente de harcèlement, alors que à la fin de la journée, la personne harcelé pouvais se réfugier chez elles, avec la naissance des réseaux sociaux, cela n'est plus possible : elle est poursuit. Il est désormais possible d'atteindre une personne en permanence, **l'ordinateur deviens alors un outil d'insulte, de menace ou de moquerie au service d'une personne pouvant rester anonyme**.

Le harcèlement scolaire est fréquemment accompagné de cyber harcèlement. En effet, **en 2006, un jeune sur dix était harcelé de manière régulière via internet**. D'après une enquête datée d'octobre 2011, 9% des élèves sont victime de cyber harcèlement par SMS ou internet.

Le harceleur bénéficie **via les technologies de l'anonymat**, ce qui peut augmenter le sentiment d'insécurité de la victime. Elle bénéficie également de l'absence de face à face, ce qui peut augmenter la violence du harcèlement, comme l'harceleur ne peut voir l'impact de ce qu'il dit sur sa victime. Puis, le caractère permanent des messages, vidéos ou photos diffusés en ligne sur les réseaux sociaux vont laisser des traces. Enfin, la diffusion massive permet des humiliations publiques visibles par un très grand nombre d'utilisateur : **la frontière spatiale n'existe plus dans ce type d'harcèlement**.

C'est ainsi que l'on voie toute l'importance que prends la cybercriminalité dans ses divers formes même si l'on n'a pas parlé de terrorisme, du trafic de drogue, d'arme ou d'humain (sur le darkweb [8] notamment) ou bien de la pédopornographie. Nous allons voire dans la prochaine partie comment on peut lutter contre ce fléau et enjeu du 21ème siècle.

8. Internet qui n'est pas accessible via les outils traditionnels de recherche

Chapitre 2

...Contre laquelle il faut lutter

Quand on pense à la cybercriminalité, on peut parler du coût financier qu'on ces attaques, ou le coût morale. Un exemple qui est arrivé le 4 décembre avec le piratage du réseau de tramway de San Francisco, rendant le service peu fonctionnel et gratuit nous rappelle que nous vivons dans une **société tout numérique où tout peut être attaqué et donc où tout doit être défendu**.

2.1 Par l'Éducation

À la fin de la première partie l'on a vu que la cybercriminalité est particulièrement active auprès des particuliers. Elle coûte de **l'argent** (près de 1.8 millards€en France par an selon Symantec), de la **sécurité des personnes**, et **une atteinte à la vie privée**. **La plupart des personnes touchées** (près de 13.7 millions de français) **par ces attaques sont les 18-34 ans** et reconnaissent eux-mêmes qu'il est indispensable de protéger ses informations personnelles.

Ceci est la preuve qu'il y a un vrai problème d'éducation et non de sensibilisation qui existe. Par exemple, qui laisserait un novice conduire sur une autoroute fréquentée ? Il va forcément avoir un accident. Pour internet c'est pareil, tout le monde peut se connecter à internet mais peu savent s'en servir ou se prémunir. Les plus jeunes ne sont pas épargnés car ils sont nés dans internet, la fameuse génération Z, **ils y passent près de 13h30 par semaine**. Ils sont conscients des risques mais n'ont eu que peu d'aide à leur autoprotection.

Aujourd'hui dans la plupart des pays du monde le système éducatif a compris **qu'il est primordial pour notre société tout numérique de former les citoyens de demain à ces nouvelles technologies**. Que ce soit pour savoir l'utilisation qui peut en être fait (comme la recherche d'information ou bien les outils collaboratifs, très utile en entreprise) que des risques qui existent. Malgré tout cette éducation est peu poussée, très scolaire et pas forcément en adéquation avec la réalité de l'utilisation des jeunes. **L'éducation tend tout de même vers une formation plus efficace** notamment en France avec les nouvelles lois liées à la république numérique, aux réformes scolaires. De plus, **des associations comme e-enfance.org organisent des ateliers de prévention aux risques sur internet dans**

les écoles, les MJC [1] et sont donc des soutiens précieux à l'éducation nationale pour la lutte contre la cybercriminalité auprès des jeunes. D'autant plus qu'un jeune qui a les bons gestes, les transmettra chez lui et donc faire d'une pierre 2 coups.

Or les adultes ne sont pas en reste puisqu'avec le développement des réseaux sociaux, du paiement en ligne, ils ont pris consciences du risque qui peut exister sur cet autoroute de l'information. Les médias ce sont donc emparés de ce sujet, à l'image de « zone interdite », « d'envoyé spécial », qui contribuent à une sensibilisation et une éducation de ces nouveaux risques auprès du grand public.

Comme on le voit **la formation et la responsabilisation des usagers d'internet** est la plus grosse partie du travail quant à la protection face à la cybercriminalité. Surtout que si l'on a des citoyens bien sensibilisés et prémunis face à ces menaces, on aura des employés qui seront actif pour la défense de leurs entreprises, comme on va le voir dans la prochaine partie.

2.2 Par l'auto-défense des entreprises

Comme on l'a vu dans la première partie, la cybercriminalité est quelque chose de nouveau et qui connaît une évolution très rapide. Mais pourquoi cette criminalité envers les entreprises ? Tout simplement, comme dans la criminalité traditionnelle, le but de l'attaquant est d'atteindre économiquement l'entreprise. Par exemple un vol de brevet, un détournement d'information financière peut être catastrophique, au point que l'on estime qu'en France il y a eu près de **3.36 milliards d'euros de dommage dû à la cybercriminalité**.

Mais alors comment se défendent les entreprises face à cette nouvelle menace ? Il faut distinguer deux types d'entreprises, les petites et moyennes et celles très grandes voire internationales.

Pour les premières les menaces sont à peu près les mêmes que pour les particuliers. Les moyens mis en place pour se défendre sont finalement les mêmes que pour les particuliers avec de l'éducation. Une différence notable est l'aide de l'ANSSI (Agence nationale de la sécurité des systèmes d'information) qui donne des conseils et sensibilise, face aux nouvelles menaces, les entreprises.

Il faut savoir que ce **sont les entreprises les plus attaquées** (80% des attaques sont contre des PME) car elles possèdent très souvent des brevets et/ou sont des sous-traitantes d'entreprises plus grosse (qui sont alors des passerelles privilégiées vers celles-ci) et qu'elles ont des systèmes de protection bien plus faibles.

Ensuite on a **les plus grosses entreprises**, et celles qui ont un intérêt industriel notable. C'est le cas des multinationales, des sociétés de haute-technologie ou d'armements. Elles sont particulièrement exposées avec l'utilisation massive de nouvelles technologies, que ce soit pour la communication interne ou externe (via les emails) , par la gestion multi-site ou les grandes

1. Maison des jeunes et de la culture

bases de données. Pour ces entreprises **la cyberdéfense est devenue une priorité**. On a aujourd'hui dans des entreprises pareilles des services entiers dédié à la **S**écurité des **S**ystèmes d'**I**nformation les **SSI**s.

Il existe aujourd'hui des **objectifs standardisés pour cette sécurité** : La **disponibilité**[2], l'**intégrité**[3], la **confidentialité**[4], et dans une moindre mesure, la **traçabilité**[5], l'**authentification**[6] et l'**imputation**[7].

Un exemple d'utilisation **des nouvelles technologies au service de la cyberdéfense d'entreprise** qui est intéressant est celui de la **Société générale**. Comme toutes les banques, elle possède un service de sécurité de l'information (pour éviter les piratages), mais depuis le début de l'année 2016, la banque a mis les big data[8] et le machine learning[9]au service de la traque des intrusions et des comportements suspects sur son système. Ce système permet de protéger les clients mais aussi les données financières de l'entreprise.

Ainsi aujourd'hui les entreprises sont de plus en plus sensibilisées à la sécurité de leurs systèmes face à la menace cybercriminel et il est aujourd'hui presque la norme d'**avoir un service dédié à cette auto-défense avec des méthodes de défense toujours plus pointue**.

2.3 Par la législation et la question de la surveillance

Internet est présent auprès du grand public déjà depuis les années 90'mais ce n'est que depuis peu de temps qu'en France le Pouvoir a pris conscience de l'impératif de créer des lois pour protéger ces citoyens.

En 10 ans, ce n'est pas moins **10 lois relatif à internet qui ont été adoptées**. Par Exemple les lois Perben II, DADVSI, Hadopi 1 et 2, Loppsi 2, LPM, loi anti-terroriste, loi sur le renseignement, loi sapin 2 et loi pour une république numérique.

Attardons-nous sur **la loi sapin 2** dans un premier temps, dont le nom complet est **« Economie : transparence, lutte contre la corruption et modernisation »** . Elle propose notamment la modernisation de la vie économique pour mieux protéger producteurs, consommateurs et épargnants. L'exemple qui est couramment cité est le problème des pubs de produit financier risqué sur certain site grand public. Beaucoup de français ont été arnaqué par des sites peu scrupuleux qui promettaient de gagner beaucoup d'argent sur des produits financiers

2. pas de coupure de service, ce qui peut avoir des dommages important sur le travail
3. les données ne doivent pas être corrompues
4. seul ceux qui ont le droit d'accéder à une donnée peuvent y accéder, peut-être le principal objectif car il empêche le vol de donnée
5. on garde un historique des accès à des données
6. gérer les utilisateurs et leurs espaces de travail
7. aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur
8. Enorme Base de donnée
9. la dernière méthode en matière d'intelligence artificielle, notamment développé par google, AlphaGo

obscurs. Avec cette loi ce genre de publicité sera interdit sur les grands site. Une première façon de **protéger les citoyens de l'arnaque**.

Ensuite que dire de la loi majeure quant à internet, la loi **« pour une république numérique »** (7 octobre 2016), qui, c'est exceptionnel pour le remarquer, a été co-écrite par 21330 citoyens avec un système de vote par article et amendement, propose **9 mesures** censées garantir une protection du citoyen sur internet.
La **neutralité du net**[10], la **portabilité des données**[11], le **droit du maintien à la connexion**[12], la **confidentialité des correspondance**[13], le **droit à l'oubli pour les mineurs**[14], **mieux informer** les consommateurs sur les avis en ligne[15], l'**ouverture des données publiques**[16], une **meilleur accessibilité**[17] et enfin **la mort numérique**[18] . Bref comme on le voie c'est une loi fortement accès sur les citoyens, leurs protections et leur vie numérique.

Ensuite, **internet étant mondial**, il a fallu mettre en place une gouvernance mondiale pour lutter partout contre la nouvelle menace. C'est ainsi qu'**INTERPOL** (Organisation internationale de police criminelle) a mis en place cette année un **Complexe mondial pour l'innovation** à Singapour qui a pour but de mettre en place des outils transnationaux de lutte contre la cybercriminalité. Mireille Ballestrazzi (directrice centrale de la police judiciaire) nous explique ainsi qu'avec la numérisation de notre société et de notre économie, il est devenu primordiale de se protéger à l'image de TV5monde pirater par des groupes terroristes. Interpol ainsi que d'autres organisation telles que l'Union Européenne cherchent donc à dépasser la simple sphère de l'entreprise ou de l'état et placer la **lutte au niveau international**.

Enfin, quelles sont les limites de cette législation, particulièrement à propos de **la surveillance et le contrôle d'internet** avec les lois Hadopi et anti-terroriste ? Aujourd'hui avec la menace terroriste, le gouvernement s'est retrouvé face à un dilemme, est-ce que l'on privilégie la liberté des utilisateurs d'internet ou bien est-ce que l'on restreint quelques libertés pour les protéger ? Question qui au final est centrale, **où est-ce que l'on place le curseur entre sécurité et liberté** ?

Avec la dernière monture de la loi de renseignement ou la nouvelle programmation militaire, le gouvernement à fait le choix d'espionner un peu à la méthode de la NSA aux Etats-Unis

10. le fait que les opérateurs ne peuvent discriminer l'accès au réseau
11. les prestataire de service doivent permettre l'exportation et l'importation de donnée venant de concurrent, les données appartiennent à l'utilisateur en somme
12. Dans une société tout numérique, l'incapacité d'accéder à internet et une source de discrimination et d'isolement, cet article garantit l'accès au réseau pour tous
13. comme pour la poste en 1950, la loi garantit que notre correspondance reste privée, même si comme on va le voir plus loin, il existe des moyens détournés pour l'état de tout de même surveillé
14. permet sur demande à la CNIL de supprimer des traces sur internet qui nuiraient à la vie de tous les jours
15. Toujours dans l'optique d'éviter les arnaques
16. tout citoyen aura le droit d'accéder au base de donnée publique en toute transparence
17. cela concerne les non-voyant et tous les citoyens en situation de handicap
18. que fait-on des données du citoyen mort ? à qui revient les données ?

pour arrêter les recruteurs, les radicalisés, les cybercriminels, qui sont très actifs sur internet.

Mais où se situe la limite entre puissance des outils de surveillance et de contrôle et liberté, neutralité du net ? D'où une vraie question de respect des libertés et de la vie privée ?

Chapitre 3

...tout en surmontant des difficultés

Comme on l'a vu dans la partie précédente, la lutte contre la cybercriminalité existe et est plutôt efficace mais nous allons voir ici que ces moyens de lutte on tout comme toutes choses leurs limites, que ce soit en terme de respect de la vie privée, des limites de la législation ou bien de l'humain même.

3.1 Le respect de la vie privée

La surveillance systématique de la population pose de sérieux problèmes. C'est une méthode efficace pour la répression, mais on ne peut pas négliger la question du respect de la vie privée.

La vie privée est l'aptitude, pour une personne, à s'isoler pour se concentrer sur elle-même et protéger ses intérêts personnels. La vie privée peut s'apparenter à l'anonymat, à la volonté de rester hors de la vie publique et à la préservation totale des informations personnelles. A notre époque, il n'est pas facile de faire la distinction entre vie publique et vie privée. En effet, la frontière est de plus en plus fine. Les utilisateurs des NTIC mettent à disposition de plus en plus de données personnelles, c'est d'ailleurs presque obligatoire pour utiliser certains services gratuits (*si c'est gratuit, c'est vous le produit*).

Une donnée personnelle est une information qui permet d'identifier une personne de manière directe ou indirecte, comme un nom, prénom, photo, date de naissance, statut matrimonial, adresse postale, e-mail, adresse IP d'ordinateur, élément d'identification biométrique, etc.

Certaines informations sont décrites comme étant sensibles car elles peuvent entraîner un comportement discriminatoire. Ces données ne sont pas censées être collectées, cependant il est possible de les traiter sous certaines conditions, notamment si la finalité du traitement l'exige et avec le consentement explicite de la personne concernée. Certains fichiers sont créés sans approbation car ils sont essentiels à une activité garantissant la sécurité du territoire ou le respect des principes de la République. C'est le cas notamment du fisc, de la justice, de la CAF, etc.

61% des français considèrent que ces fichiers représentent une violation de leur vie privée (étude demandée par la CNIL octobre 2008) . Les français âgés de 18 à 24 ans estiment à 78% que leur vie privée est mal protégée sur Internet. Effectivement, de nombreuses technologies peuvent être considérés comme intrusives, des cookies [1] jusqu'aux systèmes de géolocalisation.

A priori, **personne n'est contre l'utilisation des données personnelles de criminels pour leur arrestation**. Le problème est que pour récupérer et traiter ces données, il faut d'abord les identifier, et cela implique de capter et d'effectuer un traitement de toutes les données collectées afin de différencier celles qui indiquent un comportement illégal. Une phrase qui revient automatiquement dans un débat sur la vie privée et la surveillance de masse est **« Si vous n'avez rien à cacher alors vous n'avez rien à craindre »**. Il ne faut cependant pas oublier que les m½urs et les lois changent, et que ce qui était illégal il y a 50 ans ne l'est plus forcément aujourd'hui. Des fichiers de surveillance de masse, réalisés avec les moyens de l'époque, ont été utilisés par le passé pour faire le mal, notamment le fichier Tulard qui servit pour la rafle du Vélodrome d'Hiver. Avec des technologies plus développées, qui sait combien d'autres personnes auraient vécus l'enfer des camps ?

C'est pour cela que **de nombreuses personnes et associations luttent contre le développement** ou du moins la généralisation de ces techniques de surveillance, considérant que leur seule existence est un danger pour le peuple. Grâce ces militants, des organismes de protection des données et de la vie privée ont vu le jour partout dans le monde. En France, c'est en 1978, à la suite de la révélation **du projet SAFARI** par le journal Le Monde quatre ans auparavant, qu'est promulguée **la loi relative à l'informatique, aux fichiers et aux libertés**. Cette loi, qui est seulement la troisième du genre dans le monde après l'Allemagne et la Suède, institue la **Commission Nationale de l'Informatique et des Libertés** (CNIL).

Les missions de la CNIL sont assez claires : Elle doit informer les citoyens de leurs droits, réguler les projets de loi relatifs à la protection des données, établir des normes, veille à ce que les citoyens puissent accéder à leurs données, vérifie que la loi est respectée, peut sanctionner lorsque elle ne l'est pas, et se doit de comprendre les développements des technologies afin de protéger au mieux les citoyens.

Ces organismes se sont réunis en **2009 et sont parvenus à la Résolution de Madrid**, qui définit les principes qui devraient renforcer le caractère universel du droit à la protection de la vie privée et des Données personnelles de tous les citoyens (y compris les enfants ou personnes vulnérables, et notamment sur Internet).

Cette résolution n'est pas légalement contraignante, mais vise à la rédaction et à la signature d'une Convention Universelle pour la protection des personnes à l'égard du traitement des données personnelles.La surveillance est, comme on l'a vu plutôt, à double tranchant. Les gouvernements ont du mal à trouver un juste équilibre entre respect de la vie privée et efficacité de la défense.

1. données sauvegarder par les sites internet sur l'appareil de connexion

3.2 Les limites des législations

Même si des lois sont écrites pour protéger les populations de la cybercriminalité, elles ne sont encore loin d'être idéales.

Ainsi, la plupart des lois ne peuvent s'appliquer **que dans leur pays,** alors que la cybercriminalité **ne connaît pas de frontière**. La CNIL protège les données de citoyens français, collectées par des sites ou organismes hébergés en France. Elle ne peut pas demander à la NSA de supprimer des données sur des citoyens français par exemple. De la même façon, à cause des différences de législation entre les pays, certains deviennent des « paradis » du crime virtuel. Difficile d'arrêter quelqu'un qui a commis un crime à l'autre bout du monde sans bouger de son fauteuil.Selon Vitaly Kamluk, chercheur en chef chez Kaspersky Lab, *« Nous pouvons travailler rapidement dans l ?espace cybernétique, mais nous perdons toute notre vitesse lorsque nous avons besoin de demandes et d ?autorisations pour franchir des frontières. »*

Prenons l'exemple récent des administrateurs **du site zone-telechargement.com**. Ce site proposait des milliers de films, séries, albums, jeux-vidéos en téléchargement direct, ou en visionnage streaming. Contrairement au téléchargement pair-à-pair, il est beaucoup plus difficile d'incriminer les clients de ce site qui télécharge du contenu illégal. De la même façon, le site n'est pas directement illégal puisqu'il est légal de visionner du contenu en streaming ou d'en télécharger une copie virtuelle si l'on possède déjà une version obtenu légalement. Impossible d'arrêter les deux administrateurs et créateurs du site, qui vivaient à Andorre, pour cette raison. En revanche, les autorités ont pu les arrêter et faire fermer le site (de manière critiquable d'ailleurs) pour suspicion de fraude fiscale et travail dissimulé entre autres.

Cela montre bien que le fait que **les lois ne peuvent pas couvrir toutes les cas d'utilisations des nouvelles technologies**, ce qui demande des efforts supplémentaires pour lutter contre la cybercriminalité.

De plus, les gouvernements sont pris entre l'enclume que sont nos droits et le marteau de la surveillance de masse :

La loi relative au renseignement du 24 Juillet 2015 en est un parfait exemple : elle a reçu énormément de critiques justement sur le fait qu'elle permet de court-circuiter les procédures judiciaires et de mettre les outils de renseignement directement dans les mains de l ?exécutif.

Ainsi, le juge anti-terroriste Marc Trévidic estimait que ce nouveau projet de loi était « une arme redoutable si elle est mise entre de mauvaises mains ». Il a fait part à la presse de son inquiétude notant : « Il y a une absence de contrôle totale dans cette loi » ; il a ajouté : « Il faut arrêter de croire que c'est le renseignement, acquis grâce à des écoutes/sonorisations/balises administratives, qui permet d'arrêter les terroristes ! Seul, le judiciaire permet d'interpeller (...) On n'envoie pas en prison, on ne débarque pas chez quelqu'un sur un simple renseignement (...) Demain, si un service de renseignement me dit que vous êtes un dangereux terroriste qui

projette de poser une bombe, devrais-je croire ce service sur parole, sans aucun élément ? C'est pourtant la tendance qui se dessine. »

A l'inverse le haut fonctionnaire Bernard Squarcini, ancien directeur central du renseignement intérieur, était plus mesuré quant à la Loi. Selon lui, « ces mesures sont nouvelles. Il faudra cependant attendre la pratique pour connaître leur efficacité et voir si elles correspondent à l'esprit et à l'attente des services »

Critiquée également par la CNIL, elle est la première loi ordinaire saisie devant le Conseil Constitutionnel par le Président de la République lui-même, **ce qui montre bien la dualité des institutions sur ce sujet**. D'un côté elles créent des organismes comme la CNIL, et de l'autre elles promulguent des lois qui sont faites pour les contourner.

3.3 Le facteur humain

Ce qu'il faut comprendre absolument lorsqu'on parle de cybercriminalité, **c'est que la plupart de ces crimes sont des transpositions dans le domaine numérique de crimes « classiques »**. Arnaques, espionnage, vol ? sont des concepts qui remontent à la nuit des temps. Un de nos lointain ancêtres a inventé le couteau pour la chasse, son voisin l'a utilisé contre lui. Il semblerait que quelque soit l'outil, l'Homme a toujours trouvé un moyen de le détourner pour nuire à son prochain. Les NTIC ne sont pas différentes, et l'anonymat que procure Internet a sûrement aggravé cette tendance naturelle.

Pendant la croissance fulgurante d'Internet, il a été très souvent rappelé que l'anonymat qu'il offrait pouvait être dangereux. Le cyberharcèlement par exemple, est trop souvent devenu dangereux parce que les harceleurs ne pouvaient pas être identifiés directement, est qu'ils en profitaient pour assaillir leur victimes sans limite. **L'anonymat a tendance à déresponsabiliser**, tandis que l'éloignement dû au virtuel limite la compassion et l'empathie, ce qui rend d'autant plus facile et accessible la cybercriminalité.

Rapidement, l'anonymat sur internet est devenu plus que relatif. Des outils ont été développés pour identifier les internautes. (Ce qui, au passage, a rendu les « chasses aux sorcières » virtuelles encore plus simple). Mais pour certaines personnes, l'anonymat sur le net est une question de survie. Journalistes, résistants, lanceurs d'alertes ? C'est en partie pour eux, mais aussi pour les gens qui en ont assez d'être constamment traqués par les sites commerciaux, qu'a été lancé l**e projet TOR en 2001**. Financé et développé par la DARPA et des universités américaines, ce réseau décentralisé et superposé permet d'anonymiser de manière presque infaillible ses utilisateurs. Comme son prédécesseur, il a très vite été détourné par ses utilisateurs. Des sites proposant différents **services illégaux ont émergés, comme Silk Road**, site permettant d'acheter et vendre des produits illicites et notamment des stupéfiants et qui aurait près de 1,2 milliards de dollars de ventes avant sa fermeture par le FBI en 2014.

Le facteur humain **n'est pas seulement la faculté de l'Homme a commettre un crime**. En effet, nous sommes parfois un peu lent à réagir et peu attentif à sa sécurité en ligne. C'est ce qui a permis à la cybercriminalité d'exploser en terme de chiffres, car les

institutions ont la plupart du temps mal compris et mal anticipé le développement de ces nouvelles technologies. Mal éduqué, il est très facile de se faire avoir par une tentative de phishing. Même dans notre Institut,où une des quatre orientations concernent la sécurité informatique, et qui forment de futurs ingénieurs, certaines personnes sont apparemment capables d'ouvrir des pièces jointes de mails suspicieux en anglais, sans se douter une seconde qu'il s'agirait d'une attaque informatique. Il y a donc un manque d'éducation flagrant du grand public dans ce domaine.

Conclusion

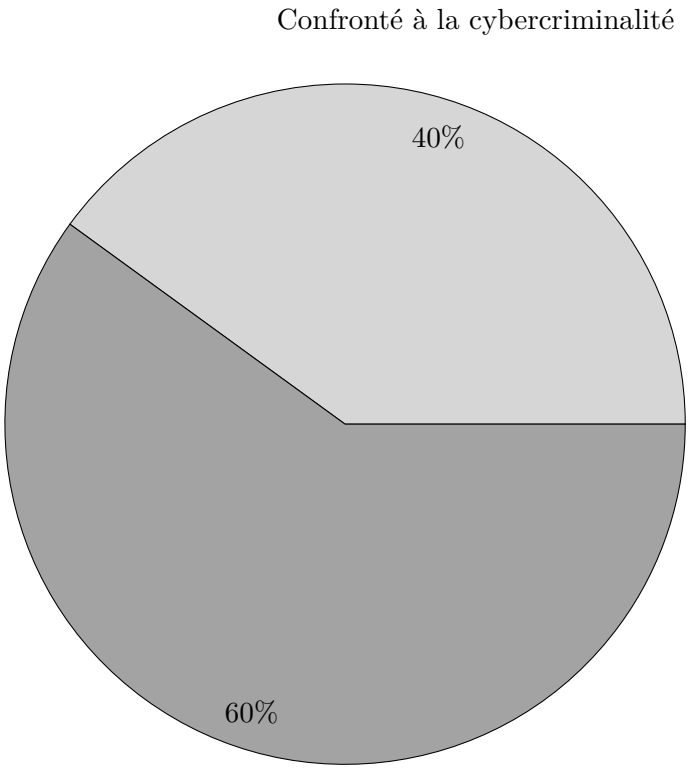
La cybercriminalité est une forme de **criminalité en plein essor**. Le développement rapide des nouvelles technologies ne font qu'aggraver ce phénomène. En effet, les sociétés n'ont eut que peu de temps pour s'y habituer et se protéger lors de leurs utilisations, et des utilisations malicieuses apparaissent toujours de plus en plus vite. L'exemple des **ransomware** est particulièrement marquant, car il n'y a toujours pas de méthode pour s'en débarrasser une fois infecté. **Les entreprises sont très ciblées** en raison des gains potentiellement plus élevés pour l'attaquant. **Les gouvernements, quant à eux, ne sont pas intouchables non plus**, même si de plus en plus d'attaques sont soupçonnées être organisées par d'autre gouvernement.

Les populations, peu éduquées sur ces sujets, n'en sont que **plus vulnérables**. Elles doivent être informées et sensibilisées au plus vite. La plupart des gens ne connaissent pas les risques d'être la cible d'un cybercrime. Les entreprises doivent aussi revoir leur sécurité, car leurs vulnérabilités peuvent mettre en danger d'autres entreprises. Comme pour un vaccin, **plus il y aura d'entreprises sécurisées, plus elles seront mieux protégées** . Les gouvernements doivent toujours se doter d'un appareil juridique à jour et efficace pour lutter contre la cybercriminalité. Mais la solution de la facilité est d'utiliser **la surveillance de masse** pour attraper les criminels. Très critiquée, cette méthode a le défaut d'être potentiellement très dangereuse pour les populations.

Il faut donc faire des **compromis entre les moyens déployés et leurs conséquences pour les peuples**. C'est pourquoi des organismes de veille ont été créés comme **la CNIL** en France. Leur but est de protéger les données personnelles des populations, et de faire du lobbying pour limiter les lois liberticides dans ce domaine. Mais ce n'est pas le seul problème dans la lutte contre la cybercriminalité. En effet, **les lois connaissent des frontières que les cybercriminels n'en ont pas sur Internet**. Procédures judiciaires (extradition par exemple) et méthodes d'investigation doivent être unifiées à l'échelle de la planète.

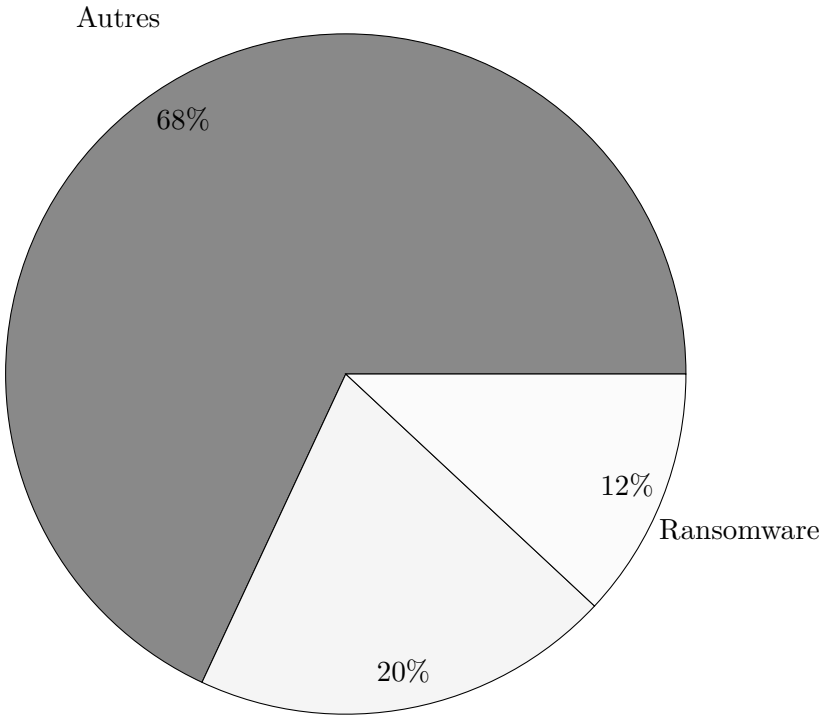
Enfin, **les faiblesses inhérentes** à notre espèce sont le plus gros facteur qui **joue en faveur de la cybercriminalité**. La plupart des utilisateurs des NTIC ne sont pas suffisamment responsables pour être protégés. Pour finir, la cybercriminalité n'est qu'une autre forme de criminalité, qui elle existe depuis aussi longtemps que l'Homme. Certaines personnes deviennent des criminels, et à ce jour, nous ne savons toujours pas comment l'empêcher, s'il est possible de l'empêcher.

A-Part de la population française confronté à la cybercriminalité



En 2014

B-Les attaques les plus fréquente



En 2014

C-Yahoo ! dément espionner ses utilisateurs sur ordre du gouvernement américain

Par Laszlo Perelstein | 05/10/2016

La décision de la dirigeante de Yahoo ! Marissa Mayer d'obéir à la directive des agences gouvernementales a "troublé certains cadres supérieurs" Mercredi dans la journée, l'entreprise a assuré que le scannage de courriels décrit par Reuters n'existait pas. Si l'information venait tout de même à être confirmée, il s'agirait du premier cas du genre, les géants de l'Internet ayant jusque là refusé un accès complet à leurs données et ne transmettant que des informations précises à la suite de demandes de renseignements. Derrière cette révélation, se cache la question du chiffrement des données de bout en bout.

De quoi ébranler Yahoo !. Le moteur de recherche et fournisseur d'adresses mail a conçu un programme pour rechercher des informations spécifiques sur les centaines de millions d'emails de ses propres utilisateurs à la demande d'agences de renseignement américaine (la NSA ou le FBI), révèle un journaliste de l'agence Reuters, qui cite trois anciens employés et une quatrième personne au courant des événements.

La décision de la dirigeante de Yahoo ! Marissa Mayer d'obéir à la directive des agences gouvernementales a "troublé certains cadres supérieurs et conduit en juin 2015 au départ du responsable de la sécurité informatique Alex Stamos", écrit Reuters. Depuis cette date, Alex Stamos occupe le même poste au sein du premier réseau social en ligne Facebook après être resté à peine 15 mois au sein de Yahoo !. Pour autant, l'entreprise s'est dite dans un premier communiqué à Reuters "respectueuse des lois", arguant qu'elle "se conforme aux lois des États-Unis". Plus tard dans la journée, un second communiqué transmis à l'AFP a réfuté les informations de Reuters. "Le scannage de courriels décrit dans l'article n'existe pas dans nos systèmes" informatiques, assure-t-il.

D'après les experts interrogés par l'agence de presse, il s'agit du premier cas du genre, les géants de l'Internet ayant jusque là refusé un accès complet à leurs données et ne transmettant que des informations précises à la suite de demandes de renseignements. Yahoo ! collabore ainsi avec les différents gouvernements du monde entier pour fournir des

renseignements sur plusieurs milliers des ses utilisateurs (29.000 demandes ont été formulée en ce sens en 2013).

Une "erreur" évitable grâce au chiffrement de données de bout en bout Derrière ce nouveau scandale, le sujet principal - récurrent ces dernières années et relancé par les attentats dans les pays occidentaux - est celui du chiffrement des données. Les géants du Net se voient en effet contraints de collaborer avec les États dans la lutte antiterroriste et ce alors qu'ils veulent également préserver les données de vie privée de leurs utilisateurs.

Dans le cas de Yahoo !, le réseau social s'est ainsi dit qu'il était inutile de porter plainte car il perdrait après que son service juridique a reçu la demande secrète des agences gouvernementales. Pourtant, si l'entreprise avait chiffré de bout en bout ses emails - une technique qui permet aux seuls destinataires du message d'y accéder, en l'état, Yahoo ! peut actuellement lire les données de ses utilisateurs -, cette surveillance de masse n'aurait pu se produire, comme le souligne le Guardian. Cette technique de chiffrement est d'ailleurs de plus en plus adoptée par les applications de messagerie. Dans la lignée de Telegram, Line, du dernier-né de Google Allo ou encore de WhatsApp qu'il possède, le réseau social de Mark Zuckerberg a ainsi activé le 5 octobre pour tous les utilisateurs de Facebook Messenger une option permettant le chiffrement des données de bout en bout. Et même Caramail, ancienne gloire de l'Internet français rachetée en 2009 par l'allemand GMX, voit cette pratique comme indispensable, l'intégrant depuis ce jeudi à son service d'emails de sorte que "leurs destinataires soient les seuls à pouvoir accéder à leur contenu". Utilisée également par Apple sur son iMessage, la technique n'est toutefois pas complètement inviolable, comme l'a démontré le long combat de la marque à la pomme contre le FBI avec au c½ur l'iPhone d'un des terroristes responsables de l'attentat de San Bernardino.

D-« La cybercriminalité est la nouvelle menace du XXIe siècle »

Par Propos recueillis par Sylvain Rolland | 26/07/2015

Mireille Ballestrazzi occupe la fonction de directrice centrale de la police judiciaire et préside le comité exécutif d'Interpol depuis novembre 2012. 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 s'impose, à 61 ans, comme la deuxième femme à occuper le prestigieux poste de directrice générale de la Police judiciaire. Également présidente du comité exécutif d'Interpol, le réseau international des polices, elle décrypte pour La Tribune comment les forces de l'ordre françaises, européennes et internationales luttent contre la cybercriminalité. Elle revient aussi sur les missions du tout nouveau Complexe mondial Interpol pour l'innovation de Singapour, une forteresse high-tech consacrée à la lutte contre les cybermenaces.

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 ?

MIREILLE BALLESTRAZZI - 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.

L'État français a-t-il pris la mesure des enjeux autour de la cybercriminalité ?

Avec les États-Unis et l'Allemagne, la France est l'un des pays précurseurs dans la lutte contre la cybercriminalité. L'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) a été créé en 2001 par le ministère de l'Intérieur. C'est l'une des premières structures au monde. Sa création, qui remonte à avant même le 11-septembre, a fait office de déclic pour mettre en place un vaste réseau international qui garantisse une réponse coordonnée face aux cybermenaces. La France est régulièrement citée en exemple, notamment en Europe, car elle a des enquêteurs d'excellent niveau, spécialisés en criminalité informatique. Ce n'est pas non plus un hasard si le siège d'Interpol se situe à Lyon. À titre de comparaison, la plateforme européenne Europol a vu le jour il y a seulement deux ans.

Comment s'organise la lutte contre la cybercriminalité en France ?

L'action est coordonnée par le ministère de l'Intérieur, où travaille un « Monsieur cybercriminalité », Jean-Yves Latournerie, dont le rôle est de coordonner les différents services. La police et la gendarmerie ont chacune des enquêteurs spécialisés. La police judiciaire dispose aussi d'une division spéciale, la Sous-direction de lutte contre la cybercriminalité (SDLC). Depuis avril 2014, elle remplace et étend l'action de l'Office, créé en 2001. Quatre-vingts policiers et gendarmes de haut niveau y travaillent pour identifier et anticiper les cybermenaces. L'une de leurs missions est de surveiller le Web. C'est un travail extrêmement difficile, moralement, psychologiquement, notamment pour les agents qui effectuent la veille au sujet de la pédopornographie. Globalement, le champ d'action de la SDLC est plus large que celui de l'Office. Elle prend aussi en compte les attaques subies par les entreprises et les particuliers. Auparavant, les PME dont les systèmes informatiques étaient attaqués, par exemple, ne savaient pas vers qui se tourner, car les policiers de base n'ont pas forcément la connaissance suffisante pour traiter ce genre de plainte. La SDLC va alors conseiller les victimes qui se tournent vers elle, mais aussi les policiers, pour leur indiquer les questions qu'ils doivent poser et ce qu'il faut mentionner dans la plainte.

Les policiers de base reçoivent-ils une formation pour comprendre les nouveaux enjeux liés à Internet ?

Nous avons un budget consacré à la formation initiale. De nos jours, il est indispensable que chaque policier ait un minimum de connaissances sur ce qu'est Internet, comment fonctionnent les réseaux sociaux, qui sont les grands opérateurs, ce qu'est la cybercriminalité... De nombreux adolescents sont victimes d'arnaques ou d'agressions sur les réseaux sociaux, et de plus en plus de personnes subissent des fraudes sur Internet, liées notamment à l'e-commerce. Si tous les policiers maîtrisent le b.a.-ba d'Internet, ils sauront mieux réagir et aiguiller les victimes. Pour l'heure, ce n'est pas suffisant mais cela va venir. Nous n'avons jamais assez de moyens, mais la France fait partie des pays les mieux dotés au monde.

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.

Bibliographie

www.latribune.fr/technos-medias/cybercriminalite-qui-sont-les-escrocs-du-darknet-francais-599111.html
www.latribune.fr/journalistes/sylvain-rolland-77
www.latribune.fr/technos-medias/internet/la-cybercriminalite-est-la-nouvelle-menace-du-xxie-siecle-485152.html
www.latribune.fr/technos-medias/internet/yahoo-a-espionne-ses-utilisateurs-sur-ordre-du-gouvernement-americain-605013.html
www.assemblee-nationale.fr/14/dossiers/transparence_lutte_corruption_economie.asp
www.legifrance.gouv.fr/affichLoiPreparation.do ?idDocument=JORFDOLE000032319792&type=genera
www.ihedn.fr/ ?q=content/guerre-froide-sur-le-net
www.inhesj.fr/sites/default/files/fichiers_site/les_publicationsles_travaux_des_auditeurs/gds6.pdf
www.ssi.gouv.fr/
www.rce-revue.com/Cybercriminalite-quels-enjeux-pour,641
www.le-vpn.com/fr/comprendre-ce-quest-la-cybercriminalite/
lexpansion.lexpress.fr/high-tech/cybercriminalite-l-attaque-des-objets-connectes_1846596.html
france3-regions.francetvinfo.fr/alsace/obernai-sensibiliser-jeunes-cyber-criminalite-1138347.html
www.jonesday.com/fr/la-lutte-contre-la-cybercriminalite–un-enjeu-majeur-pour-les-entreprises-05-22-2014
www.sciencesetavenir.fr/high-tech/informatique/les-transports-en-commun-de-san-francisco-victimes-d-un-logiciel-malveillant_108464
www.developpez.com/actu/108942/Le-Big-data-et-le-Machine-learning-sont-au-coeur-de-la-lutte-contre-la-cybercriminalite-estime-Lea-experte-en-securite-SI-chez-Societe-Generale/
www.lefigaro.fr/flash-actu/2015/08/06/97001-20150806FILWWW00381-cyberattaque-russe-contre-le-pentagone.php
www.directmatin.fr/hi-tech/2015-11-30/un-quart-des-jeunes-expose-la-cybercriminalite-en-2014-717037
www.europe1.fr/faits-divers/cybercriminalite-la-france-particulierement-vulnerable-2426983
www.cyberprotect.fr/cybercriminalite-les-entreprises-ciblees-et-leurs-points-faibles/
www.francetvinfo.fr/economie/la-cybercriminalite-explose-dans-les-entreprises-francaises_1708725.html
www.latribune.fr/technos-medias/internet/la-cybercriminalite-est-la-nouvelle-menace-du-xxie-siecle-485152.html
www.rce-revue.com/ ?Cybercriminalite-quels-enjeux-pour,641
www.20minutes.fr/high-tech/1961835-20161116-cybercriminalite-france-137-millions-victimes-an-toujours-bons-reflexes