EXAMEN FINAL ECG

Travail personnel

Quels sont les enjeux de la cyber sécurité au XXIème siècle ?

Jérémie Constantin Informaticien 4ème année IN4A
Ecole Professionnelle Technique de Sion

Table des matières

1. Préface

Ce travail est réalisé dans le cadre de ma formation d'informaticien généraliste à l'École des Métiers du Valais. Il fait partie de l'examen final de culture générale pour l'obtention du Certificat fédéral de capacité. Le sujet a été choisi de manière personnelle et de façon à s'intégrer dans le thème « Un monde en question ». Il sera traité selon trois aspects choisis parmi les huit aspects de la culture générale.

J'ai choisi un sujet qui me touche de près pour plusieurs raisons que je vais énumérer ici.

Premièrement, la passion de l'informatique ainsi que la formation que je suis actuellement me pousse naturellement à m'interroger sur cette problématique. En effet, ce sujet me sera toujours utile dans ma carrière professionnelle afin de développer des applications et solutions informatiques sécurisées et fiables.

La seconde raison est que je pratique l'éthical hacking (piratage éthique) depuis environ 4 ans. J'ai en outre découvert plusieurs failles dans la sécurité du journal « Le Nouvelliste » ainsi que dans des journaux du groupe Tamedia (20 minutes, le Matin…). De ce fait, la problématique de la sécurité informatique est un sujet que je connais aussi par la pratique et dans laquelle je m'instis aussi durant mon temps libre.

Finalement, je suis un membre actif du « Parti Pirate Suisse » et membre du comité au niveau valaisan en tant que co-président en charge de la partie romande du canton. Ce qui fait que la protection des données ainsi que la sécurité informatique me touchent directement dans cette fonction avec quelques actions concrètes telles que la suspension du dossier électronique du patient en Valais pour des raisons de manquements graves dans la mise en place de la plateforme ou encore un moratoire sur l'installation de Windows 10 dans les écoles valaisannes.

C'est donc pour toutes ces raisons que j'ai choisi ce sujet qui me touche directement et à propos duquel je peux faire partager mon expérience tant pratique que théorique sur les aspects techniques, économiques et légales dans le but de sensibiliser le plus grand nombre de personne à cette problématique complexe et souvent négligée même par les professionnels.

2. Introduction

Depuis le début des années 1980 et la démocratisation des ordinateurs personnels, la révolution numérique n'a cessé sa marche en avant. A présent, toutes les données autrefois conservées sur papier peuvent être numérisées. Certaines tâches peuvent désormais être automatisées. Dans les années 1990, c'est au tour de l'internet de bouleverser les habitudes des citoyens des pays développés. Avec l'extension de l'internet au monde entier, la société se trouve complétement transformée. La communication est désormais possible simplement entre toutes personnes du monde entier, possédant un terminal et une connexion internet. L'information peut provenir à présent de presque n'importe quel pays du globe. Les habitudes de consommation commencent à changer avec l'apparition de magasins en ligne et la possibilité de payer par carte de crédit. Dans les années 2000, la naissance du smartphone révolutionne le téléphone mobile et amène le micro-ordinateur dans la poche des utilisateurs, le suivant dans chacun de ses déplacements. Ces innovations mettent fin aux barrières géographiques et culturelles. Les échanges peuvent s'opérer de manière électronique et la mondialisation devient réalité. Les règles géopolitiques mondiales, l'économie planétaire s'en trouve totalement modifiées.

Ces innovations malheureusement, apportent aussi leur lot de nouvelles menaces. Alors qu'une lettre ne pouvait être lue que par l'expéditeur, le destinataire et éventuellement les employés du service postal, un email peut être conservé sur un serveur étranger, être lu par des robots qui indexent les mots échangés à des fins publicitaires ou d'espionnage. Les entreprises sont maintenant totalement dépendantes de l'informatique. Les banques, les plateformes boursières ou d'échanges commerciaux sont autant de secteurs dans lesquels l'informatique est omniprésente et qui sont tout aussi vulnérables aux nouvelles menaces informatiques. Les États aussi sont vulnérables, les centrales électriques, nucléaires, les trains, les signalisations, les administrations seraient paralysées face à une attaque informatique. Et dans l'avenir, la menace sera d'autant plus présente avec la démocratisation de la domotique et des objets connectés.

Afin de vraiment saisir l'importance d'une bonne sécurité informatique face aux dangers de la vie connectée, je vais donc tenter d'analyser ici les moyens mis en œuvres pour compromettre les systèmes informatiques, chercher à comprendre les enjeux géostratégiques que peuvent avoir des attaques informatiques, puis terminer par une lecture du droit suisse afin de vérifier si le citoyen est assez protégé face aux nouvelles menaces informatiques.

Tout d'abord, je vais me pencher sur les aspects techniques. Pour évaluer les dangers d'une menace, il me faut connaître quelles sont les armes à disposition de l'attaquant comme les armures et bonne pratiques permettant de se protéger de ses attaques. Quelles sont les techniques de compromission ainsi que celles pour s'en protéger ? Ces mesures sont-elles efficaces ?

Ensuite, je vais analyser l'impact des attaques informatiques au niveau mondial et centrée sur un aspect géostratégique. Les États sont de plus en plus dépendants de l'informatique, les infrastructures clés des nations sont très souvent confiées à l'informatique. Le risque donc qu'un État soit paralysé par des attaques informatique est une réalité et les virus informatiques peuvent être utilisés comme de réelles armes de guerre. C'est pourquoi je tenterais de répondre à la question suivante : Quels sont les enjeux et l'impact géostratégique des attaques informatiques ?

Pour finir, je me recentrerai sur la Suisse et sur la législation présente en cherchant quelles sont les bases légales en rapport avec la protection des données et les responsabilités en cas de hacking.

Je souhaite au lecteur de prendre autant de plaisir à plonger dans l'univers passionnant de la sécurité informatique que j'ai eu plaisir à le rédiger.

3. Aspect technologique : quels moyens d'attaques et de défenses sont-ils réalisables technologiquement ?

3.1. Introduction

> *"Si vous connaissez vos ennemis et que vous vous connaissez vous-même, mille batailles ne pourront venir à bout de vous. Si vous ne connaissez pas vos ennemis mais que vous vous connaissez vous-même, vous en perdrez une sur deux. Si vous ne connaissez ni votre ennemi ni vous-même, chacune sera un grand danger."*
>
> *Sun Tzu, L'Art de la Guerre*

Dans notre monde moderne, l'informatique prend une très grande place. En effet, presque chacune des couches qui composent une société est dotée d'un ordinateur connecté ou dans le cas échéant, un smartphone. La dépendance à l'informatique devient la règle dans de nombreux domaines, ayant comme résultante une plus grande vulnérabilité aux attaques informatiques.

Ainsi, en février 2016, un hôpital américain a été victime d'un logiciel de racket qui a chiffré tous les fichiers importants et paralysé le système. L'hôpital n'eut d'autre choix que de payer une rançon de 17'000 dollars afin de remettre en service les systèmes informatiques de l'hôpital. Le coût total se chiffra en plusieurs milliers de francs ! [1]

Le domaine médical n'est pas le seul domaine à risque, les transports sont aussi vulnérables. En janvier 2016, le ministère français des transports a été victime du même type de logiciel malveillant. [2] Des trafiquants de drogue ont par exemple infiltré le système informatique du port d'Anvers afin de récupérer les containers contenant les substances illicites grâce aux codes d'accès récupérés. [20] Le ministère français de la défense a d'ailleurs investi 1 milliard d'euros sur 5 ans afin de protéger le transport maritime. Si ces cyber-menaces inquiètent c'est parce qu'aujourd'hui dans un bateau, presque tout est informatisé. Tout est connecté à Internet entre la terre et la mer. [3]

Les domaines de la défense et des télécommunications sont bien sûr aussi en première ligne face à ces nouvelles menaces. Les infrastructures électriques, elles aussi, sont des installations critiques contre lesquelles un gouvernement en guerre ou un groupe mal intentionné pourrait lancer une attaque et faire de gros dégâts.

Les banques sont tout autant vulnérables. En mars 2016, des cybercriminels ont subtilisé plus de 80 millions à la banque centrale du Bangladesh. [4]

Et tout ceci sans compter les risques pour l'économie privée, les entreprises donc, ainsi que pour chacun de nos citoyens pris individuellement.

Afin de pouvoir évaluer la puissance de nuisance des attaques informatiques, il est indispensable de connaître les capacités effectives des cybercriminels. Qu'est-il possible de faire ou non ? Dans le même esprit, que devons-nous faire afin de nous protéger un maximum contre les nouvelles menaces informatiques ?

Ce sont à ces deux questions que nous allons répondre dans le présent chapitre.

3.2.Intrusion

La majorité des intrusions informatiques se déroule en comptant sur l'utilisateur pour faire entrer le virus dans son système. Une des techniques la plus utilisée par les cybercriminels est le phishing. Cette tentative d'intrusion mise sur la naïveté de la cible en lui envoyant un faux email, semblant légitime. Cet email comprendra le plus souvent une pièce jointe telle qu'une image, un document Word ou un PDF contenant le virus. Cela peut aussi passer par un lien internet qui redirige vers la copie d'un site légitime afin de faire télécharger une fausse mise à jour ou de récupérer des mots de passe d'authentification.

Un autre moyen d'introduire un système est de créer un « cheval de Troie » en couplant un programme légitime avec un programme malveillant. C'est ce que l'on trouve le plus souvent sur les sites de partage de fichiers illégaux. Ainsi, la cible, lorsqu'elle cliquera sur le programme, lancera un programme légitime tel qu'un jeu, une musique, une vidéo en même temps que le virus pour que la cible ne se doute de rien.

Un moyen d'introduire un virus qui est souvent négligé est simplement un accès physique à un système. Il suffit qu'une femme de ménage insère une clé USB dans un ordinateur pour l'infecter ou lui voler des informations. Parfois même, il suffit de laisser trainer une clé USB ou un CD contenant le virus dans une organisation et attendre qu'un petit curieux utilise la clé sur son poste de travail.

Les moyens les plus redoutables sont rarement utilisés par les cybercriminels du dimanche. Ces techniques utilisent des failles de programmes connus et très utilisé. Grâce à ce type de faille, il est possible d'infecter une cible sans solliciter d'action de sa part. Ces failles sont appelées des 0days. Par exemple, une 0day dans le logiciel PDF-Reader peut infecter une cible à l'ouverture d'un PDF, une faille de Java pourra infecter la cible silencieusement dès que celui-ci ouvre une page WEB utilisant Java et étant infectée. Ces failles font l'objet d'un vrai marché tant sur le marché noir qu'entre agences de renseignement. Certaines entreprises telles que ZERODIUM© sont spécialisées dans la revente de ces failles à des privés ou des gouvernements. Les prix vont de 5000$ pour des failles concernant des applications WEB simples et jusqu'à 500'000$ pour une faille dans l'IOS de l'IPhone d'Apple. De par le prix et le coût en recherche de ces failles, elles sont généralement utilisées par les mafias, les gouvernements ou des équipes de hackeurs particulièrement doués. Il arrive même que certains éditeurs d'antivirus en achètent pour les étudier et les ajouter à leurs listes de détection.

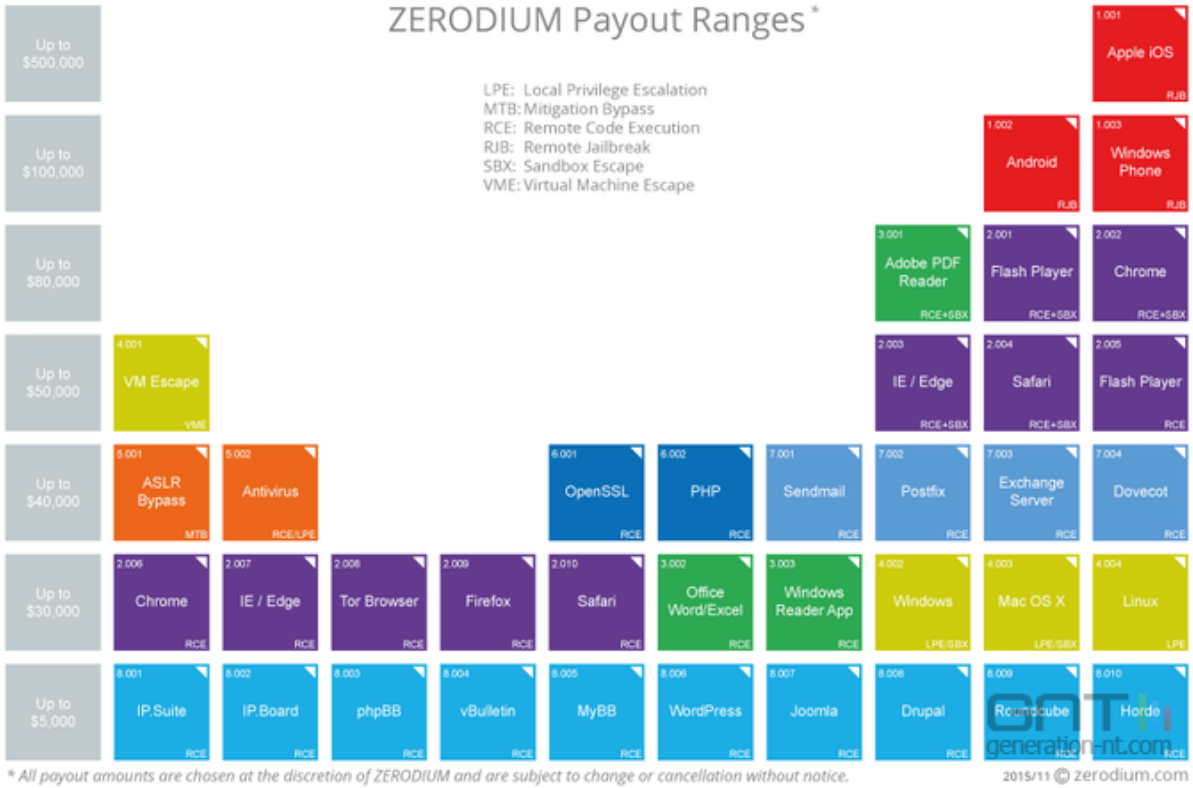

Figure 1 : liste des prix des failles 0day de la compagnie ZERODIUM. Les couleurs représentent un type de cible (mobile, protocole, programme…) et les initiales (LPE, MTB, RCE …) représentent un type de faille. En gris, nous avons les prix.

3.3.Évasion

Un antivirus et un pare-feu ne sont pas des protections absolues contre un virus. En effet, généralement, l'antivirus ne détecte que ce qu'il connait déjà. Il vérifie si le fichier testé correspond à une base de données géante de tous les programmes malicieux. Par contre, tant que le virus n'est pas répertorié, l'antivirus ne le reconnaitra pas. Afin de contourner ce système, il est possible de chiffrer le virus et de ne le déchiffrer qu'une fois dans la mémoire de travail de l'ordinateur.

Il y a aussi des antivirus plus développés qui vont analyser le comportement en lui-même du virus en l'exécutant dans un environnement virtuel. Là aussi, il est possible de facilement détecter si l'on se trouve dans un environnement réel ou non et de faire réagir le programme malveillant en conséquence.

Une autre possibilité pour ne pas se faire remarquer par l'antivirus est de prendre la place d'un processus déjà lancé et marqué comme sûr par l'antivirus. Il est par exemple possible de lancer l'application calculatrice, puis de mettre le processus sur stop et de remplacer le code du processus par notre programme malveillant. Notre programme passera donc pour le programme de calculatrice (calc.exe) de Windows.

Une méthode plus complexe pour ne pas se faire remarquer par l'antivirus est l'usage de rootkit. Ces programmes permettent de masquer l'activité de notre virus au système d'exploitation, d'effacer les traces telles que les logs et d'injecter des virus sur la machine cible. Suivant à quel niveau le rootkit travaille, il est impossible pour l'antivirus de le détecter lui, ainsi que les virus. Les antivirus ne contiennent généralement pas de détection de rootkits mais les éditeurs intègrent de plus en plus cette fonctionnalité dans leurs suites de sécurité. Malgré cela, les rootkits sont très difficile à détecter et permettent de travailler à un niveau parfois bien plus bas que le système d'exploitation (BOOT, BIOS, DOS…). [5]

3.4.Virus

Il existe plusieurs types de virus. Le premier est le virus de types vers (worm) qui s'auto-réplique et infecte automatiquement de nouvelles victimes.

Les spyware sont des logiciels espions qui récolteront beaucoup d'informations personnelles.

Les keyloggers sont des programmes interceptant les entrée clavier de l'utilisateur et les envoie sous la forme d'un fichier à l'attaquant. Cela lui permet de récupérer des mots de passe, discussions et même les numéros de carte de crédit.

Les stealers, eux, sont spécialisé dans le vol de mots de passe ou de comptes de tout type (même parfois bancaires).

Un type de virus qui est en pleine expansion est le ransomware, soit logiciel de rançon. Ce sont des programmes qui chiffrent les fichiers de la victime et lui demande de payer une rançon afin de pouvoir récupérer les fichiers. De nombreuses organisations telles que des banques ou des hôpitaux ont finalement payé une telle rançon. Les ransomwares sont actuellement les virus les plus rentables.

Un autre type de virus est ce que l'on appelle un RAT pour Remote Administration Tool. Ce type de programme n'est pas forcément utilisé comme un virus. Des programmes de gestion d'ordinateurs à distance tels que TeamViewer ou RealVNC sont souvent utilisés par des informaticiens pour effectuer des dépannages à distance. Imaginez maintenant le pouvoir d'un tel programme lorsqu'il est installé sans l'accord de l'utilisateur et ne demande pas d'autorisation pour permettre une connexion externe. L'attaquant se retrouve avec le contrôle total de l'ordinateur, comme s'il était directement devant l'écran.

3.5.Protection

$$\text{Risque} = \frac{\text{Menace x Vulnérabilité}}{\text{Contre-mesure}}$$

Figure 2 : équation du risque

Pour se protéger, il faut mettre un œuvre plusieurs processus.

Premièrement, l'installation d'un antivirus est indispensable. Même s'il est facile de le contourner pour un pirate aguerri, cela reste un bon rempart contre la majorité des menaces qui sont l'œuvre de pirates amateurs.

Un pare-feu est aussi obligatoire, il permet de filtrer les connexions. Le pare-feu est heureusement activé par défaut dans Windows. Il existe des pare-feu physiques pour l'usage professionnel qui en plus de leur fonctionnalité originelle, sont dotés de fonctions d'analyse du contenu des flux de l'Internet.

Il faut toujours faire très attention lorsque l'on télécharge depuis des sites de contenus illégaux, ces sites sont souvent truffés de Chevaux de Troie.

Lorsque l'on reçoit un email, il faut toujours contrôler l'adresse de provenance. Souvent les cybercriminels utilisent des adresses qui ont une typographie proche de l'adresse réelle. Par exemple, une adresse de type « @paypal.com » pourra être transformée en « @paypal.com ». Nous ne voyons pas vraiment de différence mais dans la deuxième adresse, le « l » est en fait un « i » majuscule. Souvent, ces emails comportent un bon nombre de fautes d'orthographe. Même si cela est de moins en moins vrai, cela reste un bon indice quant à la légitimité d'un courrier électronique. Finalement, nous n'allons jamais ouvrir les pièces jointes contenus dans ces envois.

Il n'est pas possible d'éviter les failles 0days puisqu'elles sont par définition non-découvertes par l'éditeur du logiciel. Néanmoins, une fois la faille repérée, l'éditeur publie un correctif. C'est pourquoi, il faut régulièrement mettre à jour les programmes d'un ordinateur.

Il n'y a rien à faire contre les puissants rootkits qui travaillent à un niveau plus bas que le système d'exploitation.

3.6.Conclusion

Nous pouvons constater que le panel des attaques est large et que tous les systèmes de protection peuvent être contournés par l'usage de systèmes d'évasion. Imaginons maintenant que l'on visite un site. Sur une des pages visitées, une animation publicitaire s'affiche. Vous ne le savez peut être pas, mais cette animation est réalisée grâce à la technologie Java. Ce que vous ne savez pas non plus c'est qu'un pirate a acheté une faille 0day sur le marché noir du Web et que cette faille permet le téléchargement et l'installation de logiciel malveillant. Vous êtes maintenant infecté par le virus, mais vous ne vous rendez compte de rien. Le virus n'est pas détecté par votre antivirus, soit à cause d'un complexe rootkit, soit à cause d'un chiffrement et d'une injection du virus dans un processus sain. Vous êtes désormais à la merci du cybercriminel et celui-ci aura le choix parmi tout un panel d'attaques pour vous voler, vous faire chanter ou simplement saboter votre équipement informatique. Votre ordinateur peut aussi devenir un ordinateur zombie et participer lors attaques de grandes ampleurs et cela sans même que vous le sachiez.

Pourtant, vous aviez bien votre antivirus et votre pare-feu activés. Vous n'avez jamais rien téléchargé sur des sites douteux et vous savez déjouer les faux emails.

La réalité est qu'il est impossible de se protéger contre toutes les attaques informatiques, les cybercriminels auront toujours un coup d'avance et certaines technologies sont vulnérables de par leur conception même.

4. Aspect historique et politique : quelle est l'importance d'une prise de conscience politique face aux menaces informatiques ?

4.1. Introduction

Les virus que nous avons vus dans le chapitre précédent sont certes dangereux mais visent davantage les personnes que les infrastructures. De nouveaux virus sont apparus, beaucoup plus puissants, beaucoup plus vicieux. Ce type de virus n'est pas l'œuvre de petits escrocs mais bien de professionnels et ne s'attaquent pas aux personnes privées mais aux systèmes industriels (SCADA) et infrastructures clés des États.

Il y a aussi de plus en plus d'espionnage mené par système informatique lors de négociations ou de réunions entre diplomates. L'espionnage ne touche pas seulement les cibles étatiques mais aussi de nombreuses entreprises. Comme nous le savons, certaines entreprises sont d'importance nationales et notre économie en est extrêmement dépendante. Nous pouvons citer dans cette catégorie d'entreprises les banques à risque systémiques (BNS, UBS, Crédit Suisse et Raiffeisen), l'industrie de la mécanique et de l'horlogerie (très présente dans les régions du Jura, Neuchâtel et Genève) et les secteurs de la chimie et du pharma (région bâloise). De grandes pertes dans ces domaines se traduiraient en perte d'emplois (donc augmentation du chômage) ainsi que des pertes fiscales (donc une augmentation des impôts ou une baisse des services publics). Quelles mesures doit prendre la Suisse afin de protéger son industrie et son économie ? Est-ce le rôle de l'État de protéger l'économie privée ?

Depuis une dizaine d'années, nous voyons apparaître de plus en plus souvent le terme de cyberguerre dans les médias sans qu'elle soit pour autant une réalité. En effet, il est essentiel de faire la différence entre cyberattaques et actes de guerre. Peter Singer, spécialiste en techniques de guerre moderne affirme : « on ne peut parler de « guerre » qu'en présence de deux facteurs fondamentaux : la violence et la politique. » [6]

Ce qui est sûre, c'est que les États se préparent bel et bien à affronter une cyberguerre, tant sur le plan défensif qu'offensif. Les USA, la Russie, l'Allemagne, la France, l'Estonie ou encore l'Equateur font partie de la centaine de pays qui ont mis sur pied un programme militaire dans le domaine des cyberattaques et de la cyberdéfense.

Ont-ils raison de se préparer au pire ? La menace cybernétique est-elle assez prise en compte au niveau suisse ? La Suisse doit-elle aussi mettre en place un arsenal informatique ? Ce sont à ces quelques questions que je vais essayer de répondre dans ce chapitre.

4.2. La cyberguerre, réalité ou fantasme ?

Afin d'avoir une vue d'ensemble de ce qui a déjà été fait et de ce qui risque d'arriver dans le futur, je vais faire un historique des attaques les plus importantes menées ou commanditées par des gouvernements.

4.2.1. Historique

2007 – Estonie

En avril 2007, apparut la première attaque d'ampleur contre un pays tout entier. L'Estonie était alors un des pays dont l'administration était la plus dématérialisée du monde et fut attaqué suite à un conflit avec la Russie. Une attaque par dénis de service distribué (DDOS) d'ampleur inégalée jusqu'ici fut perpétrée contre le pays en commençant par bloquer l'intégralité des sites gouvernementaux, puis des banques, des médias et des partis politique. Les numéros d'urgence tels que ceux de la police ou les secours furent bloqués durant plusieurs heures. Cette attaque fut tout autant violente que rapide : il fallut plusieurs dizaines de milliers de PC zombie afin de perpétrer une attaque de cette ampleur.

" La mobilisation d'une telle armada informatique dépasse de très loin le stade de l'initiative individuelle, voire même mafieuse. Rien de tel ne peut se faire à cette échelle sans la coopération d'un Etat, et de plusieurs opérateurs télécoms."

Linnar Viik, un gourou estonien de l'Internet, cité par *The Economist* [7]

Tous les regards se portèrent alors sur la Russie et son président V. Poutine qui démentit toute implication dans cette attaque. Nous savons qu'il existe énormément de groupes de hackers qualifiés en Russie et qu'il arrive parfois aux services russes d'utiliser ces groupes comme intermédiaires afin de rester discret.

2007 – Syrie

En 2007, l'armée israélienne s'est attaquée aux défenses anti-aériennes de la Syrie. Afin de sécuriser leurs chasseurs et bombardiers, le Tsahal a piraté les systèmes de défense aériens de la Syrie, les rendant totalement inopérants.

2008 – Géorgie

Une attaque semblable à celle de 2007 sur l'Estonie a touché la République de Géorgie en plein conflit avec son voisin russe. [8]

2010 – Iran

Un virus au nom de Stuxnet est découvert. Ce virus est le plus développé des virus découvert jusqu'alors. Il utilisait quatre failles 0day afin de se propager sur le maximum d'ordinateurs possible. Le but réel était d'atteindre la centrale nucléaire de Natanz en Iran afin de retarder un maximum les recherches nucléaires iraniennes. Le virus ciblait un module de la marque Siemens qui équipait cette centrale. Le malware a modifié la vitesse de rotation des turbines tout en affichant de faux résultats à l'écran. L'attaque était donc invisible et forçait les chercheurs à accuser des pièces de mauvaise qualité ou des erreurs

techniques afin de justifier leur retard. Ce virus aurait été lancé par les USA afin d'éviter des frappes israéliennes sur les centrales iraniennes. C'est typiquement ce genre de virus, visant les systèmes industriels (SCADA), qui peut faire de gros dégâts matériels et économiques. [9]

2015 – Ukraine

L'année 2015 marquera un tournant dans l'évolution des attaques des systèmes industriels avec la première attaque sur un réseau électrique d'ampleur réussie. L'attaque a ciblé 3 opérateurs énergétiques ukrainiens, a touché 225'000 clients durant plusieurs jours. [10]

4.2.2. Il y a-t-il de quoi avoir peur ?

A l'heure actuelle, aucune cyberguerre n'a jamais été déclarée. Néanmoins, nous pouvons nous rendre compte de l'impact que pourrait avoir une guerre numérique totale sur nos pays. Nous pouvons dès lors dégager plusieurs d'objectifs visés par les cyberattaques étatiques.

Les premières attaques décrites plus haut ont surtout visé à rendre inaccessible des sites gouvernementaux mais sans faire de dégâts matériel et sans voler de données. Les conséquences de ce type d'attaque varient suivant la durée et l'étendue, mais l'on peut citer une perte financière conséquente aux fonctionnaires qui n'auront pas pu travailler pour cause d'un service numérique inaccessible. Au niveau de la sécurité du pays, ces attaques ne sont pas vraiment dangereuses mais servent souvent comme mesures d'intimidation et de propagande.

Le second type d'attaque que l'on a pu observer est bien plus dangereux, puisqu'il est dès lors possible de réellement impacter la capacité de production énergétique d'un pays et de faire de vrais dégâts matériels et même humains. Imaginez ce qu'il se serait passé si le virus Stuxnet avait été programmé pour faire tourner les turbines de la centrale nucléaire de Natanz jusqu'à l'explosion…

Le dernier type d'attaque n'est pas encore fréquent en situation réelle mais des tests effectués en laboratoire ont permis de déceler plusieurs failles informatiques dans des systèmes étasuniens tels que des drones et des lanceurs de missiles. [11] [12] Ceci permet donc de détourner les armes de leurs objectifs et pourrait aussi être utilisé par un pays tiers pour attaquer un pays grâce à des armes étrangères. On pourrait donc faire ce qui est appelé un « false flag » en terme militaire, un pays mène une attaque en se faisant passer par un autre pays ou une autre organisation.

En conclusion, nous pouvons constater que les moyens techniques pour assister à une cyberguerre existent déjà. Il est fort probable que dans quelques années, les attaques se généralisent. Par contre, cela ne veut pas pour autant dire que les guerres classiques vont totalement disparaître, mais plutôt que les humains seront de plus en plus remplacés par des

machines, des robots ou des humanoïdes qui seront eux aussi vulnérables aux attaques informatiques. Nous assistons actuellement à une sorte de guerre froide numérique. Les gouvernements montrent leurs capacités afin d'intimider leurs adversaires mais une guerre numérique totale serait un désastre pour le monde entier et l'économie s'effondrerait par effet de bord. Comme tout monde à trop à perdre, personne n'ose encore mener ce genre de guerre mais rien ne prédit que dans l'avenir, nous ne serons pas confrontés à ce genre de conflit.

4.3.Espionnage

4.3.1. Situation de la Suisse

La Suisse est connue pour sa neutralité, sa stabilité et son goût de la discrétion. C'est pour cela qu'elle est une des principales places de négociation au monde. Genève joue un rôle important dans la diplomatie et de nombreuses négociations économiques ou pour la paix ont lieu chaque jour sur le territoire. Ceci fait aussi que la Suisse est aussi un lieu prisé par les services secrets étrangers à la recherche d'informations depuis la première guerre mondiale. [13]

4.3.2. Espionnage des négociations iraniennes

Au printemps 2015 ont eu lieu dans les cantons de Genève et de Vaud des négociations entre l'Iran, les Etats-Unis et les chefs de diplomatie russes, chinois, britanniques, français et allemands. Ces négociations visaient à trouver un accord afin de sortir du conflit entre l'Iran et l'Occident sur son programme nucléaire. Nous savons maintenant grâce à l'éditeur d'antivirus Kaspersky que 3 hôtels où ont eu lieu les négociations ont été victimes de cyberattaques. Trois hôtels ont été infectés par un virus d'origine israélienne nommé Duqu 2.0. Les pirates ont ainsi pu prendre le contrôle des caméras de sécurité et des micros, donnant une belle vue d'ensemble des négociations. [14]

4.3.3. Conclusion

Les nombreux événements internationaux se déroulant en Suisse (WEF, négociations etc.) sont vulnérables à l'espionnage. Jusqu'à présent, la Suisse était choisie pour sa sécurité et sa neutralité mais nous pouvons nous apercevoir que le niveau de sécurité est loin d'être au niveau attendu. Si la Suisse veut jouer son rôle de facilitateur dans la diplomatie internationale, elle devra mettre en place des mesures afin de protéger ses hôtes lors de négociations diplomatiques, stratégiques et économiques. Le plus grand atout de la Suisse, c'est la confiance que l'on place en elle. Pour sûr, si de nouvelles révélations sur des affaires d'espionnage en Suisse étaient révélées, il y aurait de grands risques liés à la perte de confiance. Des organisations internationales pourraient délaisser la Suisse et le pays perdrait son statut de terrain neutre et donc propice aux négociations.

4.4.Un risque pour l'économie ?

4.3.4. L'espionnage industriel

L'espionnage industriel est une chose dont on parle peu. Néanmoins, elle est une réalité dont beaucoup d'industriels se gardent d'en révéler l'existence, de peur de dévoiler ses faiblesses aux concurrents et de subir des dégâts d'image.

En 2015, le groupe Airbus Hélicoptère est victime d'un piratage visant à récupérer des informations concernant un appel d'offre de la Pologne.

Le groupe nucléaire Areva a aussi été victime d'une attaque informatique durant 2 ans, période durant laquelle le groupe a perdu un contrat pour 2 réacteurs nucléaires qu'il comptait vendre à la Corée du Sud.

Depuis les révélations d'Edward Snowden, nous savons que les Etats-Unis pratiquent l'espionnage économique par l'intermédiaire des services secrets. En effet, à la fin de guerre froide, de nombreux anciens agents des services secrets sont passés dans l'économie privée et font le lien entre les agences et les entreprises.

Le Chine est un prédateur redoutable en termes d'espionnage économique et est en guerre ouverte avec les Etats-Unis mais cible aussi beaucoup le France. [15]

La France elle-même a été plusieurs fois accusée de pratiquer activement l'espionnage industriel. [16]

Bref, la majorité des Etats du monde pratique l'espionnage industriel. Les pertes économiques sont difficilement quantifiables à cause de l'opacité du sujet mais une seule attaque peut faire perdre plusieurs millions à l'entreprise ciblée et les rentrées fiscales qui vont avec.

4.3.5. Les pertes financières liées aux cyberattaques

Il est très difficile de quantifier le coût des cyberattaques mais il existe des estimations que certains éditeurs d'antivirus ainsi que des agences étatiques publient. L'éditeur McAfee a publié une étude dans laquelle il estime le coût mondial des cyberattaques avec une fourchette large : un chiffre entre 375 et 575 milliards de dollars par an. Le rapport met aussi en lumière l'impact sur l'emploi et avance un chiffre de 200'000 postes menacés aux Etats-Unis pour 150'00 en Europe. L'impact financier pour les particuliers est lui estimé à 150 milliards au niveau mondial. Il n'y a malheureusement pas de chiffres pour la Suisse. [17]

4.5.Conclusions

Nous avons parcouru dans ce chapitre trois domaines qui sont en relation entre les tâches de l'Etat et la cyber-sécurité.

Le premier volet concerne le secteur militaire avec le risque de plus en plus grand de cyberguerres et d'attaques industrielles sur les infrastructures de base de la communauté telles que l'énergie.

Le second est, lui, porté sur le terrain diplomatique avec les risques liés à l'espionnage de négociations internationales et de rassemblements tel que le Forum économique de Davos.

Le dernier se penche sur les pertes économiques des entreprises qui sont autant de pertes en termes d'emplois et de rentrées d'impôt.

Il semble clair qu'au niveau sécuritaire, il faut absolument que l'Etat garantisse l'inviolabilité des systèmes militaires, des sources de production d'énergie, les transports publics et les télécommunications nationales. Au niveau diplomatique, il est tout aussi important de pouvoir garantir la confidentialité des échanges surtout pour un pays comme la Suisse dont la réputation de facilitateur dans les négociations pourrait en souffrir, sans compter le risque de perte financière lors de négociations économiques entre deux pays.

Le sujet le plus complexe est celui de la protection de l'économie. Cette question dépend beaucoup de la politique des pays. Les Etats libéraux seront d'avis que ce n'est pas à l'Etat de prendre en charge l'économie alors que les adeptes du keynésianisme opteront pour une protection de l'Etat contre les grandes menaces ou contre les entreprises essentielles pour l'économie du pays. Mon avis personnel est que la Confédération devrait créer un organe permettant d'informer et de collaborer entre les entreprises sur le sujet de la protection informatique.

Comme nous pouvons le voir, la révolution numériques et les nouveaux risques qui en découlent ne peuvent pas laisser les Etats de marbre et beaucoup ont déjà pris plusieurs mesures afin de se mettre à jour face aux nouvelles menaces. Plusieurs secteurs clés des pays sont directement touchés par les menaces informatiques mais malgré cela, beaucoup d'Etats ne font pas face à la menace. Celle-ci étant dématérialisée, il est difficile pour les anciennes générations de se rendre compte du réel potentiel de nuisance des attaques informatiques.

5. Aspect juridique : quelles sont les bases légales en rapport avec la protection des données et la responsabilité en cas de piratage informatique ?

5.1. Au niveau international

5.1.1. Convention sur la cybercriminalité [18]

La Convention sur la cybercriminalité a été conclue le 23 novembre 2001 à Budapest. Elle est le premier traité international concernant la criminalité informatique. Elle a été rédigée par le Conseil de l'Europe et a été ratifiée par 48 pays dont les pays européens, la Suisse, l'Afrique du Sud, l'Australie, le Canada, les USA, le Panama, la République dominicaine et le Sri Lanka.

Son but est de *« mener, en priorité, une politique pénale commune destinée à protéger la société de la criminalité dans le cyberespace, notamment par l'adoption d'une législation appropriée et par l'amélioration de la coopération internationale »* [18]

Cette convention stipule que tous ses signataires doivent prendre entre autre des mesures législatives contre l'accès et l'interception illégale aux données, l'atteinte à l'intégrité des données et des systèmes, la pornographie enfantine, la propriété intellectuelle.

Elle exige aussi que les parties doivent mettre en place un système de collecte des données en temps réel par les fournisseurs d'accès (FAI), la rétention de ces informations et la possibilité par les autorités de les consulter.

Elle inclut un volet sur le partage d'informations et la coopération internationale.

5.1.2. Manuel de Tallinn [19]

Le Manuel de Tallinn est un guide permettant de transposer le droit international aux cyberconflits. Il a été rédigé par un groupe d'experts mandaté par l'OTAN en 2013.

Le droit international existant peut en effet bien être transposé aux nouvelles technologies et est donc suffisant pour répondre aux cyberattaques. Tout comme les conflits armés classiques, la cyberguerre doit suivre les règles des conventions de La Haye et de Genève. En outre, les cyberattaques étatiques sont considérées comme des attaques armées au sens de la Résolution 3314 de la Charte des Nations unies.

Ce sont 95 règles qui sont édictées dans le manuel. Une deuxième version est prévue pour l'année 2016.

5.1.3. Règlement européen sur la protection des données [21]

Ce règlement a été adopté en hiver 2015 et devrait être accepté ce printemps par les eurodéputés, pour une mise en œuvre au plus tôt en 2018. Le règlement vise à harmoniser les législations des Etats membres de l'UE.

Ce règlement introduit une obligation de loyauté et de transparence de la part des services en ligne et doivent donc informer les utilisateurs sur la qualité et l'utilisation faite des données collectées.

Il donne plus de pouvoir aux préposés à la protection des données et permet d'infliger de lourdes amendes (jusqu'à 4% du chiffre d'affaires mondial).

Les entreprises ont aussi l'obligation de déclarer toutes fuites de données.

Les enfants de moins de 16 ans doivent demander une autorisation aux parents avant de s'inscrire à un réseau social, les moins de 13 ans ne peuvent pas s'y inscrire légalement.

Ces règles sont applicables à toutes entreprises qui comptent des utilisateurs de l'UE même celles qui se trouvent dans un pays non-européen (Google, Facebook, etc.).

Nous trouvons aussi dans le texte la notion de droit à l'oubli qui est un droit à l'effacement de ses données personnelles et au déréférencement. Ainsi, en France, Google a reçu 73.399 demandes de déréférencement en 2015. La firme a répondu négativement dans 58% des cas. Mais, en réalité Google a seulement déréférencé sur l'extension française de son site tout reste accessible depuis la version internationale (.com) ou celle d'autres pays (.at, .de, .us, .ch etc.). Le CNIL (Autorité française de contrôle en matière de protection des données personnelles) a fait recours contre Google afin que le déréférencement soit effectif sur toutes les extensions du domaine. La procédure est en cours.

5.1.4. Le Safe Harbor [22]

Une directive européenne sur la protection des données datant de 1998 interdit le transfert de données aux pays non-européens qui ont une protection des données personnelles inférieure au standard européen. Afin de se conformer à cette directive, les USA ont négocié un cadre juridique avec la Commission européenne, dénommé Safe Harbor (Sphère de sécurité). Son pendant helvétique se nomme le «U.S.-Swiss Safe Harbor Framework ». Le 6 octobre 2015, LA CJUE (Cour de justice européenne) invalide l'accord pour motif que les USA n'offrent pas le degré suffisant de protection des données et que le droit de recours n'est pas garanti par ce pays.

5.2.Au niveau Suisse

5.2.1. Constitution fédérale [23]

L'article 13 de la Constitution fédéral garantit le respect de la sphère privée et familiale, de son domicile, de sa correspondance (lettres) et des relations qu'il établit par la poste et les télécommunications (téléphone, email, internet).

Toute personne a le droit d'être protégé contre l'emploi abusif de ses données.

5.2.2. Code civil [24]

L'article 27 du code civil protège des atteintes contre la personnalité dont le respect de la sphère privée fait partie.

5.2.3. Code des obligations [25]

L'article 14 alinéas 2bis régit le droit sur la signature électronique. Elle est valable comme une signature manuscrite lorsque son certificat émane d'un fournisseur de service de certification reconnu par la Confédération.

L'article 59a régit les responsabilités cas de vol ou d'utilisation abusive d'une clé de signature par un tiers. Le détenteur peut se libérer de sa responsabilité s'il peut prouver qu'il a pris toutes les mesures de sécurité possibles contre l'utilisation excessive de la clé.

5.2.4. Code pénale [26]

L'article 143 pénalise la soustraction de données ainsi que l'intrusion dans les systèmes informatiques, tandis que l'article 144 prohibe la détérioration de données. Les peines pour ces infractions vont de la peine pécuniaire jusqu'à 5 ans de prison. Le piratage en lui-même est puni jusqu'à 5 ans de prison et jusqu'à dix ans si cette personne en fait son métier.

5.2.5. Code procédure civile [27]

L'article 177 admet les fichiers électroniques comme moyens de preuve.

5.2.6. Ordonnance concernant la tenue et la conservation des livres de compte [28]

Cette ordonnance réglemente entre autre, la durée et la forme de conservation des livres de comptes. Les livres de comptes peuvent être conservés sous forme informatique. Voir le tableau de conservation.

5.2.7. Loi sur le droit d'auteur [29]

La loi sur le droit d'auteur assure la propriété d'œuvre à son auteur. Les droits de diffusion et de modification lui sont réservés. Les programmes peuvent être considérés comme des œuvres au sens de l'article 2 alinéas 3. De plus, de nombreuses œuvres sont désormais stockées de manière informatique. Par exemple, des photos, design, livres, musiques, films, etc.

5.2.8. Loi et ordonnance fédérale sur la protection des données [30]

La loi fédérale sur la protection des données définit les contours de la politique de protection des données. Elle définit les termes de données personnelles et données sensibles dans l'article 3.

La communication de données personnelles vers l'étranger est possible dès lors que le pays respecte un certain niveau de protection des données et que la personne concernée a donné son consentement (article 6) ou si le traitement et en relation avec un contrat et que ces données concernent le cocontractant.

Toute personne peut réclamer de connaître quelles sont les données le concernant. Les entreprises suisses jouent généralement le jeu mais à l'étranger, il faut parfois plusieurs relances pour recevoir une réponse, lorsqu'il y en a une (article 8).

Dans l'article 10, les journalistes et leurs sources sont protégés contre la divulgation de données.

Les personnes traitant les données ne doivent pas porter atteinte à la personnalité des personnes concernées (article 12).

La collecte de données sensibles ou personnelles doit être portée à la connaissance de la personne concernée (article 14). C'est ce que l'on retrouve inscrit en petit dans les CGU (Contrat Général d'Utilisation) que la plupart des gens ne lit pas, tout en cochant la case affirmant le contraire.

Un préposé fédéral à la protection des données est nommé pour 4 ans par le Conseil Fédéral. Les taches du préposé est de surveiller les organes fédéraux, fournir des conseils, recommandations et d'informations. Un rapport est rendu périodiquement.

Chaque canton doit nommer un préposé et se munir d'une ordonnance cantonale sur la protection des données.

La présente loi est détaillée en profondeur dans l'Ordonnance fédérale sur la protection des données.

5.2.9. Loi fédérale contre la concurrence déloyale [31]

L'article 3 définit l'envoi répété d'email publicitaire sans accord (SPAM) comme une pratique déloyale.

5.2.10. Loi et ordonnance sur la signature électronique [32]

La signature électronique est reconnue si elle est certifiée par des organismes reconnus.

5.2.11. LSCPT et LRENS[33][34]

Il y a donc beaucoup de lois, ordonnances et conventions qui régissent le domaine de la protection des données et du piratage informatique. Il y en a encore d'autres, plus spécifiques aux services secrets, la Loi sur le renseignement (LRENS) et à la police Loi sur la surveillance de la poste et des télécommunications (LSCPT), qui leur permet de surveiller les communications.

Une des subtilités de la LSCPT est qu'elle concerne toutes les personnes mettant à disposition un moyen de communication. Ainsi, un réseau wifi ouvert ou un cyber-café sont responsables des actes de leurs utilisateurs. C'est pour cela qu'un signal wifi dépassant le périmètre privé doit être suffisamment protégé puisque c'est le propriétaire qui sera responsable de cas d'infraction commis depuis cette ligne.

Deux nouvelles versions de ces lois ont été proposées afin de mettre à niveau les moyens des enquêteurs et services secrets suisses par rapports à leurs collègues européens.

La nouvelle LRENS est combattue par référendum populaire et devra probablement passer devant le peuple, en automne prochain. Cette nouvelle version prévoit l'utilisation de Chevaux de Troie, intercepteurs téléphoniques et logiciels de piratage par les services secrets. Problème : les failles de sécurité qui seront utilisées sont les mêmes que celles que les hackers utiliseront pour commettre des méfaits. Au lieu d'informer la population et les entreprises de graves dangers, le Service Secret de la Confédération (SRC) devra faire en sorte que la faille ne devienne pas publique et donc non réparée par l'éditeur, protégeant ainsi les hackeurs et mettant en danger toute les infrastructures suisses.

La dernière version de la LSCPT est elle aussi combattue et le processus référendaire en est à la récolte de signatures. La LSCPT réglemente la collecte des données par la police, l'utilisation de virus et chevaux de Troie informatiques, la rétention des données de tous les usagers par les fournisseurs d'accès et la responsabilité des personnes fournissant ou donnant accès à un service de communication. Les clés de chiffrement de services cryptés devront être conservées, rendant illégal le chiffrement bout-en-bout et mettant à mal le marché du cloud sécurisé qui est en pleine expansion en Suisse et des services de messageries chiffrées telles que Protonmail, basé à Genève.

5.3.Conclusion

La Suisse est connue pour avoir une forte politique de protection des données. Cela vient entre autre, de la tradition suisse du secret bancaire. En effet, les lanceurs d'alerte pas toujours désintéressés qui ont contrevenu au secret bancaire sont aussi coupable d'avoir violé la loi sur la protection des données et comme ces données sont sous forme informatique et que les droits d'accès sont restrictifs, certains sont donc aussi condamnés pour intrusion dans un système informatique. La présence de plusieurs préposés à la protection des données est aussi une chose importante dans la réussite d'une politique numérique, même si l'on peut regretter le manque de pouvoir délégué à cette fonction, principalement au niveau fédéral.

La soustraction, la détérioration des données et l'intrusion dans les systèmes informatiques sont punis par le code pénal. Par contre, l'usurpation d'identité n'est pas reconnue en Suisse. Le Conseil Fédéral ne veut pas légiférer là-dessus, estimant que les infractions commises avec une fausse identité est déjà punissable. En France, ceci est puni d'un an d'emprisonnement et de 15'000 euros d'amende. [35]

Nous pouvons juger que mis à part le sujet de l'usurpation d'identité, le droit suisse est plutôt bien armé en matière de protection des données et de piratage. Par contre, la Suisse est clairement à la traîne dans tout ce qui concerne des problématiques posées par les nouvelles technologies. Des sujets tels que la neutralité du réseau internet, le droit à l'oubli, la mort numérique, le stockage des données à l'étranger (forcer les entreprises telles que Facebook à détenir les information concernant les Suisses sur le territoire suisse afin de pouvoir utiliser la législation suisse en cas de plainte), l'encadrement de services tels que Airbnb et Uber, l'utilisation de logiciels étrangers par les administrations (certains peuvent contenir des backdoors en l'absence d'un code source ouvert) et la protection des lanceurs d'alertes (souvent en contradiction avec la protection des données).

Ce qui manque surtout, c'est une stratégie de défense commune et dirigée par un organe d'inspection du niveau de sécurité des administrations et infrastructures critiques. Une stratégie de défense numérique a été publiée en avril 2016. [36] Celle-ci a été rédigée par le Département de la Défense (DDPS) et applique 16 mesures. Autant dire que cela semble particulièrement léger, d'autant plus que celles-ci sont très générales (ex. inclure des partenaires compétents en matière de cyber-risques lors de l'évaluation des infrastructures critiques). MELANI (Central d'enregistrement et d'analyse de la sureté de l'information) chapeaute déjà les entreprises d'importance nationale et les infrastructures critiques mais elle ne peut qu'émettre des recommandations et alerter lors d'attaques informatiques de grande ampleur. Comme nous avons pu le constater il y a quelque temps, cela ne suffit pas ! L'entreprise RUAG (armement, mécanique) pourtant partenaire du DDPS et de MELANI, a été piratée durant plus d'une année, certainement par un service étranger, au vu de la sophistication de l'attaque. Durant un an, pas un organe ne s'est rendu compte du fait cette attaque, jusqu'à ce qu'un service de renseignement étranger (!!!) donne l'alerte. [37] Il est assez cocasse de remarquer que les services secrets étrangers sont plus au courant que nos propres services de ce qui se passe à l'intérieur de nos frontières numériques. Répondant à cela, Guy Parmelin, responsable du DDPS, a mis sur place une task-force qui a pris 14 mesures secrètes afin de renforcer la sécurité.

Nous constatons donc que la plupart du temps, la Suisse réagit au lieu d'agir en amont du risque d'attaque. On a l'impression que plutôt que de créer une base juridique solide et une organisation

centrale dédiée à la sécurité informatique (pour le DDPS) ainsi que de renforcer les taches de MELANI (pour les privés et PME), la Suisse préfère ajouter de petits morceaux d'ordonnances et de mesures, éparpillées au gré des nouvelles attaques réussies contre nos administrations. Cela semble plus être des mesures visant à rassurer la population et les médias qu'une réelle défense centralisée et efficace.

Alors que les nouvelles LRENS et LSCPT veulent permettre à nos services secrets et police d'acheter des virus et logiciels espions, il faut aussi parer de l'achat l'année dernière par la police zurichoise du logiciel espion Galileo pour 486'500 euros. Ce logiciel crée pour le groupe de hackeur « Hacking Team » permet de s'infiltrer dans les téléphones portables. Durant l'automne dernier, la Hacking Team s'est faite elle-même piratée révélant tous ses clients, dont la police zurichoise, et les failles utilisées qui furent immédiatement colmatées part les éditeurs. La Hacking Team disparu et le logiciel devint inutile. La facture, elle, fut bien payée par le contribuable à une entreprise qui a permis à des dictateurs de déroger aux droits de l'Homme et d'assoir la répression. [38]

Le Ministère Public se veut confiant, il rappelle que plusieurs attaques sont déjouées chaque jour contre les administrations et infrastructures suisses, preuve selon lui que la sécurité est à niveau.

6. Conclusion

Après avoir pris connaissance des différentes possibilités techniques permettant d'accéder à un système de données et les moyens existant afin de s'en défendre, nous pouvons nous rendre compte de l'ampleur de la menace et des conséquences désastreuses que peuvent avoir des attaques informatiques ciblées et minutieusement préparées.

Nous avons ensuite passé en revue les différentes attaques informatiques réalisées contre des États et nous avons aussi pu évaluer la probabilité qu'une cyberguerre éclate dans les prochaines années ainsi que les risques pour l'économie et pour la réputation de la Suisse.

Pour finir, nous avons énuméré les différents textes de loi régissant la protection et la conservation des données, et ceux ayant un rapport avec le piratage en Suisse.

Nous pouvons en conclure que le risque d'une cyberguerre existe, et même si il est très faible, de nombreux pays ont développé de puissants outils permettant d'attaquer des cibles stratégiques appartenant à des nations étrangères. Des attaques de ce genre on lieux régulièrement depuis 2007 et leur nombre et leur puissance ne cesse d'augmenter. Il y a aussi de l'espionnage industriel et le sabotage qui peuvent être dévastateurs pour une entreprise dont l'économie nationale est tributaire. Les lois suisses sur la protection des données sont bonnes mais il faut faire attention aux dérives sécuritaires des services de police et de renseignement.

L'enjeu pour le futur est de pouvoir faire face à un nombre croissant de menaces contre nos infrastructures, notre économie et notre nation, tout en prenant garde de ne pas empiéter sur la vie privée des citoyens.

La Suisse a toutes les cartes en main pour devenir un acteur important sur le marché des données si la Confédération parvient à moderniser son approche des nouvelles technologies et à ouvrir les yeux l'importance d'avoir une réelle sécurité informatique.

Jusqu'à présent, la Confédération ne rassure malheureusement pas. Plusieurs projets informatiques furent des désastres avec un coût considérable. Pour exemple, l'armée a dépensé 700 millions dans un système informatique non-sécurisé et le projet fût abandonné. [39]

La récente découverte de l'attaque contre RUAG ne contribue pas non plus à la quiétude.

De plus, la Suisse ne soutient pas assez la révolution numérique. Plusieurs pays ont déjà légiféré sur l'identité numérique et mis en place des départements entiers dédiés au numérique. La France par exemple soutient activement les startups du domaine high-tech avec succès et c'est doté d'un agenda et d'secrétariat d'état au numérique.

Espérons donc que la prise de conscience soit pour bientôt.

7. Bilan

Ce fût un plaisir pour moi de travailler sur ce sujet passionnant. J'ai pu approfondir mes connaissances concernant les lois régissant le domaine informatique. Cela m'a permis en outre, d'avoir une vision globale de la situation des attaques informatiques dirigées contre des nations et de leur ampleur. J'ai apprécié travaillé sur les aspects géopolitiques et géostratégiques afin de pouvoir discerner au mieux les enjeux pour une Suisse évoluant au sein d'un monde ouvert et globalisé.

8. Bibliographie

8.1. Sites Internet

[1] « Un hôpital américain paye une rançon à des pirates informatiques » dans « Le Monde », le 18.02.12016, par Florian Reynaud.
http://www.lemonde.fr/pixels/article/2016/02/18/un-hopital-americain-paye-une-rancon-a-des-pirates-informatiques_4867296_4408996.html

[2] « Des ransomwares en pagaille au ministère des Transport » dans « Le Monde Informatique », le 20.01.2016, par Serge Leblal.
http://www.lemondeinformatique.fr/actualites/lire-des-ransomwares-en-pagaille-au-ministere-des-transports-63649.html

[3] « Les cyber attaques dans le transport maritime » sur « France inter », le 12.12.2014
http://www.franceinter.fr/emission-le-zoom-de-la-redaction-les-cyber-attaques-dans-le-transport-maritime

[4] « Une faute d'orthographe évite au Bangladesh » sur « RTS Info », le 11.03.2016
http://www.rts.ch/info/sciences-tech/7565168-une-faute-d-orthographe-evite-au-bangladesh-un-piratage-d-un-milliard.html

[5] Article Wikipédia sur les rootkits
https://fr.wikipedia.org/wiki/Rootkit

[6] « La cyberguerre aura-t-elle lieu ? » sur « ARTE », par Michèle Kalberer, le 30.09.2015 http://future.arte.tv/fr/quelles-reelles-menaces-se-cachent-derriere-la-cyberguerre/la-cyberguerre-aura-t-elle-lieu

[7] « L'Estonie dénonce les cyber-attaques terroristes russes » par Philippe Crouzillacq, le 10.06.2007 http://www.01net.com/actualites/lestonie-denonce-les-cyber-attaques-terroristes-russes-350759.html

[8] « La Géorgie victime de cyber-attaques » par Olivier Robillart, le 11 août 2008 http://www.silicon.fr/la-georgie-victime-de-cyber-attaques-30893.html

[9] « analyse de Stuxnet » par Charles Dagouat pour le magazine « L'Actusécu » février 2011 https://www.xmco.fr/actu-secu/XMCO-ActuSecu-27-STUXNET.pdf

[10] « Les détails de la cyberattaque qui a mis des centrales ukrainiennes hors service » par Julien Bergounhoux le 04.03.2016 http://www.usine-digitale.fr/article/les-details-de-la-cyberattaque-qui-a-mis-des-centrales-ukrainiennes-hors-service.N382649

[11] « Des scientifiques piratent un drone de l'armée » par Simon Koch dans la TDG du 29.06.2012 http://www.tdg.ch/high-tech/scientifiques-piratent-drone-armee/story/25715353

[12] « Le drone US capturé victime d'un Hacking ? » par Stéphane Larcher, le 16.12.2011 http://www.linformaticien.com/actualites/id/22753/le-drone-us-capture-victime-d-un-hacking.aspx

[13] « La Suisse neutre cachait un nid d'espions » par Pascal Fleury le 28.08.2015, dans « La Liberté » http://www.laliberte.ch/news/histoire-vivante/la-suisse-neutre-cachait-un-nid-d-espions-296919

[14] « Israël a écouté les pourparlers avec l'Iran » le 12.06.2015 dans « 24 Heures » http://www.24heures.ch/monde/moyen-orient/israel-ecoute-pourparlers-iran/story/28704366

[15] « Le boom de l'espionnage économique » par Jacques Monin le 04.09.2015 sur « France inter » http://www.franceinter.fr/emission-lenquete-le-boom-de-lespionnage-economique

[16] « La France accusée d'être championne en espionnage industriel » par l'AFP le 05.01.2011

http://tempsreel.nouvelobs.com/monde/20110105.OBS5720/la-france-accusee-d-etre-championne-en-espionnage-industriel.html

[17] « Étude de McAfee Security sur l'impact économique des malwares »

http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

[18] « Convention sur la cybercriminalité »

https://www.admin.ch/opc/fr/classified-compilation/20100537/index.html

[19] « Manuel de Tallinn »

http://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf

[20] « Comment Anvers a été piraté et s'en est sorti » par Christophe Lamfalussy, le 25.10.2013

http://www.lalibre.be/economie/actualite/comment-anvers-a-ete-pirate-et-s-en-est-sorti-5269e7ea35708def0d93513c

[21] « Règlement européen sur la protection des données »

http://www.numerama.com/content/uploads/2015/12/reglement-donnes-personnelles-compromis.pdf

[22] « Les conséquences de l'invalidation de l'accord « Safe Harbor » sur les données personnelles » Par Cécile Ducourtieux (Bruxelles, bureau européen), Martin Untersinger et Damien Leloup dans « LE Monde », le 06.10.2015

http://www.lemonde.fr/pixels/article/2015/10/06/safe-harbor-que-change-l-arret-de-la-justice-europeenne-sur-les-donnees-personnelles_4783686_4408996.html

[23] « Constitution fédérale »

https://www.admin.ch/opc/fr/classified-compilation/19995395/index.html

[24] « Code civil suisse »

https://www.admin.ch/opc/fr/classified-compilation/19070042/index.html

[25] « LOI COMPLÉTANT LE CODE CIVIL SUISSE »
https://www.admin.ch/opc/fr/classified-compilation/19110009/index.html

[26] « CODE PÉNAL SUISSE »
https://www.admin.ch/opc/fr/classified-compilation/19370083/index.html

[27] « CODE DE PROCÉDURE CIVILE »
https://www.admin.ch/opc/fr/classified-compilation/20061121/index.html

[28] « ORDONNANCE CONCERNANT LA TENUE ET LA CONSERVATION DES LIVRES DE COMPTES »
https://www.admin.ch/opc/fr/classified-compilation/20001467/index.html

[29] « LOI FÉDÉRALE SUR LE DROIT D'AUTEUR »
https://www.admin.ch/opc/fr/classified-compilation/19920251/index.html

[30] « LOI FÉDÉRALE SUR LA PROTECTION DES DONNÉES »
https://www.admin.ch/opc/fr/classified-compilation/19920153/index.html

[31] « LOI FÉDÉRALE CONTRE LA CONCURRENCE DÉLOYALE »
https://www.admin.ch/opc/fr/classified-compilation/19860391/index.html

[32] « LOI FÉDÉRALE SUR LES SERVICES DE CERTIFICATION DANS LE DOMAINE DE LA SIGNATURE ÉLECTRONIQUE »
https://www.admin.ch/opc/fr/classified-compilation/20011277/index.html

[33] « LOI FÉDÉRALE SUR LA SURVEILLANCE DE LA CORRESPONDANCE PAR LA POSTE ET TÉLÉCOMMUNICATION »
https://www.admin.ch/opc/fr/federal-gazette/2013/2483.pdf

[34] « LOI SUR LE RENSEIGNEMENT »
http://www.news.admin.ch/NSBSubscriber/message/attachments/33840.pdf

[35] Article de François Charlet sur l'usurpation d'identité, le 14.10.2013

https://francoischarlet.ch/2013/usurpation-didentite-le-conseil-federal-ne-legiferera-pas-et-il-a-tort/

[36] Stratégie « Suisse numérique »

http://www.bakom.admin.ch/themen/infosociety/?lang=fr

[37] « Les questions que pose l'affaire de cyberespionnage contre Ruag » par Lise Bailat, le 05.04.2016, dans « Le Temps »

https://www.letemps.ch/suisse/2016/05/05/questions-pose-affaire-cyberespionnage-contre-ruag

[38] « Les logiciels espions des polices soulèvent un tollé » par Lucie Monnat dans « 24 heures », le 08.07.2015

http://www.24heures.ch/suisse/logiciels-espions-polices-soulevent-tolle/story/19433482

[39] « L'armée a gaspillé 700 millions dans un projet raté » par Arthur Grosjean, dans « Le Matin », le 26.03.2012

http://www.lematin.ch/suisse/armee-gaspille-700-millions-projet-rate/story/22015841