Zeitschrift: Revue Militaire Suisse
Band: - (2015)
Heft: 2

Artikel: Cyber Défense : Les nations investissent pour se protéger : quid de la Suisse?
Autor: Bischof, Sébastien / Ruch, Grégory
DOI: https://doi.org/10.5169/seals-781252

Cyber

Cyber Défense : Les nations investissent pour se protéger, *quid* de la Suisse ?

Sébastien Bischof et Grégory Ruch
Membres du team Cyberdéfense et experts en sécurité des systèmes d'information et de communication chez ELCA Informatique SA

Décryptage – L'Etat islamique (EI) fait la une sur Internet grâce à leur progression rapide en cyber sécurité. Ils ne sont pas seuls, toutes les grandes puissances investissent dans le domaine. Où se situe la Suisse dans le paysage de la cyber défense ?

A l'heure actuelle, il n'est plus anodin d'apercevoir sur nos écrans des images choc telles qu'une séance de décapitation collective ou appel au djihad par de jeunes Européens brûlant leurs passeports. Ceci est dû au fait que toutes les récentes provocations de l'EI sont très rapidement repérées et relayées sans relâche par les médias. Cette couverture médiatique de l'EI n'est pas le fruit du hasard et la recette de leur succès n'est pas nouvelle, ce type de propagande existant depuis plus d'une trentaine d'année. C'est le résultat d'une stratégie médiatique qui a débuté dans les années 1990 avec l'apparition des premières vidéos réalisées par les talibans en Afghanistan.

Une vingtaine d'années plus tard, la technologie a grandement évolué notamment avec l'essor d'Internet, mais les buts des djihadistes demeurent les mêmes, à savoir, terroriser l'ennemi et trouver des nouveaux candidats au djihad. Dans ce deuxième cas, l'EI cherche à recruter de jeunes personnes et pour atteindre leur public cible, ils ont recours à des moyens de communication modernes tels que les réseaux sociaux et le marketing viral. Cette évolution saute aux yeux lorsqu'on regarde les derniers films de propagande, dignes de films d'action hollywoodiens tels que *Flames of War* et *Salil Sawarim (Clanging of swords)*.

Mais qui dit nouvelles technologies, dit aussi nouveaux risques. C'est à leur dépends que les partisans de l'EI l'ont appris. Des cellules terroristes ont été éliminées par bombardement grâce aux métadonnées des photos que leurs membres ont publié sur les réseaux sociaux. Dans le cas concret mentionné ci-avant, celles-ci contenaient des données de géolocalisation et les dates de prise des clichés. Avec ceci il a été facile localiser et donc d'éliminer le groupuscule à l'origine des dites images.

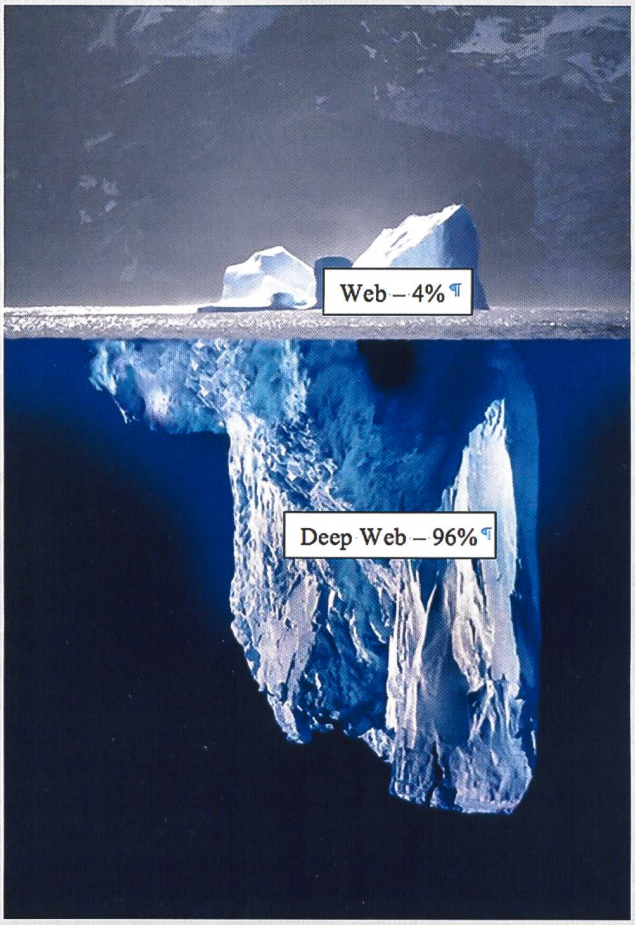
En un temps record, l'EI a appris de ses erreurs et s'est mis à publier des lignes directrices concernant ces nouvelles technologies et a donc commencé à former ses partisans à l'utilisation des nouveaux moyens à disposition. Cette évolution rapide s'explique par le fait que contrairement aux états occidentaux, les conséquences de la mauvaise utilisation de ces outils ne sont pas d'ordre financier ou judiciaire, mais bel et bien un danger de mort. Il leur était donc nécessaire de diminuer ce risque, sans compter la préservation de leur cause.

Il est intéressant d'observer que cet apprentissage constitue un processus itératif. A chaque erreur commise, il y a eu apprentissage et modification de comportement. Contrairement aux idées reçues, on ne peut pas les catégoriser de « *digital migrants* » (individus d'un certain âge, habitués au format papier et qui doivent se familiariser avec les outils informatique), car même si les personnalités à la tête du mouvement font partie de ceux-ci, en revanche, la majorité des partisans actifs pour leur cause sur Internet sont des « *digital natives* » (individus ayant grandi avec les nouvelles technologies de l'information et de la communication). Il ne faut pas oublier non plus que parmi leurs partisans, on trouve des personnes hautement qualifiées qui ont suivi des hautes études dans le domaine des technologies de l'information (parfois en Europe et même aux Etats-Unis).

Pour corroborer cela, un exemple flagrant de cette adoption des moyens modernes de communication par l'EI est le tournant de celui-ci vers les outils du Deep Web (voir encadré) ou plus communément appelé Darknet. Le graphique ci-dessous montre l'augmentation de l'utilisation du réseau **Tor** (voir encadré) suivant l'offensive de l'EI en Irak. Le creux et la diminution qui s'ensuit montrent la réponse du Gouvernement Irakien : dans une première phase, celui-ci

Le deep web

est une section de l'Internet qu'on ne peut atteindre par les chemins conventionnels.



Le web traditionnel ne représente environ que 4% de l'Internet. Les 96% restants sont la partie cachée de l'iceberg. Ce sont des sites et des fichiers qu'on ne peut pas localiser avec les moteurs de recherche traditionnels comme Google, par exemple.

Le *deep web* a été initialement créé par et pour des personnes qui voulaient protéger leurs communications, comme les gouvernements ou les militants pour les droits de la personne. Celui-ci est également fréquenté par des individus qui souhaitent se soustraire à toute forme de surveillance comme les anarchistes, les pirates informatiques ou les libertaires du web.

C'est également un lieu de prédilection pour ceux qui s'adonnent à des activités illicites. De nombreux commerces illégaux y fleurissent et on peut notamment se procurer des numéros de cartes de crédit, de faux passeports, des armes, de la drogue, des tueurs à gages, ou encore de la pornographie infantile.

Malgré tout, l'utilisation du *deep web* reste marginale mais depuis les révélations fracassantes d'Edward Snowden à propos des opérations d'espionnage de la NSA, de plus en plus d'internautes, méfiants, lorgnent ce territoire protégé.

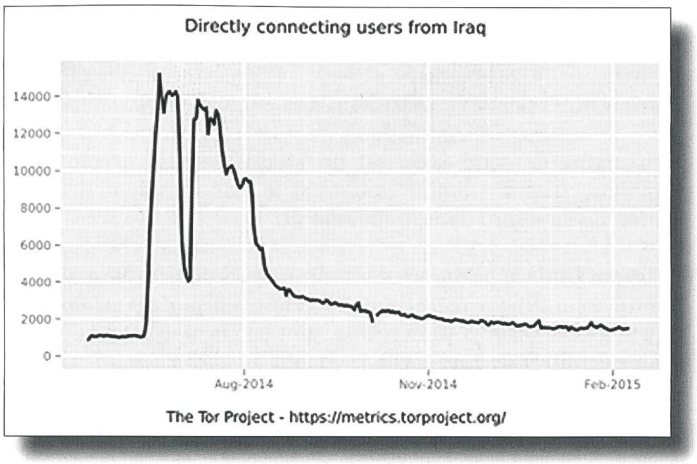
a fait fermer l'accès à ce service. Dans une deuxième phase, celui-ci a été contraint de couper l'accès Internet de certaines régions du pays.

Tor, la porte d'entrée

Le logiciel le plus populaire pour accéder au deep web se nomme Tor, qui est un acronyme de «The Onion Router». C'est un logiciel créé par le laboratoire de recherche de la marine américaine qui permet de créer des sites ou d'offrir des services qui assurent l'anonymat à ses utilisateurs.

La montée en puissance de l'EI dans le domaine de la protection de l'information n'est donc qu'un exemple parmi les autres; entre les groupuscules mafieux et les nations qui améliorent constamment leurs technologies en investissant dans ce domaine qui est un des fondements de la cyber-défense. Toutefois, le point fort de l'EI est la rapidité avec laquelle il a réduit sa fracture numérique à néant pour se trouver aujourd'hui au même niveau de connaissance que certaines nations occidentales, voir plus avancé. Cette force provient de la participation volontaire de ses membres pour défendre leur cause. Contrairement aux nations occidentales, où l'on doit recruter des ressources qualifiées, les rémunérer, trouver des locaux et du matériel, l'EI dispose du savoir-faire de ses membres qui le mettent à disposition de l'organisation.

Si l'on élargit le champ de vision, l'engouement général pour les nouvelles technologies fait que le monde cybernétique évolue plus rapidement que le monde réel. Cela se ressent fortement dans les pays qui conçoivent ces nouvelles technologies car il n'est pas rare que les lois aient un pas de retard et ne soient pas applicables telles quelles aux nouvelles problématiques induites.



En plus d'évoluer rapidement, le monde cybernétique a commencé à prendre le pas sur le monde réel en allant jusqu'à bousculer les règles et les rapports de puissance établis qui contribuaient jusque-là à l'équilibre mondial.

La protection des nations contre le « cyber crime » ou les « cyber attaques » est devenu un sujet extrêmement important. Les nouvelles règles amenées par le monde cybernétique remettent en question les modèles de conflits connus. Il y avait, il y a et il y aura toujours des différences entre les nations, ne serait-ce qu'en termes de moyens, de technologies, de culture ou d'opinion publique, pour ne citer que celles-là. Les notions de conflits symétrique, dissymétrique ou asymétrique permettaient de comprendre aisément que si la Suisse devait affronter militairement les Etats-Unis d'Amérique, la balance ne pencherait pas en notre faveur. Mais lorsqu'on inclut ces nouvelles technologies dans l'équation, on comprend que les règles du jeu ont changé. Car dans le monde cybernétique, une personne seule avec un ordinateur et le savoir nécessaire pourrait faire trembler une nation aussi puissante que les USA.

Les USA sont encore aujourd'hui les concepteurs de la plupart de ces outils informatiques, et de ce fait, il ne leur est pas difficile d'y cacher des logiciels espions ou des portes dérobées (voir encadré). Cela et leur expertise leur donne un avantage stratégique indéniable sur le reste du monde. Mais le jour où les groupes terroristes et les nations moins avancées se mettront à créer leurs propres outils, cet avantage stratégique certain sera perdu. En attendant l'EI a recours à une parade « *low-tech* » qui consiste à ne pas communiquer d'informations sensibles au travers de ces technologies et de revenir à la « bonne vieille méthode » du messager.

Et pour la Suisse ?

En ce qui concerne la Suisse, certains outils sont développés dans le pays mais la plupart proviennent en grande majorité de technologies israélo-américaines. De ce fait, la Suisse est sujette aux mêmes risques d'espionnage, même dans les hautes sphères. Cela est notamment arrivé à la chancelière allemande Angela Merkel qui était sous écoute car elle utilisait un Iphone.

Prenons par exemple les statistiques d'utilisation des systèmes d'exploitation en Suisse, on s'aperçoit que quasiment l'entier de ces systèmes (plus de 99,9%) sont issus d'entreprises de technologies américaines (Microsoft, Apple et Google). Ces sociétés étant sujettes au Patriot Act (voir encadré) et poussant les consommateurs à utiliser leurs technologies Cloud dont les données sont stockées sur le sol américain, n'ont certes pas la volonté d'espionner leurs utilisateurs mais si une demande officielle leur est faite, ils sont forcés d'y accéder.

Que-ce qu'une porte dérobée ?

En informatique, Une « porte dérobée » ou « *backdoor* » est une fonctionnalité d'un logiciel inconnue de l'utilisateur légitime. La personne connaissant la porte dérobée peut l'utiliser pour surveiller les activités du logiciel, en prendre le contrôle, voire contrôler l'ensemble des opérations de l'ordinateur.

Les pirates informatiques sont les plus grands utilisateurs de portes dérobées notamment pour surveiller ce que fait l'utilisateur légitime, pour copier ou détruire des données ayant une valeur (mots de passe, clé privée pour déchiffrer des messages privés, coordonnées bancaires, secrets commerciaux) ou simplement prendre le contrôle d'un ordinateur et de pouvoir l'utiliser pour mener des actions malveillantes.

En plus des acteurs précités, il y a les gouvernements qui installent des portes dérobées pour des besoins d'espionnage. La découverte de ce type de portes dérobées devient de plus en plus fréquente. La dernière date du début du mois de mars 2015 et été baptisée « Freak. » Elle permet de déchiffrer les communications web sécurisées.

L'origine de cette faille est un affaiblissement cryptographique, inséré volontairement par la NSA lors de la définition du standard dans les années 90.

Ils ont bridé le protocole de communication sécurisé « SSL » en s'assurant que cette limitation était suffisante pour protéger les échanges commerciaux, tout en permettant à la NSA de déchiffrer les flux si elle le voulait.

Le Patriot Act

est une loi américaine qui autorise les services de sécurité américains à accéder aux données informatiques des particuliers et des entreprises sans autorisation préalable et sans notifications aux utilisateurs.

Cette loi est la conséquence directe des attentats du 11 septembre 2001. Un mois et demi après cette tragédie, le Congrès américain a voté dans l'urgence un texte de 300 pages qui fût accepté sans polémique car le peuple Américain était traumatisé.

La loi étend les pouvoirs des autorités en matière de surveillance. Elle renforce l'action des agences de renseignement. Par exemple, elle permet au FBI de fouiller dans les données personnelles, les documents et les relevés bancaires d'un individu, sans avoir à justifier qu'ils sont en rapport avec une enquête terroriste. Le *Patriot Act* donne aussi la possibilité aux forces de l'ordre de surveiller les messages électroniques sur internet sans prévenir les intéressés, d'effectuer des écoutes téléphoniques sans autorisation préalable de la justice.

Au départ, le *Patriot Act* devait être une loi d'exception, pour une durée de quatre ans. Mais le Congrès américain l'a reconduite à plusieurs reprises jusqu'en juin 2015.

Des élus, des militants des droits de l'homme et même des industriels n'en veulent plus sous sa forme actuelle. L'affaire Snowden, qui a révélé les écoutes massives de la NSA en Amérique et dans le monde entier, a achevé de les convaincre. En revanche, les partisans de cette loi affirment qu'elle a permis de protéger les Etats-Unis contre les attentats.

Certaines nations avec suffisamment de moyens comme la Russie, la Chine et l'Inde ont bien compris cette problématique et ont commencé à développer eux-mêmes leurs systèmes d'exploitation.

Toutefois, cette problématique ne se limite pas aux systèmes d'exploitation. En s'intéressant de plus près aux techniques utilisées par les espions et leurs logiciels malveillants, on comprend que ceux-ci exploitent sans scrupules les chaînes de production de masse de matériel informatique afin de répandre sur le marché des appareils dotés, par exemple, de logiciels de prise de contrôle à distance dormants. Ceux-ci, peuvent aussi être directement intégrés au matériel et deviennent donc indétectables par les antivirus.

Quelles devraient être les prochaines étapes pour la Suisse ?

Dans le domaine de la sécurité, l'état doit apporter un ensemble de mesures de protection pour ses citoyens et ses entreprises. Si c'est le cas pour la sécurité traditionnelle, ce n'est pas encore le cas dans l'espace cybernétique. Aujourd'hui en Suisse, les entreprises et les particuliers sont quasiment livrés à eux-mêmes face aux cyberattaques.

Ce qu'il manque à la Suisse, en premier lieu, c'est un organe indépendant de prévention de cyberattaques et de gestion de la cyberdéfense pour l'ensemble du pays soit un « centre de compétences cyberdéfense national ». Les missions principales de cette agence seraient la protection des personnes morales et physiques contre le cybercrime ainsi que la protection des infrastructures critiques contre toute sorte de cyberattaques. La listes des infrastructures critiques à protéger est longue; production, transport et distribution d'électricité, d'eau potable, les télécommunications, la santé publique avec ses hôpitaux et ambulances, les services de sécurité avec la police, la protection civile et l'armée, etc.

Ce nouvel organe devrait être mis en place sous la forme d'une plateforme de collaboration entre les citoyens, l'état et l'industrie. Il y aurait une communication bidirectionnelle entre le centre de compétences cyber-défense et les entreprises suisses. Dans un sens, ces dernières pourraient obtenir des informations précises concernant les dernières vulnérabilités des systèmes d'information et également être rapidement au courant des cyberattaques qui ont lieu dans notre pays en temps réel. Et dans l'autre sens, pour que ce flux d'informations puisse être créé et délivré aux entreprises, il faut fournir à celles-ci une interface leur permettant de remonter des informations anonymisées. Cela permettra d'avoir une plateforme d'échange d'information modérée et administrée par une entité de confiance.

Dans un deuxième temps, c'est lui qui prendrait en charge les problèmes de cybersécurité avec une étroite collaboration avec l'industrie spécialisée dans le domaine de la sécurité des systèmes d'information et de communication. Il faut une coordination nationale dans l'optique de rétablir la situation au plus vite avec, en cas de nécessité, une « milice cyberdéfense » qui serait composée d'experts privés, entraînés régulièrement pour réagir à ce genre de situations.

La Suisse, étant une pionnière dans bon nombre de technologies de pointe dont l'informatique, a toutes les cartes en main pour réaliser de manière efficace une telle entité.

Un autre organe public qu'il manque dans le paysage de la cyberdéfense suisse est une agence de contrôle dédié aux technologies de l'information comme le FIPS pour les Etats-Unis. Cela permettra aux citoyens et aux entreprises Suisses soucieux de la sécurité de leurs données personnelles d'avoir une base sur laquelle se reposer, ce qui n'est pas le cas actuellement.

Cette organisation devra par exemple, commencer par analyser en profondeur les outils de bureautique du marché les plus utilisés et les certifier comme « exempts de logiciel espion » le cas échéant ; et dans le cas contraire, mandater une entreprise Suisse pour développer un Ersatz sain. L'étape ultime serait la création d'un système d'exploitation « Suisse » qui pourrait se baser sur des briques certifiées comme « saines » par des analyses en profondeur.

Lorsque cela sera fait, la Suisse pourra offrir une suite bureautique exempte de portes dérobées et d'une fâcheuse tendance à envoyer des informations dans les data center américains. A l'inverse, la Suisse pourra jouer de son image de qualité (Swiss-made) et mettre en avant sa neutralité et sa stabilité politique pour investir les marchés du stockage d'information.

En utilisant des data center localisés physiquement sur notre territoire, dotés de ces technologies « agrées » et certifiées comme sûres, la Suisse pourra se démarquer facilement de ses concurrents en garantissant la sécurité des données et devenir, en quelques sortes, la banque d'information mondiale du futur. A l'inverse du secret bancaire, la loi sur la protection des données est inscrite dans notre constitution, mais surtout dans la convention des droits de l'homme et ce n'est pas la pression d'un état « outre-atlantique » qui pourra changer cela.

Ces quelques lignes ont permis de donner un éclairage sur une des premières lignes de la défense qui est la protection de l'information et l'utilisation de moyens informatiques protégés contre l'espionnage. Ce n'est qu'ensuite que d'autres méthodes pourront être mises en place, notamment au niveau des contre-mesures.

S. B. et G. R.