Le centre d'opération de la NSA en 2012.
© Photo NSA.

Cyber

Pour une cybersécurité et une cyberdéfense à la hauteur des enjeux auxquels est confronté la Suisse

Prof. Dr. Solange Ghernaouti
Directrice du Swiss Cybersecurity Advisory & Research Group, Université de Lausanne

Le cyberespace estompe les frontières entre les mondes civil et militaire. Le sommet de l'OTAN de septembre 2014[1] a consacré les cyberattaques massives comme acte de guerre auquel il pouvait être répondu militairement. Si un membre de l'OTAN en était victime, ce serait considéré comme une atteinte à l'ensemble des membres de l'OTAN. Cette déclaration n'a rien de surprenant à l'heure où les conflits se déclinent désormais également dans le cyberespace via le plus souvent des cyberattaques sur des infrastructures informatiques civiles et militaires et par la manipulation de l'information. Le cyberespace est devenu, comme l'air, la mer, la terre et l'espace un champ de bataille à part entière. Les technologies de l'information peuvent être considérées comme des armes de guerre et la dualité de leurs usages militaire et civil est donc une de leurs caractéristiques intrinsèques.

Sur Internet, le marketing de la guerre et du terrorisme jouxte celui des entreprises licites et illicites et le marché noir de la cybercriminalité se porte bien. Internet est un terrain privilégié d'expression de la criminalité, de la communication d'influence et de la surveillance. Faire dysfonctionner des infrastructures vitales d'un pays, servir des stratégies criminelles, générer des pertes de productivité, de compétitivité ou des prises de pouvoir est non seulement possible mais largement facilité par l'Internet.

Une nouvelle expression de la violence légitime au XXIe siècle

Dans un contexte d'hypercompétitivité économique et de connectivité mondiale, nos systèmes d'information sont à travers le cyberespace la cible de conflits permanents orchestrés par certains Etats ou acteurs économiques ainsi que par des groupes criminels ou terroristes. Cela signifie que des cyberattaques peuvent prendre pour cible des infrastructures vitales comme celles relevant des secteurs de la santé, de l'énergie, de l'eau et l'alimentation, des télécommunications ou encore de la finance. Le haut fourneau attaqué en Allemagne[2] en 2014 ou l'attaque Stuxnet contre l'Iran en 2010 par exemples, en a démontré la faisabilité.

Produire de la sécurité nécessite de comprendre le monde dans lequel nous vivons. C'est comprendre que l'Internet marque une rupture dans l'histoire de l'humanité et que c'est au travers de son prisme qu'il faut trouver une clé de lecture des enjeux de la maîtrise du cyberespace et de la cybersécurité. Il nous faut décrypter la place des logiques industrielles et commerciales des acteurs de l'Internet dans les stratégies de puissance des Etats, sans oublier de décrypter les logiques criminelles et leur modes opératoires dans le cyberespace, pour espérer répondre efficacement aux besoins de protection de nos valeurs fondamentales, de notre patrimoine numérique, de notre économie, de notre territoire et de notre souveraineté digitale.

Le cyberespace est devenu un élément de civilisation dont nous sommes dépendants. Disposer d'infrastructures robustes et résilientes face à toutes sortes d'incidents, notamment cyber, est donc impératif pour maitriser le risque systémique induit par l'usage extensif des technologies de l'information et l'interdépendance des infrastructures, y compris vitales.

De l'intérêt de lutter contre la cybercriminalité

Quelles que soient la finalité des cyberattaques, les outils de cybermalveillance sont identiques. La nature et l'ampleur des impacts[3] varient selon la cible et la motivation des

1 http://www.nato.int/cps/en/natohq/news_112107.htm?selectedLocale=en, NATO Wales Summit Guide - Newport, 4-5 September 2014

2 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf

3 *Cyber-Defence: Quo vadis? Teil 2: Entwicklung der Bedrohung, Nationale Strategie, Rolle der Armee, Sicherheitspolitische Aspekte,*

attaquants, toutefois, les modes opératoires et les outils utilisés pour nuire sont identiques. Aucun Etat, aucune organisation, aucun internaute n'est à l'abri de cybernuisances, qu'elles soient d'origine criminelle ou non.

Pour un Etat, lutter contre la cybercriminalité suppose de disposer d'un cadre légal national et compatible au niveau international ainsi que des forces de justice et de police opérationnelles. Ces dernières doivent de plus, être dotées de ressources et de compétences adaptées et s'appuyer sur un système d'entraide internationale efficace pour combattre le crime transnational. Un défaut d'efficacité en matière de lutte contre la cybercriminalité profite aux criminels qui le plus souvent agissent en toute impunité. Ils considèrent le cyberespace comme une couche d'isolation protectrice et un champ d'action mondial, l'Internet comme un levier de la performance criminelle (crime économique, blanchiment d'argent, trafic d'êtres humains, de drogue, d'armes...).

Lutter contre la criminalité a de tout temps été complexe, la cybercriminalité a renforcé cette complexité et augmenté la difficulté dans la lutte contre celle-ci. Si les exploits de cybercriminels sont régulièrement relatés, il ne semble pas que leur soient opposé des mesures suffisamment efficaces pour limiter leur montée en puissance, ni pour diminuer le nombre de leurs victimes. Il y a toujours peu d'arrestations ou de procès au regard de la réalité des actes malveillants et peu de sentiment de justice pour les victimes. Les cas ne sont pas suffisamment dénoncés et peu font l'objet d'investigation. Les victimes sont alors doublement pénalisées: d'abord par les attaques qu'elles subissent, ensuite par l'inefficacité des instruments censés contribuer à leurs protection et réparation.

A la recherche d'un optimum

Pour un pays, avoir une force militaire compétente, dédiée aux questions « cyber » est impératif comme l'est sa préparation à pouvoir gérer des crises majeures dues à sa dépendance aux technologies de l'information ainsi qu'à son approvisionnement énergétique. La stabilité d'un pays, sa souveraineté et son développement économique dépendent désormais de sa capacité à maitriser les cyberrisques.[1] Assurer la cybersécurité des personnes, des biens matériels et immatériels mais aussi la sûreté publique s'inscrit dans un projet politique au service d'une stratégie de développement durable de notre société qui tient compte de sa culture et de ses valeurs. Cela nécessite l'implication de tous.

Puisque ce sont les mêmes outils qui sont utilisés à des fins criminelles ou conflictuelles, la cybercriminalité concerne aussi les militaires en tant que facteur amplificateur des risques. Il s'agit dès lors d'appréhender le continuum qui existe entre la cybersécurité et la cyberdéfense et d'optimiser les synergies et complémentarités.

Nos infrastructures critiques, notre tissu économique, notre population sont-ils suffisamment protégés? Serons-nous assez réactifs en cas de Pearl Harbour numéri Existe t-il un à l'instar du laboratoire de Spiez la défense atomique et chimique, une structur « cyberprotection civile »?

Bien que nous soyons tous convaincus de la néc d'agir, nous sommes pour autant encore désem par la complexité du problème et réticents à dé les ressources nécessaires. Il s'agit toujours aujou de savoir qui va payer et comment collaborer ent différents acteurs fédéraux, cantonaux et privés. question en suspens reste un frein à la mise en d'une véritable stratégie nationale de cybersécurit serait également au service des habituels laissés compte, c'est à dire les citoyens et les petites et moy entreprises, en fait, de la population au sens large.

Il est important de protéger et de défendre les patrim numériques des individus, des organisations et de l les infrastructures qui les supportent ainsi qu infrastructures vitales par des actions complémen de protection (au sens civil) et de défense (da acceptation militaire du terme). Développer une de la cybersécurité et de la cyberdéfense, tout en fav un dialogue international sur ces questions, devrai un monde complexe, conflictuel et incertain, contri un certain niveau de confiance et de stabilité, à co que chaque partie prenante agisse de manière respo et loyale. En effet, la cybersécurité ne devrait p uniquement un instrument de domination et d'exp de la puissance des états mais plutôt celui mis au du développement de la paix.

Une action de sécurité ne se limite pas à une déma protection, mais intègre celles de réaction, de répr voire d'attaque. Dans le cyberespace, être en me réagir est fondamental. Se doter d'une force de informatique, en faire la démonstration pour di peut être également nécessaire. Certains pa bien compris l'intérêt de disposer d'une inform offensive et défensive et la course à l'arm cybernétique est en plein essor. Pour notre souv nationale, il est essentiel de ne pas accum retard dans ce domaine ou d'apparaître com parent pauvre. Si vous n'êtes pas assis à la t négociation, c'est que vous faites partie du me protection des intérêts politiques et économi la Suisse passe désormais aussi, par une cyber et une cyberdéfense complémentaires et Avons-nous fait les efforts suffisants pour maît cyberrisques et maintenir les cybernuisances d limites acceptables?

Objectif « cybersécurité »: Une vision Suisse

Afin de répondre à la problématique « cyber » devrait pouvoir s'appuyer notamment sur les inst suivants:

- une politique cohérente de recherche et de dévelo en sécurité informatique et cybersécurité;
- une politique industrielle qui comprend entres

1 *Cyberpower : crime, conflicts and security in cyberspace*, Solange Ghernaouti, EPFL Press 2013.

soutien aux entreprises innovantes en matière de sécurité informatique et sécurité de l'information (notamment pour éviter leur rachat par des acteurs étrangers);
- des mesures pour assurer notre souveraineté numérique et réduire notre dépendance aux services et technologies de sécurité produits par des acteurs ou fournisseurs étrangers;
- des actions visant à renforcer la robustesse et la résilience de nos infrastructures informatique et télécom (redondance des systèmes, capacité à pourvoir continuer à travailler en mode dégradé, ...);
- une politique de sensibilisation (du plus jeune au sénior), de formation dans tous les niveaux d'enseignement, quelles soient les disciplines enseignées et de formation continue (sans oublier les dirigeants politiques et économiques, les personnes en charge du système de justice et police);
- un renforcement du dispositif légal et des dispositifs liés à l'entraide judiciaire internationale et des moyens cantonaux et fédéraux aptes à lutter contre la cyber-criminalité et l'espionnage économique);
- des actions visant à assurer la cohérence du Continuum civilo-militaire de Cybersécurité et de Cyberdéfense et à assurer la prise de responsabilité des acteurs publics et privés et l'efficacité de leurs actions;
- le renforcement de la diplomatie relative aux questions «cyber,» car la Suisse doit profiter de sa position privilégiée et son histoire pour se poser en acteur international majeur dans le domaine de la cyberdiplomatie (avenir d'Internet, gouvernance, traité international du cyberespace, etc).

Conclusion

Assurer la sûreté publique, la sécurité économique ou encore la sécurité nationale de la Suisse se situe plus que jamais dans un continuum de sécurité civile et militaire. Il est donc important que cela se reflète également dans les stratégies cybersécurité et cyberdéfense de la confédération afin d'optimiser l'efficacité et l'efficience de la démarche et de répondre au mieux aux besoins de la population, que cela soit en temps de paix ou de conflits.

La sécurité de la Suisse passe par une véritable maitrise des risques «cyber» et une implication de tous les acteurs. Des civils, il est attendu qu'ils rendent la société et l'économie moins vulnérables et aussi résistantes et résilientes que possible aux cyberrisques, de l'armée qu'elle prenne le relais lorsque la situation l'exige et assure sa mission traditionnelle en tenant compte du contexte cybernétique. Il est crucial que chacun fasse sa part de travail car si par exemple les civils ne le font pas, l'armée pourrait au mieux servir de «pompier.» De plus, la Suisse, qui en possède tous les atouts, devrait se donner les moyens de devenir un centre d'excellence mondialement reconnu pour la qualité de sa cybersécurité et de sa cyberdéfense. Il s'agit d'agir rapidement et de considérer ce champ d'action comme des opportunités et des leviers au service notamment de la place économique suisse et de la souveraineté nationale. Attendre serait une erreur car les menaces ne sont pas virtuelles, en fait, la Suisse, n'a pas vraiment le choix!

S. G.

Photo aérienne de la NSA en 2013. © Photo de Trevor Paglen.