Oblast d'Ivano-Frankivsk, zone la plus touchée par les attaques de 2015.

Cyberdéfense

La règle, c'est que le général qui triomphe est celui qui est le mieux informé

Sgt Valentin
Ecole de recrues cyber

Le général chinois Sun Tzu, auteur de l'ouvrage de stratégie *L'Art de la guerre*, l'avait compris il y a plus de 2'000 ans déjà : l'information joue un rôle crucial dans un conflit armé. Avec le développement de l'informatique, de plus en plus d'aspects de nos vies en dépendent.

L'importance de l'informatique, tant pour une armée que pour une nation, est telle qu'il n'est pas rare de voir aujourd'hui des infrastructures informatiques comme cibles dans un conflit militaire. L'apparition de la première cyber-arme de l'histoire et même des unités militaires spécialisées dans les attaques informatiques ont changé les enjeux des batailles à venir, révélant la vulnérabilité des systèmes de communication, d'approvisionnement énergétique, de gestion des flux financiers, de contrôle d'appareillages dans tous les domaines, pour n'en citer que quelques-uns. Les combats du XXIe siècle non dès lors plus rien à voir avec ceux des guerres précédentes. L'ennemi est partout, peut être n'importe qui et peut prendre n'importe quelle forme y compris des 1 et des 0…

Stuxnet : La première cyber-arme

Signalé pour la première fois par l'entreprise biélorusse VirusBlockAda en juin 2010, Stuxnet est un virus dont le développement est attribué à la NSA et à son équivalent israélien, l'Unité 8200, une unité de renseignement de l'armée spécialisée dans le renseignement d'origine électromagnétique ainsi que du décryptage de codes.

Stuxnet est aujourd'hui considéré comme la première cyber-arme de l'histoire et le premier ver découvert capable de reprogrammer des systèmes industriels. D'après l'entreprise américaine Symantec, Stuxnet aurait au total infecté plus de 45'000 machines dont 30'000 en Iran. La cible principale était la centrale nucléaire de Bouchehr à quelques kilomètres de la ville du même nom, un site d'importance du programme d'armement nucléaire du pays.

Un *malware* d'une taille de 500 Ko, c'est ce qui a suffi pour freiner un des sites les plus sécurisés du programme d'armement nucléaire d'une nation qui en 2014 faisait partie des 15 plus grandes puissances militaires mondiales.

Pour éviter de se faire attaquer de l'extérieur, le réseau de la centrale est isolé d'Internet. Difficile donc d'y pénétrer mais pas impossible. N'ayant pas accès au réseau, les ingénieux auteurs de l'attaque ont trouvé une alternative qui s'est avérée payante. Effectivement, Stuxnet aurait atteint sa cible par le biais d'un ordinateur infecté d'un des ingénieurs d'une autre centrale nucléaire, Natanz, lequel se serait ensuite connecté aux machines de la centrale de Bouchehr, permettant ainsi la propagation du ver.

Malgré tout ce qui a été mis en place pour sécuriser la centrale, un élément lui a été fatal : le manque de rigueur dans l'application des mesures de sécurité.

Russie vs Ukraine : Un combat pas comme les autres

En février 2014, la révolution ukrainienne explose, opposant des habitants pro-européens et des nationalistes à des partisans pro-russes.
Pratiquement deux ans après le début des affrontements, le 23 décembre 2015, une partie de la population

ukrainienne se voit privée d'électricité. Ces coupures résultent d'attaques contre trois compagnies électriques ukrainiennes. Même si le mode opérationnel est moins évolué que celui appliqué dans le cas de la centrale nucléaire de Bouchehr présenté dans l'article consacré à Stuxnet, il n'en reste pas moins intéressant. Les *hackeurs* ont utilisé un *malware* du nom de BlackEnergy, développé par le groupe russe Sandworm mais disponible sur Internet. Il s'agit d'un cheval de Troie qui, dans le cas des attaques en Ukraine, aurait été déployé à l'aide de documents Word et Excel.

Bien que l'identité des *hackeurs* n'ait pas été confirmée, on sait que les adresses IP responsables proviennent de la Fédération Russe. Il s'agit de la première attaque réussie sur des réseaux électriques.

Un point important est à noter concernant les attaques conte l'Ukraine et l'Iran : les deux attaques ont été rendues possibles grâce à la négligence des utilisateurs des infrastructures.

Le rôle des *hackeurs* dans l'armée

Alors que la présence d'unités informatiques dans certaines armées est quasi inexistante, les superpuissances ont de leur côté très vite compris l'importance de ces unités aux caractères spéciaux et les bénéfices qu'elles pouvaient en tirer.

Alors que certains *hackeurs* agissent pour leurs intérêts personnels ou ceux du groupe au sein duquel ils agissent, il existe aujourd'hui des unités militaires spécialisées dans l'attaque ainsi que la défense des systèmes de l'information. Les USA, la Chine, la Russie et Israël représentent aujourd'hui les plus grandes puissances du cyberespace. Tous ces pays adoptent cependant un positionnement différent envers les *hackeurs*. En Russie, le gouvernement n'est pas très rigoureux concernant les attaques informatiques lancées par ses citoyens à la condition que celles-ci ne soient pas dirigées contre le pays. Dans l'armée israélienne, les cyber-soldats ont tous acquis de l'expérience dans des entreprises privées avant d'intégrer leur unité. Les USA et la Chine ont également des structures militaires à la pointe de la technologies, spécialisées dans les actions dans le cyberespace, qu'intègrent des diplômés des plus grandes universités.

La formation en cybersécurité de l'armée suisse

Jusqu'alors gérée par les professionnels de la Base d'Aide au Commandement (BAC), la protection des infrastructures de l'armée suisse ne cesse de prendre de l'importance et le processus établi ne suffit plus. Depuis l'été 2018, l'armée suisse a mis en place un programme visant à former des recrues dans le domaine de la sécurité informatique.

La formation en cybernétique se déroule sur une période de 40 semaines. L'incorporation ne s'effectue pas pour l'instant lors du recrutement mais après l'intégration dans l'armée. Les candidats doivent donc être aptes au service militaire. De plus, ceux-ci doivent être disposés à suivre un avancement au grade de sergent afin de compléter l'entièreté de l'instruction.

Insigne de la Base d'Aide au Commandement (BAC).

Lors de l'Instruction Générale de Base (IGB), les intéressés seront soumis à une première phase de sélection qui permettra d'évaluer leurs compétences générales. Cette étape franchie avec succès, les recrues devront passer une deuxième période d'examens orientés sur l'informatique et leur personnalité. A cette occasion, elles auront le plaisir de fréquenter la plus belle caserne de Suisse, Jassbach (BE), durant une période de 3 jours au cours desquels s'enchaîneront interviews, questionnaires et travaux de groupes.

Le stage de formation débute lors de l'Instruction de Base Spécifique à la Fonction (IBF), au début de la 7e semaine de l'Ecole de Recrue. Une fois l'ER terminée, les futurs cyber-soldats débuteront l'Ecole de Sous-Officier pour une durée de 4 semaines pendant lesquelles ils seront formés, comme les militaires d'autres fonctions, à devenir des cadres. Après leur promotion au grade de sergent, les militaires reprendront leur formation avec 6 semaines de cours supplémentaires avant de la terminer par un stage pratique visant à mettre au défi les compétences acquises et profiter d'une immersion dans le monde pratique de la cybersécurité. Pour cette étape, les miliciens seront répartis dans 3 groupes :

Spécialiste Computer Network Operation (CNO): Tâches relevant notamment du développement d'outils logiciels ainsi que de l'analyse d'événements, de cyberattaques et de défaillances du système.

Spécialiste Cyber Fusion Center (CFC): Tâches relevant notamment de l'analyse au sein d'un Security Operation Center (SOC), par exemple de menaces cybernétiques au niveau des systèmes informatiques et de communication de l'armée, gestion des incidents, investigations techniques et informatique légale (analyse forensique).

Spécialiste Cyberdefense: Tâches relevant notamment de l'analyse et de la présentation électronique de la situation, en vue d'apporter un support (sur le plan technique et forensique), de conseiller et de former les troupes actives dans le terrain.

Les personnes ayant terminé avec succès le stage de formation pourront, après une année d'expérience dans le domaine de la cybersécurité, accéder aux examens permettant de décrocher un diplôme fédéral de Cyber Security Specialist. La reconnaissance académique de la formation fait toujours l'objet de clarifications. La Haute Ecole de Lucerne (HSLU) est la première école à reconnaître la formation et accorder 21 crédits ECTS.

L'instruction à la conduite suivie lors de l'avancement au grade de sergent peut également être sanctionnée par un certificat reconnu au niveau civil.

En plus des avantages académiques exposés ci-dessus, la formation permet de préserver le tissu économique suisse. Les coûts engendrés par les attaques informatiques atteignent des sommets en 2018. D'après une étude américaine, une attaque par *malware* réussie contre une entreprise coûte en moyenne 2,5 millions de dollars. Or, dans les sections consacrées à Stuxnet et aux attaques en Ukraine, il a été relevé que le point faible des systèmes de protection en matière d'infrastructures informatiques reste principalement l'inconscience des utilisateurs à l'égard des dangers auxquels ils sont exposés, lesquels pourraient compromettre le fonctionnement de toute l'entreprise, voire même du pays.

En formant des jeunes militaires à la protection des systèmes informatiques, l'armée contribue à la diffusion des mesures de sécurité et à l'application des bonnes pratiques en la matière jusque dans le domaine privé. En effet, les miliciens pourront à leur tour sensibiliser d'autres personnes dès leur retour à la vie civile, sur leur lieu de travail par exemple, et ainsi contribuer activement à la défense du cyberespace suisse.

D'un point de vue personnel, le stage de formation offert par l'armée m'a permis de m'épanouir dans un cadre de prestige. J'ai pu renforcer mes connaissances dans le domaine, nouer des contacts qui me seront utiles dans ma vie professionnelle et observer de l'intérieur la façon dont s'organise la défense d'infrastructures aussi importantes que celles de l'armée. J'encourage fortement

Formation cyber de l'armée suisse.

les futures recrues à tenter l'aventure. J'ai pu constater que cette formation représente une véritable plus-value sur le marché du travail.

Je pense que la réalisation d'un tel programme dans le cadre d'une armée de milice constitue un véritable défi. Pour ma part, j'ai été positivement surpris par la qualité de l'instruction dispensée et par l'organisation efficace des cours. Faisant partie de la seconde volée de cybersoldats, je n'ai aucun *feedback* négatif à formuler, pas plus d'ailleurs que mes camarades. D'autre part, les responsables de la formation sont ouverts aux remarques et ne tardent pas à prendre les mesures appropriées.

Il reste encore une longue route à parcourir mais je suis très confiant quant au futur de la formation en cybernétique. Je pense que c'est un atout considérable pour l'armée et pour l'industrie et il est très réjouissant de voir l'investissement témoigné par les hauts cadres de l'armée, notamment son chef, le commandant de corps Süssli, que mes camarades et moi avons eu la chance de rencontrer en personne.

V.

Sources utilisées

https://fr.wikipedia.org/wiki/Stuxnet
https://fr.wikipedia.org/wiki/Vuln%C3%A9rabilit%C3%A9_zero-day
https://en.wikipedia.org/wiki/Russian_military_intervention_in_Ukraine_(2014%E2%80%93present)
https://www.vtg.admin.ch/fr/actualite/themes/cyberdefence.html
https://www.vtg.admin.ch/de/armee.detail.news.html/vtg-internet/verwaltung/2019/19-04/fub---21-ects-punkte-fuer-den-cyber-lehrgang.html
https://www.varonis.com/blog/cybersecurity-statistics/