L'instruction à la cyberguerre : un exercise dans le (cyber) terrain

Autor(en): **Baudoin, Guillaume**

Objekttyp: **Article**

Zeitschrift: **Revue Militaire Suisse**

Band (Jahr): **- (2022)**

Heft 6

PDF erstellt am: **01.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-1035382

Cyber

L'instruction à la cyberguerre : Un exercice dans le (cyber) terrain

Plt Guillaume Baudoin
Président central AFTT

C'est un dimanche chargé pour la section Vaudoise de l'AFTT, l'Association Fédérale des Troupes de Transmission, engagée pour un soutien aux organisateurs de la course Montreux-Rochers de Naye. Le départ est donné avant l'aurore depuis l'abri de Chailly. Les relais ont été installés la veille et reliés par une liaison WiFi à Internet. Les radios sont distribuées aux postes de garde, aux organisateurs ; la centrale radio fait les contrôles de liaison, les postes sont prêts. C'est, jusqu'ici, un exercice tout à fait semblable à ce qui se fait dans les troupes de l'aide au commandement. Sauf que cette fois-ci, il faut aller encore plus loin.

Avoir un réseau de transmission ne suffit plus, les commandants, tout comme le comité d'organisation, ont des besoins d'informations en temps réel sur la situation du terrain. Cela est permis, cette année-là, par l'affichage en direct sur une carte nationale de la position de toutes les radios du dispositif. Affichage qui peut être projeté sur un écran ou consulté depuis un téléphone mobile. Combiné au système de chronométrage de la course, l'information disponible permet un déroulement de la course et un suivi des performances fort apprécié.

Mais tout d'un coup, la seule antenne mobile disponible au sommet, lieu d'arrivée de la course, refuse les connexions. Trop de public, pas assez de capacité. Tout en tapotant sur leur téléphones devenus muets, le public et les organisateurs se rendent compte que plus aucune information ne peut leur parvenir.


Interface de communication extérieur

C'est à ce moment qu'une des jeunes membres de la section, fort de son expérience acquise auprès du bataillon cyber 42, propose de fournir une connexion WiFi depuis le poste de contrôle. Comment s'assurer que le bon fonctionnement des infrastructures installées ne sera pas compromis par ces nouveaux utilisateurs imprévus ? Comment garantir la sécurité des communications, alors même qu'il est possible que cette perturbation du réseau téléphonique ait été volontaire ? L'agilité et l'expérience acquise lors des engagements précédents permet d'installer rapidement une antenne relais et de la configurer de telle sorte que le chronométrage et autres utilisateurs puissent y accéder sans encombre.

Cette problématique et sa résolution est maintenant de plus en plus fréquente lors d'une opération militaire. Il s'agit pour les responsables transmission de pouvoir intégrer rapidement un élément civil dans un environnement militaire (comme une antenne satellite), ou de pouvoir mettre à disposition une ressource du réseau militaire pour la sécurisation du réseau civil (comme un connexion transitant par le réseau d'ondes dirigées). L'armée peut aider ses partenaires à maintenir une capacité opérationnelle dans toutes les dimensions.

Une petite troupe d'élite

Le détail de la formation suivie par les militaires incorporés dans cette petite troupe d'élite se trouve dans les brochures mises à disposition[1] des futurs conscrits de l'armée Suisse. On y apprend que le stage de formation cyber est composé de 800 heures de formation. En plus des 350 heures d'instruction « verte » militaire, et 150 heures d'exercices et d'engagement, 300 sont à choisir parmi trois domaines principaux :

Tout d'abord, le domaine « cyberdéfense ». Il s'agit là de pouvoir présenter la situation actuelle de la menace, soutenir les troupes dans le terrain et assurer un suivi de l'effet des recommandations fournies. Dans notre exercice, cela a été fait dans les réunions préparatoires avec les organisateurs, pour les instruire à l'utilisation du réseau mis à leur disposition ainsi que des procédures en

[1] https://www.vtg.admin.ch/fr/actualite/themes/cyberdefence.html

assurant la sécurité, en situation normale ou d'urgence. Le deuxième est le domaine « milCert ». Le plus connu dans le monde civil, il s'agit ici d'assurer la surveillance des infrastructures, de réagir aux événements de sécurité et de gérer le risque des mises à jour et des vulnérabilités. Dans un exercice de l'AFTT, cela permet de s'assurer que le réseau fonctionne ou de savoir d'où vient la perturbation quand elle se produit.

Finalement, le domaine « CNO », soit les opérations sur réseau informatique. Il s'agit du domaine de développement de capacités offensives, sous forme d'armement et de méthodes d'engagement. Connaître le matériel et les méthodes utilisées pour compromettre des réseaux WiFi permet à ceux qui les sécurisent de mettre en place le niveau de protection adapté à la menace. Cela a permis, dans l'engagement, de mettre à disposition un réseau protégé pour le chronométrage et un autre, plus accessible mais bien plus limité en vitesse et en priorité pour l'équipe de bénévoles de la course.

Ces trois aspects sont interdépendants et nécessitent pour chacun des compétences qu'il faut non seulement construire, mais aussi maintenir dans la durée. Le modèle actuel de fonctionnement en petits détachements lors du service ne permet que très difficilement la mise à jour de la formation. C'est là tout l'intérêt de la pratique hors du service. De la même façon que les stands sont à disposition des sociétés de tir, les compétences cyber bénéficient de la mise en œuvre des connaissances dans des situations réelles en dehors des périodes de service. L'émulation permet aussi aux membres incorporés ou vétérans de partager leur connaissances, ainsi qu'aux membres juniors de montrer leurs expériences dans ces outils qui évoluent constamment dans leur forme, mais peu dans leur finalité d'échange d'information.

La formation initiale actuelle, de par sa longueur, ne peut se faire que dans le cadre d'une école de sous-officier. Les engagements du service pratique se font soit au sein du Commandement Cyber (ex BAC) pour les besoins de l'armée, soit auprès d'entreprises sur mandat de la confédération, ou en plus grand nombre pour des événements ponctuels comme des exercices du CCDCOE, tels que « Locked Shields ».

Cours prémilitaires de cybersécurité

Pour faire partie du bat cyber 42, la sélection est sans pitié. La liste des candidats est dès le départ conditionnée à un cursus scolaire plutôt technique et le nombre d'élus est limité à la capacité de l'ER 64. La densité de la formation rend cette sélection nécessaire, car le temps actuellement disponible dans ER/ESO est toujours principalement dédié à l'apprentissage militaire. Une solution est toutefois prévue sous la forme de cours prémilitaires.

Une partie du matériel de l'AFTT à disposition.

De façon similaire à ce qui s'était fait pour les cours de télégraphie morse, qui commencent dès l'âge de 16 ans jusqu'à l'entrée en service, ces cours s'adressent aux jeunes citoyens, quelques années avant leur école de recrue.

Ces cours prémilitaires ont comme nom de programme « SPARC[2] ». Ils sont planifiés sur une durée de quatre ans, pendant quelques heures par mois. Proposés par une coalition d'entreprises privées choisies par le commandement cyber, cette formation qui combine des cours en ligne ainsi que des événements dans différentes villes du pays se dote d'un avantage de taille : Les participants qui valident leurs acquis par un test se verront récompensés, au milieu et à la fin de cette formation, par des certificats qu'ils pourront utiliser dans leur carrière civile. Même ailleurs qu'au bataillon cyber 42, ces connaissances employées et partagées dans d'autres armes ou à la protection civile, contribueront à l'amélioration de la sécurité du pays.

Parce qu'il commence de façon très graduelle et est ponctué d'événements motivants, ce programme s'adresse autant aux passionnés du sujet ainsi qu'à ceux qui ont la curiosité de la découverte. De la même façon que rejoindre une connaissance au stand de tir peut être le début d'une passion pour ce sport, s'essayer à la cybersécurité dans un rôle actif peut être le déclencheur d'une carrière surprenante.

Un brevet fédéral à la clé

Une fois la formation militaire terminée. Il est possible de se présenter à l'examen du brevet fédéral en spécialiste de cyber sécurité ICT Formation professionnelle[3] avec le contenu acquis pendant le service d'instruction. Les frais d'examens peuvent être partiellement couverts avec les indemnités de formation de l'armée.

Le militaire qui aurait suivi le cursus complet pourra se présenter à de futurs employeurs avec les deux certificats du cours prémilitaire, une solide expérience pratique acquise lors de son ER/ESO, un réseau personnel étendu d'experts, la maîtrise d'outils modernes dans des environnements réels et un brevet fédéral !

Cette collaboration avec le privé continue aussi pour les étudiants de l'université avec le campus cyberdéfense, qui offre par exemple des bourses de recherche (CYD Fellowships) pour les niveaux « Master », doctorants et

[2] https://www.vtg.admin.ch/fr/actualite/themes/cyberdefence/cyber-milice/sparc.html

[3] https://www.ict-berufsbildung.ch/formation-continue/brevet-federal-/cyber-security-specialist-bf

post-doctorants. Ce campus[4] organise régulièrement des manifestations afin de permettre la collaboration entre le secteur privé, le monde académique et le département de la défense.

Une indispensable diversité

La cybersécurité et le bat cyber 42 sont des domaines relativement nouveaux dans l'organisation de l'armée. Cela leur permet d'avoir dès le début un avantage compétitif sur d'autres armes, qui est de pouvoir attirer des talents dans un domaine très proche des préoccupations actuelles. Le bataillon a été une troupe mixte dès le début ou chacun et chacune à pu prendre pleinement place au sein d'une équipe dynamique et bienveillante.

Cette relation entre experts s'observe dans ce domaine tout autant dans la vie privée et à l'étranger, les événements publics et conférences ne connaissent aucune barrière de genre, d'âge ou de parcours professionnel. Cela apporte un souffle bienvenu qui se prolonge dans les activités hors service, ce qui renforce d'autant plus l'esprit de camaraderie.

La cohésion de l'équipe du bat cyber 42 a pu se vérifier lors du récent exercice « Locked Shields » du CCDCOE, le centre de compétence cyber de l'OTAN, ou, bien qu'arrivée dans une salle vide, elle s'est organisée en un temps record pour se procurer des ordinateurs portables, opérer une sélection de logiciels, s'organiser en spécialités selon les épreuves à résoudre et documenter l'expérience. Arrivée dans les dix premières places, l'équipe renouvellera certainement cette expérience, si le calendrier le permet.

Un combat sans loi ni doctrine ?

Il n'existe pour le moment aucun règlement propre à l'armée suisse décrivant les opérations de cyberguerre. Le manuel de Tallinn, édité par le CCDCOE fournit des informations précieuses quant au contexte international de ces opérations. Des règles concernant la neutralité dans le cyberespace (règles 150 à 155) y sont également présentes, mais il s'agit pour la plupart des points d'une translation de la neutralité territoriale.

Cela soulève des questions épineuses, puisque le cyberespace n'est pas limité par des frontières géographiques. Comme on a pu le voir lors de la création de l'« IT Army of Ukraine » en 2022, les capacités et le nombre de ces volontaires permettent d'obtenir de façon fiable du renseignement actionnable et des effets réels sur le déroulement des opérations sur le terrain, au travers de multiples plateformes d'échange d'informations.

Les activités hors service offrent là aussi l'opportunité de se former dans le plus strict respect des règlements. Les cours et conférences ayant trait à ces sujets d'actualités sont les plus remplis et l'intérêt ne risque pas de faiblir pour les temps à venir.

Un travail d'information

L'effort de l'ensemble de l'armée et de la société civile est plus que jamais nécessaire. Il faut propager les leçons apprises dans la conduite de cette guerre moderne à toute l'armée, car une petite troupe d'élite ne peut être qu'engagée là où c'est le plus efficient. Chaque commandant se doit de connaître les éléments essentiels de la conduite de la cyberguerre, car ils ont un impact sur sa mission. Même si le cyber bataillon a reçu les moyens d'augmenter ses effectifs, son effet doit être multiplié au travers de chaque militaire qui applique les recommandations, de chaque citoyen qui sait se défendre dans le cyberespace. On voit trop souvent dans le secteur privé que seules les personnes ayant un métier directement lié à la sécurité informatique disposent d'une sensibilisation sur les risques au quotidien. Maintenant que (presque) toute la population porte sur lui de qui accèder au cyberespace, il faut savoir s'en protéger et protéger les autres des effets d'un adversaire qui ciblent ses victimes dans cette dimension.

L'AFTT et ses exercices

L'Association Fédérale des Troupes de Transmission compte parmi ses membres des militaires de tous grades provenant en majorité des « gris », l'aide au commandement de l'armée. Elle est l'association de référence lorsqu'il s'agit d'utiliser du matériel de transmission militaire lors d'une manifestation hors du service.

Grâce à la motivation de ses membres et des besoins toujours grandissants en communication, elle accède à du matériel militaire en prêt et dispose d'un complément de radios, relais et antennes civiles. Organisée en sections qui couvrent l'ensemble du territoire, des exercices internes ou combinés avec l'ASSO, l'ARTM, les pontonniers et autres permettent d'assurer la communication quel que soit le terrain, les conditions ou le nombre de participants.

La cyberdéfense est maintenant une composante de ces exercices combinés, afin de pouvoir tester un dispositif contre tout risque, naturel ou non. La mise à disposition d'une infrastructure réseau permet de former les participants d'un côté à la sécurisation de cette infrastructure, mais aussi à la façon d'attaquer le dispositif. La mise en pratique du matériel et des méthodes propres à la cyberguerre permet de mieux se rendre compte de la complexité de la tâche des défenseurs et cela permet d'apprendre à chaque fois un nouvel aspect de ce domaine si passionnant.

Le site Web aftt.ch renseigne sur les activités, la présence sur les réseaux sociaux et agenda des prochaines manifestations des sections. La plupart des exercices sont accessibles à tous et vous y apprendrez de toute façon quelque chose qui vous surprendra !

G. B.

[4] https://www.ar.admin.ch/fr/armasuisse-wissenschaft-und-technologie-w-t/cyber-defence_campus.html