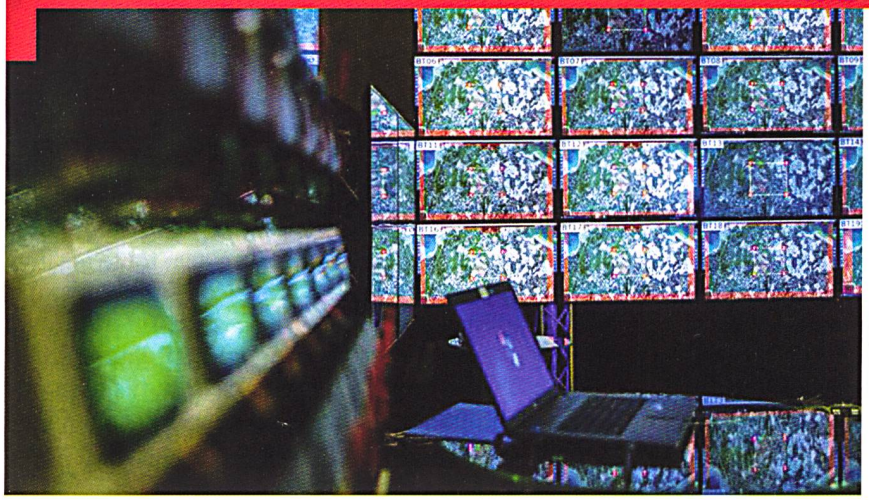
Zeitschrift: Revue Militaire Suisse
Herausgeber: Association de la Revue Militaire Suisse
Band: - (2018)
Heft: [2]: Numéro Thématique 2

Artikel: Enseignements des exercices de cyberdéfense : le rocher de Sisyphe?
Autor: Wanner, Bastien
DOI: https://doi.org/10.5169/seals-823447



Début de l'exercice phare de cyberdéfense CYBER COALITION de l'OTAN en Estonie en 2017 © NATO https://www.nato.int/cps/ic/natohq/news_149233.htm

Cyber

Enseignements des exercices de cyberdéfense – le rocher de Sisyphe?

Maj EMG Bastien Wanner
Doctorant en cyberdéfense, Université de Lausanne

Dans le cyberespace comme dans les autres domaines d'opérations, l'instruction a pour but de rendre les militaires et leurs formations aptes à remplir la mission. La participation à des exercices permet de mesurer les performances afin d'orienter l'instruction ainsi qu'adapter les processus et les moyens.

Le domaine d'opération cyber se distingue par des caractéristiques telles que le virtuel, la transversalité et l'interconnexion. Ces attributs en font un domaine particulier pour y conduire des exercices car on y entraine des capacités qui sont multidisciplinaires et qui requièrent un grand nombre de compétences et d'expertises. Les biens et technologies qui composent le cyberespace étant à double usage (civil & militaire), il faut prendre en considération dans les exercices militaires les autres parties prenantes qui jouent un rôle capital dans le cyberespace. Il s'agit donc d'inclure les autorités civiles, les opérateurs d'infrastructures critiques, l'enseignement supérieur, les juristes, les relations publiques, les diplomates et les *techies*. Enfin, étant donné que le cyberespace fait fi de toute territorialité et surtout de toute frontière, la coopération internationale est capitale.

Entrainer les capacités de cyberdéfense

Depuis quelques années, la Suisse participe à des exercices de cyberdéfense plusieurs fois par an. Ces exercices permettent d'entrainer les compétences des organisations participantes à plusieurs niveaux de décisions :

- Cyber Coalition, organisé depuis 2008 par l'Organisation du traité de l'Atlantique nord (OTAN), permet d'entrainer la collaboration en termes de cyberdéfense au sein de l'Organisation au niveau tactique et opératif. La Suisse y participe dans le cadre du partenariat pour la paix (PfP).
- Locked Shields, organisé depuis 2010 par le Cooperative Cyber Defence Centre of Excellence (CCD COE) de Tallinn en Estonie, permet d'entrainer, dans un environnement virtuel appelé *cyber range*, différentes tâches techniques des nations participantes. Depuis 2016, il comporte également un volet stratégique qui permet d'entrainer les équipes de conseil juridique, de communication et de diplomatie. La Suisse y participe activement depuis 2012.
- Cyber Pakt, organisé depuis 2015, par le Dépar-tement fédéral de la défense, de la protection de la population et des sports (DDPS), permet de tester les processus stratégiques et opératifs de cyberdéfense internes au DDPS en collaboration avec les partenaires des autres départements fédéraux.
- Defnet, organisé depuis 2014 par le Commandement de Cyberdéfense (COMCYBER) français, permet d'entraîner la gestion de crise ainsi que la planification et la conduite des mesures de cyberdéfense. L'industrie et des étudiants en informatique y participent également et depuis 2018 un volet dédié à la coopération internationale afin de développer l'interopérabilité a été lancé. La Suisse y a participé comme observateur en 2018.
- Cyber Phalanx, organisé depuis 2018 par l'Agence européenne de défense (EDA), permet d'entrainer la coopération en matière de cyberdéfense dans la planification d'une opération militaire multinationale. La Suisse y a été invitée en tant que partenaire du Multinational Capability Development Campaign (MCDC) dans le cadre du PfP.

Le principal enseignement que l'on peut tirer des participations à ces exercices est que la Suisse, en comparaison internationale, est dans le *trend*. Les performances dans les exercices de cyberdéfense sont globalement bonnes, il reste néanmoins des domaines d'améliorations.

Terminologie

Le lexique des termes utilisés dans le cyberespace a une origine informatique incontestée. Et la langue de

Briefing lors de l'exercice CYBER PHALANX 18 © Bundesheer
https://www.facebook.com/bundesheer/photos/a.578073482279115.1073741829.561631860589944/1757222847697500/?type=3&theater

la programmation informatique est principalement anglaise. Ainsi pourquoi ne pas utiliser dans le domaine cyber des termes à consonance anglaise comme c'est le cas dans le domaine de l'aviation ?

La doctrine militaire suisse a cette particularité d'être traduite en minimum trois langues. Or, certains termes ne sont pas traduisibles intégralement. Par exemple le terme *Abwehr* ne possède pas de traduction française propre. Il a été traduit en « défense combinée » soit le bouclier pour la protection et l'épée pour l'action. Dans le cas d'une mesure active de cyberdéfense, qui a trois caractéristiques :[1] but défensif, effectué en dehors du propre périmètre et avec un facteur de perturbation, on utilise le terme allemand *Cyber Abwehr* qui correspondrait à la « cyberdéfense combinée ». A l'international les termes anglophones pour décrire ces nuances sont *Defensive Cyber Operation (DCO)* et *Response Action (RA)*. Une mesure active de défense dans le cyberespace serait abrégée « DCO-RA ». Au regard de cette diversité, l'idéal serait d'unifier les terminologies autour de concepts et définitions permettant une compréhension univoque tant pour garantir l'interopérabilité que pour une communication précise.

Le défi juridique du cyberespace

L'administration fédérale a des conseillers juridiques spécialisés dans le droit international public, en particulier le droit de la guerre (*ius ad bellum*) et le droit humanitaire (*ius in bello*). Ils doivent aujourd'hui prendre en compte les particularités du cyberespace et juger chaque situation afin d'être en mesure de donner des conseils aux preneurs de décisions. Dans le cadre des exercices notamment, il leur est demandé de fournir dans un temps limité des conseils juridiques face à plusieurs événements du scénario. Par exemple, une question récurrente est de juger, à plusieurs étapes du développement d'un scénario, si une cyberattaque en cours atteint un seuil de violence telle qu'elle pourrait être considérée comme un emploi de la force qui viole l'art. 2 al. 4[2] de la Charte des Nations Unies et si elle pouvait être en outre qualifiée comme une agression armée donnant ainsi un droit naturel à la légitime défense selon l'art. 51[3] de la Charte. La problématique actuelle est donc l'applicabilité du droit international dans le cyberespace et en particulier la définition des seuils (*thresholds*) qui permettent d'invoquer différents articles et ainsi d'user de contre-mesures en toute légalité. Un outil indispensable pour répondre à ces questions est le manuel de Tallinn (*Tallinn Manual 2.0 on International Law Applicable to Cyber Operations*) issu d'un exercice académique international et rédigé par dix-neuf experts qui fournissent divers avis sur les manières d'appliquer le droit international dans le cyberespace.

Dans une autre situation d'exercice, la troupe engagée était la cible d'une cyberattaque qui semblait provenir d'une ferme de serveurs immergée en plein milieu de l'océan. Dans ce cas, quel droit s'applique et que peuvent faire les militaires ? C'est ainsi qu'un officier de marine étranger s'est écrié *« seek the flag »* soit chercher le pavillon. En effet, c'est le pavillon du caisson immergé, pour autant qu'il en ait un, qui définit la nationalité et indique donc à quelles règles de droit est soumise cette ferme de serveurs et quelles mesures peuvent être prises par la troupe ciblée par l'attaque.

Dans le cadre d'une opération militaire, le droit s'applique selon plusieurs principes sur des secteurs définis d'avance. Le droit permettant ou interdisant d'effectuer des actions est donc intimement lié au territoire et ceci en deux dimensions pour les forces terrestres et en trois dimensions pour les forces aériennes. Dans le cadre d'une opération militaire dans le cyberespace cela est plus complexe du fait de ses caractéristiques dématérialisées et la notion de territoire y est très floue.

Cyberespace, territorialité et responsabilité

La doctrine militaire actuelle découpe le territoire en plusieurs secteurs soumis à différentes règles de droit. Imaginons une vaste étendue géographique considérée comme le théâtre de guerre dans lequel sont conduites plusieurs opérations successivement ou en parallèle. Chaque opération est menée dans un secteur placé sous la responsabilité d'un commandant (*Area of Responsability – AOR*) composé d'un secteur d'opération (*Area of Operation – AO*) auquel s'ajoute un secteur d'intérêt (*Area of Interest*). Dans tout le secteur de responsabilité il est autorisé de faire ce que les règles d'engagement (*Rules of Engagement – ROE*) permettent. Cet ensemble de secteurs géographiques et les règles y relatives sont des notions clairement définies pour les militaires des forces terrestres ou aériennes. Ce qui n'est pas encore le cas dans le domaine cyber.

1 Kello, L. (2016). *Private-Sector Cyberweapons: Strategic and Other Consequences*

2 Les Membres de l'Organisation s'abstiennent, dans leurs relations internationales, de recourir à la menace ou à l'emploi de la force, soit contre l'intégrité territoriale ou l'indépendance politique de tout Etat, soit de toute autre manière incompatible avec les buts des Nations Unies.

3 Aucune disposition de la présente Charte ne porte atteinte au droit naturel de légitime défense, individuelle ou collective, dans le cas où un Membre des Nations Unies est l'objet d'une agression armée, jusqu'à ce que le Conseil de sécurité ait pris les mesures nécessaires pour maintenir la paix et la sécurité internationales. Les mesures prises par des Membres dans l'exercice de ce droit de légitime défense sont immédiatement portées à la connaissance du Conseil de sécurité et n'affectent en rien le pouvoir et le devoir qu'a le Conseil, en vertu de la présente Charte, d'agir à tout moment de la manière qu'il juge nécessaire pour maintenir ou rétablir la paix et la sécurité internationales.

La tendance actuelle est de rajouter au secteur de responsabilité un secteur d'opération cyberdéfense (*Cyber Defence Operation Area – CDOA*). Ce secteur d'opération cyberdéfense comporte tout le secteur d'opération ainsi que le secteur d'intérêt. Il peut également s'étendre à toute une liste (de systèmes et de réseaux, composés de matériels, de logiciels et de données) qui est capitale à la réussite de la mission, sans restriction quant à leur localisation géographique. Dans ces secteurs, les règles d'engagement pourraient par exemple : dans le secteur d'intérêt – permettre de faire de la recherche active de renseignement (en termes cyber cela s'appelle de l'*exploitation*), et dans le secteur de responsabilité – interdire d'effectuer des cyberopérations offensives (*Offensive Cyber Operation – OCO*) tout en autorisant des cyberopérations défensive (*Defensive Cyber Operation – DCO*) y compris des mesures actives (*Response Actions – RA*) en cas d'auto-défense.

Lors d'une opération militaire conventionnelle, si une troupe stationnée dans son pays proche de la frontière est l'objet de tirs provenant de l'autre côté de la frontière, elle a le droit de riposter afin de faire cesser l'attaque. Mais est-ce que cette même troupe aurait le droit de contre-attaquer si elle était la cible d'une cyberattaque provenant de l'autre côté du globe ?

Il y a plusieurs possibilités afin de se prémunir des effets d'une potentielle cyberattaque. La plus triviale étant de ne pas connecter un système à l'Internet et de rester hors ligne, bien que cela ne donne pas de sûreté absolue. Il est également possible de se connecter à Internet tout en augmentant sa protection dite passive (qui est cantonnée à l'intérieur du propre système informatique). Enfin, il est possible de préparer des mesures actives afin de « perturber, empêcher ou ralentir l'accès à des informations » au plus vite lorsque « des systèmes et réseaux informatiques de l'armée sont attaqués ».[4] Sachant qu'il n'est pas possible de tout protéger ni de tout attaquer en même temps, il s'agit d'effectuer, dans le secteur d'opération cyberdéfense, une analyse des terrains-clé cyber (*Cyber Key Terrain – CKT*) afin d'identifier les actifs cyber (aspects physique, logique et social des technologies de l'information et de la communication) qui sont critiques pour la réussite de la mission. Après validation par le commandant, une liste d'actifs cyber qui doivent être prioritairement protégés et défendus (*Cyber Defense Prioritized Assets List – CDPAL*) sera dressée sur la base des propres terrains-clé cyber. En contrepartie, une liste des actifs cyber qui pourraient être de potentielles cibles devrait également être dressée sur la base des terrains-clé cyber adverses. Comme dans les autres dimensions terre, air et mer, le cyber fait également partie du processus du ciblage (*targeting*).

Perspectives de cyberdéfense

En conclusion, la Suisse s'est dotée des bases légales, en particulier l'article 37 de la Loi fédérale sur le renseignement (LRens) et l'article 100 al. 1 let. c de la Loi fédérale sur l'armée et l'administration militaire (LAAM), qui régissent les activités de cyberdéfense en temps de paix. Il reste maintenant à mettre en œuvre ces textes en réelles capacités opérationnelles. Les ressources, en particulier financières et humaines, nécessaires à cette concrétisation doivent être libérées afin de ne pas prendre de retard face à ce cyberespace en très rapide changement. Il faut également former continuellement les personnes afin d'avoir toujours des connaissances à jour et de ne pas être dépassé par les dernières évolutions.

Dans le cadre de cette mise en œuvre, un effort principal devrait être mis sur l'unification de la terminologie et la création d'un lexique reconnu et partagé afin d'avoir un langage cyber commun. Cela permettrait de réduire les ambiguïtés entre les civils et les militaires, les secteurs public et privé, les générations et surtout entre les différentes zones linguistiques du pays. De plus, cela permettrait une meilleure communication avec nos partenaires internationaux.

Concernant la défense, il s'agit maintenant d'adapter au cyber les propres processus à chaque échelon et d'intégrer les aspects de cyberdéfense dans la planification et la conduite des opérations. Les exercices sont de bons instruments pour tester les capacités et identifier les lacunes qu'il s'agit de combler et orienter en conséquence l'instruction. Les processus doivent être appliqués en collaboration avec toutes les parties prenantes et en intégrant les partenaires non militaires car la portée d'événements cyber sera certainement plus étendue que le seul périmètre de la défense. Ces processus concrets doivent être distribués, reconnus et utilisés au sein de l'Armée, du DDPS et de l'administration fédérale afin de pouvoir être entraînés et adaptés régulièrement. En outre, l'Armée et les Services de renseignement doivent augmenter leurs capacités de renseignement et d'actions dans le cyberespace car ils en ont maintenant reçu le mandat et les bases légales pour le faire.

Finalement, tout en respectant le droit de la neutralité et la politique de neutralité, la Suisse doit absolument continuer de participer aux exercices de cyberdéfense afin de développer un savoir-faire et entretenir de bonnes relations avec ses partenaires. Car dans le cyberespace plus qu'ailleurs, l'absence de frontière et l'hyperconnectivité demandent de connaitre ses partenaires, de coopérer et de s'entrainer ensemble, tant au niveau national qu'international et ce de manière itérative en raison de la nature très évolutive du cyberespace. Il est également important d'intégrer des participants de plusieurs horizons et de plusieurs cultures, apportant toutes les expertises nécessaires à la résolution du problème et au rétablissement au plus vite d'une situation normale. La participation aux exercices cyber permet non seulement de se familiariser avec le sujet mais également de connaître les acteurs impliqués afin de créer de la confiance, de l'interopérabilité et d'augmenter la crédibilité de la Suisse à faire face à toutes situations dans le cyberespace.

B.W.

4 Loi fédérale sur l'armée et l'administration militaire (LAAM), art. 100 al. 1 let. c