Cyberdéfense : protection des infrastructures critiques dans le cyperespace

Autor(en): **Wanner, Bastien**

Objekttyp: **Article**

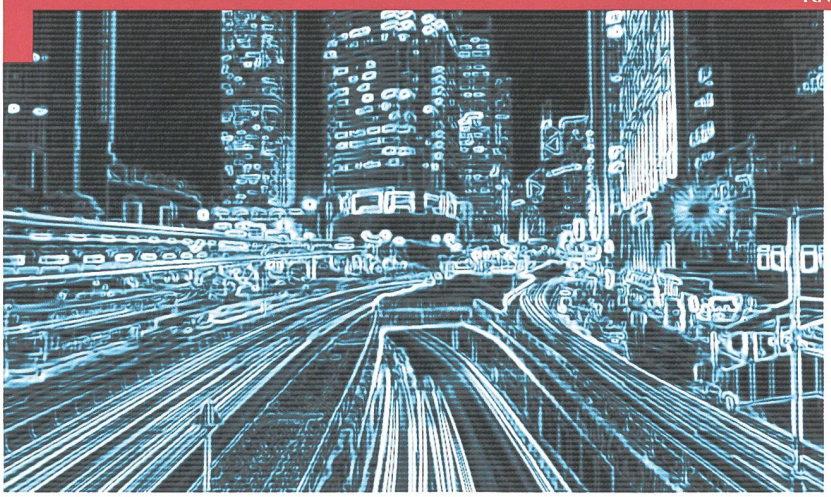
Zeitschrift: **Revue Militaire Suisse**

Band (Jahr): **- (2019)**

Heft 1

PDF erstellt am: **14.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-867928



Cyber

Cyberdéfense – protection des infrastructures critiques dans le cyberespace

Maj EMG Bastien Wanner
Doctorant en cyberdéfense, Université de Lausanne

Dans la doctrine militaire de nombreux pays, les missions dans le cyberespace sont séparées en trois catégories distinctes: la cyberprotection, la cyberdéfense et la cyberattaque. Concrètement, il s'agit tout d'abord de protéger les propres systèmes d'information afin d'avoir la liberté de manœuvre nécessaire pour pouvoir conduire des actions dans le cyberespace. Ces mesures de protection ne sont pas spécifiques à une menace particulière et se concentrent sur les technologies de l'information. Leur but est de garantir l'intégrité et la résilience des systèmes et réseaux informatiques tant au niveau du matériel, des logiciels, des données que des utilisateurs. La deuxième catégorie est la cyberdéfense où il s'agit, par des mesures passives et actives, de prendre l'avantage sur l'adversaire. Pour ce faire, il faut identifier les terrains-clés cyber qu'il faut en priorité défendre. Les mesures de cyberdéfense sont axées sur la mission et répondent à une menace spécifique. Les mesures actives de cyberdéfense ont trois caractéristiques:[1] but défensif, effectué en dehors du propre périmètre et avec un facteur de perturbation Elles visent à produire, réactivement ou proactivement, un effet sur un adversaire. Enfin, la troisième catégorie est la cyberattaque, qui a pour but de projeter du pouvoir dans et au travers du cyberespace.

Au cours des cinq dernières années, le nombre de nations qui ont acquis des capacités actives dans le cyberespace a plus que doublé. Selon le rapport de l'UNIDIR[2] « The Cyber Index : International Security Trend and Realities » de 2013, 41 nations avaient les moyens d'effectuer des mesures actives dans le cyberespace et 17 développaient ces capacités. Aujourd'hui se sont plus de 60 nations qui sont capables de mettre en œuvre des mesures actives de cyberdéfense et près de 40 gouvernements investissent dans de telles capacités. Pour pouvoir effectuer ces actions, l'Etat doit se doter de bases légales et on remarque que le cadre légal change dans cette direction pour autoriser ces mesures actives.

Les mesures actives de cyberdéfense en Suisse – *statu quo*?

L'Etat garantit la sécurité des citoyens et le respect des lois dans les mondes réel et virtuel. Pour cette sécurité, l'Etat dispose de plusieurs moyens permettant la surveillance, la protection et la défense de sa population. Au cours des 18 derniers mois, la Suisse a adopté la loi fédérale sur le renseignement (LRens) et la loi fédérale sur l'armée et l'administration militaire (LAAM). Ces lois permettent maintenant à la Suisse de se doter de mesures actives de cyberdéfense.

En outre, la Suisse a revu sa stratégie nationale de protection contre les cyberrisques (SNPC)[3] en avril 2018. La protection des infrastructures critiques y a la priorité maximale et est le point de mire de toutes les mesures de la SNPC. Un principe central de cette stratégie est que chacun est responsable de la gestion de ses propres risques, ainsi la responsabilité de la maitrise des cyberrisques est partagée entre tous les acteurs. L'Etat joue un rôle subsidiaire et n'intervient que lorsque « les acteurs privés ne sont pas capables ou désireux de résoudre le problème eux-mêmes ». La mesure[4] « capacité à mener des mesures actives dans le cyberespace » stipule que le Service de renseignement de la Confédération (SRC) et l'armée doivent disposer des compétences (en nombre et en qualité) adéquates ainsi

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

2 Institut des Nations unies pour la recherche sur le désarmement

3 https://www.isb.admin.ch/isb/fr/home/ikt-vorgaben/strategien-teilstrategien/sn002-nationale_strategie_schutz_schweiz_cyber-risiken_ncs.html

4 Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018–2022, mesure 23, p. 24

que des capacités pour perturber, empêcher ou ralentir des attaques visant les infrastructures critiques et ce conformément au cadre légal.

Alors que la LAAM ne s'applique qu'à l'armée et aux cyberattaques ciblant les systèmes et les réseaux informatiques de l'armée, la LRens s'applique au SRC et aux cyberattaques provenant de l'étranger et ciblant les infrastructures critiques de la Suisse.

L'article 37 de la LRens[5] intitulé « Infiltration dans des systèmes et réseaux informatiques » stipule que le SRC peut infiltrer des systèmes et réseaux informatiques qui se trouvent à l'étranger lorsqu'ils sont utilités pour attaquer des infrastructures critiques en Suisse. Ceci afin de perturber, empêcher ou ralentir l'accès à l'information. De plus, le SRC peut également infiltrer des systèmes et réseaux informatiques étrangers afin de rechercher des informations qu'ils contiennent ou qui ont été transmises à partir de ces systèmes et réseaux. Cela met en lumière les deux raisons principales d'effectuer des mesures actives dans le cyberespace : recherche de renseignements et cessation d'une attaque en cours.

L'article 25 de l'ordonnance sur le service de renseignement (ORens)[6] stipule que le SRC peut collecter des informations par l'exploration du réseau câblé. Il peut le faire, dans le domaine de l'exploration de la cybermenace et de la protection des infrastructures critiques, pour « élucider la nature de l'engagement, l'origine et les caractéristiques techniques des moyens de cyberattaques et pour mettre en œuvre des mesures efficaces de défense ». La recherche de renseignements est donc utilisée dans le but de caractériser le type d'attaque, le vecteur, le mode opératoire, identifier d'un point de vue technique l'origine de l'attaque et son auteur. L'intention de l'attaquant, son but et surtout sa nationalité ne sont pas considérés dans la caractérisation mais uniquement lors de l'attribution qui est un processus politique du ressort du gouvernement d'un Etat. La caractérisation d'une cyberattaque permet de mieux pouvoir s'en protéger, voire de la faire cesser plus rapidement.

La loi précise le cadre et les conditions d'utilisations des mesures actives de cyberdéfense : il faut que l'attaque provienne de l'étranger et cible des infrastructures critiques en Suisse. L'inventaire des infrastructures critiques est effectué par l'Office fédéral de la protection de la population (OFPP). Il englobe neuf secteurs, subdivisés en 27 sous-secteurs (branches).[7] Il est intéressant de noter qu'actuellement le SRC confie l'exploration du réseau câblé au centre des opérations électroniques (COE) de la base d'aide au commandement (BAC) qui en est le service exécutant[8]. Mais il n'est pas fait mention de quel pourrait être le service exécutant des mesures actives de cyberdéfense. Au vu de l'organisation

actuelle de la cyberdéfense, il est fort probable que cela soit également la BAC qui en aurait la responsabilité.

Les mesures actives de cyberdéfense en Suisse – *quo vadis ?*

Les mesures actives de protection des infrastructures critiques entreraient donc dans la deuxième caté-gorie des missions dans le cyberespace qu'est la cyberdéfense. Dans la doctrine militaire suis-se, les mesures actives de cyberdéfense sont englobées dans le terme « cyberdéfense combinée » (*Cyber-Abwehr*)[9] et se définit comme suit : « Partie de la cyberguerre visant à protéger nos réseaux informatiques et systèmes d'information, à identifier et à parer une menace concrète ainsi qu'à mettre un terme à une attaque adverse. Elle comprend entre autres : l'exploration, les actions défensives sur réseaux informatiques, les actions d'exploitation et offensives sur réseaux informatiques en vue d'une contre-attaque ». Ces actions (défensives, d'exploitation et offensives) sur les réseaux informatiques sont plus connues sous leurs appellations informatiques anglophones – *computer network operations (CNO)* et ses trois composantes tactiques : *computer network defence (CND), computer network exploitation (CNE)* et *computer network attack (CNA).* Elles constituent le cœur des actions dans le cyberespace et pourraient être mise en œuvre, dans un cadre subsidiaire, au profit des infrastructures critiques qui le demanderaient. La cyberdéfense combinée repose donc sur une cyberprotection qui constitue la base de chaque action dans le cyberespace. En fonction de la menace et de la mission, diverses mesures de cyberdéfense passives (telles que du renforcement de terrains-clés cyber) voire actives (telles que des contre-attaques en dehors du propre périmètre) peuvent être prises afin de produire des effets dans le cyberespace. Le but étant d'atteindre l'état final recherché qu'est la cybersécurité (de ses infrastructures) en perturbant celle de l'adversaire.

B.W.

5 https://www.admin.ch/ch/f/rs/c121.html

6 https://www.admin.ch/ch/f/rs/c121_1.html

7 https://www.babs.admin.ch/fr/aufgabenbabs/ski/kritisch.html

8 art. 26 ss ORens

9 Recueil des termes pertinents pour la doctrine au niveau de l'armée 18