Politique de sécurité: **analyses du CSS**

CSS
ETH Zurich

N° 71 • avril 2010

CYBERGUERRE: CONCEPT, ÉTAT D'AVANCEMENT ET LIMITES

Les conflits politiques, économiques et militaires se déroulent toujours plus dans le cyberespace. Conceptuellement, le terme de cyberguerre n'englobe cependant qu'une partie minime des cyberconflits. Les capacités de cyberguerre sont de plus en plus importantes au niveau opérationnel. Des guerres informatiques stratégiques ne se déroulant plus que dans l'espace virtuel restent cependant improbables. Pour des Etats comme la Suisse, il est nécessaire d'agir surtout dans le domaine de la cyberdéfense.

Istock.com

L'importance de l'espace informationnel en tant que lieu où se déroulent les conflits a augmenté ces dernières années. Une partie de chaque conflit politique, économique et militaire a aujourd'hui lieu sur Internet. Le terme de cyberguerre est devenu un slogan très utilisé dans ce contexte. Il désigne souvent n'importe quelle dispute dans le cyberespace assortie d'une dimension internationale. Mais une acception aussi large du terme n'est guère judicieuse. Il est plutôt nécessaire de catégoriser conceptuellement les différentes formes de conflit dans le cyberespace. C'est uniquement sur cette base que l'on pourra évaluer le danger concret et sa portée, attribuer des responsabilités, mettre en œuvre des contre-mesures préventives et réactives et entamer d'éventuelles enquêtes pénales.

La cyberguerre ne couvre par conséquent qu'une partie minime de toutes les attaques cybernétiques. Il faut, sous l'angle militaire, l'entendre comme faisant partie de la guerre de l'information. Pour pouvoir déterminer la teneur et l'importance du concept de «cyberguerre», il faut aussi, après en avoir délimité le contenu, opérer une distinction entre sa dimension opérationnelle et sa dimension stratégique. Il faut en outre faire la différence entre mesures de cyberguerre offensives et défensives, le rôle de l'armée étant restreint dans la cyberdéfense.

La cyberguerre en tant que concept partiel

Il est de plus en plus difficile, dans la pratique, de catégoriser principalement les cyberattaques en fonction de leurs auteurs. Comme les assaillants savent de mieux en mieux brouiller les pistes, un classement rapide et clair est souvent impossible. L'intention derrière une attaque revêt cependant, si elle peut être déterminée, une importance conceptuelle, toutes les cyberattaques étant loin d'être motivées par des raisons militaires et ne faisant pas partie d'une cyberguerre. Une autre différence importante est l'étendue potentielle des dégâts d'un incident. On utilise pour illustrer cette dernière l'image d'une cyber-échelle: plus on se rapproche du haut de l'échelle, plus le dégât possible est important.

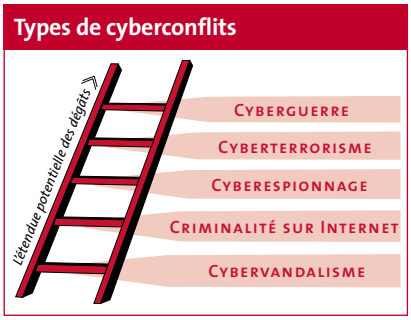
Le cyberhacktivisme ou cybervandalisme se situe sur le premier échelon. Il s'agit d'une modification ou destruction virtuelle de contenus, comme p.ex. le piratage de sites Web ou la fermeture d'un serveur par un trop-plein de données. Le cybervandalisme est la forme la plus courante de cyberconflit et suscite une grande attention de la part du public. Les effets de ces actes sont cependant limités dans le temps et relativement inoffensifs, d'autant plus qu'ils n'ont pas une motivation politique ou économique.

La criminalité sur Internet et le cyberespionnage se situent sur les échelons deux et trois. Ils se produisent tous deux en permanence et indépendamment de conflits. La principale victime est l'économie: même s'il est extrêmement difficile de recueillir des données, les coûts globaux de ces phénomènes sont estimés à environ un billion de dollars par an. Les réseaux gouvernementaux renfermant des informations classifiées sont également touchés mais constituent une cible comparativement plus rare.

On entend par cyberterrorisme, sur l'échelon quatre, les attaques illicites perpétrées

par des acteurs non étatiques contre des ordinateurs, des réseaux et les informations qui y sont stockées dans le but d'intimider ou de forcer un gouvernement (et/ou la population) à des actes spécifiques. Une cyberattaque n'est donc qualifiée de cyberterrorisme que si elle débouche sur une violence physique contre des personnes ou des choses ou cause au minimum des dégâts tels qu'elle engendre une terreur considérable. L'étendue potentielle des dégâts doit être classifiée comme très grande, aucun cas de cyberterrorisme n'ayant été enregistré jusqu'à présent dans la pratique.

La cyberguerre constitue l'échelon supérieur de l'échelle. On entend par cyberguerre l'affrontement guerrier dans l'espace virtuel principalement avec des moyens du domaine de l'informatique. La cyberguerre recouvre une partie de la guerre de l'information. A l'intérieur de ce concept plus large qui a pour but, au niveau de l'information et des systèmes d'information, d'influencer la volonté et la capacité de décision de la direction politique et des forces armées d'un adversaire et/ou l'attitude de la population civile dans les territoires d'intervention (cf. analyse CSS n° 34), la cyberguerre englobe les activités dans le cyberespace. Conceptuellement, la cyberguerre reflète donc la forme de guerre de plus en plus technicisée à l'âge de l'information qui se base sur l'informatisation, l'électronisation et la mise en réseau de presque tous les domaines et intérêts militaires.



Il faut, dans le cadre de la cyberguerre, faire, au niveau doctrinal, la distinction entre trois formes d'*opérations dans les réseaux informatiques (Computer Network Operations* (CNO)): l'arrêt total ou la destruction décidé(e) des capacités de réseaux adversaires est qualifié(e) d'*attaque de réseaux informatiques* (*Computer Network Attack* (CNA)). Subsidiairement, l'*exploitation de réseaux informatiques* (*Computer Network Exploitation* (CNE)) vise à retrouver à l'aide d'ordinateurs, au sens des services de renseignements, des informations sur des ordinateurs ennemis. Finalement, la *défense de réseaux informatiques* (*Computer Network Defense* (CND)) englobe les mesures de protection des ordinateurs et systèmes informatiques propres contre les CNA et la CNE adversaires.

Réalité opérationnelle

Le potentiel de dégâts d'une cyberguerre pour la sécurité et le bien-être d'un Etat est énorme. Il faut cependant surtout entendre aujourd'hui les capacités de CNA comme *un* moyen opérationnel dans le cadre d'interventions militaires. L'importance de ce moyen augmentera indubitablement à l'échelle mondiale dans les prochaines années. Des scénarios d'une cyberguerre stratégique, c.-à-d. d'un conflit ne se déroulant plus que dans l'espace informationnel, semblent par contre peu réalistes à l'heure actuelle.

Il manque des connaissances assurées en ce qui concerne le niveau de développement actuel des capacités offensives de cyberguerre. C'est pourquoi, à la différence des échelons inférieurs de la cyber-échelle, le débat sur la cyberguerre est très spéculatif. Il est clair que la CNE est d'ores et déjà une réalité que l'on ne peut plus ignorer. L'incertitude concerne surtout l'étendue des capacités de CNA déjà disponibles. Plusieurs estimations semblent ici exagérées ou peu fondées.

C'est ainsi que l'on avance sans cesse des exemples d'utilisation de CNA. Les Etats-Unis auraient par exemple fermé, pendant la guerre d'Irak, les réseaux locaux de téléphonie mobile et informatiques pour empêcher les insurgés de planifier des attentats à la bombe. Dans le contexte de l'attaque aérienne israélienne contre une installation atomique syrienne en septembre 2007, on a également spéculé que les avions israéliens avaient pu infiltrer l'espace aérien syrien grâce à une cyberattaque contre le système de défense antiaérienne syrien. Mais de tels rapports donnent toujours lieu à interprétation, d'autant plus qu'ils utilisent souvent le mot «cyberguerre» comme synonyme de guerre informatique et que personne n'est sûr que des capacités de CNA aient vraiment été mises en œuvre.

Les indicateurs utilisés par les services secrets pour déterminer les capacités de CNA, tels que doctrine, formation, simulation ou coopération industrielle, ne sont guère parlants. Il est cependant incontestable que les capacités offensives de cyberguerre constituent un thème important aux Etats-Unis. Une équipe consacrée à la guerre de l'information au Pentagone se penche depuis 1999 sur la mise sur pied de tels moyens. L'ancien président américain George W. Bush a ordonné en 2002 l'élaboration d'une stratégie fixant les directives et critères de conduite d'une cyberguerre. Mais on ne sait pas très bien à quoi ces efforts ont abouti. On attribue aussi des capacités offensives à la France, à Israël, à la Russie et à la Chine. La Bundeswehr allemande serait, si l'on en croit certains rapports médiatiques, en train de mettre sur pied un service d'«opérations d'information et de réseaux informatiques» qui disposerait de moyens de CNA. On discute dans plusieurs autres Etats du développement de capacités correspondantes. Mais les débats n'en sont souvent qu'à leurs balbutiements.

Une cyberguerre stratégique?

La cyberguerre est souvent représentée comme un type de guerre fondamentalement différent qui serait moins onéreux, plus «propre» (sans effusion de sang) et moins risqué pour un agresseur que d'autres formes de conflit armé. L'attente selon laquelle nous vivrons à l'avenir non seulement une course à l'armement dans le cyberespace mais aussi des cyberguerres stratégiques est liée à ces évaluations positives. Quelques questions s'imposent cependant à ce sujet.

Il y a toujours des doutes considérables quant à la faisabilité d'une cyberguerre stratégique. Si l'on en croit les experts, il est par exemple toujours impossible aujourd'hui de réaliser des attaques cybernétiques de manière ciblée, ce qui remet à son tour en question la logique d'une cyberguerre stratégique. Des effets de causalité inverse incontrôlables dans l'espace virtuel où tout est mis en réseau recèlent des risques considérables même pour un Etat agresseur. Ce facteur est d'autant plus important que les Etats qui seront les premiers à posséder ou à pouvoir développer le savoir-faire technologique pour la cyberguerre stratégique sont particulièrement dépendants de leurs propres structures informationnelles et donc très vulnérables dans la guerre informatique. En raison d'effets secondaires incontrôlables, une guerre cybernétique serait aussi liée à un minage à long terme de la confiance dans

le cyberespace, ce qui pourrait avoir des conséquences négatives pour l'économie mondiale et donc également pour tous les acteurs. A cela vient s'ajouter le fait que le développement de ces capacités de cyberguerre est certainement beaucoup plus coûteux qu'on ne le prétend souvent.

La dimension offensive de la cyberguerre reste aussi controversée du point de vue légal, ce qui touche la cyberguerre tant dans sa dimension stratégique qu'opérationnelle. Cela s'explique par le fait qu'une séparation entre cibles civiles et militaires n'est plus possible et/ou que des infrastructures civiles sont délibérément attaquées dans la cyberguerre. La question de savoir si l'utilisation d'ordinateurs peut être qualifiée d'arme et de recours à la force militaire n'a pas été éclaircie du point de vue du droit international public. Il faut aussi déterminer dans quelle mesure la simple infiltration par un organe étatique de réseaux informatiques dans le cadre de la CNE pour se procurer des informations enfreint le droit international public.

Défense: rôle limité de l'armée

Vu les imprévisibilités considérables caractérisant les capacités offensives de cyberguerre, des appels à un contrôle du cyberarmement se sont déjà fait entendre. Il est cependant difficile d'imaginer actuellement comment un mécanisme correspondant pourrait être mis en œuvre efficacement, par exemple dans le domaine de la vérification. Un processus reposant sur des déclarations politiques de renonciation constituerait une alternative concevable, mais beaucoup d'Etats pourraient se garder de limiter leur marge de manœuvre à ce sujet.

D'une manière ou d'une autre, il faut admettre que la majorité des forces armées se penchera, dans les prochaines années, de manière prioritaire sur la cyberdéfense au détriment des moyens offensifs. La *défense de réseaux informatiques* revêt déjà aujourd'hui une grande importance. Des attaques contre l'informatique, la manipulation d'informations ou un espionnage réussi peuvent affaiblir massivement la performance de l'armée d'un pays. Les réseaux militaires doivent par conséquent être protégés contre toutes les formes de cyberconflit.

Le concept de CND est cependant limité aux réseaux militaires. Les contre-mesures sur tous les échelons de la cyber-échelle, qu'elles soient préventives ou réactives, sont dominées par des mesures civiles. Il est donc aussi judicieux de souligner l'importance des acteurs civils dans ce domaine parce que, par rapport au nombre d'incidents réels et à l'étendue estimée des dégâts, la criminalité sur Internet (liée au cyberespionnage) représente de loin le problème le plus grave auquel le monde se voit confronté aujourd'hui.

Les contre-mesures pour les échelons un à trois sont d'une part la sécurité de l'information (*information assurance*) dont est responsable chaque citoyen et chaque société, et d'autre part des mesures de droit privé et pénal. L'Etat doit protéger ses propres réseaux et veiller, en tant que législateur, à combler d'éventuelles lacunes dans le droit d'Internet. Dans ce contexte, la coopération internationale est primordiale. Au plus tard à partir de l'échelon 4, ces aspects sont complétés par la protection des infrastructures critiques (cf. analyse CSS n° 16). Ces concepts de protection exigent principalement un partenariat civil étroit entre Etat et économie ainsi qu'une coopération interétatique intensive. L'armée peut cependant fournir d'importantes contributions, par exemple pour détecter la désinformation ennemie ou pour protéger les structures de commandement nationales.

La cyberguerre en Suisse

En Suisse, la mise sur pied de capacités en vue de réaliser des opérations d'information stagne ces dernières années (cf. analyse CSS n° 34), ce qui s'explique entre autres par des ambiguïtés juridiques, des difficultés financières et un manque de personnel ainsi que des réserves politiques vis-à-vis par exemple d'opérations psychologiques. En ce qui concerne le domaine partiel de la cyberguerre, de premières démarches ont été entreprises au niveau de l'armée. L'armée suisse n'est cependant pas en mesure aujourd'hui, selon ses propres dires, de détecter un piratage professionnel contre sa propre infrastructure et de déclencher ensuite une réaction adéquate dans les temps. L'attaque massive contre le DFAE en octobre 2009 a illustré combien les services ministériels étaient vulnérables aux cyberattaques.

On est actuellement en train de mettre sur pied au sein du Centre des opérations électroniques (COE) de la Base d'aide au commandement de l'armée deux domaines consacrés à la cyberguerre. Il s'agit d'une part d'un *Computer Emergency Response Team* militaire (milCERT) dont la tâche est de surveiller les systèmes et réseaux de l'armée et de déclencher l'alarme le cas échéant. La coordination avec le *Government Computer Emergency Response Team* (GovCERT) existant, qui est un élément important de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI), fait surtout partie des défis centraux de cette équipe en sus de l'élargissement du personnel.

D'autre part, une cellule *Computer Network Operations* est aussi mise sur pied au sein du COE. Un avis de droit du DFJP et de la Direction du droit international public du DFAE a révélé à ce sujet en mars 2009 que les bases juridiques actuelles en Suisse suffisaient pour la cyberdéfense (CND), mais que les CNA offensives et la CNE à des fins de renseignements ne seraient possibles dans l'état actuel que dans le service actif (c.-à-d. surtout en cas de défense).

Le DPPS a l'intention, selon ses propres dires (cf. avis de droit), de mettre sur pied tant des capacités de CND que de CNE et de CNA. Les activités suisses de cyberguerre devraient cependant se situer à l'heure actuelle de manière prépondérante dans les mesures défensives. Des ressources supplémentaires en personnel s'imposent ici, ce qui est d'ailleurs aussi valable pour MELANI qui est, comme le COE, insuffisamment financé par rapport aux autres pays. Une étroite coopération civilo-militaire dans laquelle il faut aussi inclure le Service de coordination de la lutte contre la criminalité sur Internet (SCOCI) est en outre importante dans la cyberdéfense. Une cyberdéfense efficace exige finalement aussi une collaboration

Cyberguerre en Suisse: liens utiles

- Avis de droit (10.3.09)
- Interpellation Schlüer: Sécurité Internet (17.3.09)
- Interpellation Segmüller: Opérations d'information (9.3.09)
- Interpellation Graber: Guerre électronique (18.12.08)
- Le DFAE victime d'une attaque informatique
- Base d'aide au commandement de l'armée
- Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI)
- Service de coordination de la lutte contre la criminalité sur Internet
- Cooperative Cyber Defence Centre of Excellence

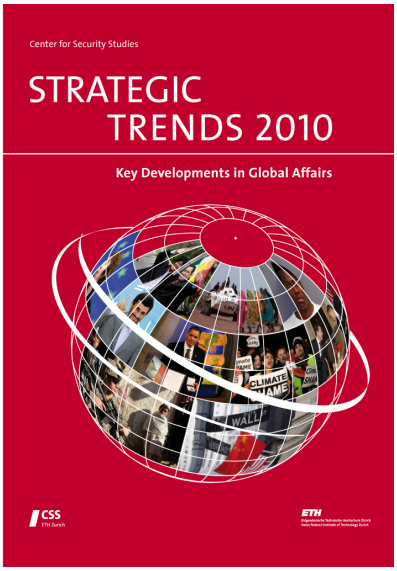
internationale, le *Cooperative Cyber Defence Centre of Excellence* créé en 2008 en Estonie pouvant évoluer pour devenir un important cadre multilatéral.

La mise sur pied de capacités de CNE pour les organes d'acquisition de renseignements de la Confédération pour des activités en dehors du service actif est tout à fait digne d'être examinée et répondrait à la tendance internationale. La création des bases juridiques correspondantes pourrait cependant faire l'objet de controverses politiques. Il faudrait s'assurer par exemple que la CNE ne puisse pas être utilisée à mauvais escient pour de l'espionnage économique.

Dans le cas des CNA, la question du droit ne se pose pas car la Suisse n'utiliserait cette capacité que dans le service actif en réaction à une attaque contre ses propres systèmes. Le problème juridique central concerne bien plus ici la faisabilité et la nécessité d'une telle capacité. Comme il s'agit d'une question d'importance stratégique, ce sont les niveaux correspondants tant dans l'armée que dans la politique qui devraient s'en occuper.

- Editeur responsable: Daniel Möckli analysen@sipo.gess.ethz.ch
- Commande d'analyses et abonnement gratuit: www.ssn.ethz.ch

Nouvelle publication CSS



www.sta.ethz.ch

Parus précédemment

N° 72: Réforme du Conseil de sécurité: un noeud gordien?
N° 71: Cyberguerre: concept, état d'avancement et limites
N° 70: Le Yémen: lutte difficile contre le terrorisme
N° 69: La politique énergétique de l'UE face à de grands défis
N° 68: Finlande: gestion de crises et défense territoriale
N° 67: Engagements de l'armée à l'étranger: bilan et options
N° 66: L'Organisation de coopération de Shanghai: signification pour l'occident
N° 65: Die Krise des NVV: Vor der Überprüfungskonferenz 2010
N° 64: Politique de défense britannique: pression réformiste
N° 63: Promotion civile de la paix: potentiel et limites
N° 62: Communication du risque: utilité pour la politique de sécurité
N° 61: Politique extérieure de la Suisse 2009: Etat des lieux
N° 60: La résilience: un concept pour la gestion des catastrophes et crises
N° 59: Iran: Crise interne et marge de manoeuvre des etats occidentaux
N° 58: Prix du pétrole et géopolitique: les gagnants et les perdants
N° 57: Le nucléaire gagne du terrain: le risque de prolifération
N° 56: Le voisinage oriental de l'Europe entre influence russe et ancrage à l'Ouest
N° 55: Opération Atalante: piraterie et politique de sécurité de la Suisse
N° 54: Alliance de contradictions: l'OTAN après le sommet anniversaire
N° 53: Désarmement atomique: l'Amérique et la Russie reprennent les négociations
N° 52: Prospective stratégique: anticipation et capacité d'agir
N° 51: Afghanistan: nouvelle stratégie et nombreuses questions
N° 50: Rapport sur la politique de sécurité: points cruciaux et débats
N° 49: Le conflit au Proche-Orient après la guerre de Gaza
N° 48: Lutte antiterrorisme: bilan intermédiaire
N° 47: Pakistan: partenaire de sécurité et foyer de crise
N° 46: Livre blanc: nouvelle stratégie de sécurité nationale de la France
N° 45: L'importance croissante des acteurs civils dans les conflits violents
N° 44: Politique étrangère suisse: nouvelles orientations
N° 43: Le conflit nucléaire iranien: état d'avancement et options
N° 42: Une approche globale dans la gestion internationale des crises
N° 41: Politique extérieure américaine sous Bush: bilan et perspectives
N° 40: Sécurité et développement: entre convergence et concurrence
N° 39: Crise du Caucase: épreuve pour la Russie et l'Occident
N° 38: Importance stratégique croissante de l'Afrique
N° 37: Politique européenne de la Suisse: le bilatéralisme – solution permanente?
N° 36: La sécurité énergétique en Europe: état et perspectives
N° 35: Politique suisse au Proche-Orient: ambitieuse et controversée
N° 34: Opérations d'information: tendances et controverses
N° 33: Lézardes sous la fondation: l'OTAN après le sommet de Bucarest
N° 32: Open Source Intelligence: nouveau paradigme du renseignement?
N° 31: Secteur européen de l'armement: l'Etat sera obligé de s'adapter
N° 30: Gestion des risques et politique de sécurité
N° 29: L'indépendance contestée du Kosovo
N° 28: La PESD après le Traité de Lisbonne
N° 27: Tendances stratégiques actuelles
N° 26: Changement climatique et politique de sécurité
N° 25: Après Annapolis: processus de paix fragile au Proche-Orient
N° 24: Conflits liés à l'environnement: importance et solutions
N° 23: Gestion stratégique des crises: tendances et concepts
N° 22: Comparaison des forces de réaction rapide de l'OTAN et de l'UE
N° 21: La Turquie à l'orée d'une réorientation stratégique?
N° 20: Neutralité et capacité d'action extérieure de la Suisse
N° 19: Corée du Nord: vers le désarmement nucléaire?
N° 18: La montée des islamistes au Proche-Orient: démarcation et dialogue
N° 17: Après les élections: la politique étrangère de la France en transition
N° 16: Infrastructures critiques: vulnérabilités et protection
N° 15: Que veut la Russie? Ambitions et limites d'une grande puissance
N° 14: Politique de défense allemande: continuité et évolution