Zeitschrift: Revue Militaire Suisse
Herausgeber: Association de la Revue Militaire Suisse
Band: - (2010)
Heft: [1]: Contre-Insurrection (COIN)

Artikel: Guérilla cybernétique : espace nouveau, tactiques anciennes
Autor: Varesio, Pascal
DOI: https://doi.org/10.5169/seals-514491

Les armées développent leurs capacités de défense cybernétique, et parfois le font savoir, comme l'US Air Force.

Guérilla

Guérilla cybernétique : Espace nouveau, tactiques anciennes

Col Pascal Varesio

Chef de la section des opérations d'information à l'Etat-major de conduite de l'armée

L'importance des télécommunications et de l'échange de données au niveau mondial a augmenté de façon exponentielle ces quinze à vingt dernières années, et ce aussi dans le domaine militaire. La société de l'information en réseau est de plus en plus vulnérable aux activités criminelles – voire terroristes – qui sévissent dans les réseaux informatiques et sur Internet. Des acteurs de tous bords, aussi bien étatiques que non étatiques, opèrent indifféremment contre des cibles civiles ou militaires.

Le développement fulgurant de la technologie permet à pratiquement n'importe qui de causer déjà de gros dégâts avec des moyens comparativement minimes (un ordinateur portable et un accès à Internet). La rapidité, la répartition géographique et l'anonymat de ces agissements font qu'il est très difficile d'en démasquer les auteurs, sans même parler de les poursuivre en justice. En cela, les cyberattaques criminelles s'apparentent aux tactiques de la guérilla.

La guérilla numérique

De manière générale, la guérilla est caractérisée par une très grande mobilité et une très grande flexibilité. Il est très difficile d'identifier les guérilleros, car ils se « fondent » dans la population ; n'importe qui peut appartenir à la guérilla, en permanence ou de façon épisodique, et la soutenir sur les plans militaire, logistique ou politique. Dans ces conditions, les formes de combat traditionnelles des forces armées régulières sont vouées à l'échec dans une large mesure.

A l'ère du numérique, on observe la présence de formations de combat similaires dans l'espace virtuel : la cyberguérilla. Avant d'introduire cette notion, il nous faut définir les deux concepts apparentés de « guerre de l'information », ou infoguerre, et de « guerre informatique » ou cyberguerre. La guerre de l'information au sens large s'entend aussi bien sous l'angle civil que sous l'angle militaire. De leur côté, les activités militaires sont regroupées sous le terme d'opérations d'information. Ces dernières visent à influencer les informations et les systèmes d'information de l'adversaire tout en protégeant les systèmes propres. Cela peut se faire, entre autres, au moyen des médias électroniques, des médias écrits ou de mesures techniques. L'une des caractéristiques principales des opérations d'information est la coordination des différents instruments susceptibles d'être utilisés dans la dimension de l'information. Les opérations dans les réseaux informatiques (Computer Network Operations, CNO) font partie de ces instruments.

Par cyberguerre, en revanche, on entend l'affrontement guerrier dans l'espace virtuel principalement avec des moyens appartenant au domaine de l'informatique. La cyberguerre désigne ainsi une forme de guerre de plus en plus technicisée qui se base sur l'informatisation, l'électronisation et la mise en réseau de presque tous les domaines et intérêts militaires. Les instruments utilisés proviennent du domaine de la technologie de l'information. Les attaques visent les liaisons informatiques dans le but de couper la communication ou même de prendre le contrôle de systèmes informatiques spécifiques. Les méthodes usuelles de la cyberguerre comprennent l'espionnage, le défacement (modifications du contenu d'un site web), diverses formes d'ingénierie sociale, l'introduction dans le circuit de matériel qui causera des dommages, les attaques par déni de service et les attaques physiques contre le matériel informatique (destruction, sabotage, mise hors service).

Du côté des logiciels, les hackers exploitent en priorité les failles présentes dans beaucoup d'applications Internet. Ces opérations se déroulent dans l'espace virtuel, c'est-à-dire dans les réseaux informatiques.

La cyberguérilla est une notion relativement nouvelle qui allie la guérilla classique aux développements technologiques de l'espace cybernétique. Les

caractéristiques spécifiques de la cyberguérilla dans une situation de conflit sont les suivantes :

- Toute cyberattaque déclenche en règle générale une réaction de défense de la part des victimes, dans la mesure où l'offensive est détectée.
- Les assaillants disposent la plupart du temps de moins de possibilités techniques que la défense, mais la défense ne peut pas parer à toutes les éventualités.
- De plus, les victimes de cyberattaques pourraient bien ne jamais parvenir à déterminer l'identité de leurs agresseurs.
- L'assaillant contrevient au droit en vigueur, alors que les mesures de prévention et de défense doivent respecter les prescriptions légales.
- L'assaillant est généralement très alerte et mobile. Il peut pirater un système depuis n'importe quel endroit équipé d'un accès au réseau.
- Au contraire de la guérilla terrestre, la cyberguérilla est capable de porter un coup fatal aux systèmes d'un adversaire.

Le terme de cyberguérilla est ainsi une désignation relativement nouvelle d'une forme de guerre qui se déroule entre des adversaires inégaux, avec des ressources et des moyens différents et le plus souvent laissés dans l'ombre. La cyberguérilla utilise différentes méthodes relevant de la guerre de l'information, principalement dans l'environnement civil, mais aussi dans le domaine militaire. Elle avantage l'attaquant. En Suisse, la cyberguérilla sévit donc actuellement aussi dans l'environnement civil, ce qui, du point de vue légal, exclut les contre-mesures militaires.

L'avenir de la cyberguérilla

Le chapitre suivant présente trois théories traitant des possibilités de propagation de la cyberguérilla et de ses différents acteurs.

1. L'importance du cyberespace en tant que lieu où se déroulent les conflits a considérablement augmenté ces dernières années et continuera à croître.
L'espionnage militaire, l'espionnage industriel et la criminalité informatique sont très répandus. Les cas qui touchent aussi bien les systèmes militaires que civils se multiplient. La création d'une asymétrie de l'information vis-à-vis de la concurrence est l'un des mobiles des vols de données. Mais l'altération de contenus devient aussi de plus en plus fréquente ; par exemple, le groupe de hackers serbe CHC est parvenu à s'introduire dans les serveurs web des Etats de l'OTAN et à inonder leurs sites internet de contenus anti-OTAN.

L'Internet permet aussi à des groupuscules de type guérilla de mener à bien de plus en plus d'attaques à caractère politique ou religieux. On va jusqu'à trouver sur la toile des instructions portant sur la manière de pirater ou de paralyser efficacement des sites web. Les pirates informatiques disposent sur Internet d'un véritable marché de logiciels malveillants téléchargeables. Après coup, il est souvent difficile d'établir qui tire véritablement les ficelles.

Le réseau fantôme *(Ghostnet)*, découvert en 2008, dont l'exploitation est communément attribuée à des Chinois, a servi à l'infiltration d'ordinateurs industriels, militaires et gouvernementaux du monde entier, notamment ceux de l'Allemagne et de partisans d'un Tibet indépendant. Or, on ne sait toujours pas avec certitude si les auteurs proviennent des sphères étatiques ou du domaine privé. Relevons encore que les Etats-Unis, l'Allemagne et d'autres États occidentaux sont considérablement plus vulnérables que d'éventuels pays en développement du fait de leur haut niveau de numérisation et de mise en réseau. La progression de la mise en réseau et l'importance grandissante de l'espace virtuel pour l'économie et la politique favorisent également la multiplication des conflits qui s'y jouent.

2. Dans les années à venir, la majorité des forces armées se penchera de manière prioritaire sur la cyberdéfense au détriment des moyens offensifs.
A l'encontre de cette thèse, des informations parues dans la presse font état de la constitution, notamment à la Bundeswehr allemande, d'une division des « opérations d'information et de réseaux informatiques » équipée de moyens appelés Computer Network Attack (CNA). L'utilisation de moyens CNA est également un sujet d'actualité outre-Atlantique. Ainsi, pendant la guerre en Irak, les États-Unis auraient fermé des réseaux locaux de téléphonie mobile et informatiques pour empêcher les insurgés de planifier des attentats à la bombe. Des spéculations similaires existent en ce qui concerne Israël : dans le contexte de l'attaque aérienne israélienne contre une installation atomique syrienne en 2007, les avions israéliens auraient pu infiltrer l'espace aérien syrien grâce à l'utilisation de moyens CNA pour mettre le système de défense antiaérienne syrien hors service.

Mais de tels rapports laissent toujours planer un doute sur le fait que des capacités CNA aient vraiment été mises en œuvre. La majeure partie des Etats dispose tout au plus de capacités de défense (Computer Network Defense, CND), mais pratiquement pas de plans de développement de capacités offensives. Il en va de même pour la Suisse. Au sein du Centre des opérations électroniques (COE) de la Base d'aide au commandement de l'armée (BAC), on est actuellement en train de mettre en place deux domaines consacrés à la cyberguerre, et donc aussi à la cyberguérilla. 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, et d'autre part d'une cellule Computer Network Operations également mise sur pied au sein du COE. Selon les bases juridiques actuelles, les CNA offensives et la CNE à des fins de renseignements ne sont possibles que pendant le service actif. La CND reste donc prioritaire et les ressources correspondantes sont engagées.

3. Une cyberattaque de nature criminelle nécessite une collaboration rapide aux niveaux national et international ainsi qu'entre les acteurs civils et militaires.
Les cyberattaques sont souvent sources de désaccords diplomatiques entre les victimes et les pays soupçonnés de les commanditer, bien que l'intention des auteurs de

La prolifération des appareils high tech au sein des forces armées, militaires ou non, accroit à la fois l'efficacité des troupes et la vulnérabilité de leurs informations.

cyberattaques soit plus de faire de l'espionnage industriel que de commettre une agression dirigée contre l'Etat lui-même, comme le piratage de Google qui a touché de nombreuses entreprises américaines en janvier 2010. Ces coups de froid diplomatiques seraient plus faciles à éviter s'il existait une coopération interétatique adéquate. La politique militaire américaine a notamment intérêt à ce que le plus possible d'Etats associent leurs forces armées au système d'information des Etats-Unis afin que ce pays devienne le « chef de la coalition nationale » lors d'engagements militaires (comme pour les troupes IFOR/SFOR en Bosnie).

En 2008, le Centre d'excellence pour la cyberdéfense (Cooperative Cyber Defence Center of Excellence) a vu le jour en Estonie. Ce centre est appelé à devenir une plate-forme multilatérale cruciale pour la collaboration internationale en matière de cyberdéfense, ce qui renforce cette thèse. L'émergence du phénomène des brigades de pirates internationales organisées, qui traduisent leurs convictions politiques ou tout simplement leur « envie de pirater » en cyberattaques dirigées par exemple contre les Etats-Unis et l'OTAN, exige un renforcement de la coordination internationale des procédures appliquées dans le domaine CND.

Conséquences pour l'armée suisse

Pendant que la BAC met en place le savoir-faire technique et l'infrastructure nécessaire dans le domaine CNO, la section des opérations d'information de l'Etat-major de conduite de l'armée (EM cond A) est responsable de coordonner efficacement le CNO avec les autres moyens de l'armée. Sur la base de la situation générale de la politique de sécurité et du droit en vigueur, un accent particulier est mis aujourd'hui sur les mesures CND. Pour le monde civil, nous préconisons majoritairement des mesures de défense civiles. La collaboration avec les autres services de l'administration fédérale (par ex. MELANI) ou avec les entreprises TI joue ici un rôle important.
Du point de vue militaire, pour faire face à l'intensification de la cyberguérilla, il faut :

- renforcer la sensibilisation des milieux civils et militaires au danger potentiel représenté par la cyberguérilla et accorder une grande importance aux exercices en situation réelle ;
- intensifier la collaboration avec la Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI du DFJP ;
- acquérir des informations pertinentes du point de vue de la prévention sur les scènes de piratage actives (via les forums, les réseaux sociaux, etc.), afin d'estimer plus justement les futurs dangers potentiels ;
- poursuivre le développement du savoir-faire et aménager les bases légales nécessaires pour que l'armée puisse lutter à armes égales avec l'adversaire, au moins en ce qui concerne la défense.

P.V

Sources :

BENDRATH, RALF, «Der Kosovo-Krieg im Cyberspace», 19.07.1999, http://www.iwar.org.uk/iwar/resources/kosovo.htm

CSS ETH Zurich, Politique de sécurité : analyses du CSS, « Opérations d'information : tendances et controverses », N°34, mai 2008.

CSS ETH Zurich, Politique de sécurité : analyses du CSS, « Cyberguerre : concept, état d'avancement et limites », N°71, avril 2010.

LEWIS, JAMES A., «Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats", in CSIS, December 2002.

MYERSON, JUDITH M., "Cyber guerilla networking", 02.09.2003, www.c2040.com/**Cyberguerilla**.pdf

PATALONG, FRANK, «Rede nicht von Krieg, wenn Du Kriminalität meinst» im *Spiegel Online*, 09.05.2010

ROTZER, FLORIAN, «Terror.net: «Online-Terrorismus» und die Medien», 15.07.2004, http://www.heise.de/bin/tp/issue/r4/dl-artikel2.cgi?artikelnr=17886&mode=print

Informations complémentaires :
http://www.cybercrime.ch
http://www.melani.admin.ch