Cyberguerre: Nouveau visage de la guerre?

Cahiers de la pensée mili-Terre n° 43

le Commandant Jean-Sun LUIGGI

publié le 03/04/2018

Histoire & stratégie

De nombreux États, organisations terroristes ou mafieuses continuent à développer ou à améliorer leurs capacités «cyber», les plus avancés d'entre y consacrant des moyens humains et financiers très importants. La France a relevé ce défi en faisant les investissements intellectuels et matériels nécessaires. L'auteur de ces lignes plaide cependant pour une réflexion plus ambitieuse: la cyberdéfense doit être globale, concerner les aspects offensifs; elle doit devenir la cyberguerre.

En 2012, constatant «probablement l'attaque la plus destructrice que le secteur privé ait jamais vécu» contre des sociétés pétrolières et gazières ainsi que plusieurs banques, le secrétaire d'État américain Leon Panetta a affirmé qu'il existait désormais un risque de cyber Pearl Harbor. Les sociétés occidentales modernes sont-elles devenues «cyberdépendantes» en se reposant à ce point sur la technologie? Quelle imprudence d'ignorer les nouvelles modalités d'affrontement via Internet et les nouvelles technologies de l'information, tant la compétition avec certaines nations émergentes est inéluctable dans le cyberespace! Les possibilités offertes renouvèlent les capacités opérationnelles. Le nouveau Livre blanc sur la sécurité et la défense nationale de 2013 réaffirme la nécessité d'entrer dans une cyberdéfense de plus en plus active[1]. Mais si le terme de cyberdéfense évoque la défense des infrastructures critiques, il est également transposable dans le champ des opérations offensives.

Les symptômes d'une rupture

Le stratège chinois Sun-Tzu recommandait une guerre brève afin d'engager le moins de ressources possibles. «On ne saurait tenir les troupes longtemps en campagne sans

porter un très grand préjudice à l'État et sans donner une atteinte mortelle à sa propre réputation». Quoi de mieux qu'une arme nouvelle pour surprendre et vaincre rapidement un adversaire?

- Champs d'application et niveau de menace

L'armée de Terre a fait le choix de la numérisation de l'espace de bataille et développe le programme SCORPION. L'arrivée de ce programme majeur comprend la livraison de nouveaux matériels «connectés» aux systèmes d'information et de commandement. La dépendance de nos forces armées aux technologies de l'information paraît de plus en plus forte. Quels sont les risques encourus? Les cyberattaques sont en progression constante et représentent un coût financier significatif par secteur industriel. En 2014, elles ont coûté en moyenne 145 millions de dollars contre 130 millions en 2013[2].

Si de fortes présomptions existent sur l'origine de ces attaques, rien ne prouve juridiquement l'implication d'un État en particulier[3]. La difficulté pour en «attribuer» l'origine est d'ordre technique et juridique. On parle de notion d'attribution décrivant une action technique dans le cyberespace et de notion d'imputation relevant du domaine politique[4]. En termes juridiques, c'est au niveau international que le problème se pose. Les Pays-Bas n'autorisent pas la divulgation de l'identité d'une personne sur la base de son adresse IP[5]. Il est donc aisé de trouver asile en fonction des différentes législations nationales existantes.

- Perturbation de l'équilibre des forces…

Un attaquant bénéficie d'une relative impunité. Si l'une des forces en présence se trouve incapable de riposter à des cyberattaques, un déséquilibre s'ensuit. On parle de «rupture technologique».

Le risque est de ne pas déterminer la provenance d'une cyberattaque et donc de ne pouvoir riposter, faute de savoir qui est l'adversaire. Les États se trouvent potentiellement opposés à des organisations transnationales aux contours flous. Le conflit informationnel s'est en effet déplacé au niveau d'acteurs tiers parfois éloignés des logiques nationales. Ainsi, si la motivation des «Hacktivistes» est de protéger les libertés individuelles sur le net, on aura du mal à anticiper les réactions de ces groupes. À la suite des attentats des 7 et 8 janvier 2015 en France, la lutte entre cyberjihadistes et membres des Anonymous a démontré la similarité de leur mode d'action (défiguration de sites internet, attaques en déni de service, propagande par voie de réseaux sociaux).

- …s'inscrivant dans une asymétrie miscible dans le combat conventionnel

Depuis quelques années, la cyberguerre profite d'un terreau d'expansion très favorable. Certains pays ont lancé leur programme de création d'«unités cyber». Ainsi la Chine, la Syrie, les États-Unis ou la Grande-Bretagne ont largement investi dans la mise sur pied de cyberbataillons. La prise de conscience des Chinois, face à l'obsolescence technologique de leurs équipements militaires dans les années 90, a accéléré la recherche d'une

vulnérabilité qui leur permettrait de devancer les États-Unis. Cette vulnérabilité réside notamment dans la dépendance des nations occidentales aux technologies de l'information. La création d'un corps d'armée cyber de 9.600 hommes par la Chine, dont les unités 61398 et 61046[6], répondent clairement à la volonté de mener une guerre dans le cyberespace.

Les conflits futurs risquent de mélanger guerres conventionnelles et cyberguerre. Les objectifs tant militaires que civils seraient ciblés. Dans la crise ukrainienne, qui a révélé d'anciens rapports de force sous-jacents des relations OTAN-Russie[7] l'utilisation des médias et des réseaux sociaux pour influencer l'opinion est parfois très ciblée. Ainsi, les forces séparatistes de l'est de l'Ukraine ont diffusé sur Youtube les images de volontaires français combattant dans leurs rangs.

La cyberguerre: quels schémas?

La cyberguerre est-elle une guerre à part entière ou un moyen complémentaire de la guerre?

- Guerre hybride et cyberguerre: de nouvelles règles?

Les cyberattaques sont-elles destinées à faire partie d'une panoplie de techniques soumettant l'adversaire à sa volonté et menant à la victoire? Les moyens déployés récemment par la Russie en Ukraine s'apparentent à un nouveau genre de guerre dite non linéaire qui implique de multiples acteurs: médias, actions diplomatiques, humanitaires, économiques, influence, mercenariat et volontaires. L'emploi combiné de ces moyens s'apparente à une interpénétration de soft et hard power[8]. Cette diversité d'acteurs exprime paradoxalement la recherche d'une concentration d'efforts afin de remporter la bataille de l'information. Sans liens apparents les unes avec les autres, ces actions participent à un même but: convaincre les opinions publiques du bien fondé de telle ou telle opération. Dans un tel cadre la dimension cyber prend toute sa place[9]. En réalité, si certaines actions, telles les opérations d'influence, de campagne d'information et d'aide aux populations sont appliquées par les nations de l'OTAN, elles appartiennent déjà aux guerres du passé. To Win hearts and minds est un concept datant de la guerre du Vietnam, issu de l'expérience des guerres coloniales européennes.

Le principe français de concentration des efforts implique tactiquement de porter l'effort en un certain point avec un maximum de forces. L'intérêt de la cyberguerre est de se concentrer là où n'opère pas la force militaire. Des frappes conventionnelles peuvent se dérouler sur un secteur, alors que les moyens de cyberguerre peuvent opérer ailleurs. On se rapproche alors du concept d'attaque parallèle des cinq cercles de John Warden, où le but est de frapper au plus près du centre de commandement lorsque l'attention se focalise sur les forces conventionnelles. L'auteur cite le cas de la guerre du Vietnam, où le Viêt-Cong a réussi à renverser l'opinion publique américaine…

Tactiquement, au niveau des unités de combat, il est encore délicat de mettre en pratique la guerre numérique. Si la littérature militaire développe des théories nouvelles sur l'usage des moyens informatiques («Perspectives Tactiques» du Général Guy Hubin), ou émet des comparaisons avec des modes d'actions connus (la cyberguerre est comparée au combat en zone urbaine dans «Cybertactique, conduire la guerre numérique» de Bertrand Boyer), la réalisation concrète du combat numérique généralisé par les unités au contact n'est pas encore à l'ordre du jour. L'armée de Terre utilise des unités légères de guerre électronique qui interviennent en opération. Sur ce modèle, des unités de combat numérisées dûment formées et équipées pourraient un jour compléter l'arsenal militaire tactique.

- Arme du faible ou moyen universel?

Bien que l'application de la notion de guerre préventive rapportée à la sphère virtuelle puisse ouvrir de nouvelles perspectives, une cyberattaque n'est pas dans l'intention première d'une nation déjà puissante sur le plan militaire. Une cyberattaque est davantage utilisable par le faible comme moyen de contourner cette puissance à peu de frais. Les pays peu dotés en moyens technologiques offrent peu de prise aux actions de cyberguerre. Une attaque contre ces nations n'offrirait pas de massification des effets et ne présenterait d'intérêt que dans le cadre d'objectifs ponctuels à forte valeur ajoutée (cas des centrales d'enrichissement pour Stuxnet). En revanche, les nations techno-dépendantes offrent une cible de choix où l'effet domino joue à plein. L'Estonie, qui a subi en 2007 les effets d'attaques DDoS (Distributed Denial of Service) relativement simples à mettre en œuvre, a été progressivement paralysée par une attaque successive de tous les systèmes économiques, financiers et gouvernementaux. 58 sites internet ont été bloqués, dont le site de la principale banque en ligne du pays. La paralysie a duré trois semaines, la plupart des Estoniens se trouvant dans l'incapacité de retirer de l'argent aux distributeurs automatiques. Ce type d'opération est opéré à moindre coût, au prix de l'entretien d'une petite armée cybernétique dûment formée ou de hackers mercenaires non rattachables à un quelconque gouvernement. De l'aveu de certains «hacktivistes» russes, les protections informatiques de l'Estonie étaient inexistantes.

- Technologie «tire et oublie»

Une cyberattaque permet bien souvent à son auteur de garder l'anonymat et de masquer ses intentions. Si le virus Stuxnet put être détecté rapidement sur de multiples supports informatiques à travers le monde par des entreprises de sécurité informatiques comme Kaspersky, son but réel se révéla lorsque son objectif fut atteint: les centrifugeuses iraniennes.

Le cyberattaquant conserve sa liberté d'action, n'étant pas «fixé» au moment de l'attaque. Dans «Perspectives Tactiques», le Général (2S) Guy Hubin avait souligné cette remise en question de la notion de fixation à l'heure des nouvelles technologies. Les cyberattaques s'apparentent davantage à l'utilisation d'une technologie «tire et oublie» peu contraignante qu'au déploiement de moyens militaires classiques à forte empreinte politique et logistique. Même s'il est toujours possible de retrouver un cyberattaquant (l'étude approfondie des virus a permis de relier Israël et les États-Unis pour les attaques par Stuxnet, Duqu puis Flame pour ralentir le programme nucléaire iranien), le temps nécessaire à cette recherche ne permet pas d'inquiéter réellement le coupable au moment des faits. Cette idée trouve également son accomplissement dans les nombreux

cas exposés dans les trente-six stratagèmes chinois, qui privilégient des moyens d'action détournés: frapper avec une épée d'emprunt.

La cyberguerre peut être utilisée afin d'atteindre un objectif limité. Dans le cas de Stuxnet, une infrastructure vitale a été détruite, ce qui peut être l'objet d'une guerre dite «limitée» ou un simple objectif tactique.

Logique de confrontation indirecte et action coercitive

En Occident, la ruse a longtemps été dénigrée du fait d'une tradition chevaleresque[10]. Or, les résultats peuvent être spectaculaires et participer au principe d'économie des moyens.

- Une analogie avec **«**L'art de la guerre**»**

Selon «L'art de la guerre», «conserver les possessions des ennemis est ce que vous devez faire en premier lieu, comme ce qu'il y a de plus parfait; les détruire doit être l'effet de la nécessité». En frappant quelques lignes de codes, l'ennemi peut se voir dépossédé de ses ressources. La crise estonienne est révélatrice de ce mode d'action. Le but des cyberattaques contre ce pays n'était pas le vol, mais la paralysie de ses institutions économiques et financières.

Cette nouvelle cohabitation de moyens symétriques et asymétriques prolonge l'interpénétration des actions Yin et Yang (également nommées forces directes et indirectes) décrite dans «L'art de la guerre» de Sun-Tzu: «Usez généralement des forces directes pour engager la bataille, et des forces indirectes pour emporter la décision».

De plus, l'intérêt de la cyberguerre en matière de renseignement apparaît naturellement quand les serveurs et systèmes informatiques infectés le sont à l'insu de leur victime. Assurément, la cyberguerre permet de réaliser les buts du treizième chapitre de «L'art de la guerre», notamment la désinformation et la subversion.

- Cyberguerre: le graal de la théorie des cinq cercles

La guerre cybernétique et informationnelle au sens large permet d'appliquer la théorie des cinq cercles de J. Warden. Frapper les infrastructures critiques de l'adversaire – centrales énergétiques, réseaux de communication, réseaux routiers ou de distribution (les deuxième et troisième cercles), demeure le cœur de cible de la cyberguerre. Ces atteintes peuvent toucher durablement l'économie d'un État, mais également sa population (le quatrième cercle), bien plus sûrement qu'un embargo. Dans «Enemy as a system», J. Warden explique que frapper les forces armées de l'adversaire (le cinquième cercle) n'est pas le plus important. Atteindre sa volonté de combattre et engendrer une paralysie stratégique obligera le commandement adverse (le premier cercle) à un compromis[11].

La cyberguerre constitue déjà un nouveau pan de la réflexion stratégique. Une nation ou un système d'alliances repose pleinement sur ses ressorts civils. Or, la cyberguerre permet l'exercice d'une forme de guerre totale et s'applique parfaitement à la théorie des cinq cercles.

Saut capacitaire ou retard technologique?

La cyberguerre se rapporte à un renouveau de la guerre moderne, comprenant la guerre informationnelle sous toutes ses formes où l'interpénétration des moyens militaires conventionnels et le niveau stratégique sont prégnants. C'est pourquoi il convient d'intégrer les composantes de cyberdéfense défensives comme offensives avec ses moyens civils et militaires. L'Estonie a fondé un centre d'excellence de cyberdéfense au profit de l'OTAN et se repose sur l'Alliance pour développer cette capacité. Faut-il renoncer à conserver une cyberdéfense nationale? L'affaire Snowden prouve le contraire, si l'on se remémore les actes d'espionnage de certains de nos alliés. L'agence nationale de sécurité des systèmes d'information, créée en 2008, répond à cette exigence en fournissant à la France des moyens nationaux et indépendants. Le plan d'action cyber 2014 du ministre de la Défense traduit en actions concrètes les mesures à prendre concernant le risque cyber.

C'est l'absence de moyens pour contrer la cyberguerre, un fossé capacitaire, qui constitue une rupture technologique pour les États qui en sont dépourvus. La cyberguerre ne fait que renouveler des méthodes éprouvées avec des moyens techniques novateurs et pluriels.

Il y a une convergence entre la conduite de la guerre symétrique, l'exercice du soft power et la lutte asymétrique de la cyberguerre. La guerre de demain, si ce n'est d'aujourd'hui, combinerait des moyens conventionnels avec les outils de la cyberguerre pour atteindre des objectifs particuliers, créer la confusion chez l'ennemi et au sein de sa population. Dans un contexte de contraintes économiques, la cyberdéfense au sens large n'est pas l'apanage de nations riches ou de grandes alliances militaires. Cet enjeu vital reste à la portée de la France. Le risque de cyberattaques majeures sur fond de terrorisme international constitue aujourd'hui une réelle mise à l'épreuve.

[1] «Toutefois, la croissance continue de la menace, l'importance sans cesse accrue des systèmes d'information dans la vie de nos sociétés et l'évolution très rapide des technologies imposent de franchir une étape supplémentaire pour conserver des capacités de protection et de défense adaptées à ces évolutions. Elles nous imposent aujourd'hui d'augmenter de manière très substantielle le niveau de sécurité et les moyens de défense de nos systèmes d'information, tant pour le maintien de notre souveraineté que pour la défense de notre économie et de l'emploi en France. Les moyens humains qui y sont consacrés seront donc sensiblement renforcés à la hauteur des efforts consentis par nos partenaires britannique et allemand». LBDSN 2013, page 105.

[2] Cost of Data Breach Study 2014, Ponemon Institute, basé sur un échantillon de 314 entreprises de dix pays différents

[3] Les virus se cachent sur des serveurs distants multiples et plusieurs hébergeurs de différents pays. Le virus STUXNET aurait été dissimulé, entre autre, sur un serveur indonésien d'un club de football.

[4] Voir à ce sujet «Cybertactique, conduire la guerre numérique». Bertrand Boyer (éd. Économica).

[5] Internet Protocol: sorte de «numéro d'immatriculation» servant à identifier chaque connexion

[6] L'unité 61398 est en charge de la zone États-Unis / Amérique et l'unité 61046 de l'Europe.

[7] On peut citer le cas de la Moldavie avec la sécession de la Transnistrie depuis 1992, mais aussi la récente crise géorgienne de 2008,

[8] Terminologie de Joseph Nye, différenciant les notions découlant d'un leadership non coercitif (soft power) et d'hégémonie (hard power) dans les relations internationales. «Bound to Lead: The Changing Nature of American Power», New York: Basic Books, 1990.

[9] À ce titre, il existe, depuis le 9 septembre 2000, une doctrine de sécurité informationnelle de la Fédération de Russie qui expose clairement une vision globale de la sécurité de l'information comme rempart, mais aussi vecteur culturel de la civilisation slave. Voir «La cyber stratégie russe» de Y. Harrel (éd. Nuvis).

[10] Voir «La Ruse et les formes contemporaines de la guerre» de Jean-François Holeindre dans «La fin des guerres majeures» (ch.3, Éd Économica).

[11] «The latter we call strategic paralysis. Which parts of the enemy system we attack (with a variety of weapons ranging from explosives to nonlethal computer viruses) will depend on what our objectives are, how much the enemy wants to resist us, how capable he is, and how much effort we are physically, morally, and politically capable of exercising». J Warden dans "Enemy as a system". Il est clairement fait mention des cyberattaques dans ce contexte.

Responsable du domaine pyrotechnique et de la sécurité des systèmes d'information de divers établissements du matériel classés SEVESO II durant sa première partie de carrière, le Commandant Jean-Sun LUIGGI a été en poste aux écoles militaires de Bourges entre 2012 et 2015. Il y a dirigé la section d'enseignement de la numérisation de l'espace de bataille et des systèmes d'information logistique. Il est actuellement officier stagiaire à l'École de guerre (23ème promotion).

Titre : le Commandant Jean-Sun LUIGGI

Auteur(s) : le Commandant Jean-Sun LUIGGI

Date de parution 17/02/2018