EPIDOSIS
Regards croisés sur l'innovation
n°19
Hebdo
Mai 2014

L'arme et la cuirasse à l'heure numérique

Originellement, une arme est un outil destiné à neutraliser un adversaire tandis qu'une cuirasse est une pièce d'armure dont la fonction est de protéger le corps de celui qui la porte. Aujourd'hui que l'une et l'autre s'affrontent dans le cyberespace par 0 et 1 interposés, il est intéressant de se pencher sur cette lutte vieille comme le monde.

Dès l'Antiquité, vers l'an 3000 avant J-C, les premières armées organisées dotent les hommes de lances et de boucliers. La catapulte, le trébuchet, la baliste puis les arcs et les flèches signent une première évolution dans l'art du combat, moins archaïque que le simple corps à corps. Au XIVe siècle, l'apparition de la poudre à canon crée une nouvelle rupture dans l'art de la guerre : à la force humaine succède la puissance purement mécanique. Puis, après les préparations d'artillerie de la Première Guerre mondiale et les bombardements intensifs de la Seconde, l'arme absolue est utilisée le 6 août 1945 à Hiroshima, jusqu'à ce que des illuminés en imaginent une nouvelle, utilisant des avions de ligne comme arme par destination contre les tours de Manhattan en 2001.

Aujourd'hui, l'attaque est imprévisible et le « brouillard de la guerre » cher à Clausewitz n'a jamais été si avéré : il s'agit autant de voir venir le coup et d'identifier celui qui l'a porté, que de s'en protéger. Les armes conventionnelles sont de plus en plus foudroyantes et les terroristes de plus en plus inventifs dans leur approche asymétrique. A cela s'ajoutent des agressions d'un genre nouveau qui se règlent à coup de kilo-octets. Cette perspective nécessite de s'intéresser au cyberarmes et aux cybercuirasses du temps présent.

Selon un rapport de l'Union internationale des télécommunications (UIT), plus d'un tiers de la population mondiale a accès à l'internet. Associée aux progrès en matière de composants électroniques, la potentialité innovatrice des nouvelles technologies numériques semble infinie. Civils et militaires ont ceci en commun que tous deux sont liés à des réseaux interconnectés et ne peuvent plus s'en passer. Ces réseaux constituent certes une importante source de pouvoir, par l'accès à l'information stratégique et la rapidité de réaction qu'elle procure, et de progrès, par l'immense champ d'action qu'elle autorise, mais leurs vulnérabilités inspirent aussi la malveillance d'acteurs cachés derrière un ordinateur que seule une adresse IP peut éventuellement dénoncer.

Aux Etats-Unis, le cyberespace est passé du statut de « fournisseur de services » en 2009 à celui de « capacité » en 2011 puis de « domaine » en 2013, au même titre que l'air, la terre, la mer et l'espace Il est désormais le 5e espace de bataille où s'affrontent attaques cyber (les armes) et dispositifs de sécurité (les cuirasses). En France, le *Livre blanc sur la défense et la sécurité nationale* de 2013 souligne le caractère prioritaire des cybermenaces et la nécessité de prendre conscience de leur importance. Si l'origine des attaques est le plus souvent imperceptible, la nature des motivations de l'agresseur peut revêtir des finalités diamétralement opposées. Les différents acteurs vont

EPIDOSIS

Dans la littérature grecque, le terme επίδοσις, issu du verbe επιδίδωμι, est employé pour exprimer le don volontaire, l'engagement personnel. Par extension, notamment chez Isocrate, le terme prend le sens du progrès effectué, de l'innovation. Don de soi et innovation, deux valeurs que l'armée de l'air porte en ses gènes.

Cette publication du CESA a pour vocation de susciter des échanges, de croiser les regards entre les aviateurs, le personnel de la Défense et les décideurs publics et privés.

www.cesa.air.defense.gouv.fr

du pirate informatique isolé (*hacker*) agissant par défi pour vanter ses exploits sur la toile, au voleur expert de l'hameçonnage (*phishing*) capable de soutirer des informations confidentielles au moyen d'un cheval de Troie, jusqu'à l'activiste dont le but est de paralyser un réseau *via* une bombe logique ou un virus.

Dans notre société contemporaine, les Etats modernes ont une certaine capacité d'agir dans la sphère cyber en régulant notamment l'accès à internet – pratique courante dans les pays non démocratiques – mais ils peuvent aussi bien être l'agresseur que l'agressé. Même si ce n'était certainement pas la première du genre, c'est en 2007 qu'a été révélée la toute première cyberagression contre un Etat quand des attaques informatiques ont directement touché et paralysé des systèmes étatiques et économiques estoniens (institutions publiques, banques et entreprises). Depuis, bien d'autres attaques ont été relevées. Ces cyberattaques appliquées aux organismes d'Etat ou aux grandes entreprises ne signifient pas pour autant que les populations civiles sont éloignées du danger.

Alors le vieux paradigme de l'arme et de la cuirasse est-il encore d'actualité en 2014 ? On l'a vu, du fantassin de l'Antiquité au cyberterroriste, il a fallu autant innover pour créer les armes que pour imaginer les cuirasses, l'une et l'autre s'étant tour à tour imposées. A y regarder de près, on peut se demander si, aujourd'hui, le cyberespace n'introduit pas une nouvelle forme de dissuasion que l'on pourrait appeler « dissuasion digitale ». Au même titre qu'une frappe nucléaire, les attaques cybernétiques offrent un champ de confrontation quasi illimité et peuvent causer d'immenses dégâts (attaque d'infrastructures vitales, coupure de réacteur nucléaire, ouverture des vannes d'un barrage…), en s'attaquant notamment aux intérêts vitaux d'un Etat. D'une certaine manière, un lien conceptuel semble ainsi exister entre dissuasion nucléaire et cyberdéfense.

Si aujourd'hui, une cyberattaque est difficilement identifiable tant l'opérateur peut utiliser des systèmes écran ou intermédiaires, ne peut-on pas penser qu'à l'avenir, un Etat pourra lancer un avertissement à un autre quand les limites acceptables seront en passe d'être franchies ? Cela n'a-t-il pas déjà été le cas entre les Etats-Unis et la Chine en 2013 ? Le journal *Le Point* reportait en mai de cette année la question du vol attribué à Pékin de données sensibles américaines, gouvernementales et privées[1]. Il faisait état de conversations « musclées » entre le Président américain et son homologue chinois. Il en a résulté un rapport présidentiel de dix-huit pages intitulé *Offensive Cyber Effects Operations* (OCEO)[2] destiné à l'élaboration d'une doctrine d'emploi américaine visant l'établissement d'actions contre d'éventuelles cyberattaques. Dès lors, il est important de réfléchir aux solutions permettant de prévenir la survenance d'une cyberattaque dont les conséquences pourraient être incalculables.

Trois voies s'offrent aux décideurs. Tout d'abord, la sécurité des systèmes d'information repose sur la prévention, *via* la sensibilisation des utilisateurs de réseaux aux menaces informatiques et la mise en place de procédures permettant d'y parer, et sur les moyens techniques de protection passive. La deuxième est celle de la technologie. Dans le cadre du vol de données intéressant aussi bien le monde civil que militaire, la signature électronique et le chiffrement offrent des mécanismes difficilement contournables ; par exemple, le programme *CertiPath* assure aux membres du monde de l'aéronautique et de la défense différents niveaux de sécurisation pour leurs échanges d'informations. Les instruments juridiques constituent la troisième voie : des sanctions pénales internationales adaptées aux conséquences possibles d'une cyberactivité peuvent empêcher un Etat d'être mis au ban de la communauté internationale et un acteur isolé de se lancer dans l'aventure.

En conclusion, la transparence est le pire ennemi du cyberattaquant, qu'il soit étatique ou isolé. Pour dissuader un Etat ou un individu « cybervelléitaire », l'utilisation de moyens de prévention, de protection et d'action, alliée à la capacité de mettre en œuvre une stratégie offensive, digitale ou juridique, remet l'éternelle logique du glaive et de la cuirasse à l'ordre du jour.

Capitaine Océane Zubeldia

1. Cf. l'article « Sommet entre Obama et son homologue chinois Xi Jinping début juin », paru le 21 mai 2013 sur www.lepoint.fr.
2. Ce rapport n'a jamais été rendu public, seuls certains éléments non classifiés ont fait l'objet d'une communication.

ARMÉE DE L'AIR 1934 80 ans 2014

Epidosis
Une publication du CESA

Directeur de publication :
colonel Bruno Mignot

Contact :
bruno.mignot@intradef.gouv.fr
Tél : 01 44 42 83 71

Centre d'études stratégiques aérospatiales
1, place Joffre
75700 Paris SP 07

www.cesa.air.defense.gouv.fr