Vers une dissuasion cybernétique?

cahier de la pensée mili-Terre

Chef d'escadron PRETEUX

publié le 21/10/2018

Sciences & technologies

À l'heure où l'intelligence artificielle, le big data, les objets connectés donnent à l'échange d'informations une ampleur sans précédent dans l'histoire de l'humanité, le monde virtuel a pris une importance considérable, en particulier pour les armées. La puissance des moyens cyber est telle que de nombreux journalistes et observateurs du monde militaire s'interrogent sur le parallèle qui pourrait être fait entre dissuasion nucléaire et cyber.

La création, mais surtout l'expansion et l'usage de l'internet ont radicalement bouleversé la vie, les us et coutumes, les méthodes de réflexion des sociétés. Ils modifient considérablement le rapport à la connaissance et à l'information de chaque citoyen. L'internet est par conséquent devenu un vecteur privilégié, un «effecteur», non plus potentiel mais incontournable, pour quiconque souhaite atteindre un objectif particulier. Au-delà de l'internet, c'est bien en fait l'ensemble de ce que l'on peut appeler la sphère cybernétique (cf. Encart) qui est devenu un enjeu majeur pour les États. La description de la cybermenace, apparaissant pour la première fois dans le Livre blanc sur la défense et la sécurité nationale de 2008 et reprise et renforcée dans celui de 2013, montre bien la prise en compte de ce nouvel espace. Le LBDSN de 2013 place d'ailleurs les cyberattaques en troisième position par ordre d'importance (après l'agression contre le territoire national et les attaques terroristes), alors que les Américains, quant à eux, les placent en première position, avant même les attaques terroristes. Le cyberespace y est d'ailleurs décrit comme la «quatrième dimension», après la terre, l'air et la mer. Plus récemment encore, dans son discours à l'occasion de la visite à la Direction générale de l'armement/maîtrise de l'information, le ministre de la Défense Jean-Yves Le Drian prône l'augmentation des moyens, autant humains que financiers et matériels, alloués à la maîtrise de ce nouvel espace. Ainsi décrit et considéré, le domaine cyber ne pouvait être que porté par une politique forte et ambitieuse, afin de permettre à la France d'y tenir son rang autant que dans le monde physique. Pour ce faire, elle a choisi trois axes complémentaires:

- un renseignement efficace, qui est la première de toutes les missions et qui contribue à mener bien l'ensemble des missions suivantes;
- une posture défensive robuste, en mesure de protéger non seulement les infrastructures et systèmes cybernétiques du ministère de la Défense, mais également, en lien avec l'ANSSI, toutes les structures d'intérêt stratégique;
- un panel de capacités offensives, de la veille internet aux capacités destructives, que la France se garde le droit d'utiliser à tout moment sur décision du président de la République.

Cette complémentarité entre un schéma défensif et un spectre complet de capacités parfaitement maîtrisées n'est pas sans rappeler le monde physique et le large spectre de ses capacités. Ainsi, nous verrons que même s'il est tentant de pousser l'analogie et imaginer une dissuasion cybernétique qui permettrait d'atteindre, par d'autres moyens, l'objectif préventif fixé aux armées, le champ sémantique de la dissuasion doit rester circonscrit au nucléaire, ainsi que l'a rappelé le ministre de la Défense dans son allocution.

Dans un premier temps, il est ainsi nécessaire de se demander à quoi correspond la dissuasion.

Dissuader: Faire renoncer quelqu'un à son intention de faire quelque chose (Larousse).

Sur un plan diplomatique, la dissuasion consiste à empêcher un acteur d'intenter des actions contre l'État (son territoire, ses intérêts vitaux) en le persuadant que son action aura un coût inacceptable et bien supérieur aux éventuels gains qu'il pourrait en percevoir[1].

On peut voir ici les éléments qui sont constitutifs de la dissuasion nucléaire.

Tout d'abord, la dissuasion repose sur la volonté des acteurs d'empêcher tout passage à l'acte. Pour ce faire, il faut donc que ces acteurs soient identifiés. Les détenteurs de capacités nucléaires sont connus, qu'ils le soient de manière légitime ou de fait. Mais ils sont dans l'ensemble connus ou tout du moins soupçonnés[2]. La capacité d'attribution d'une attaque est donc indispensable à la dissuasion afin de pouvoir cibler l'éventuelle réponse.

Enfin, la dissuasion, comme indiqué précédemment, repose sur un coût inacceptable et bien supérieur aux gains. Cela implique la crédibilité des actions de représailles possibles. La crédibilité de l'arme nucléaire repose en particulier sur l'histoire (Hiroshima, Nagasaki) et sur les essais nucléaires réalisés par certains pays. Tout le monde sait ce que peut faire une bombe nucléaire. La perte de (très) nombreuses vies humaines, la destruction de toute structure à des kilomètres à la ronde, l'irradiation pérenne du «fallout», jusqu'à 25 km alentour sont autant de conséquences inacceptables, en tout cas à l'heure actuelle.

Les capacités cyber françaises

La France dispose du spectre complet des capacités cybernétiques, autant en termes d'actions offensives que défensives. Les actions dans l'espace cyber ont été définies comme étant de quatre types: actions défensives, actions offensives, actions contre-

narratives et renseignement.

Les actions défensives consistent à mettre en place les moyens (physiques, logiciels et humains) nécessaires afin d'empêcher au mieux, de limiter au pire tout type d'attaque sur les points d'intérêt stratégique français et, en particulier, sur les réseaux du ministère de la Défense. Les attaques possibles sont de types très variés et peuvent être commises par des acteurs eux aussi particulièrement variés. Du jeune geek qui s'amuse à «hacker» pour le plaisir jusqu'aux attaques d'États organisés, en passant par les «hacktivistes» et le grand banditisme, les multiples formes que peuvent prendre ces attaques obligent à maintenir une veille technologique constante ainsi que des outils dédiés à ce travail. Le CALID[3], au sein du ministère de la Défense, colocalisé avec l'ANSSI[4], regroupe une centaine d'experts du domaine dont la mission est d'assurer cette protection.

Les actions offensives consistent quant à elle à frapper, de différentes manières, un point particulier afin d'obtenir l'effet désiré. Ces actions peuvent revêtir plusieurs formes, phishing, spamming, DOS[5], vers, virus, chevaux de Troie. Elles peuvent être destructives ou non, ciblées ou non. La France est en mesure de mettre en œuvre la totalité de ces capacités si nécessaire.

Les actions contre-narratives: un aspect particulier a émergé de l'expansion d'internet depuis une dizaine d'années, qui est l'importance des réseaux sociaux. Ils sont devenus un puissant vecteur de propagande, d'information et de désinformation, mais également un vecteur de planification et de publicité d'actions illicites. Les actions contre-narratives ont pour but de surveiller les réseaux sociaux, d'y repérer les contenus suspects et/ou potentiellement dangereux et d'y agir soit en traçant les différents intervenants, soit en menant des actions de contre-propagande et d'information. Ce domaine particulier du cyber recoupe la couche sociale du cyberespace évoquée plus haut, et son ampleur va grandissant.

Enfin, le renseignement, comme dans le domaine physique, est une priorité car on ne peut bien agir que lorsqu'on est correctement renseigné. Les moyens de renseignement cyber dont dispose la France sont définis par la loi de programmation militaire et permettent de recueillir le renseignement nécessaire, en particulier par l'exploitation des sources ouvertes et du Big Data.

L'exclusion d'une dissuasion cybernétique

Au vu de ces capacités, il serait en effet tentant d'établir un parallèle entre le monde physique et le monde cyber, en particulier en ce qui concerne la dissuasion. Le journaliste Eric Mettout n'hésite d'ailleurs pas à faire ce parallèle dans son article «Russie États-Unis: la cyberguerre froide a commencé» dans le journal L'Express en décembre 2016.

Pourtant, si l'analogie est intéressante, la dissuasion cybernétique n'est tout d'abord pas techniquement envisageable à l'heure actuelle. En effet, pour qu'elle soit efficace, une éventuelle dissuasion cyber devrait être crédible et afficher un pouvoir destructeur particulièrement élevé. La France dispose bel et bien de capacités offensives destructives dont les conséquences pourraient se révéler inacceptables (destruction ou contrôle des réseaux d'énergie par exemple). Mais il manque, pour cette crédibilité, un «Hiroshima cybernétique» qui permettrait (au-delà des films que l'on a pu voir) de se rendre compte des conséquences désastreuses que pourrait avoir une telle action. Les applications seraient pourtant multiples:

- prise de contrôle des flux énergétiques d'un pays (en particulier électrique);
- coupure de l'ensemble des réseaux de communication;
- coupure d'un système de refroidissement conduisant à une explosion;
- coupure des data centers des centres financiers, remettant à zéro l'ensemble des données financières mondiales.

Pourtant, l'aspect non directement létal, mais très démonstratif de ces capacités rend acceptable de telles actions. L'actualité, récente comme ancienne, regorge d'exemples d'actions directes ou indirectes plus ou moins destructives. Du vers STUXNET, responsable de vingt ans de retard (selon les experts) pour les Iraniens dans leur programme nucléaire, aux soupçons d'interférence des Russes dans les élections américaines de 2016, les actions cybernétiques forment un type d'action stratégique à part entière. Encore récemment, la capacité d'une attaque à prendre pour cible directement un État a été démontrée par le Botnet Mirai 14[6] qui a saturé l'unique point d'entrée internet d'un État tout entier, le Libéria. Si les conséquences de cette attaque ont été minimes du fait de la faible densité de population reliée à l'internet, les capacités stratégiques d'une cyberattaque sont ici évidentes!

De plus, un des principes de la dissuasion est de savoir à qui l'on a affaire. Cette attribution de la primo attaque potentielle est donc nécessaire pour pouvoir parler de dissuasion cybernétique. Or, l'attribution avec certitude d'une attaque cyber est quelque chose d'assez mal maîtrisé. De nombreux indices permettent alors de porter des soupçons sur des groupes actifs, et seules des spéculations poussées, mais jamais prouvées, amènent les analystes à imaginer la responsabilité d'une entité étatique. Une réponse officielle, dans le cadre d'un programme dissuasif, devient alors inenvisageable car difficile à justifier au regard du droit de la guerre et des mœurs communément admis au sein du jeu diplomatique mondial.

Enfin, et en s'éloignant des considérations techniques et de faisabilité, la dissuasion doit garder son caractère strictement nucléaire. En effet, lors de la mise en place d'une politique de dissuasion cyber par un des acteurs internationaux, le jeu diplomatique impliquerait une escalade des moyens, et de nombreux États pourraient ainsi se doter d'une «dissuasion cyber» car les moyens à mettre en œuvre seraient certes compliqués, mais beaucoup plus abordables qu'une dissuasion nucléaire, aussi bien du point de vue technique que financier. Cela bouleverserait également grandement l'équilibre entre les puissances et modifierait considérablement les rapports entre États. Les membres permanents du conseil de sécurité de l'ONU ont cela en commun d'être les maîtres officiels du jeu de la dissuasion nucléaire. Les pays qui ont voulu rejoindre ce «club» très fermé des puissances nucléaires l'ont fait à grand frais, ce type de programme étant exorbitant, autant en termes de recherche qu'en termes de mise en œuvre. A contrario, un programme de cyberdéfense avancé nécessite beaucoup moins d'investissement.

Cette accessibilité relative à une éventuelle dissuasion cyber vient également de la grande différence entre le monde physique et le monde virtuel en matière de normes, de contrôle et, d'un point de vue plus philosophique, de morale. Si le monde physique dispose de nombreux traités, lois, règlements, conventions qui permettent de réguler plus ou moins efficacement la prolifération de l'arme nucléaire, il n'en est rien dans le monde cybernétique. À cet égard, le ministre de La Défense a estimé que le droit international s'appliquait au monde cyber[7]. Pourtant, celui-ci est considéré par la plupart des protagonistes comme un territoire vierge, neutre et libre, rendant ce monde virtuel très difficilement contrôlable. Ainsi, on estime que l'internet que nous connaissons, le web, ne représente que 5% de l'Internet total, le deepweb et le darkweb se partageant les 95% restants. Dans ces deux «territoires», aucune loi étatique n'a de prise, ce qui permet aux différents groupes de s'épanouir et de lancer leurs actions ciblées. Ainsi, une

dissuasion cyber cohérente ne pourra jamais voir le jour tant que l'Internet dans son ensemble, ou en tout cas dans sa grande majorité, ne sera pas réglementé par les États.

Pourtant, le caractère inacceptable d'une action cybernétique pourrait être admis dans le cas de la prise de contrôle d'un réacteur nucléaire ou d'un arsenal nucléaire adverse. Cela pourrait prôner pour une dissuasion cybernétique. Mais le problème doit se voir autrement. La dissuasion nucléaire française disposait de trois composantes, terrestre, aérienne et maritime, réduite aux deux composantes aérienne et maritime dans les années 1990. Il pourrait alors être intéressant de ré-envisager une troisième composante, cybernétique cette fois, capable de s'attaquer aux infrastructures nucléaires de par le monde et d'en prendre le contrôle. On ne parlerait pas alors de dissuasion cybernétique, mais toujours de dissuasion nucléaire, mise en œuvre par sa composante cybernétique vers les seules entités disposant de l'accès à l'atome.

Ainsi, même s'il est nécessaire de ne jamais sous-estimer les capacités destructrices ou de nuisance des capacités cyber de groupuscules actifs ou d'États-nations, à l'heure actuelle le champ sémantique de la dissuasion se doit de rester restreint à la force de frappe nucléaire. Car technologiquement, tout d'abord, les moyens d'une éventuelle dissuasion cyber ne sont pas encore au point (attribution, démonstration des effets), et qu'ensuite et surtout cela risquerait de remettre en cause et de redessiner les forces et interactions entre les acteurs internationaux et complexifier encore plus le jeu diplomatique mondial, rompant ainsi l'équilibre déjà fragile qui existe entre ces acteurs. Cependant, il est indispensable de continuer à penser et à réfléchir sur la notion de dissuasion cybernétique comme une possibilité afin de parer à toute éventualité.

[1] Article Wikipédia sur la dissuasion nucléaire française. https://fr.m.wikipedia.org/wiki/Dissuasion_nucléaire

https://fr.m.wikipedia.org/wiki/Force_de_dissuasion_nucléaire_française

[2] Article «Les armes nucléaires dans le monde» par Damien Hypolite du Figaro, 12 avril 2010.

http://www.lefigaro.fr/international/2010/04/12/01003-20100412ARTFIG00537-les-armes-nucleaires-dans-le-monde-.php

[3] Centre d'analyse de lutte informatique défensive.

[4] Agence nationale de la sécurité des systèmes d'information.

[5] Deny of service. Une attaque par déni de service consiste à envoyer un très grand nombre de requêtes à un serveur afin de le saturer et ainsi le neutraliser durant une certaine période.

[6] Article «Un Botnet Mirai met à genoux l'accès internet au Libéria» par la rédaction du site zdnet.fr.

http://www.zdnet.fr/actualites/un-botnet-mirai-met-a-genoux-l-acces-internet-au-liberia-39844240.html

[7] Discours du Ministre de La Défense à l'occasion de la visite à la DGA/MI du 12 décembre 2016.

http://www.defense.gouv.fr/ministre/prises-de-parole-du-ministre/prises-de-parole-de-m.-jean-yves-le-drian/cyberdefense-discours-de-jean-yves-le-drian-lundi-12-decembre-2016

Saint-cyrien de la promotion «Général Vambremeersch» (2001-2004), le Chef d'escadron PRETEUX a tout d'abord servi dans l'arme du train au sein du 121ème régiment du train comme chef de section, au régiment médical comme commandant d'unité puis à la brigade logistique avant d'intégrer l'École de guerre en 2015. Passionné de nouvelles technologies et en particulier celles liées aux systèmes d'information, il suit actuellement une formation en master spécialisé à l'école Centrale Paris.

Titre : Chef d'escadron PRETEUX

Auteur(s) : Chef d'escadron PRETEUX