# Les capacités numériques peuvent-elles participer à la dissuasion?

cahier de la pensée mili-Terre

Chef de bataillon Frédéric GERLINGER

publié le 26/10/2018

Sciences & technologies

**La multiplication, ces dernières années, des attaques dans le cyberespace, impliquant notamment de grandes puissances, appelle à s'interroger sur le rôle que pourraient jouer dans l'avenir les capacités numériques dans la dissuasion. L'objectif de cet article est de rappeler brièvement les fondements de la dissuasion nucléaire, d'étudier le potentiel du numérique dans le domaine de la dissuasion, avant d'analyser s'il est possible d'envisager la mise en œuvre d'une cyberdissuasion face à des attaques informatiques ou, de manière plus globale, éventuellement en complément de la dissuasion nucléaire.**

Le développement du numérique offre aujourd'hui de nouvelles opportunités aux États. En effet, le relatif anonymat dont disposent les acteurs du cyberespace[1] permet à nouveau d'envisager des opérations offensives tout en limitant les risques de représailles. Ce changement de paradigme pourrait ainsi être comparé à celui intervenu avec l'apparition de l'arme nucléaire dans les prémices de la guerre froide. Initialement envisagée pour des opérations offensives, l'arme nucléaire s'est peu à peu imposée comme un outil de dissuasion, permettant d'éviter les conflits directs entre les puissances nucléaires et de limiter les affrontements périphériques non pas en nombre, mais en intensité. La multiplication ces dernières années des attaques dans le cyberespace, impliquant justement ces grandes puissances, appelle à s'interroger sur le rôle que pourraient jouer dans l'avenir les capacités numériques dans la dissuasion. Certains États ont annoncé développer des moyens de cyberdéfense en vue de renforcer leur dissuasion. C'est le cas notamment du Royaume-Uni, qui considère Internet comme faisant partie intégrante du «champ de bataille» et, à ce titre, a revendiqué par l'intermédiaire de son ministre de la défense en 2011 la création d'une force de dissuasion cybernétique capable de protéger les installations stratégiques du pays contre des attaques terroristes[2]. En France, les forces armées ont également pris la mesure des enjeux futurs en créant récemment un commandement des opérations cyber et en développant les synergies avec le secteur civil. En parallèle, le ministère de la Défense doit procéder à un recrutement massif de «combattants numériques» pour atteindre en

2019 un effectif de 2.600, auxquels viendront s'ajouter 600 spécialistes de la DGA[3] et 4.400 réservistes[4] de cyberdéfense. Pour autant, le ministre français de la Défense, Jean-Yves Le Drian, déclarait le 12 décembre 2016[5]: «Je ne vois pas en quoi, en effet, l'arme cyber exercerait l'effet de retenue ou de dissuasion très spécifique que nous constatons et entretenons avec la dissuasion nucléaire. Et le mode de fonctionnement de la dissuasion nucléaire est profondément différent des batailles cyber. C'est la raison pour laquelle je rattache plus volontiers, dans nos modes de raisonnement, les problématiques cyber aux problématiques conventionnelles».

L'objectif de cet article est de rappeler brièvement les fondements de la dissuasion nucléaire, d'étudier le potentiel du numérique dans le domaine de la dissuasion, avant d'analyser s'il est possible d'envisager la mise en œuvre d'une cyberdissuasion face à des attaques informatiques ou, de manière plus globale, éventuellement en complément de la dissuasion nucléaire.

**Qu'est-ce que la dissuasion? Sur quoi repose-t-elle?**

Il paraît tout d'abord nécessaire de revenir sur la définition de la dissuasion avant d'en étudier ses fondamentaux. Pour le cas particulier de la France, le Centre interarmées de concepts de doctrines et enseignements des opérations rappelle que «la dissuasion est exercée pour la défense des intérêts vitaux de la France par la menace de provoquer, par l'emploi de tout ou partie de ses armes nucléaires, des dommages de toute nature, hors de proportion avec l'enjeu des intérêts mis en cause et, de ce fait, inacceptables pour tout adversaire qui voudrait leur porter atteinte»[6]. On peut ainsi distinguer deux formes différentes de dissuasion: soit par interdiction en mettant en place toutes les mesures possibles pour empêcher et convaincre un adversaire qu'il ne pourra pas atteindre ses objectifs, soit par représailles grâce à la menace que représentent les capacités nucléaires pour un adversaire qui chercherait à nuire aux intérêts vitaux de la nation.

Par conséquent, la dissuasion repose tout d'abord sur des capacités militaires crédibles. Elle nécessite à ce titre des éléments concrets qui ont pour objectif de persuader un agresseur potentiel qu'il subira avec certitude une riposte nucléaire en cas d'attaque. Les capacités nucléaires ont ainsi une double exigence: être visibles et ostentatoires par l'intermédiaire d'essais (nucléaires ou non), d'entraînements ou d'exercices[7] (c'est en France un des rôles des forces aériennes stratégiques), et être discrètes pour assurer la permanence de la menace nucléaire (c'est notamment le rôle de la force océanique stratégique). Mais la crédibilité de cette dissuasion repose également sur l'expression de la volonté politique par des signaux clairs, notamment la cohérence des budgets, la stratégie opérationnelle et la stratégie des moyens. En effet, la doctrine, les stratégies publiques de dissuasion et les déclarations des dirigeants politiques permettent d'afficher la volonté d'un État et ainsi de renforcer la crédibilité de sa dissuasion.

En dépit de la difficulté de connaître l'efficacité de la dissuasion ou le rôle de l'arme nucléaire dans la retenue entre grandes puissances, la plupart de celles-ci considèrent que leurs enjeux vitaux sont mieux défendus par son existence que par son absence ou son élimination progressive. La dissuasion nucléaire demeure cependant réservée à un nombre limité de puissances[8]. La démocratisation des capacités cybernétiques semble quant à elle pouvoir offrir à certains pays des capacités de dissuasion jusqu'alors inaccessibles.

**La cyberdissuasion, un potentiel intéressant?**

Le développement par certains pays de capacités numériques en vue de les intégrer dans une stratégie de dissuasion montre que cette théorie n'est pas totalement illusoire. En effet, l'apparition de nouveaux outils laisse entrevoir une possible utilisation de ces moyens dans le domaine de la dissuasion. Certaines opérations, telles que l'opération Olympic Game[9] visant les centrifugeuses iraniennes d'enrichissement d'uranium ou les récentes perturbations du réseau électrique ukrainien, montrent que des attaques informatiques peuvent provoquer de graves dégâts sur un système industriel. À ce titre, ces armes peuvent aujourd'hui être assimilées à des armes de destruction massive et disposer d'un véritable effet dissuasif. Les conséquences de telles attaques peuvent de plus être décuplées lorsqu'elles sont dirigées contre des pays fortement numérisés comme cela a été le cas en Estonie[10] en 2007. Ces exemples n'ont certes entraîné aucun dégât comparable à une riposte nucléaire, mais ils prouvent que, sans une certaine retenue des commanditaires, les conséquences auraient pu être catastrophiques. En outre, le cyberespace permet d'offrir une meilleure gradation des réponses face à une attaque. Cela permet à la fois d'élargir le champ d'application de la dissuasion, ne la cantonnant plus uniquement aux agressions les plus graves, et d'effectuer des avertissements avant une riposte plus importante.

De plus, alors que la dissuasion nucléaire est régulièrement remise en cause en raison de l'effort financier considérable qu'elle demande, la cyberdissuasion semble beaucoup plus abordable. Tout d'abord, d'un point de vue économique, les investissements nécessaires au développement de capacités de cyberdéfense ne sont en rien comparables avec l'effort budgétaire demandé par la dissuasion nucléaire. À titre d'exemple, la France consacre aujourd'hui environ 3 à 4 milliards d'euros par an à son outil de dissuasion alors qu'elle a annoncé investir dans le cadre du «pacte défense cyber» environ un milliard d'euros sur la période de la loi de programmation militaire 2014-2019. D'un point de vue industriel et technique, la maîtrise des moyens cybernétiques ne requiert ni les mêmes exigences ni le même niveau d'expertise que l'arme nucléaire. Enfin, si la ressource humaine demeure critique dans nombre de pays, les capacités numériques ne sont pas dépendantes d'un quelconque approvisionnement en matière première et peuvent donc être difficilement contrôlées ou limitées.

Enfin, d'un point de vue normatif, il n'existe aujourd'hui aucun traité de non-prolifération d'armes cybernétiques. Leur développement n'est en effet pas réglementé par le droit international et, à ce titre, un État peut se doter de ses propres capacités en vue de mettre en place une stratégie de cyberdissuasion sans craindre de sanctions économiques ou diplomatiques.

Ainsi, les capacités cybernétiques semblent en apparence pouvoir s'intégrer dans une stratégie de dissuasion et faciliter leur appropriation par de nouveaux acteurs qui en étaient jusqu'à présent exclus. Pour autant, le potentiel réel de la cyberdissuasion semble aujourd'hui toujours incertain.

**Peut-on envisager une cyberdissuasion globale?**

La mise en œuvre d'une stratégie globale de cyberdissuasion se heurte cependant toujours à des difficultés majeures. Tout d'abord, il n'existe aujourd'hui aucune arme cybernétique absolue capable d'être employée contre une cible inopinée sur court préavis. En effet, une arme numérique efficace, comparable à celle utilisée au cours de l'opération Olympic Game et capable d'infliger des dommages conséquents, nécessite

une préparation longue. À l'instar d'une opération militaire classique, une attaque informatique complexe demande une planification minutieuse, une collecte du renseignement exhaustive sur la cible et son environnement technique et humain, et enfin l'élaboration d'une arme spécifique qui devra ensuite être développée et testée pour démontrer son efficacité. À chaque cible correspond donc un mode d'action et une arme. Il est par conséquent difficile d'anticiper l'élaboration de ce type d'outil. Cela peut cependant être planifié en amont en identifiant des ennemis potentiels et des cibles à haute valeur ajoutée. Pour autant, ces armes s'appuient sur et exploitent des failles et des vulnérabilités de type «zéro day»[11] qui peuvent être découvertes et corrigées, rendant ainsi aléatoire voire inefficace le mode d'action choisi contre une cible donnée. Les moyens numériques ne peuvent donc garantir à un dirigeant politique la capacité d'infliger des dommages inacceptables avec certitude, à tout moment et sur court préavis à tout agresseur potentiel.

Pour être efficace, la dissuasion doit de plus persuader un ennemi qu'il encourt des représailles disproportionnées en cas de menace contre les intérêts vitaux d'une nation. Or, l'efficacité des capacités numériques repose entre autres sur la préservation du secret, notamment des moyens et des modes d'action choisis pour attaquer une cible. Cet exigence semble donc antinomique avec la crédibilité de la dissuasion, qui nécessite de montrer de manière ostentatoire ses capacités de représailles. L'arme cybernétique n'est de plus pas aussi effrayante que l'arme nucléaire, du moins pour l'instant. Il n'existe en effet aucun exemple à ce jour d'un «cyber Pearl Harbor» ou d'un «cyber 11 septembre» comme le prophétisait l'ancien secrétaire américain de la défense Léon Panetta en 2012. À ce titre, la cyberdissuasion ne pourra pas être crédible tant qu'un acteur du cyberespace n'aura pas démontré concrètement les capacités de destruction d'une arme cybernétique, comme cela avait été fait les 6 et 9 août 1945 pour l'arme nucléaire.

Enfin, même si des armes numériques complexes sont façonnées pour agir contre une cible particulière, le risque de dommages collatéraux ne peut être exclu. Le ver informatique Stuxnet a en effet infiltré des milliers d'ordinateurs dans le monde. Or l'interconnexion des réseaux et la dépendance de nos sociétés modernes au numérique nécessitent une utilisation des armes cybernétiques prudente et limitée. Un État ne peut se permettre de mettre en œuvre une riposte contre un agresseur et occasionner des dommages équivalents à un allié ou un partenaire. Les difficultés rencontrées pour maîtriser la propagation d'une attaque numérique et par conséquent limiter les dommages collatéraux semblent donc un nouveau frein au développement d'une cyberdissuasion globale.

Les capacités numériques ne semblent donc pas en mesure de répondre aux différentes exigences et fondamentaux de la dissuasion. À ce titre, l'arme nucléaire apparaît toujours comme le moyen le plus efficace et le plus sûr pour dissuader un agresseur étatique de menacer les intérêts vitaux d'un pays. On peut cependant étudier s'il est possible de mettre en œuvre une cyberdissuasion efficace permettant de prévenir des attaques informatiques destructrices.

**Peut-on utiliser la cyberdissuasion pour se prémunir d'attaques numériques d'ampleur?**

Nous distinguerons dans cette dernière partie les deux types de dissuasion: par interdiction et par représailles. Tout d'abord, rappelons que la cyberdissuasion doit empêcher les attaques sophistiquées capables de menacer les intérêts vitaux d'une

nation. Or, ces attaques bénéficient aujourd'hui du relatif anonymat qu'offre l'espace numérique et des difficultés rencontrées pour établir l'origine et attribuer ces agressions. En effet, même si le nombre d'acteurs disposant des capacités techniques, financières et humaines indispensables à la mise en œuvre d'attaques complexes de types APT[12] demeure limité, l'attribution[13] consiste en un processus long à l'issue incertaine. Les preuves accumulées au cours des investigations débouchent rarement sur une attribution formelle, laissant planer un certain degré d'incertitude. Les indices recueillis ne peuvent de plus pas toujours être communiqués, au risque de dévoiler des capacités sensibles. Le processus d'attribution consiste finalement en une décision politique, basée sur un certain nombre d'hypothèses et pouvant par conséquent souffrir d'un manque de légitimité sur la scène internationale.

Le cyberespace a de plus bousculé le jeu des alliances traditionnelles, comme l'ont démontré certaines révélations, notamment au cours de l'affaire Snowden. La confiance dans les alliés d'hier est aujourd'hui remise en cause. Le nombre d'acteurs à dissuader est ainsi démultiplié. Or, à la différence de la dissuasion nucléaire, la préparation d'une arme numérique dissuasive nécessite la désignation préalable d'un adversaire et d'une cible particulière. Cela confirme le dilemme de sécurité explicité par Ben Buchanan[14]. En effet, dans le domaine numérique, celui-ci est potentiellement plus intense dans la mesure où l'intrusion dans les réseaux des autres est un préalable nécessaire à la défense, voire à l'attaque préventive. Les risques de mauvaise interprétation et de crise de confiance entre partenaires sont par conséquent démultipliés.

Pour autant, si la dissuasion par représailles semble illusoire face à des attaques numériques complexes, il apparaît que la dissuasion par interdiction peut en partie expliquer l'absence d'un «Cyber Pearl Harbor». En effet, la mise en place de défenses actives et passives, toujours plus sophistiquées et efficaces, augmente le coût des attaques. À ce titre, les acteurs capables de s'introduire dans des systèmes d'information critiques dans le but de causer des dommages importants demeurent limités. De plus, si les investissements nécessaires pour préparer et conduire une attaque dépassent les gains espérés, la dissuasion par interdiction aura prouvé son efficacité.

En définitive, on constate que la cyberdissuasion par représailles demeure pour l'heure utopique. La retenue observée par les États lorsqu'ils utilisent des moyens numériques s'explique davantage par la crainte de créer un précédent. Cet équilibre, que l'on peut qualifier d'équilibre numérique, n'empêche en rien l'augmentation exponentielle d'agressions de moindre ampleur qui, en demeurant sous un certain seuil, n'entraînent aucune véritable riposte de la part des pays agressés. L'interconnexion des réseaux et la dépendance des sociétés modernes au numérique permettent également d'expliquer l'absence d'un «cyber 11 septembre». Même les attaques contre la sphère cognitive n'ont pas donné lieu à l'exercice de représailles massives. Cela signifie que l'on reste dans l'exercice de la proportionnalité en ce qui concerne la réponse. L'arme nucléaire continue par conséquent à jouer son rôle dissuasif. Les États tentent cependant de se prémunir des attaques informatiques en mettant en place une véritable dissuasion par interdiction et en menaçant les agresseurs de représailles au moyen de forces conventionnelles[15]. C'est d'ailleurs la posture française, rappelée par le ministre de la Défense le 8 janvier 2017 lors d'un entretien avec Le Journal du dimanche: «La France se réserve le droit de riposter par tous les moyens qu'elle juge appropriés. Cela peut passer par l'arsenal cyber dont nous disposons, mais aussi par des moyens armés conventionnels. Tout dépendra des effets de l'attaque».

[1] «Espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques». Défense et sécurité des systèmes d'information stratégie de la France, ANSSI, 2011.

[2] Bonnemaison Aymeric et Dossé Stéphane. «Attention cyber! Vers le combat cyber-électronique». Paris, Économica, 2014.

[3] Direction générale de l'armement.

[4] Soit 4.000 réservistes citoyens de cyberdéfense et 400 réservistes opérationnels.

[5] Discours prononcé à l'occasion de la visite de Jean-Yves Le Drian à la Direction générale de l'armement/Maîtrise de l'information (DGA-MI) dans le cadre de l'inauguration du pôle d'excellence cyber le 12 décembre 2016.

[6] Glossaire interarmées de terminologie opérationnelle, document cadre DC-004_GIATO (2013), N° 212/DEF/CICDE/NP du 16 décembre 2013, amendé le 1er juin 2015.

[7] Exemple de l'exercice MINOTAURE simulant un raid nucléaire des forces aériennes stratégiques en direction du Moyen-Orient en septembre 2015.

[8] États-Unis, Russie, France, Royaume-Uni, Chine, Inde, Pakistan. L'État hébreu n'a jamais officiellement reconnu la possession de l'arme nucléaire, et l'efficacité des capacités de la Corée du Nord doit encore être prouvée.

[9] Le ver informatique Stuxnet découvert en 2010 a probablement été conçu par la NSA en collaboration avec l'unité 8200 de l'armée de défense d'Israël en vue de ralentir le programme nucléaire iranien.

[10] L'Estonie a subi en 2007 une attaque prolongée de type «déni de service» contre des sites de l'administration, de banques et de journaux. Cette attaque, qui a perturbé le fonctionnement des institutions estoniennes pendant plusieurs semaines, semble avoir été lancée par des groupes d'activistes russes.

[11] Une vulnérabilité Zero day (en français: jour zéro) est une vulnérabilité informatique n'ayant fait l'objet d'aucune publication ou n'ayant aucun correctif connu (Wikipédia).

[12] APT: une Advanced Persistent Threat est une attaque informatique furtive et continue, souvent orchestrée par des «organisations» à des fins d'espionnage ou de sabotage. Une APT vise généralement une organisation pour des motifs d'affaires ou un État pour des motifs politiques (Wikipédia).

[13] L'attribution est un processus complexe consistant à recueillir des preuves techniques et environnementales en étudiant le contexte politique, économique, social et géopolitique d'une attaque. C'est l'ensemble de ces indices qui vont permettre à un décideur politique d'attribuer une agression à un État ou à un groupe avec un certain degré d'incertitude.

[14] Ben Buchanan, "The cybersecurity dilemma: hacking, trust and fear between nations", Londres: Hurst & Co., 2017.

[15] Également reprise par les États-Unis et le Royaume-Uni

Officier de l'armée de Terre, de la promotion «Général Béthouart» 2000-2003 de l'École spéciale militaire de Saint-Cyr, le Chef de bataillon GERLINGER a servi au 1er régiment d'artillerie de marine de Laon-Couvron, au régiment d'infanterie de marine du Pacifique Nouvelle-Calédonie et au Centre d'analyse technico-opérationnelle de défense de la Direction générale de l'armement. Breveté de la 23ème promotion de l'École de guerre (2015-2016), il est actuellement stagiaire au mastère spécialisé des Écoles de Saint-Cyr Coëtquidan «Opérations et gestion des crises en cyber-défense».

**Remerciements**

L'auteur remercie vivement M. Stéphane Taillat et M. Jean-Pierre Letanche pour leurs conseils judicieux et leur investissement.

**Bibliographie:**

- Ben Buchanan, "The cybersecurity dilemma: hacking, trust and fear between nations", Londres: Hurst & Co., 2017.
- BOYER, Bertrand. «Cybertactique: conduire la guerre numérique». Éditions Nuvis, 2014.
- Bonnemaison Aymeric et Dossé Stéphane. «Attention cyber! Vers le combat cyber-électronique». Économica, 2014.
- Kello Lucas, Richard Thomas, et al. «Les cyberarmes: dilemmes et futurs possibles», Politique étrangère, 2014, no 4, p. 139-150. Kempf Olivier, Introduction à la cyberstratégie. 2012.

- Kempf Olivier. «Introduction à la cyberstratégie». 2012.
- Boyer Bertrand. «Cyberstratégie: l'art de la guerre numérique». Nuvis, 2012.
- Lupovici Amir. «Cyber warfare and deterrence: trends and challenges in research». Military and Strategic Affairs, 2011, vol. 3, no 3, p. 49-62.
- Dogrul Murat, Aslan Adil et Celik Eyyup. «Developing an international cooperation on cyber defense and deterrence against cyber terrorism». Dans : Cyber conflict (ICCC), 2011 3rd international conference on. IEEE, 2011. p. 1-15.
- NATIONAL RESEARCH COUNCIL et al. «Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy». National Academies Press, 2010.
- Goodman Will. «Cyber deterrence: tougher in theory than in practice?» Senate (United States) Washington Dc, Committee on armed services, 2010.
- Libicki Martin C. "Cyberdeterrence and cyberwar". Rand Corporation, 2009.
- Power Marcus. «Digitized virtuosity: video war games and post-9/11 cyber-deterrence». Security Dialogue, 2007, vol. 38, no 2, p. 271-288.


**Titre :** Chef de bataillon Frédéric GERLINGER

**Auteur(s) :** Chef de bataillon Frédéric GERLINGER

**Date de parution** 10/10/2018