L'OTAN dans la cyberguerre : stratégie globale et capacités opérationnelles

mercredi 12 avril 2017, par Simon BALLARIN

Quelles sont les problématiques de la cyberdéfense de l'OTAN ? Simon Ballarin présente un tableau d'ensemble très utile pour saisir l'ampleur des défis de ce champ opérationnel particulier.

PERCEVOIR le rôle de l'OTAN dans la cyberguerre implique premièrement de bien définir et percevoir la problématique imposée. Le terme de « cyberguerre » demeure entouré d'un profond flou sémantique, s'inspirant plus volontiers d'un imaginaire de science fiction commun que d'une réalité scientifique. En effet, dans *Le Monde diplomatique*, Camille François, chercheuse au *Berkman Center for Internet and Society* de l'Université d'Harvard, explique ainsi que le terme 'cyberguerre' est utilisé bien improprement, car « aucun acte de violence informatique n'a encore déclenché un conflit armé » [1]. En ce sens, la belligérance numérique peut apparaître comme un questionnement récent, qu'elle s'inscrive dans un cadre national ou multilatéral. Plusieurs attaques informatiques, visant les réseaux de l'OTAN, se sont succédées et ont mené à un véritable processus de *mise sur agenda*des impératifs liés à la cyberdéfense. La forte médiatisation de ces différentes attaques a ainsi poussé le commandement otanien à intégrer la cyberdéfense dans sa chaîne opérationnelle. Plutôt qu'une chronologie commentée des différentes créations institutionnelles et sommets évoquant peu ou prou les problématiques de cyberdéfense, cet article tente d'interroger les différentes questions s'imposant à l'Alliance dans le domaine cybernétique. De même, cette approche n'étant pas un travail de spécialiste, les aspects politiques et stratégiques sont privilégiés face aux questions purement techniques, d'autant qu'une grande partie des documents scientifiques sont classifiés ou à diffusion restreinte. L'auteur a fait le choix de s'intéresser tout particulièrement aux enjeux d'une applicabilité des articles 4 et 5 sur la réponse collective du Traité de l'OTAN au cyberespace. Rappelons brièvement que les articles 4 et 5 fondent les principes de la défense collective, en affirmant qu'une attaque armée dirigée contre un des membres de l'Alliance constituerait une attaque contre tous les Etats-membres et pourrait mener à des représailles communes contre le pays à l'origine de l'agression. L'éventualité d'une riposte est en outre légitimée au sein de l'article 5 par le recours à l'article 51 de la Charte des Nations-Unies sur la légitime défense en cas d'agression armée. Considérons successivement les précédents et mise sur agenda des problématiques de cyberdéfense ; Le domaine cyber comme champ d'action opérationnel : aspects juridiques de référence ; OTAN et cyberguerre : les enjeux de la réponse collective ; De la difficulté à désigner l'ennemi dans le cadre du cyberespace ; enfin, les capacités opérationnelles.

> Pour mémoire, début 2017, l'OTAN compte 28 pays dont les Etats-Unis et le Canada mais aussi 22 des 28 Etats membres de l'Union européenne. Même après un "Brexit" effectif il y a fort à parier que le Royaume-Uni sorti de l'UE reste membre de l'OTAN.

Précédents et mise sur agenda des problématiques de cyberdéfense

La guerre du Kosovo de 1999 peut être perçue comme une première prise de conscience, marquée par le souvenir des attaques par *defacement* de la page Web du SHAPE et des attaques par *déni de service* contre le site de l'Alliance menées par des activistes serbes s'opposant aux bombardements de l'Alliance.

En 2007, des attaques DDOS visent les sites gouvernementaux estoniens, aboutissant à une paralysie totale de certains services administratifs pendant trois semaines. Attribuées à des hackers russes, il apparaît cependant délicat de prouver formellement le véritable responsable de ces attaques et surtout, leur commanditaire. En 2008, précédant l'attaque terrestre par les forces russes en Géorgie, une vaste opération cybernétique par déni de service a frappé la page web du président géorgien. Très rapidement, le Kremlin est perçu comme le commanditaire de l'attaque. Bien que concernant un pays non-membre de l'OTAN, l'attaque perpétrée contre la Géorgie a contribué à la mise sur agenda des problématiques de cyberdéfense et à la prise de conscience globale d'un *activisme croissant* visant les différents réseaux dans le cadre, ou non, d'un conflit armé. Dans les discours officiels portés, tant par les dirigeants de l'Alliance qu'au sein des textes de référence, les problématiques liées à la cyberguerre s'imposent dès lors dans la stratégie globale de l'OTAN qui a, « institutionnalisé la problématique de cyberdéfense en créant de multiples entités au sein des structures civiles et militaires » [2].

Le domaine cyber comme champ d'action opérationnel : aspects juridiques de référence

Les aspects juridiques demeurent primordiaux pour l'Alliance afin de lui permettre de définir une approche globale de sécurité dans le cadre *cyber*. Le *Manuel de Tallin,* publié en 2007, constitue le document de référence dans la définition des règles et normes établies dans la cyberguerre. Cependant, il s'agit simplement d'une interprétation qui ne saurait pour le moment présager d'une doctrine juridique officielle de l'OTAN. Ce texte normatif définit ainsi les opérations *cyber* comme des *attaques armées* et tente de transposer le droit international aux cyberconflits.

Dès lors, la première avancée fondamentale est de considérer que le droit international humanitaire et la Charte des Nations Unies s'appliquent dans le champ du cyberespace. Plusieurs points de consensus ont pu être définis par les experts mandatés, ainsi de la qualification d'emploi de la force, de la qualification d'agression armée et de la définition même de l'attaque *cyber*. *L'applicabilité* de l'article 5 sur la défense collective, issu du Traité de l'OTAN, au cadre cybernétique résulte ainsi de l'esprit du *Manuel de Tallinn*. Cependant, selon Olivier Kempf, chercheur associé à l'Institut des Relations Internationales et Stratégiques (IRIS), l'applicabilité de l'article 5, si elle existe en droit, pourrait ne pas se concrétiser *de facto* et s'apparente plus à une déclaration de principe, empreinte cependant d'une puissante portée symbolique. **L'objectif est donc de conserver une volontaire *ambiguïté* stratégique dans l'éventuelle réponse apportée**. En ce sens, Jamie Shea, adjoint aux Défis de sécurité émergents, préfère évoquer *'a case-by-case basis*' dans les potentielles représailles menées suite à une attaque cybernétique.

OTAN et cyberguerre : les enjeux de la réponse collective

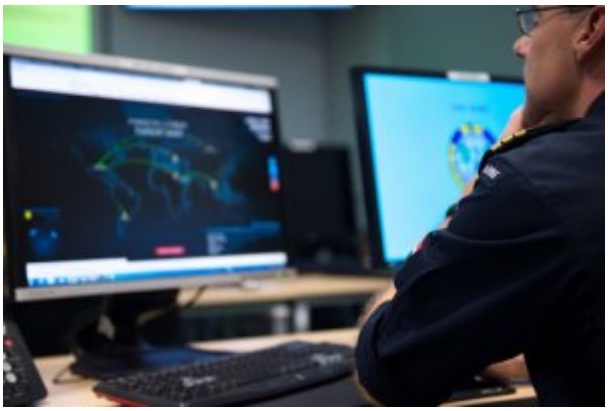
L'OTAN adopte, dans le cadre *cyber*, une stratégie purement défensive et tente avant tout de protéger ses propres réseaux et données. La notion de *dissuasion* demeure fondamentale dans la stratégie cyber de l'OTAN et rejoint la vocation de défense collective de l'Alliance. Vincent Joubert, chargé de recherche à la Fondation pour la Recherche Stratégique (FRS), dans une note de recherche de l'Alliance, pointe la nécessité de développer « un système de défense robuste avec des standards de sécurité améliorés, se concentrant sur la prévention, la résilience et la non-redondance ». A cette *deterrence by denial*, doit s'ajouter une *deterrence by punishment*, fondée sur une capacité à répondre très sévèrement à toute forme d'attaque *cyber*. Le rôle des États-Unis dans ce processus de dissuasion est explicite, les textes nationaux affirmant ainsi toute que forme d'acte hostile dans le cyberespace pourrait mener à des représailles collectives, relevant des articles 4 et 5 du Traité de l'OTAN [3]. La poursuite de ces deux types de dissuasion permet de maintenir une forme *d'ambiguïté* volontaire dans la stratégie otanienne. Cependant, cette interprétation équivoque des articles 4 et 5 peut se percevoir tant comme une volonté consciente et assumée de laisser toute forme d'agresseur potentiel dans un état *d'incertitude* sur les éventuelles conséquences d'une attaque contre les intérêts et les capacités cybernétiques de l'alliance,

mais aussi comme un manque de volonté politique et une incapacité chronique à assumer l'éventualité d'une réponse collective. Dès lors, cette ambiguïté manifeste pourrait conduire un adversaire potentiel à préférer, au sein de son *répertoire d'action*, une attaque de type cybernétique plutôt qu'une approche conventionnelle.

Certains experts proposent de transposer le concept stratégique MC 14/3, initialement destiné au risque nucléaire, au champ cybernétique, permettant de riposter, « soit au niveau choisi par l'agresseur, soit - au vu des enjeux du conflit et des intentions présumées de l'adversaire – de procéder à une escalade délibérée (symétrique ou asymétrique), soit d'exercer d'emblée des dommages majeurs à l'agresseur » [4]. Là encore, une transposition simpliste d'un concept stratégique au cadre cybernétique ne permet pas d'apporter une réponse absolument cohérente. En effet, le flou méthodologique actuel reste persistant dans la définition du *seuil*, pourtant primordial pour la mise en œuvre d'une réponse *proportionnée*, en l'absence d'outils de mesure objectifs et scientifiques [5]. Lucas Kello, *senior lecturer* en relations internationales à l'université d'Oxford, déplore en ce sens « l'absence de tables de conversion connues ou agréées qui pourraient guider l'application du principe d'équivalence » [6], ce qui complexifie d'autant plus la réponse potentiellement apportée, qui pourrait être perçue comme bien supérieure aux dommages causés par l'Etat visé, surtout si elle se déroule dans un cadre conventionnel.

De la difficulté à désigner l'ennemi dans le cadre du cyberespace

Une des caractéristiques majeures du cyberespace relève de la difficulté manifeste de *désigner l'ennemi* et renforce la difficulté juridique d'une réponse collective légalement justifiée. En effet, selon Didier Danet, professeur à l'ESM Saint-Cyr, « la combinaison continuum [Défense et Sécurité] / asymétrie / attaque conduit à une forme d'indistinction de l'adversaire (qui peut être un individu aussi bien qu'une puissance étatique) et qui est susceptible d'attaquer sans crainte de riposte ou de représailles les forces armées aussi bien que les intérêts vitaux ou la population d'un pays aussi bien protégé soit-il » [7]. Bien que l'auteur de l'article cité ait tenu à nuancer cette hypothèse, **la désignation de l'ennemi au sein du cyberespace pose un problème majeur**, notamment dans la possibilité d'applicabilité des articles 4 et 5. En effet, savoir si une attaque a été perpétrée par un groupe activiste ou une structure étatique nécessite des moyens conséquents d'analyse et une marge d'erreur existe, laissant ainsi une *imprécision* dommageable, d'autant que les capacités d'attaque *false-flag* peuvent être bien plus aisément réalisables dans le champ cybernétique que dans un cadre conventionnel. Il est, d'une part, extrêmement délicat de déterminer précisément l'origine d'une attaque, tant « les ramifications internationales des *botnets* (les réseaux d'attaques en déni de service) sont telles que toute cartographie des agissements dans le cyberespace se trouve vite soumise à des limites méthodologiques » [8]. D'autre part, s'il s'avère qu'une majorité des attaques est localisée dans un pays particulier, la désignation exacte du responsable et/ou commanditaire de l'attaque n'est pas évidente. Il est en effet malaisé de réussir absolument à « prouver les liens formels entre *state resident* et *state authority* dans le cas de cyberattaques » [9]. Dès lors, les difficultés dans la fourniture de preuves évidentes de la culpabilité d'un Etat commanditaire dans le domaine de l'attribution posent à l'OTAN des questions déterminantes dans l'optique d'une réponse collective.



Exercice de la Capacité d'intervention en cas d'incident informatique de l'OTAN (NCIRC), 2016
Copyright : OTAN, Edouard Bocquet 2016

Capacités opérationnelles

Les contraintes posées de plus en plus lourdement sur la sécurité de l'OTAN obligent, à travers les créations institutionnelles, au développement accru de capacités opérationnelles viables et efficaces. D'un point de vue purement opérationnel, les capacités de défense otanienne en matière de cybersécurité semblent relativement limitées. L'organe de contrôle centralisateur des capacités opérationnelles de l'OTAN est rassemblé au sein du programme *NCIRC* (NATO Computer Incident Response Capability), divisé en un siège à Bruxelles et un centre technique à Mons. Les missions confiées au NCIRC répondent à la volonté « d'assurer diverses tâches critiques, de la détection et de la prévention des virus informatiques et intrusions non autorisées dans les réseaux de l'OTAN à la gestion des dispositifs cryptographiques pour l'internet » [10]. Le NCIRC a aussi une vocation centralisatrice, afin non seulement de posséder un outil opérationnel de coordination à l'échelle otanienne, mais aussi d'éviter toute forme de duplication qui serait néfaste aux capacités de l'Alliance. La gestion de crise et l'urgence évidente inhérente aux différentes formes d'attaques informatiques revient aux *Rapid Reaction Team* (RTT). Les RTT doivent permettre une intervention et une gestion de l'attaque éventuelle en moins de 24 heures.

La création du *NATO Cooperative Cyber Defence – Centre of Excellence* (CCD-COE) double les capacités opérationnelles de l'Alliance d'une réalité conceptuelle et d'une capacité de formation et d'instruction des pays membres. L'élaboration des doctrines et concepts de l'alliance en matière de cyberdéfense, la formation des alliés par des stages et exercices réguliers, la recherche et le développement, le conseil aux différentes structures nationales et otaniennes ainsi que l'étude des différentes attaques passées afin de pouvoir fournir des Retours d'expérience (RETEX) détaillés constituent les principales missions de ce centre d'expertise.

En 2008, l'OTAN s'est aussi dotée d'une nouvelle autorité de coordination, la *Cyber Defense Management Authority* (CDMA), qui a vocation à fonctionner en parallèle avec le NCIRC, dans un but de « commandement central pour les activités techniques, politiques et de partage de l'information menées par les membres de l'Alliance, ainsi que diriger et gérer les entités de cyberdéfense de l'OTAN existantes ». Les capacités opérationnelles de l'OTAN s'inscrivent dans l'objectif de protéger uniquement les réseaux de l'Alliance. Cependant, une certaine imprécision entoure les potentialités d'aide aux États membres. En effet, les RTT peuvent envoyer des experts appuyer les capacités nationales dans certains cas, même si la sécurité des réseaux nationaux a vocation à être assurée par les Etats eux-mêmes, qui s'engagent ainsi à développer les moyens nécessaires pour la mise en œuvre de la protection globale des réseaux cybernétiques. En ce sens, « l'OTAN (…) s'emploiera donc, avec le concours des autorités nationales, à définir les principes et les critères garantissant un niveau minimum de cyberdéfense aux points d'interconnexion entre les réseaux des pays et ceux de l'OTAN » [11].

*

En conclusion, le rôle et les capacités de l'OTAN dans le domaine de la cyberdéfense demeurent encore imprécis. Si un consensus existe autour de la nature prioritairement défensive de l'Alliance dans ce domaine, deux blocs semblent se dessiner dans les objectifs à atteindre de la part de l'OTAN. En effet, la défense globale des réseaux de l'OTAN est un objectif largement partagé par l'ensemble des membres. Cependant, si les pays d'Europe balte, centrale et orientale souhaiteraient bien volontiers un rôle global élargi de l'OTAN, les puissances militaires, comme la France ou la Grande-Bretagne refusent d'accorder à l'OTAN un rôle trop volontariste dans la protection de leurs réseaux, au nom de la souveraineté et par crainte d'un potentiel effritement de leur indépendance nationale. Dans un système fondé sur une décision commune regroupant l'ensemble des Etats membres, la capacité à trouver un consensus politique demeure extrêmement problématique et freine toute forme d'intégration accrue, ce qui peut apparaitre bien dommageable pour certains petits Etats aux moyens nécessairement limités.

P.-S.

Etudiant en Master 2 Histoire militaire comparée, géostratégie, défense et sécurité à l'Institut d'Etudes politiques d'Aix-en-Provence.

Notes

[1] Camille François, « Penser la Cyberpaix », Le Monde diplomatique, avril 2016

[2] Joubert Vincent, Samaan Jean-Loup, « L'intergouvernementalité dans le cyberespace : étude comparée des initiatives de l'OTAN et de l'UE », Hérodote 1/ 2004 (n°152 – 153), p. 261 - 275

[3] « [w]ben warranterd, we [The United States] will respond to hostile acts in cyberspace as we would to any other threat to our country ». All states possess an inherent right to self-defence, and we reserve the right to use all necessary means -diplomatic, informational, military and econmic- to defend our Nations, our Allies, our partners, and our interests ». Department of Defense Cyberspace Policy Report, A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, section 934, November 2011,

[4] Gruselle Bruno, Tertrais Bruno, Esterle Alain, « Cyberdissuasion », Recherche et Documents, Fondation pour la Recherche Stratégique, mars 2012, N°03/2012

[5] NDLR : C'est dans la nature même de la dissuasion, nucléaire ou cyber, d'entretenir une incertitude sur les règles d'usage.

[6] Kello Lucas, Traduit de l'anglais par Richard Thomas, « Les cyberarmes : dilemmes et futurs

possibles », Politique étrangère 4/2014 (Hiver) , p. 139-150

[7] Danet Didier, « La stratégie militaire à l'heure des NTIC et du « Big Data » : quelles hypothèses structurantes ? » Revue internationale d'intelligence économique 2/2013 (Vol. 5), p 125 – 139

[8] Douzet Frédérick, Samaan Jean-Loup, Desforges Alix, « Les pirates du cyberespace », Hérodote 3/2009 (n°134), P,176 - 193

[9] Kulesza Joanna, State Responsability for Cyber-Attacks on International Peace and Security », 29 POLISH Y.B INT'I. (2009), 131 pp, 149-150

[10] Sverre Myrli, « l'OTAN et la cyberdéfense », Assemblée parlementaire de l'OTAN, Rapports de commission, 173 DSCFC 09 F bis, 2009

[11] Olivier Kempf, « l'OTAN et la Cyberdéfense », Sécurité globale, N°19, printemps 2012