Aspects juridiques internationaux de la cyberdéfense : premières vues.

Barbara LOUIS-SIDNEY[♣], Oriane BARAT-GINIES[♦], Cécile DOUTRIAUX[♠], EVE TOURNY[♥], Eric POMES[*], Jean-Yann MARIE-ROSE[#]

Octobre 2013 – Article n°III.11

Résumé : *Comme tout espace, le cyberespace, né de l'interconnexion des réseaux informatiques, est le siège de conflits. Ce cinquième champ de conflictualité, caractérisé par la multidimensionnalité, accroît, en les renouvelant, les menaces et les modes d'actions hostiles. Or, ces cyberattaques[1] ne possèdent pas encore de définition normative. Cette absence de définition et la nouveauté de ces attaques nécessitent de s'interroger sur leur qualification au regard à la fois du jus ad bellum et du jus in bello.*

Le cyberespace est né de l'accroissement des interconnexions des réseaux informatiques mondiaux. Certains y voient un nouveau territoire, un nouvel espace au sens géographique. Son importance est telle qu'il serait aujourd'hui devenu le 5ème champ de conflictualité après la terre, la mer, l'air et l'espace. Malgré une réalité évidente le cyberespace fait difficulté pour les juristes. Aucune définition normative n'a été pour l'heure arrêtée dans un instrument de droit international.

Tentative de qualification du cyberespace

Avant d'établir une définition, déterminer sa composition parait judicieux. Le cyberespace ne serait pas un environnement unique mais un espace composé de plusieurs dimensions.
La première dimension, souvent négligée, est physique. Elle englobe les infrastructures du réseau de réseaux qu'est Internet (serveurs racines, bases de données, satellites, câbles sous-mains, fibres optiques, les ordinateurs, câbles et disques durs…) Ces infrastructures sont souvent critiques. Vient ensuite la dimension logique. Celle-ci comprend les logiciels et protocoles du réseau. Elle constitue la cible principale des attaques informatiques. Enfin, on trouve la dimension cognitive qui se compose de

♣ Doctorante en droit.
♦ Docteur en droit.
♠ Avocate, officier de la réserve citoyenne de la gendarmerie et surtout membre de la chaire cyberdéfense des écoles de St-Cyr.
♥ Docteur en droit.
* Docteur en droit, Institut Catholique d'Etudes Supérieures, chercheur associé au CERDES, EA n°3180, Université de Nice Sophia Antipolis et au CREC Saint Cyr.
# Officier de l'Armée de Terre. Chargé d'études en Droit des Conflits Armés Droit et nouvelles technologies Direction des Affaires Juridiques Ministère de la Défense.
1. Le groupe de travail recourra aux termes opération cybernétique ou attaque non cinétique. L'expression cyberattaque a, en effet, été utilisée de manière excessive la vidant quelque peu de son sens. Mais surtout, ce terme renvoie à la fois à l'action et au moyen (virus...) Il convient donc de distinguer l'action du moyen d'action. D'autre part, elle n'a pas de réalité juridique : les juristes utilisent agression armée (dans le *jus ad bellum*), et d'attaque (dans le *jus in bello*).

l'ensemble des données, des informations, du contenu circulant au sein du réseau. Ces trois dimensions font du cyberespace une entité protéiforme complexe à appréhender.
Pour les besoins de l'étude la définition du cyberespace proposée par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) pourrait être retenue car elle a le mérite de synthétiser ces trois axes. Le cyberespace est défini comme un « *espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques* ».
Espace de communication et d'échange généralisé, le cyberespace est le support ou la cible de nombreux actes hostiles et/ou illicites commis par des Etats, des groupes ou des particuliers. Comment le droit appréhende-t-il ces actes ? La réflexion portera principalement sur le domaine de la cyberdéfense et plus particulièrement la définition de cyberattaque[2]. La cyberguerre, notion non validée en terme juridique au niveau international constitue, après « la guerre économique » et la « guerre contre le terrorisme », le nouvel avatar de la conflictualité contemporaine. Chacun de ces termes souffre cependant de la même absence de définition normative.

Cyberespace et recours à la force

Pourtant, la littérature scientifique[3] comme les médias laissent penser que ces actes sont courants. Les attaques cybernétiques peuvent être regroupées en trois catégories selon leur forme. Tout d'abord, il y a les attaques ciblant les données numériques, leur exploitation, leur extraction, leur destruction ou leur corruption comme l'envoi d'un fichier corrompu destiné à récupérer des données importantes ou à détruire les répertoires d'un disque dur. Ensuite, il y a les attaques visant les systèmes d'information et de communication afin de les identifier et permettre ainsi de détecter leurs failles et de pouvoir ainsi les attaquer en perturbant leur fonctionnement, de façon temporaire ou définitive. Enfin, il y a des attaques visant, à travers le cyberspace, des équipements, des infrastructures ou des installations critiques hors du cyberspace dont le but est de perturber leur fonctionnement ou de les détruire. Ce risque est d'autant plus important dans un contexte d'accroissement et de généralisation de l'usage d'Internet à l'échelle internationale (taux de pénétration Internet de plus en plus importants, efforts de réduction de la fracture numérique, multiplication des usages mobiles et des objets connectés, mais aussi connexion au réseau Internet - délibérée ou non - d'infrastructures sensibles, vulnérabilités informatiques omniprésentes, dématérialisation, etc.). Les « attaques » menées par l'entremise des virus *Stuxnet*, *Flame*, *Shamoon* ont montré que ces actes dont le mode opératoire use de moyens « virtuels » ou numériques pouvaient avoir des répercussions dans le monde physique. Aussi, ils font peser des risques réels sur les Etats (et leurs actions militaires) et sur les personnes privées (physiques ou morales), tant en période de conflit qu'en temps de paix.

Loin de toute vision catastrophiste, quel regard le juriste peut-il porter sur ces faits ? Leur nature et leur milieu de réalisation, le cyberespace, font naître deux visions antinomiques. La première estime qu'il s'agit d'une évolution telle que le droit existant serait inapplicable ; l'adoption de nouvelles normes adaptées au cyberespace serait nécessaire. L'autre, au contraire, estime pouvoir l'appliquer à ces faits (vision interprétative).

La première vision doit être rejetée car elle s'appuie sur une conception du cyberespace à la fois utopique et fausse. Elle considère en effet que celui-ci serait totalement détaché du réel formant ainsi un nouveau milieu naturel s'ajoutant aux espaces terrestre, maritime et aérien[4]. Or, le cyberespace d'une part n'est pas naturel, il est une création humaine et d'autre part les effets qui s'y produisent ont également des conséquences dans l'espace physique[5]. L'apport de cette vision est toutefois de

[2]. Voir par ex. *Tallinn Manual on the International Law Applicable to Cyber Warfare*.
[3]. S. J. SHACKELFORD, « From Nuclear War to Net War: Analogizing Cyber Attacks in International Law », *Berkley Journal of International Law*, 2008, vol. 25, n° 3, pp. 191-250.
[4]. D. R. JOHNSON, D. G. POST, « Law and Borders - The Rise of Law in Cyberspace », *Stanford Law Review*, 1996, vol. 48, pp. 1367-1402.
[5]. C. ROJINSKY, « Cyberespace et nouvelles régulations technologiques », *D.*, 2001, Chron., p. 844.

souligner la nécessité de repenser certains principes cardinaux du droit international : souveraineté, principe de territorialité…

'il est acquis que le vide juridique n'existe pas, l'application de normes telles quelles dans le cyberespace sans tenir compte de ses spécificités serait une erreur.
Ses spécificités sont son caractère transfrontières (absence de frontières dans ses dimensions cognitives et logiques), son omniprésence sur plusieurs espaces naturels (terre, air, mer, espace extra atmosphérique), la volatilité et rapidité des échanges, la dualité des applications, etc.
Ainsi, par exemple, la régulation des cyberarmes parfois évoquée ne saurait se faire par simple application des règles existant pour le contrôle des armes classiques. Ceci en raison de l'usage dual d'un code : comment en effet distinguer clairement un code malveillant d'un code conçu pour la recherche, quand seule leur finalité ou leur usage caractérise une éventuelle nature « armée » ?

De la même manière, la qualification de la cyberattaque au regard du droit international pose de vraies difficultés dès lors que les notions et institutions en cause ont été pensées pour des attaques cinétiques[6].
Plusieurs qualifications peuvent donc être imaginées :

- usage de la force
- mesures de police

L'article 2 par. 4 de la Charte des Nations Unies interdit le recours à la force armée contre un autre Etat et l'article 51 n'autorise le recours à la légitime défense qu'en cas d'agression armée[7]. Or, dans deux actions cybernétiques du mois d'août 2012 (l'entreprise d'Etat saoudienne *Saudi Aramco* (le 15), et *RasGas* (le 30), entreprise d'Etat qatarie, ont été victimes d'un nouveau virus, *Shamoon*, qui s'attaque aux ordinateurs et à leurs disques durs), il n'y a eu à aucun moment de recours à la force armée entendu comme des opérations cinétiques (bombardements…). L'objectif de l'action consistait à détruire le parc informatique des entreprises visées par l'utilisation d'un virus c'est-à-dire un programme qui effectue des opérations sur l'ordinateur qui l'héberge (modification ou destruction de données). Il n'y a donc pas d'utilisation de la force armée mais de codes qui n'ont pas eu en l'espèce de véritable prolongement dans le monde physique. La qualification d'agression armée ne peut donc être retenue.

Est-il pour autant possible de conclure définitivement que seules des mesures physiques peuvent être qualifiées de force armée[8] ? Une telle interprétation doit aujourd'hui être relativisée dès lors que des mesures immatérielles peuvent potentiellement provoquer des dommages aussi importants que des mesures physiques. La Cour Internationale de Justice dans son avis de 1996 *Licéité de la menace ou de l'emploi d'armes nucléaires*, en examinant les dispositions relatives à l'usage de la force, a d'ailleurs précisé que « [c]es dispositions [articles 2 par. 4, 42, 51 de la Charte] ne mentionnent pas d'armes particulières. Elles s'appliquent à n'importe quel emploi de la force, indépendamment des armes employées » (par. 39). Une arme s'entend de « toutes choses, toutes matières et tous objets, de nature physique, chimique ou biologique, employés dans les opérations de combat pour réaliser une atteinte à la vie, à l'intégrité physique, à la santé, ou, d'une façon générale, à l'état physiologique ou psychique des personnes ennemies, ou à l'intégrité physique des biens de l'ennemi ». En somme, si la nature « virtuelle » de ces attaques pourrait conduire à ne pas considérer les « codes » comme des armes, il découle de notre réflexion que les programmes informatiques malveillants (et plus généralement les cyberattaques, une cyberattaque pouvant découler d'un acte physique comme la destruction d'un câble sous-marin) ne peuvent être d'emblée exclus de la qualification de mesures

[6]. P. WALKER, « Rethinking Computer Network 'Attack': Implications for Law and U.S. Doctrine », *Journal of National Security Law & Policy*, 2011, vol. 1, n°1, pp. 33-67.
[7]. M. ROSCINI, « World Wide Warfare - 'Jus Ad Bellum' and the Use of Cyber Force », *Max Planck Yearbook of United Nations Law*, 2010, vol. 14, pp. 85-130.
[8]. M. C. WAXMAN, « Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4) », *Yale Journal of International Law*, 2011, vol. 36, pp. 421-459.

« armées »[9]. Il convient plutôt de les analyser au regard de deux critères[10]. Le premier, subjectif, consiste à se demander si ces mesures visent l'Etat. Toutefois, ceci est insuffisant pour être constitutif d'un recours à la force armée. Il convient, dans un second temps, que la mesure dépasse un certain seuil : c'est le critère objectif. Au-dessous de ce seuil, les mesures pourraient être qualifiées de mesures de police violant la souveraineté de l'Etat et ne pourraient être justifiées que dans la mesure où l'Etat auteur puisse démontrer qu'il se trouve dans l'une des circonstances excluant l'illicite. Au-delà de ce seuil ces mesures immatérielles constitueraient un recours à la force armée ne pouvant être justifié que par une autorisation du Conseil de sécurité ou la légitime défense[11]. Aussi le choix de la qualification entre mesure de police ou recours à la force armée pourrait reposer sur la gravité des conséquences de ces attaques présumées.

Mais surtout la discrétion de la plupart de ces actions pose des questions quant à l'attribution de ces actes. Comment prouver ces actes et les relier à des Etats ou à des groupes ?

Des réponses apportées à ces interrogations dépendent les réponses juridiques à ces attaques. Une piste de réflexion est de considérer non une unicité de qualification mais une pluralité de qualification selon le type d'attaque. Aussi la réponse ne pourra être identique et devra s'adapter selon le type d'attaque.

*
* *

De ce qui précède découle plus de questions que de réponses. En premier lieu qu'est-ce qu'une cyberattaque ? Comment positionner la cyberattaque au sein de la notion traditionnelle de conflit armé international[12] ? Une telle attaque constitue-t-elle le premier acte d'un conflit armé ou plutôt une nouvelle manière de mener les hostilités ? Comment appréhender la cyberattaque n'ayant que des effets « virtuels » et non physiques ? Comment riposter légalement ? Comment répondre de la manière la plus appropriée, avec les moyens (régaliens) dont nous disposons ? Comment éviter les erreurs d'interprétation et la disproportion dans les réponses à donner ?
Comment identifier son auteur, et quel statut lui attribuer[13] ? Cette question se pose d'autant plus avec l'émergence de pirates informatiques « patriotes » se réclamant des Etats ou des hacktivistes[14].
Quid de la neutralité des Etats dans le cyberespace[15] ? Quid de la responsabilité des Etats ? Faut-il repenser la souveraineté ? Faut-il repenser le droit ou simplement le réinterpréter à la lumière de la donne informatique et d'Internet ?
Cette liste - non exhaustive et destinée à s'enrichir - de questions, constitue une ébauche de ce que sera la feuille de route de ce groupe de travail dédié aux aspects juridiques de la cyberdéfense.

---

[9]. R. KOLB, *Ius contra bellum. Le droit international relatif au maintien de la paix*, Bruxelles, Bruylant, 2003, p. 172.
[10]. O. CORTEN, *Le droit contre la guerre. L'interdiction du recours à la force en droit international contemporain*, Paris, Pédone, 2008, p. 65 et sq, Y. DINSTEIN, « Computer Network attacks and Self-Defense », *International Law Studies, Naval War College*, 2002, vol. 76, pp. 99-120.
[11]. M. HOISINGTON, « Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense », *Boston College International and Comparative Law Review*, 2009, vol. 32, pp. 439-454.
[12]. M. N. SCHMITT, « Wired Warfare: Computer Network Attack and jus in bello », *ICRC*, 2002, vol. 84, n° 846, pp. 365-399.
[13]. S. WATTS, « Combatant Status and Computer Network Attack », *Virginia Journal of International Law*, 2010, vol. 50, n° 2, pp. 391-447.
[14]. L'hacktivisme est l'utilisation non violente des nouvelles technologies de l'information et de la communication, par des activistes, pour diffuser leurs revendications politiques.
[15]. E. T. JENSEN, « Sovereignty and Neutrality in Cyber Conflict », *Fordham International Law Journal*, 2012, vol. 35, pp. 815-841.

Fondation Saint-Cyr, Ecole militaire, 1 place Joffre, 75007 Paris

Téléphone: 01-45-55-43-56 - courriel: contact@chaire-cyber.fr; SIRET N° 497 802 645 000 18

La chaire remercie ses partenaires