Conflits armés non internationaux et « nouveaux conflits »
IVème Cours international pour la formation des aumôniers catholiques militaires au Droit international humanitaire
Conseil Pontifical Justice & Paix
Rome 26 & 27 octobre 2015

Nicolas ARPAGIAN
Directeur scientifique du cycle « Sécurité Numérique » à l'Institut National des Hautes Etudes de la Sécurité et de la Justice (INHESJ), France.
Directeur de la stratégie, Orange Cyberdefense.
Auteur, notamment, de « La Cybersécurité », Presses Universitaires de France (2015).
Site : www.arpagian.eu

La guerre cybernétique

La société de l'information se caractérise par la diffusion croissante et continue des systèmes d'information dans nos organisations personnelles, professionnelles, qui sont toutes affectées par l'introduction de l'informatique. Pour créer, stocker, analyser et le cas échéant détruire des données. Nous devons l'apparition du mot « cybernétique » à Norbert Wiener, enseignant au *Massachusetts Institute of Technology* (MIT) qui dans un livre[1] paru en 1948 établit cette définition de ce terme qui désigne « le champ entier de la théorie de la commande et de la communication, tant dans la machine que dans l'animal ». Il puise sa racine du grec *kuberneïn* qui signifie « diriger ».
Avec l'instauration et le déploiement du cyberespace, nous sommes entrés concrètement dans l'ère de la « Nouvelle Frontière », telle qu'elle a été décrite par John F.Kennedy le 15 juillet 1960 dans son discours[2] d'acceptation d'investiture à la Convention du Parti démocrate :

« Mais je vous dis que nous sommes devant une Nouvelle Frontière, que nous le voulions ou non. Au-delà de cette frontière, s'étendent les domaines inexplorés de la science et de l'espace, des problèmes non résolus de paix et de guerre, des poches d'ignorance et de préjugés non encore réduites, et les questions laissées sans réponse de la pauvreté et des surplus »

La guerre cybernétique va donc intégrer les usages offensifs et défensifs de ces systèmes d'information dans le cadre de l'affrontement entre les nations. En ciblant les infrastructures militaires mais également les équipements administratifs, économiques, financiers, industriels et sociaux.
Ce mode d'agression tous azimuts conduit à considérer de nouveaux paradigmes et à identifier de nouvelles problématiques qu'il conviendra de résoudre. Pour répondre à l'exigence de synthèse de ce cours nous allons nous limiter à l'énoncé de ces éléments. Naturellement chacun de ces items justifie à lui seul une réflexion plus élaborée qu'il

[1] Norbert Wiener, *Cybernetics*, Paris, Hermann, 1948.
[2] Texte intégral du discours disponible sur le site de la Bibliothèque John F. Kennedy : http://www.jfklibrary.org/Asset-Viewer/AS08q5oYz0SFUZg9uOi4iw.aspx

conviendra de mener lors de séances ou de contributions futures. Ce sont là des pistes de réflexion pour bâtir une approche renouvelée et réaliste de la guerre à l'ère numérique.
Avec l'avènement de la société numérique, c'est la notion même de frontière qui est remise en cause. Les domaines autrefois bien définis par des contours admis de tous deviennent poreux. Modifiant *de facto* le droit applicable, les précautions à prendre, les populations impliquées et les conséquences géopolitiques. Une redéfinition menée tambour battant : à la vitesse de la diffusion des technologies et des outils numériques. Quand Internet devient la scène mondiale et l'économie de la donnée la nouvelle source de création de valeur, cela bouleverse l'équilibre des puissances. Et redessine des frontières installées au début de l'ère industrielle.

I. Les quatre nouveaux paradigmes de la frontière nés de la guerre cybernétique

1) La frontière entre la paix et la guerre.

La première déclaration de guerre formelle de la part d'un Etat remonte à la Renaissance. Depuis lors, notamment avec la Convention de La Haye de 1899, les Etats ont veillé à codifier cette entrée dans la guerre. Les gouvernements ont ainsi édicté des procédures établissant les trêves, les armistices et les capitulations. De même que les traités de Paix formalisent les conditions dans lesquels les belligérants mettent un terme à leur conflit. Rien de tel dans le cyberespace où les assauts sont insidieux. On ne débute ni ne clôt officiellement une vague de cyberattaques. Seules les pénétrations informatiques qui commettent des dégâts (vol de données, destruction ou blocage d'équipements, détournement de fonds…) signalent la commission de tels actes. Les chancelleries ne tiennent fondamentalement pas à ce que le recours à ces arsenaux numériques fassent l'objet d'une procédure juridique trop formelle. La proposition formulée en février 2010 lors du Forum de Davos par Hamadoun Touré, secrétaire général de l'Union International des Télécommunications (UIT) d'élaborer un traité international interdisant les cyberattaques n'a reçu qu'un accueil diplomatiquement poli. Quelques années plus tard, après les révélations du consultant Edouard Snowden en 2013 et de nombreuses cyberattaques ayant visé des gouvernements et des multinationales, la situation évolue peu. En septembre 2015, Pékin et Washington ont entrepris d'établir un pacte de non-agression[3] dans le cyberespace. Mais sans que le détail de ses critères d'application ni les sanctions encourues en cas de non-respect de celui-ci soient connus. Loin d'une discussion multilatérale, on semble s'orienter vers des négociations bilatérales entre puissances qui savent chacune ce qu'elles ont à craindre de l'autre. La construction d'un arc de triomphe incarnant une victoire numérique ou l'établissement d'une paix durable dans le cyberespace n'est pas prête de débuter.

2) La frontière entre les mondes civils et militaires.

Le Droit International Humanitaire et le Droit des Conflits Armés ont permis d'établir des distinctions dans le traitement qui doit être réservé aux populations civiles lors d'un conflit. Rien de cela en matière de cyberguerre où les cibles non militaires ne bénéficient d'aucun traitement privilégié. Les banques, les entreprises, les hôpitaux, les particuliers, les universités ou les écoles sont visées régulièrement par des cyberattaques. Afin d'amplifier les

[3]« U.S. and China Seek Arms Deal for Cyberspace », *The New York Times*, David E.Sanger, 19th september 2015 - **http://www.nytimes.com/2015/09/20/world/asia/us-and-china-seek-arms-deal-for-cyberspace.html?partner=rss&emc=rss&_r=1**

dysfonctionnements dans le pays ciblé ou pour accroître l'exposition médiatique de l'agression. Comme ce fut le cas en 2007 lorsque le tissu économique de l'Estonie fut temporairement mis hors d'état de fonctionner après une campagne informatique de grande ampleur. La porosité entre les mondes civil et militaire se constate également de la part des équipementiers. La notion de « complexe militaro-industriel » s'étend désormais bien au-delà des fabricants de missiles, d'hélicoptères de combat ou de chars d'assaut. Par exemple, aux Etats-Unis, les géants privés du numérique ou GAFAM (Google, Apple, Facebook, Amazon, Microsoft…) travaillent largement en osmose avec la sphère gouvernemental. En mars 2015, le quotidien économique *The Wall Street Journal*[4]explique comment l'état-major de Google a bénéficié d'une rencontre par semaine à la Maison Blanche depuis le début de la Présidence Obama. Et Eric Schmidt, Executive Chairman d'Alphabet, le nouveau nom de la société qui gère le moteur de recherche Google, siège au très officiel *Office of Science and Technology Policy* (OSTP)[5] placé auprès du Président des Etats-Unis. Des illustrations de cette proximité existent avec tous les acteurs de la SiliconValley. Qui, si on met de côté les activités financées par le fonds de la CIA, In-Q-Tel[6], ou par l'Agence ministérielle pour les projets avancés de recherche en matière de défense (DARPA)[7], sont avant tout des sociétés commerciales n'ayant pas d'activité directe liée à la Défense ou à la sécurité nationales. Mais leur savoir-faire et leur expertise numériques sont souvent au cœur des missions de protection des intérêts stratégiques. Ces firmes au déploiement largement international conservent donc un fort ancrage national.
Enfin, on voit de plus en plus d'individus isolés prenant quelques heures de leur temps ou mettant temporairement leur maîtrise des technologies au service d'une cause. Licite ou non. Ce ne sont pas des combattants aguerris ou coalisés mais ils donnent de l'argent via des financements participatifs, mettent à la disposition d'une cause la puissance de calcul de leur ordinateur voire participent à des opérations en déni de service pour paralyser les équipements informatiques de leur adversaire. Ils peuvent le faire de chez eux, sans se connaître ni se déplacer. Quel statut pour ces activistes à temps partagé ? Leur engagement peut être limité à certains sujets, et ne durer que quelques heures en fonction de leurs disponibilités familiales ou professionnelles. Doit-on leur attribuer le statut de combattant ? Sont-ils toujours de simples civils ?

3) La frontière entre les mondes physiques et technologiques.

La technologie est sans frontières. Il suffit de quelques secondes pour déplacer des fichiers d'un ordinateur à un autre et donc possiblement d'un pays à un autre. En plus ce n'est pas parce que l'origine d'une attaque informatique a été localisée dans un pays, que l'on peut déterminer avec une certitude absolue cette identification. Il peut s'agir d'un énième rebond technique pour leurrer les pisteurs informatiques. Et cela ne signifie pas que les autorités du pays en question sont nécessairement informées que l'action en question part de leur territoire. Ni qu'elles ont donné leur accord pour cela. C'était plus fréquemment le cas lorsqu'on avait à faire à des armées physiques. La localisation n'implique donc pas *de facto* la responsabilité du pays dans lequel se trouvent les auteurs présumés de l'attaque informatique. Il n'y a pas de lien systématique. Cela est important à prendre en compte dès lors qu'une riposte serait envisagée.

[4] http://www.wsj.com/articles/google-makes-most-of-close-ties-to-white-house-1427242076
[5] Site officiel de la Maison Blanche : https://www.whitehouse.gov/administration/eop/ostp/pcast/about/members
[6] Site officiel d'In-Q-Tel : https://www.iqt.org/
[7] Site officiel de la DARPA : http://www.darpa.mil/

4) La frontière entre les domaines stratégiques.

Au regard de la guerre dans le cyberespace, les industries d'armement deviennent moins stratégiques. Tandis que les serveurs informatiques, les équipements en télécommunications et la maitrise des logiciels s'avèrent cruciaux. A quoi bon avoir un système d'arme élaboré si l'informatique qui le fait fonctionner peut être piraté ou ses outils de commande déréglés à distance. Les frontières entre les industries stratégiques se redessinent. La souveraineté trouve désormais sa source chez des industriels du numérique. Or, tous les pays ne disposent pas de telles sociétés. Ou sont dépendants de certaines technologies pour faire fonctionner leurs arsenaux et leurs industries vitales. Chaque Etat doit donc s'interroger sur sa capacité à disposer des ressources techniques lui permettant de rester maître de l'établissement et de l'application de sa stratégie. Et cela dans les domaines de la Défense et de l'économie en général (flux financiers, moyens de communications, traitement des eaux, énergie, santé, transports…).

II. Les neuf nouvelles problématiques nées de la guerre cybernétique

1) L'imputabilité de l'attaque.

Lorsqu'une cyberattaque est constatée, se pose la question d'en identifier les auteurs. Pour que des sanctions soient prises et des responsabilités mises en cause. Il s'agit donc de disposer de l'expertise technique pour rassembler les éléments permettant de remonter le cheminement informatique ayant conduit à la cyberagression. Comment être sur d'être remonté effectivement à la source ? Tout dépend de la coopération internationale. Comment s'assurer d'éléments de preuve non contestables ? Quels moyens mettre en œuvre pour collecter ces données ? Sachant que l'on ne pourra pas en déduire que ces agissements ont été nécessairement organisé ou facilité par l'appareil d'Etat dudit pays. Qui pouvait même en ignorer l'existence.

2) Le statut de victime.

Une attaque informatique peut se dérouler à l'insu de sa cible, qui ignorera donc son statut de victime. C'est par exemple le cas lorsqu'une intrusion informatique vise à intercepter des communications ou à dérober des données. L'assaillant a intérêt à agir le plus discrètement possible vis à vis de sa cible afin que celle-ci ne se doute de rien et ne change rien à ses procédures. Et ne tente pas de l'intoxiquer avec des informations délibérément fausses.
Lors d'une cyberguerre, les cibles ne sont pas que militaires : les entreprises, les administrations, les infrastructures médicales ainsi que les services aux particuliers peuvent également être atteints.
Le traumatisme, notamment au sein de la population, peut être largement différé après l'attaque. Et ne survenir que lorsque l'agression a été constatée. Il convient de prendre en compte ce possible décalage dans le temps entre l'offensive numérique et le ressenti de son impact dans l'opinion publique. La crise médiatique et politique venant alors étoffer le dommage subi par la seule cyberattaque.

3) La nature de la riposte.

Une fois connue, la cyberattaque peut susciter l'envie de riposte. Mais cela pose quatre questions majeures.

- **La proportionnalité :** dès lors qu'on n'est pas sûr d'avoir toute la mesure de l'ampleur de l'attaque, en fonction de ce qui a pu être identifié, comment doser la riposte ?
- **La simultanéité :** quand considère-t-on que la cyberattaque est survenue ? Quand elle a été initiée ou lorsque ses effets se sont fait sentir ? Ce qui pose la question d'une riposte plusieurs mois ou années après une attaque informatique élaborée pour se déclencher après une certaine durée.
- **L'imputabilité :** pour riposter il faut savoir désigner une cible. Comment est-on certain d'avoir déterminé les auteurs de l'attaque ? Si des ordinateurs de particuliers ont été mis à contribution à leur insu pour conduire l'opération, peuvent-ils faire l'objet d'une riposte ?
- **La nature même de la riposte.** Dès 2009, des hauts fonctionnaires de la Défense aux Etats-Unis ont estimé qu'une cyberattaque pouvait susciter une réponse militaire conventionnelle. Et en 2011, Washington a officiellement reconnu qu'une cyberattaque pouvait être assimilée à un acte de guerre[8]. Au-delà de cette affirmation solennelle se pose donc l'appréciation de l'ampleur et de la nature de l'action qui viendrait sanctionner une agression numérique.

4) L'absence de Droit International du cyberespace.

Il n'existe qu'un seul texte de dimension internationale dans le cyberespace : la Convention de Budapest [9] de novembre 2011 relative à la cybercriminalité. Malgré les tentatives diplomatiques dans le cadre des Sommets mondiaux sur la Société de l'Information (SMSI)[10] organisés par l'Union International des Télécommunications en 2003 à Genève et en 2005 à Tunis. Depuis lors, ces réunions internationales n'ont abouti sur rien de concret. Comme si les Etats se complaisaient dans ce morcellement juridique et institutionnel qui les met à l'abri d'investigations trop poussées quant à leurs agissements dans le cyberespace. Interpol, Europol et Eurojust s'organisent pour faciliter la coopération policière et judiciaire. Mais leurs procédures et leurs moyens techniques ou juridiques sont encore très loin de pouvoir rivaliser avec l'hyperréactivité de l'informatique. Et avec la créativité continue des attaquants.

5) La question des ressources humaines.

En matière de cybersécurité, les Etats se trouvent sur le marché de l'emploi en concurrence avec les entreprises et les organisations criminelles. Ces compétences informatiques sont très recherchées. Pendant très longtemps, les cursus de formation, même et surtout dans les écoles d'ingénieurs, ont négligé l'apprentissage des techniques de sécurisation. Aujourd'hui que le risque est généralisé il y a une véritable pénurie de ressources humaines formées à ces métiers. Et face à la modestie des sanctions encourues nombre de techniciens peuvent être tentés de verser dans l'illégalité. Par conviction ou par appât du gain. Les mouvements terroristes peuvent également être des recruteurs pour ces personnes capables de détourner des fonds, de mener des campagnes de propagande sur la Toile ou de susciter des

[8] « Pentagon to Consider Cyberattacks Acts of War », *The New York Times*, David E. Sanger et Elisabeth Bumiller, may 31st, 2011 - http://www.nytimes.com/2011/06/01/us/politics/01cyber.html

[9] Détail de la Convention sur le site Internet du Conseil de l'Europe : http://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/185

[10] Site Internet officiel : http://www.itu.int/net/wsis/index-fr.html

dysfonctionnements dans les systèmes d'information des Etats qui les pourchassent. Les sympathisants à leur cause peuvent même contribuer en direct de chez eux sans se soumettre à des contrôles aux frontières.

6) La dépendance numérique.

A force de s'appuyer sur des équipements essentiellement techniques, nos organisations se rendent de plus en plus dépendantes de leur bon fonctionnement. On ne sait plus s'en passer. Et on est paralysé si les écrans deviennent noirs. En outre, nous faisons de plus en plus confiance aux informations que nous remontent les machines. Avec le *Big Data*, la gestion en temps réel de quantités massives de données, on se prend à croire à la capacité de prédiction par la compilation et l'ordonnancement d'informations passées. En oubliant que dans ce contexte, ce qui n'est pas numérisé n'existe pas et n'est donc pas pris en compte. On se trouve moins à l'aise pour identifier et neutraliser un ennemi rustique, qui ne se mesurerait pas en références informatisées. La base de données permet de retrouver ce que l'on connaît déjà. Elle est nettement moins pertinente pour désigner des personnes ou des comportements qui nous sont inconnus. En outre, les données peuvent être leurrées, altérées, modifiées…

7) Les notions de front et d'arrière n'existent plus.

La lecture des récits et des lettres des soldats envoyés depuis le Front lors de la Première Guerre mondiale donne une idée aux personnes restées à l'arrière de la violence des combats. Dans la dimension cybernétique, ces notions de front et d'arrière perdent de leur sens. L'affrontement est continu et ne connaît pas de telles distinctions. La preuve ? Par exemple, en 2010, quelque deux cents soldats israéliens[11] se confiaient à une prétendue jeune femme sur leurs déplacements et les activités de leurs unités. Il s'agissait en fait d'une opération d'espionnage palestinienne pour anticiper les opérations de Tsahal. Les « milblogs », ces sites Internet dans lesquels des militaires en activité s'épanchent sur leurs missions sont désormais actifs dans un très grand nombre de forces armées. Outils de propagande ou de libre expression ? Les smartphones et la capacité pour chacun de capturer des images ou des vidéos en haute définition d'un simple clic changent la donne. La production d'information n'est plus l'apanage des seuls services de communication des armées. Et la diplomatie de l'émotion peut venir influencer les gouvernements, notamment en Occident où les populations prennent souvent la mesure des conflits par ce qu'ils en voient sur les réseaux sociaux.

8) Combattre vs. Empêcher de se battre.

L'arme numérique permet d'intercepter, d'altérer voire de détruire des systèmes d'information. Elle introduit encore davantage dans la panoplie guerrière la possibilité d'empêcher l'adversaire de se battre. Soit par une cyberattaque qui crée des dysfonctionnements tels dans le camp ennemi que celui-ci est désorganisé au point de ne pouvoir plus se défendre. Ce fut le cas en 2010 quand le programme informatique*Stuxnet* est venu saboter les centrifugeuses iraniennes, au point de retarder de plusieurs années le déploiement de son armement nucléaire. Soit par des campagnes de communication pour alerter les opinions publiques contre les agissements de leurs dirigeants. Afin que la

[11] « Online-Spionage:Die schöne Facebook-Freundin der Elitesoldaten », *Der Spiegel*, Sarah Stricker, 17 mai 2010. http://www.spiegel.de/politik/ausland/online-spionage-die-schoene-facebook-freundin-der-elitesoldaten-a-694582.html

mobilisation médiatique influe directement sur la stratégie menée par le gouvernement. Coupé d'un soutien populaire il ne persistera guère dans ses actions. La capacité à diffuser facilement à un grand nombre de personnes des documents élaborés (textes, images, films…) grâce aux canaux d'Internet devient un élément à part entière d'une stratégie d'influence.

9) La notion d'allié est à redéfinir.

L'appartenance à une alliance comme l'OTAN ou autrefois le Pacte de Varsovie permettait de déterminer ses amis et ses ennemis de manière plutôt claire. Dès lors qu'il s'agissait de questions militaires et de diplomatie les ensembles étaient aisément identifiables. Même les bien nommés « Non Alignés » avaient trouvé leur place sur l'échiquier géopolitique. Dès lors que la concurrence entre les Etats est de moins en moins idéologique et militaire et de plus en plus économique, les clivages s'estompent. On peut être des alliés diplomatiques, et parfois militaires, mais demeurer en concurrence frontale en ce qui concerne l'économie. « La pérennité des gouvernements démocratiques et leurs victoires aux élections successives tiennent principalement à la performance de deux indicateurs : le taux de chômage et l'équilibre des finances publiques, ce dernier ayant un impact direct sur la fiscalité des particuliers et des entreprises »[12]. Cette situation explique que les Etats mettent tous leurs services de renseignement, longtemps dédiés à la seule sécurisation des personnes et des biens notamment face au risque terroriste, à contribution pour collecter des informations économiques. Et rien de tel que l'outillage numérique pour mener ces interceptions en toute discrétion. C'est ainsi que les Etats-Unis ont pu espionner le téléphone portable personnel de la Chancelière Angela Merkel, et que les services allemands ont consciencieusement écouté les téléphones mobiles des présidents français Jacques Chirac, Nicolas Sarkozy et François Hollande. Idem pour la NSA étatsunienne et son homologue britannique, le GCHQ, qui pratiquent les interceptions à grande échelle au profit de leurs entreprises respectives. Alliés contre Daesh mais concurrents sur les marchés internationaux. Les chancelleries ne semblent pas y voir de contradictions flagrantes.

Conclusion provisoire

L'espionnage et les attaques entre partenaires ne datent certainement pas de la fin du XXème siècle, toutefois la numérisation des échanges a permis d'industrialiser ces pratiques. Et au fur et mesure que la concurrence s'est élargie à de nouveaux acteurs asiatiques ou africains, les dispositifs de captation de données ou de cyberattaques ont suivi la même progression. Les capacités de traitement permettant d'absorber les quantités d'informations produites. La différence réside donc plus que jamais dans l'analyse. Souhaitons que cela reste encore longtemps un domaine d'excellence pour le cerveau humain. Caravec la morale et l'éthique c'est le dernier pan qui reste encore spécifiquement humain. Les machines ayant depuis longtemps dépassé notre capacité individuelle à produire, stocker et restituer des volumes de données si conséquents.
La collectivité humaine n'aura rien à gagner et tout à perdre à laisser les commandes de cette guerre cybernétique qui s'annonce aux seules machines. Pour paraphraser les scientifiques

[12] « Internet et la fiscalité vont imposer le fédéralisme à l'Europe », Nicolas Arpagian, *Les Echos*, 19 août 2015.
http://www.lesechos.fr/idees-debats/editos-analyses/021265470242-internet-et-la-fiscalite-vont-imposer-le-federalisme-a-leurope-1145360.php?gAIhqObQlbbI6Itx.99#

atomistes de l'Université de Chicago avec leur « Horloge de l'Apocalypse / *Doomsday Clock*»[13], il devient urgent de bâtir un corps de doctrine d'emploi efficient de l'arme numérique. Qui soit à la hauteur de ce que nous confions à ces technologies, et que nous souhaitons protéger, durablement.

[13] Site Internet officiel : http://thebulletin.org/