note n°17/19

12 septembre 2019

GAL (2S) Olivier Kempf
Chercheur associé, Fondation pour la recherche stratégique

FONDATION pour la RECHERCHE STRATÉGIQUE

Du cyber et de la guerre

Au XXIe siècle, la guerre sera forcément imprégnée de digital. La seule question pertinente reste de savoir si cela constitue une révolution stratégique ou si, comme souvent, il n'y aura pas de bouleversement majeur. Le cyber est aussi l'instrument d'une convergence de luttes dans des champs autrefois distincts. Il y a ainsi de forts liens entre la cyberconflictualité et la guerre économique qui rendent malaisée la juste appréciation du phénomène, pourtant nécessaire pour appréhender une dimension fondamentale de la guerre au XXIe siècle.

Disons un mot rapidement de cette notion de révolution stratégique. Une révolution stratégique change les modalités de la guerre et peut imposer de nouvelles règles stratégiques, sans pour autant que la grammaire de base soit annihilée (que celle-ci trouve son inspiration dans Clausewitz ou Sun -Tsu).

Selon ce critère, plusieurs révolutions stratégiques peuvent être identifiées à partir du révélateur de l'énergie. La vapeur est allée de pair avec le moteur correspondant (locomotive, *steamer*) qui a influé sur les guerres de la deuxième moitié du XIXe siècle (Guerre civile américaine, Guerre de 1870, mobilisation de 1914, etc.). On inventa alors la guerre industrielle et donc la massification du rôle des fantassins. Avec l'essence vint le trio « camion, char & avion », mis au point au cours de la première moitié du XXe siècle (Seconde Guerre mondiale, Guerre de Corée, Guerre des Six jours) : nul besoin d'expliciter son influence durable (et encore perceptible) sur l'ossature blindée-mécanisée de nombreuses armées contemporaines. La détonation nucléaire de 1945 orienta toute la seconde moitié du XXe siècle, avec la dissuasion et la polarisation de la Guerre froide. Il semble qu'avec la donnée, décrite par certains comme l'énergie de l'âge digital[1], nous

[1] Voir par exemple « The World's most Valuable Resource is no longer Oil, but Data », *The Economist*, 6 mai 2017 (https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data). L'expression « data is the new oil » semble devoir être attribuée au mathématicien britannique Clive Humby, dès 2006. Mais beaucoup discutent cette idée de la donnée comme énergie : voir par exemple « Here's why Data is not the New Oil », *Forbes*, 5 mars 2018 (https://www.forbes.com/sites/bernardmarr/2018/03/05/heres-why-data-is-not-the-new-oil/#213eb40a3aa9).

faisions face à une nouvelle révolution stratégique qui conditionnera cette première moitié du XXIe siècle.

Cette mise en perspective permet de relativiser le rôle de ces révolutions stratégiques : elles sont indubitablement importantes, mais n'annihilent pas d'un coup les grammaires stratégiques antérieures. Autrement dit, le digital n'abolira pas la dissuasion qui n'a pas aboli pas le char qui n'avait pas aboli le fantassin suréquipé, etc. Ceci précisé, le digital constitue donc bien une révolution stratégique. Il affecte la conduite de la guerre. Examinons donc les liens entre ce cyberespace et la guerre.

Cyber : Qu'est-ce que cela recouvre

Since Depuis les années 1980, nous avons assisté à plusieurs vagues successives de la révolution informatique, considérée comme un tout continu : la première fut celle des ordinateurs individuels, dans les années 1980. Puis est arrivé l'Internet – dans le grand public -, au cours des années 1990. Ce fut ensuite l'âge des réseaux sociaux et du web 2.0 dans les années 2000. Nous sommes aujourd'hui en présence d'un quatrième cycle, celui de la transformation digitale (TD), qui secoue toujours plus violemment nos sociétés et particulièrement le monde économique. On pourrait bien sûr désigner tout ce monde informatique massif de « cyberespace ».
Ces différents cycles ont eu leurs applications dans le domaine stratégique.

Petite histoire du cyber

Avant l'apparition des notions de numérisation de l'espace de bataille et de guerre réseau-centrée (*network centric warfare*), l'essor de l'informatique a très tôt suscité des inquiétudes stratégiques.

Si l'on remonte au début des années 1960, les Etats-Unis fondèrent l'ARPA (ancêtre de la DARPA) pour faire face aux efforts remarqués des Soviétiques en calcul et en ce qu'on appelait alors la cybernétique : ce fait mérite d'être rappelé quand on connaît le rôle joué par la DARPA dans l'invention d'Internet. Cette inquiétude fut rappelée plus tard par Zbigniew Brezinski, qui, dès 1970, parlait alors de *Révolution technétronique*[2] : la puissance informatique est considérée par lui comme le moyen de la victoire sur la puissance soviétique. Plus récemment, il faut se replonger dans les débats des années 1990 sur la Révolution dans les affaires militaires (RMA) : il s'agissait alors de prendre en compte les changements apportés par les ordinateurs individuels, mais aussi par les mises en réseau de masse, autrement dit nos deux premières vagues informatiques. *Cyberwar is coming*, comme l'affirmaient en 1993 deux auteurs de la Rand[3] .

Tous ces débats n'illustrent finalement qu'une seule perception : l'utilisation de la puissance informatique pour donner de nouveaux moyens aux armées. L'informatique n'est vue que comme un outil, un multiplicateur de puissance. Elle s'applique aux armes comme aux états-majors. C'est d'ailleurs cette même idée qui préside à la définition de la *Third offset strategy*, lancée par les Etats-Unis depuis quelques années : avancer technologiquement à marche forcée pour ne pas être dépassé par une autre puissance dans le domaine des capacités.

La mise en réseau des états-majors et l'embarquement d'informatique dans les armes a provoqué une augmentation certaine de l'efficacité. On parle aujourd'hui de systèmes d'armes, de systèmes de commandement. Et il est vrai que l'efficacité est obtenue : observez la précision des missiles ou encore les capacités d'un avion de chasse moderne… Désormais, un avion n'est plus un porteur de bombes, c'est un ordinateur qui vole et qui transporte des ordinateurs qui explosent sur leurs cibles préalablement identifiées et désignées par des ordinateurs en réseau.

Cette informatique embarquée est donc la cible naturelle des agresseurs cyber. Face à une bombe qui tombait, on ne pouvait que s'abriter. Désormais, on peut imaginer lui envoyer un code malveillant qui donnerait de fausses informations qui feront dévier le projectile de sa trajectoire.

Mais c'est en matière de commandement que l'évolution est la plus nette. Les Anglo-Saxons utilisent le terme de *Command and Control* pour le désigner, simplifié en C2[4]. Au cours des années 1990, l'informatisation de la fonction commandement a conduit à bâtir un

[2] Zbigniew Brezinski, *Révolution technétronique,* Calmann-Lévy, Paris, 1970, 387 p.

[3] John Arquilla & David Ronfeldt, « Cyberwar is Coming », *Comparative Strategy*, Vol. 12, No. 2, Spring 1993, pp. 141-165. Rand Corp., 1993 (https://www.rand.org/pubs/reprints/RP223.html).

[4] Qu'il faut traduire par « commandement et conduite ».

C4 puis un C4ISR puis un C4ISTAR[5] et puis… cela s'est arrêté là[6]. Revenons à notre C4 (la fonction *ISR* étant particulière au renseignement, et la *Target Acquisition* au ciblage) : il s'agit non seulement du *Command*, du *Control* mais aussi de la *Communication* et du *Computer*. On a automatisé les fonctions de commandement grâce à l'informatique en réseau. Il fallait aussi dissiper le brouillard de la guerre mais également accélérer la boucle OODA[7]. La méthode a pu donner des résultats (que l'on songe aux deux Guerres du Golfe) sans pour autant persuader qu'elle suffisait à gagner la guerre (que l'on songe à l'Afghanistan et à l'Irak).

Au fond, cette guerre en réseau – dans la littérature stratégique américaine des années 1990-2000 on parlait de *network centric warfare* - est une guerre très utilitaire et très verticale, « du haut vers le bas ». Tous les praticiens savent que bien souvent, les réseaux de commandements servent à nourrir le haut d'informations et au risque d'augmenter le micro-management, tandis que les utilisateurs du bas profitent finalement beaucoup moins du nouvel outil.

Grandeur et imprécision du cyberespace

Quand on parlait de cyberespace à la fin des années 2000, il s'agissait de désigner cette informatique distribuée et en réseau, mais aussi de déceler ses caractéristiques stratégiques. Peu à peu, on a oublié la notion de cyberespace pour passer à celles de cyberdéfense et de cybersécurité que recouvre aujourd'hui dans les organismes chargés de la sécurité et de la défense le préfixe cyber. Ce glissement s'est effectué au cours de la décennie 2010.

Les premiers cas d'agression cyber remontent aux années 1980 (*Cuckoo's egg* en 1986, *Morris Worm* en 1988). Avec des attaques plus systématiques (première attaque par déni de service en 1995, première attaque connue contre le *Departement of Defe*nse en 1998, première affaire « internationale » avec *Moonlight Maze* en 1998), la stratégie s'empare du phénomène. Elle rejoint le débat de l'époque sur la Révolution dans les affaires militaires qui évoque alors la guerre en réseau. C'est la fusion de ces deux approches par Arquilla et Ronfeldt qui leur fait annoncer dès 1993 que « *Cyberwar is coming* »[8].

Ces interrogations infusent au cours des années 2000. La création d'un *Cybercommand* américain en 2009, l'affaire Stuxnet en 2010, les révélations de Snowden sur la NSA (2013) montrent que les Etats-Unis sont très en pointe sur le sujet. En France, dès le *Livre blanc* de 2008, le cyber est identifié comme un facteur stratégique nouveau, approche encore plus mise en évidence dans l'édition de 2013 et confirmée par la Revue stratégique de 2017. L'OTAN s'empare du sujet à la suite de l'agression contre l'Estonie en 2007, couramment attribuée à la Russie même si, comme quasiment toujours en matière cyber, les preuves manquent[9]. Jusqu'alors simple sujet d'intérêt, le cyber s'élève dans l'échelle des menaces pour devenir une préoccupation prioritaire. Désormais, une agression cyber pourrait, le cas échéant, provoquer la mise en œuvre de l'article 5 du traité de Washington. Les Alliés s'accordent même à définir le cyber comme « un milieu de combat », au même titre que les autres milieux physiques. Sans entrer dans des débats conceptuels sur l'acuité de cette assimilation, constatons que cette approche globalisante encapsule tout ce qui est informatique dans le terme cyber.

La notion de cyber a évolué

Est-ce pourtant aussi simple ?

Il faut en effet constater que la notion même de « cyber » a évolué. D'autres préfixes et adjectifs lui ont succédé : *électronique* (e-réputation, e-commerce) ou tout simplement, *numérique* ou *digital*. Cette évolution sémantique provoque aujourd'hui un cantonnement du cyber dans le champ de la

[5] *Computerized Command, Control, Communications, Intelligence, Surveillance, Target Acquisition and Reconnaissance.*

[6] Il semble que l'on parle de C5 dans la littérature stratégique américaine récente, le 5ème C valant pour cyber. Ce qui pose la question de la différence entre *computer* et cyber… (voir https://www.army.mil/article/157832/ccdc_c5isr_center). En février 2019, l'ancien CERDEC est devenu le CCDC C5ISR center de l'US Army (https://c5isr-ccdc.army.mil/inside_c5isr_center/history/). Mais on trouve d'autres extensions de cet acronyme où le cinquième C vaudrait pour « *combat systems* » (par exemple https://www.acronymfinder.com/Command%2c-Control%2c-Communications%2c-Computers%2c-Combat-Systems%2c-Intelligence%2c-Surveillance%2c-and-Reconnaissance-(C5ISR).html).

[7] La boucle OODA (*OODA loop*) est un concept inventé par le pilote de chasse John Boyd de l'United States Air Force en 1960 : « *Observe, Orient, Decide and Act* » (« observer, s'orienter, décider et agir »), son raccourcissement est censé être la garantie de l'initiative stratégique.

[8] https://www.rand.org/pubs/reprints/RP223.html

[9] Plus exactement : s'il est indéniable que la plupart des attaques contre l'Estonie ont été opérées par des Russes, il n'est pas prouvé que cela fut orchestré par le Kremlin : ainsi, de nombreux « hackers patriotes » ont joué un grand rôle dans cette affaire. Toutefois, *a minima*, le Kremlin a laissé faire, manière d'avaliser l'opération. En cela, sa responsabilité est engagée.

sécurité, de la défense et de la stratégie. Le Forum de Lille est un Forum international de Cybersécurité, le commandement américain est un Cybercommand.

Au fond, s'il y a dix ans on craignait le peu de prise de conscience de la dangerosité du cyberespace, il faut bien constater que finalement la prise de conscience a eu lieu et que le cyber désigne notamment la fonction de protection qui entoure les activités informatiques de toute nature. Désormais, quand on parle de cyber, on évoque surtout la conflictualité associée au cyberespace, qu'il s'agisse de criminalité ou de défense : d'un côté, on a les caractéristiques de protection et de défense proprement dites, de l'autre les caractéristiques d'agression, classiquement l'espionnage, le sabotage et la subversion. Cette activité s'exerce dans les trois couches du cyberespace (physique, logique, sémantique)[10].

Pour simplifier, le cyber s'occupe désormais de la lutte opposant des acteurs divers utilisant des ordinateurs pour atteindre leurs fins stratégiques ou tactiques. Les réseaux et les ordinateurs sont le véhicule d'armes diverses (vers, virus, chevaux de Troie, DDoS, *fakes, hoaxes*[11], etc.) qui permettent d'atteindre le dispositif adverse et de le neutraliser, le corrompre, le détruire ou le leurrer.

Pour conclure sur ce point, la cybersécurité repose sur la maîtrise des réseaux, des données et des flux, ce qui passe souvent par un contingentement de ceux-ci et par des restrictions d'utilisation, qu'il s'agisse d'hygiène informatique ou de dispositifs plus sécurisés, durcis en fonction de l'information manipulée. Autrement dit, la cybersécurité a tendance à restreindre les usages que l'informatique entendait simplifier, automatiser ou libérer.

Il n'y a pas de cyberguerre

Cybersécurité ou cyberdéfense ?

Les notions de cybersécurité et de cyberdéfense sont proches. Les distinguer paraît cependant nécessaire car il existe des liens évidents entre la cybersécurité et la « défensive », tout comme entre la cybersécurité et le ministère de la Défense (aujourd'hui renommé ministère des Armées) : mais ces liens entretiennent une confusion qu'il faut clarifier.
On pourrait tout d'abord considérer que la cybersécurité est du domaine du civil quand la cyberdéfense appartient aux compétences des armées et du militaire. Cette approche est souvent partagée, mais elle est inexacte. Par exemple, dans le cas de la **France, c'est l'ANSSI (agence civile) qui est l'autorité nationale en matière de sécurité et de défense des systèmes d'information**. Toutefois, le mot défense est un faux-ami qui entraîne ici des confusions.

On pourrait ensuite estimer que la cybersécurité est un état quand la cyberdéfense est un processus. Afin d'atteindre la cybersécurité (d'être en cybersécurité), il faut assurer une cyberdéfense. Dans un cas un verbe d'état, dans l'autre un verbe d'action. Cette approche, conceptuellement juste, est malheureusement peu suivie par les praticiens. Surtout la cyberdéfense est parfois considérée comme le tout (l'action stratégique dans le cyberespace) et comme une partie de ce tout (la fonction défensive de l'action stratégique dans le cyberespace).

Une approche plus opérationnelle est donc recommandée qui évite le mot de cyberdéfense et ne conserve le mot de cybersécurité que dans un cas très précis (que nous décrirons ci-dessous). D'une façon générale, il convient d'éviter le préfixe cyber apposé devant tout substantif, car les termes sont rarement bien définis et cela introduit de nombreuses confusions.

La cyberguerre n'aura pas lieu

Cyberwar will not take place : voici le titre d'un remarquable petit livre de Thomas Rid, paru en 2013 à Oxford[12]. Déjà, il remettait en cause la notion de cyberguerre. Or, l'expression « cyberguerre » sonne bien. Elle est régulièrement employée par des journalistes ou des commentateurs peu avisés. Pourtant, elle est fausse, ce qui ne signifie pas que la guerre ignore le cyberespace (il y a au contraire toujours plus de cyber dans la conduite des conflits).

Le problème avec l'expression de « cyberguerre », c'est le mot guerre. Nous

[10] Pour l'analyse des catégories stratégiques du cyberespace, voir Olivier Kempf, *Introduction à la cyberstratégie*, Paris, Economica, 2015, 2ème édition.
[11] DDoS : déni de service distribué – Fake : fausse nouvelle – Hoax : Canular.
[12] En réponse à l'article d'Arquilla et Ronfeldt paru vingt ans avant, avec peut-être une citation de l'œuvre pessimiste de Giraudoux, *La guerre de Troie n'aura pas lieu* (1935), puisqu'à la fin de la pièce de théâtre, la guerre de Troie eut bien lieu.

nous sommes régulièrement interrogés[13] sur sa signification profonde, celle d'autrefois mais aussi d'aujourd'hui. Si la *grande guerre* d'autrefois est morte, la guerre mortelle subsiste, souvent à bas niveau même si elle peut être alors très meurtrière. Elle n'est plus le monopole des États. On assiste à une forte montée en puissance et une vraie diversification de la criminalité armée[14] où des acteurs s'affrontent et portent des coups, y compris à des États faibles (nous pensons bien sûr au Mali et à nombre de pays africains).

Quand la guerre n'est plus le fait d'armées organisées et ni le plus souvent nationales, quel est alors son critère distinctif ? La létalité : la mort violente de vies humaines pour des motifs politiques. Désormais, le critère de la guerre qui demeure est celui de l'existence – ou non – de morts humaines touchant soit les parties militaires au conflit, soit les populations environnantes (civiles). On peut bien sûr retenir le nombre de mille morts militaires par an, identifié par les polémologues pour marquer le seuil à partir duquel il y a guerre et non pas conflit armé. Sans aller jusque-là (les noyés en Méditerranée, pour avoir tenté de rejoindre l'Europe, sont-ils victimes d'une guerre ?), constatons que pour l'heure, il n'y a pas de mort directement imputable à une agression cyber. Aujourd'hui, le cyber ne tue pas ; du moins pas encore.

Par ailleurs, il faut se méfier de tout le discours produit sur ce thème : un « cyber-Pearl Harbour » menacerait, le cyberespace serait le cinquième théâtre physique de la guerre, il nous faut des cyberarmées, etc. On reconnaît là un schéma de pensée américain qui militarise tout d'emblée, de façon à justifier des budgets et une approche quantitative et destructrice des oppositions politiques. Sans avoir la cruauté de rappeler les échecs répétés de cette approche depuis plus de soixante-dix ans, signalons simplement qu'il n'y a pas d'échanges d'électrons qui se foudroieraient réciproquement avec des vainqueurs et des vaincus[15]. Les choses sont plus subtiles que ça.

Cela ne veut pas dire que le cyber ne soit pas dangereux, ni qu'il ne soit dans la guerre. Plutôt que de cyberguerre, parlons de cyberconflictualité. Elle est partout.

Opérations dans le cyberespace

Actions cyber

Le livre de T. Rid rappelait déjà l'essentiel, à savoir que les trois types de cyber agressions sont bien connus (l'espionnage, le sabotage et la subversion), et qu'elles ne justifient pas les excès d'une certaine militarisation du cyber.
L'espionnage cyber constitue la première brique de la cyberconflictualité. En effet, quasiment toutes les actions offensives cyber débutent par une phase d'observation de la cible et donc, dans les cas les plus aigus, d'espionnage. Qu'il s'agisse de *défacer* un site ou de le bombarder de requêtes (technique basique dite des DDoS : déni de service distribué) ou d'aller, au contraire, beaucoup plus avant dans le système à la recherche d'informations sensibles, il faut délimiter le contour de l'objectif, ses points forts et ses points faibles. C'est la première phase commune à toutes les actions. Soit parce qu'on recherche d'abord l'information, soit parce qu'elle va servir à autre chose. Il s'agit là d'ailleurs d'un point commun à toutes les opérations militaires : quoique vous vouliez faire, vous commencez toujours par vous renseigner. Il reste que le cyberespace a pour essence de manipuler de l'information, soit pour la stocker, soit pour l'échanger avec des correspondants dûment identifiés. Il y a une profonde intrication entre les méthodes de renseignement (ou d'information) et les caractéristiques du cyberespace. Or, le cyberespace démultiplie les capacités d'espionnage. On s'en est largement rendu compte avec les révélations d'Edward Snowden qui a appris au monde le potentiel de la NSA américaine, qui passait son temps à espionner le monde entier, y compris ses alliés et amis.

Or, une propriété commune à la souveraineté et à la liberté d'action est la préservation de ses secrets. C'est évident pour les États, mais c'est également vrai pour les entreprises. Dès lors, un cyberespionnage massif peut modifier les relations internationales ou inter-entreprises. Certes, « *on s'est toujours espionné, même entre amis* », un argument développé par les défenseurs de la NSA, au premier rang desquels Barack Obama[16]. À ceci près que l'ampleur des moyens mis en œuvre

[13] Voir La Vigie (www.lettrevigie.com) , La France en guerre (janvier 2015), La guerre et Etat (LV 74&75, août 2017), La Guerre mélangée (LV 98 bis, juillet 2018).
[14] Voir J.-F. Gayraud, *Théorie des hybrides*, Paris, CNRS éditions, 2017.
[15] Ceci explique aussi pourquoi la notion de cyberdissuasion, très employée dans les milieux stratégiques américains, peine à convaincre. Voir à ce propos O. Kempf, *op. cit.*, chapitre 8.
[16] Lequel justifiait en partie l'espionnage d'alliés en tant que protection et révélation de leurs propres failles ; c'est la théorie du *third party espionnage*.

et la profondeur d'intrusion permise par la technique ont modifié le sens de cette pratique. Le cyberespionnage est bien la première forme d'agression cyber.

Le sabotage cyber constitue la deuxième. Elle est perçue comme l'attaque principale par l'opinion populaire qui réduit souvent l'agression cyber à ces virus qui cassent les systèmes des ordinateurs. De Stuxnet à NotPetya, ces vers, virus et maliciels ont défrayé souvent la chronique (les journalistes ratant rarement l'occasion d'expliquer qu'on n'avait jamais connu une telle agression dans toute l'histoire, pour oublier leur assertion imprudente la semaine suivante). Il y a ainsi un grand discours de la peur autour du sabotage, permettant les meilleurs fantasmes, à l'image des scénarios absurdes de James Bond où des pirates informatiques géniaux détruiraient les systèmes collectifs et provoqueraient des morts en pagaille.

La réalité est plus banale : il y a certes beaucoup d'attaques mais aujourd'hui, on observe surtout des opérations de rançonnage (contre des particuliers ou des organisations, notamment des villes : Atlanta ou Baltimore[17]) où les assaillants bloquent le fonctionnement en échange d'une rançon. Mais cela peut aussi avoir des motifs politiques : l'entreprise saoudienne Aramco a ainsi été bloquée il y a quelques années par des agresseurs, visiblement des voisins iraniens.

La subversion cyber est le troisième mode d'agression. Elle vise à modifier les décisions d'un individu ou d'un groupe, que ce soit par des sabotages (par exemple, le *défacement* d'un site Internet pour faire apparaître la tête d'Hitler à la place du dirigeant de l'entreprise/pays) ou d'autres procédés, plus ou moins évolués. Beaucoup négligeaient cette agression subtile jusqu'au développement des débats sur la post-vérité et la question des infox[18].

Ainsi, ces trois procédés sont fréquemment utilisés dans ce qu'il faut bien nommer la réelle cyberconflictualité contemporaine. Relevons deux caractères spécifiques. Le premier est celui des acteurs concernés : désormais, tous les acteurs (individus, groupes, agences ou Etats) peuvent être à la fois les auteurs et les cibles de ces agressions. Le second, par conséquent, est que les motifs des attaques sont extrêmement variés (économiques politiques, culturels, réputations, egos, etc.). Cela donne à ce champ de bataille une dimension hobbesienne, celle du *conflit de tous contre* tous que l'on pensait avoir réglé avec l'ordre westphalien il y a trois siècles et demi. Cela est plus profond que le *multisme* politique ou que la notion de guerre hybride.

Réponses stratégiques dans le cyberespace

Nier l'existence de la cyberguerre ne revient pas à nier l'importance du cyber dans la conduite de la guerre, bien au contraire. Le cyber est désormais partout dans les opérations militaires. Il est au cœur des armements : on s'interroge sur la grande autonomie de ces armes, envisageable grâce à la robotisation et à l'intelligence artificielle. Le cyber anime tous les réseaux de commandement et de conduite, qu'on désigne sous le terme de Systèmes d'information et de commandement (SIC).
L'action stratégique dans le cyberespace est une approche générale. Considérons qu'elle est normalement à la portée de toutes les organisations (voire des individus) sauf le cas particulier de l'offensive, qui est une prérogative étatique (et pour le coup, spécifique au ministère des Armées, du moins en France). Autrement dit, les actions offensives non-étatiques sont toutes illégales.
Il y a ainsi, d'abord, une première fonction qu'on désignera sous le terme de défensive, aussi appelée cybersécurité (à proprement parler). Elle constitue pour les praticiens l'essentiel de la cyberconflictualité. Elle recouvre :

- Les mesures de protection (ou cyberprotection, ou de sécurité des systèmes d'information -SSI- au sens strict du terme), qui consistent en l'ensemble des mesures passives qui organisent la sécurité d'un système (pare -feu, antivirus, mesures d'hygiène informatique, procédures de sécurité). Cette notion de « mesures passives » ne signifie pas qu'on reste inactif, au contraire : un responsable SSI sera sans cesse aux aguets, en train de remettre à jour son système et de mobiliser l'attention de ses collaborateurs.

- Les mesures de défense (ou lutte informatique défensive, LID) qui comprennent l'ensemble de la veille active et des mesures réactives en cas d'incident (systèmes de sonde examinant l'activité du réseau et ses anomalies, mise en place de centres d'opération 24/7, etc.).

[17] http://www.leparisien.fr/faits-divers/etats-unis-paralyse-par-une-attaque-informatique-baltimore-ne-paiera-pas-de-rancon-28-05-2019-8082099.php
[18] Voir F-B. Huyghe, O. Kempf et N. Mazzucchi, *Gagner les cyberconflits*, Paris, Economica, 2015.

- La résilience consiste en l'ensemble des mesures prises pour faire fonctionner un réseau attaqué pendant la crise, puis revenir à un état normal de fonctionnement après la crise (y compris avec des opérations de reconstruction, dans les cas les plus graves).

La deuxième fonction est celle du renseignement. Il est évident qu'elle a partie liée à la défensive. Cela étant, le renseignement se distingue comme une activité propre. On distingue ici le renseignement d'origine cyberespace (ROC), qui est celui qui vient *du* cyberespace mais contribue à nourrir la situation globale du renseignement militaire ; et le renseignement d'intérêt cyberdéfense (RIC) (qui n'est pas forcément exclusivement d'origine cyber) et qui vise à construire une situation particulière de l'espace cyber, aussi bien ami et neutre que surtout ennemi. C'est ainsi un renseignement *sur* le cyberespace. Il est évident que dans une manœuvre militaire globale, le ROC intéresse plus le décideur tandis que dans le cas d'une manœuvre particulière à l'environnement cyber, le RIC sera prédominant. Le RIC permet en effet de renforcer la défensive mais aussi de préparer l'offensive. A titre d'exemple, les mots de passe des comptes des réseaux sociaux de TV5 Monde, visibles dans un reportage de France 2, constituent du RIC, tandis que les cartes dynamiques de course de l'application Strava, permettant par l'observation de l'activité de soldats, de repérer des sites militaires, sont du ROC.

La troisième fonction est logiquement l'offensive. Sans entrer dans trop de subtilités, elle recouvre aussi bien la Lutte informatique offensive (LIO) que l'influence numérique (la LIN). La première est tournée vers le sabotage, la seconde vers la subversion. S'agissant de l'influence, citons l'ex-chef d'état -major des armées (CEMA), le général de Villiers[19] : Il estime ainsi début 2016 qu'un « *nouveau théâtre d'engagement* » est celui de « *l'influence et des perceptions* ». « *C'est l'ensemble des domaines – dont le cyber espace – qui permet de porter la guerre pour, par et contre l'information. Ce champ de bataille, qui n'est pas lié à une géographie physique, offre de nouvelles possibilités pour la connaissance et l'anticipation, ainsi qu'un champ d'action pour modifier la perception et la volonté´ de l'adversaire* ». La propagande de l'Etat Islamique sur les réseaux sociaux a rendu urgente cette prise en compte de la « *bataille des perceptions* ».

Environnement cyber

Ces opérations se conduisent dans l'environnement cyber. Ce terme d'environnement permet d'échapper à la notion de milieu, bien qu'elle soit devenue une doctrine OTAN. Parler d'environnement cyber (comme on parle d'environnement électromagnétique) met cette fonction cyber à sa juste place. Elle est au fond une arme d'appui bien plus qu'une arme de mêlée. Cette approche favorise d'ailleurs la résolution avantageuse du dilemme entre les échelons stratégiques et tactiques, dilemme qui suscite encore bien des débats feutrés mais essentiels. C'est dans ces conditions que le cyber est bien présent dans les opérations militaires, et ce dans les trois couches du cyberespace (physique, logique et sémantique). Si les opérations sont discrètes, elles n'en sont pas moins réelles. Mais cela ne signifie pas que le cyber n'interviendra pas dans d'autres opérations, non-militaires cette fois. Il s'agit alors de bien autre chose, même si cela relève de la cyberstratégie.

Cyber et nouvelles formes de conflit

Nous avons parlé jusqu'à présent des liens entre le cyber et les actions militaires, mais aussi avec quelques actions civiles (notion de cybersécurité). Le cyber est incontestablement dans la guerre, avons-nous démontré. Mais la guerre n'est peut-être plus seulement dans la guerre. Autrement dit, on observe désormais de nouvelles formes de conflictualité interétatique qui sont en dessous du seuil de la guerre : sanctions juridiques, blocus économiques, amendes, guerre économique, actions massives d'influence, les formes en sont énormément variées. Le cyberespace est un remarquable outil pour l'ensemble de ces actions hostiles.

Extension du domaine de la cyber-lutte

En effet, cette cyberconflictualité ne se déroule pas seulement sur le terrain des opérations militaires. Celui-ci permet certainement de mieux comprendre ce qui se passe, de déceler les principes opérationnels : pourtant, il ne saurait cacher que la cyberconflictualité se déroule surtout en dehors d'actions militaires classiques.

L'observateur relève en effet plusieurs traits de cette cyber-lutte : elle est accessible à

[19] http://www.opex360.com/2016/01/18/pour-le-general-de-villiers-le-domaine-de-linfluence-constitue-nouveau-champ-daction

beaucoup, ce qui ne signifie pas que tout le monde est capable de tout faire. S'il n'y a que dans les romans qu'un individu surdoué réussit à défaire les grandes puissances, il est exact que de nombreux individus peuvent agir – et nuire – dans le cyberespace. Celui-ci a en effet deux qualités qui sont utilisées par beaucoup : un relatif anonymat pour peu que l'on prenne des mesures adéquates (et malgré le sentiment d'omnisurveillance suscité aussi bien par la NSA que par les GAFAM) ; et une capacité à agréger des compétences le temps d'une opération (ce qu'on désigne sous le terme de coalescence).

Dès lors, quel que soit le mobile (motivation idéologique ou patriotique, lucre et appât du gain, forfanterie pour prouver sa supériorité technique), de nombreux acteurs peuvent agir dans le cyberespace (ce qui explique notre prudence dans l'analyse du cas estonien). Autrement dit encore, le cyberespace connaît une lutte générale qui mélange aussi bien les intérêts de puissance (traditionnellement réservés aux États), les intérêts économiques (firmes multinationales, mafias), les intérêts politiques ou idéologiques (ONG, djihadistes, Wikileaks, Anonymous, cyberpatriotes) ou encore les intérêts individuels (du petit *hacker* louant ses services au lanceur d'alerte Edward Snowden).

Il s'ensuit une conflictualité généralisée, mobilisant tous dans une mêlée d'autant plus vivace qu'elle est relativement discrète. En effet, on n'a pas d'exemples de coups mortels donnés *via* le cyberespace[20] même si le fantasme d'un cyber-Pearl Harbour est sans cesse ressassé par les Cassandre. Avant d'être témoin d'un éventuel drame extrême, constatons que la cyberconflictualité ordinaire fait rage quotidiennement. Et que surtout, elle est fortement teintée de guerre économique, avant d'être politique.

[20] Il y a toutefois une complémentarité des opérations, notamment sur la couche physique. Ainsi, lors de l'opération Verger (*Orchard*) conduite en 2007 par les Israéliens contre les Syriens, le réseau de radars antiaérien fut déconnecté par une opération cyber, chaque radar étant par ailleurs aveuglé par du brouillage électromagnétique, ce qui permit aux chasseurs israéliens de passer et d'aller effectuer leur raid. On peut de même envisager la destruction de centres nodaux cyber ou d'émetteurs wifi. Ainsi, Israël a annoncé avoir mené des raids contre certaines installations à Gaza pour dissuader les Palestiniens du Hamas de lancer des cyberattaques, voir par exemple « Après avoir subi une cyberattaque, Israël répond par la force », *Le siècle digital*, 6 mai 2019, https://siecledigital.fr/2019/05/06/apres-avoir-subi-une-cyberattaque-israel-repond-par-la-force/

Cyber et guerre économique : la convergence des luttes

Ne nous y trompons pas : l'essentiel réside dans la guerre économique. Celle-ci est allée de pair avec le développement de la mondialisation, elle-même rendue possible par ce qu'on appelait à l'époque les Technologies de l'information et de la communication (TIC). Cela a du coup radicalement modifié le socle préalable qui régissait le monde économique, celui de la concurrence pure et relativement parfaite. Ce socle n'existe plus et désormais, tous les coups sont permis. Le cyberespace favorise justement ce changement profond. Espionner, saboter et subvertir sont désormais des armes quotidiennement et souterrainement employées.

Que nous a en effet appris Snowden ? Que la NSA, sous prétexte de lutte contre le terrorisme, espionnait surtout les concurrents des États-Unis. Qu'elle collaborait activement avec les grands acteurs économiques américains, notamment les GAFAM, dans une relation à double sens. Que si ceux-ci devaient coopérer activement avec les services d'Etat (qui a cru sérieusement qu'Apple refusait de collaborer avec le FBI dans l'attentat de San Bernardino ? en revanche, ce fut un remarquable coup marketing), ces derniers n'hésitaient pas à transmettre des informations pertinentes à leurs industriels.
La Chine a quant à elle pratiqué une stratégie opiniâtre d'espionnage économique, par tous les moyens, notamment cyber. Les exemples abondent et les dénonciations américaines en la matière révèlent une probable vérité. Israël a une symbiose très étroite entre ses services spécialisés (autour de la fameuse unité 8200) et son écosystème de jeunes pousses (ayant été le plus loin dans la construction d'une « start-up nation »). On pourrait relever des liaisons similaires en Russie ou à Singapour.
Autrement dit, il y a désormais une certaine convergence des luttes, bien loin de celle imaginée par les radicaux *alter* en France : entre acteurs (collaboration entre Etats et entreprises, « contrats » passés entre des entreprises et des hackers souterrains) et entre domaines (la géopolitique n'est jamais très loin des « intérêts » économiques : il n'y a qu'à voir le nombre de chefs d'entreprise qui accompagnent les dirigeants lors de leurs voyages officiels). Le cyber permet cette convergence grâce à ses effets en apparence indolores (sera-t-il jamais possible d'évaluer le coût d'informations sensibles qui ont été

volées par un concurrent ?), à sa discrétion évidente, à son anonymat confortable.

Une conflictualité englobante

Le cyber est désormais au centre de toutes les stratégies conflictuelles, qu'elles soient militaires ou non. Sa plasticité et sa transversalité permettent en effet le développement d'une multitude de manœuvres par des acteurs de tout type.

Agir dans le cyberespace, que l'on soit chef militaire, responsable politique, dirigeant économique ou simple RSSI (responsable de sécurité de systèmes d'information), impose de prendre conscience de cette dimension générale. Au fond, le cyberespace ne peut se réduire à un simple environnement technologique dont on laisserait la gestion à des responsables techniques mais subordonnés. Le cyberespace permet la mise en place d'une nouvelle conflictualité qui va, d'une certaine façon, fusionner les champs traditionnels des hostilités : aussi bien les guerres militaires que les oppositions géopolitiques ou les concurrences économiques. C'est pourquoi parler de cyberguerre est extrêmement trompeur : c'est tout d'abord faux (car le critère de létalité n'est pas rempli) et surtout réducteur car la conflictualité du cyberespace a certes des dimensions militaires, mais elles sont également plus larges et souvent plus insidieuses que la « simple » manœuvre de force et de coercition à la base des actions militaires.

En ce sens, il y a une globalisation de la cyberconflictualité. En prendre la mesure est la première étape d'une stratégie adaptée, quelle que soit l'organisation dont on a la charge, Etat, armée ou entreprise.

La Fondation pour la Recherche Stratégique est une fondation reconnue d'utilité publique. Centre de recherche indépendant, elle réalise des études pour les ministères et agences français, les institutions européennes, les organisations internationales et les entreprises. Elle contribue au débat stratégique en France et à l'étranger.

WWW.FRSTRATEGIE.ORG

4 BIS RUE DES PÂTURES 75016 PARIS TÉL : 01 43 13 77 77 FAX 01 43 13 77 78

ISSN : 2273-4643