Cyberdéfense et conflits armés

Laurent Prosperi

laurent.prosperi@ens-paris-saclay.fr

17 juillet 2021

Ce travail est financé par la Chaire Grands Enjeux Stratégiques Contemporains
(`https://chairestrategique.pantheonsorbonne.fr/`).

« Le combat dans le cyberespace est de nature asymétrique, hybride, parfois invisible et en apparence indolore. Pourtant, l'emploi de l'arme cyber est susceptible de porter gravement atteinte aux capacités et aux intérêts souverains des États. » [1] Le cyberespace est désormais reconnu, tant dans les forces qu'au niveau politique, comme « un champ de bataille à part entière » [2]. En France, comme aux États-Unis, la création d'un commandement opérationnel unifié fait du cyber une composante au même titre que celles terrestres, aériennes, maritimes et extra-atmosphériques. Les armées françaises ont amorcé leur développement capacitaire dès 2008 suite à la parution du Livre blanc sur la défense et la sécurité nationale (LBDSN), la mission donnée aux forces étant de développer une capacité militaire afin de pouvoir défaire un adversaire. Le débat sur l'usage du cyber a débuté dans les années 1990 et a pris son essor au début des années 2000 notamment dans une optique de soutien aux forces armées. Les années 2010 marquent l'autonomisation des forces cyber et une évolution vers une stratégie cyber autonome au sein des armées mais aussi à l'extérieur du domaine militaire afin de poursuivre des objectifs de nature politique ou économique.

Le cyberespace est devenue la dimension englobante de la conflictualité contemporaine et en particulier, des conflits armés actuels. « Dès maintenant, perdre dans le cyber, c'est perdre tout court ! » [3] même si les opérations cyber ne sont pas, encore, en mesure d'en déterminer l'issue. Comment le cyber permet-il d'atteindre l'effet final recherché et quelles sont les nouvelles vulnérabilités des forces ? Dans un premier temps, il nous faut spécifier le cyber, c'est à dire son rapport au temps, à l'espace, les modes d'action en son sein, sa technologie et les perturbations des pratiques qu'il induit. En outre, l'autonomisation de la stratégie cyber et son caractère englobant pose la question de son intégration avec les autres dimensions.

1 Cadre stratégique

Le milieu d'emploi se distingue par des caractéristiques spécifiques de temps et d'espace. Il y a une *contraction temporelle des effets* et, à l'inverse, une dilatation dans sa préparation de par la nécessité d'une longue planification dans le cadre d'opérations ciblées. D'autre part, son usage entraine un affaiblissement entre temps de paix et de conflits, seul un seuil flou d'intensité et de violence les sépare. L'emploi offensif permet de s'*affranchir des distances et des frontières* et de frapper avec des moyens sur le territoire national, il n'est pas forcément nécessaire de déployer des combattants cyber sur le théâtre ni d'en prépositionner comme pour les forces conventionnelles [4]. L'isolation entre les différents domaines s'est affaiblie depuis l'introduction du numérique, car ce dernier est devenu l'un des composants essentiels et partagés de tous les autres domaines. Ces

1. COMCYBER. *Éléments publics de doctrine militaire de lutte informatique offensive*. Janvier 2019, p. 12.
2. J.-M. (Bockel. *La cyberdéfense : un enjeu mondial, une priorité nationale*. 18 juillet 2012.
3. A. Bonnemaison et S. Dossé. *Attention : Cyber ! : vers le combat cyber-électronique*. Economica, 2014, p. 10.
4. Dans certains cas, il peut être intéressant de positionner de forces sur place pour disposer d'un accès physique à certains réseaux ou systèmes.

particularités d'espace et temps permettent une action dans la profondeur en s'affranchissant des frontières physiques et géographiques. A l'inverse, les frontières techniques entre les systèmes, notamment ceux non rattachés à un réseau, sont déterminantes car certaines failles peuvent mettre en danger des systèmes décorrélés et géographiquement distincts, peu de modifications pour l'attaquant sont nécessaires.

La complexité de la défense provient de la fragmentation de la responsabilité et des systèmes [5], du rythme rapide de la publication et d'évolution des produits, de la complexité croissante de ceux-ci [6] et de leur maintien en condition de sécurité [7]. Afin de maitriser les coûts, de nombreuses fonctionnalités superflues sont présentes dans les différents systèmes du fait de la convergence technologique, par exemple des serveurs web préinstallés. La compréhension du milieu est perturbée par la difficulté de cartographie et de visualisation du cyberespace, elle d'autant plus génée par la multiplicité des acteurs et par leurs liens de dépendance. La complexité intrinsèque aux trois couches (infrastructure, logique et sémantique) combinée à celle résultant de leurs interactions renforce les opportunités d'actions offensives et de déstabilisation de l'adversaire. Si les pratiques et les produits évoluent rapidement, le coeur technologique sous-jacent suit des cycles plus longs qui peuvent se compter en décénies.

D'un coté, l'*incertitude* est réduite [8] dans quatre des cinq composantes (terre, mer, espace extra-atmosphérique, air) grâce au développement des technologies de l'information et des communications comme par example avec le développement de l'infovalorisation et la mise en réseau des capacités dans les nouveaux programmes d'armement (au coeur des systèmes SCAF, MGCS et GRIFFON). De l'autre, pour la composante cyber, l'incertitude reste maximale [9] par la complexité des systèmes à défendre, de celle des menaces et à cause de la difficulté d'attribution des attaques (de l'effecteur, du donneur d'ordre ou de l'objectif recherché, le tout combiné à des attaques qui peuvent être des leurres). L'intégration croissante du cyber dans les autres composantes risque d'obscurcir de nouveau le brouillard de la guerre en perturbant les capteurs, les communications et les systèmes de traitement automatisés de l'information mis en oeuvre dans le cadre de la transformation numérique des Armées. Au delà de l'aspect opérationnel, une cyberattaque peut être utilisée pour « produire de l'incertitude politique » [10]. Dans le cyber, les objectifs d'une opération sont flous et se rapprochent plus du monde du renseignement que de l'action militaire. La difficulté d'appréciation de la situation est renforcée par les logiques de prépositionnement dans les réseaux d'adversaires potentiels, afin de garder un accès pour un usage ultérieur, ce qui permet de ralentir la vitesse d'exécution des étapes d'une opération cyber afin d'augmenter la furtivité en noyant les traces dans la masse.

À l'incertitude exogène vient s'ajouter le spectre d'une *menace endogène*, rejoignant en cela les problématiques du renseignement. Celle-ci provient le plus souvent d'un acte involontaire, c'est ce qu'exploitent les différentes techniques d'ingénierie sociale afin de faire pénétrer les charges utiles sur les infrastructures cibles en contournant leurs protections périmétriques. La menace peut aussi provenir d'actions volontaires du personnel. Réduire ce risque passe par une sensibilisation à l'hygiène numérique pour se prémunir des actes involontaires, par la limitation de l'exposition informationnelle des employés en cybersécurité [11] notamment sur les réseaux sociaux, par un contrôle d'accès (physique, logique) et par l'instauration d'un besoin d'en connaître afin de cloisonner les systèmes à tous les niveaux.

Le milieu cyber offre un *avantage écrasant à l'action offensive* en terme d'initiative (déjà le cas dans les conflits traditionnels), de réactivité mais aussi en matière d'économie de ressources. Le défenseur doit protéger l'intégralité des systèmes car il suffit d'une seule faille dans un ensemble

5. Par un recours massif à la sous-traitance et au fonctionnement en écosystème.

6. La complexification des systèmes de sécurité en fait la clé de voûte des entités à défendre et des cibles de choix.

7. Le délais moyen entre la publication d'une zero-day et l'application d'un patch est de plus de deux mois (SGDSN. *Revue stratégique de cyberdéfense*. 2018).

8. Par une remontée plus rapide de l'information, l'instantanéité des échanges et l'abstraction de la distance.

9. S. Bombal et V. Le Bihan. « Planifier et conduire les opérations numériques ». In : *La Cyberdéfense*. U. Paris : Armand Colin, 2018, p. 218-232, p. 227.

10. J. Nocetti. « Géopolitique de la cyber-conflictualité ». In : *Politique étrangère* Été.2 (2018), p. 15-27, p. 19.

11. Les experts sont des cibles de choix pour les agences de renseignement comme pour les chasseurs de tête, du fait de la très fort tension dans le recrutement.

de systèmes pour le compromettre. Pour compliquer le tout, la surface d'attaque des systèmes à protéger est en expansion permanente du fait de l'introduction de nouveaux usages et de nouvelles technologies souvent peu matures et peu connues des défenseurs. Ceci entraine une relation asymétrique en terme de moyens nécessaires, à l'inverse de la relation classique entre attaque et défense. Ces attaques peuvent être menées en tout temps et en tout lieu (même lorsque la cible est déconnectée du réseau, il suffit d'utiliser un vecteur humain), le tout en restant discret, voire indétectable, pendant une longue période de temps, et en prenant des risques assez faibles. Le processus d'attribution favorise l'offensive, par le délai important entre attaque et attribution, l'impossibilité de fournir des preuves irréfutables affaiblit la capacité dissuasive des acteurs, la grande difficulté de répondre dans la même temporalité que l'attaque et la détermination politique de la victime [12]. De plus, attribuer pose un dilemme au défenseur entre risque d'escalade et coût réputationnel d'un coté et, de l'autre, le risque d'être de nouveau victime d'autres attaques par la suite. Dans le contexte du cyberespace, la défense a perdu tout avantage stratégique. La place de l'offensive est à nuancer au niveau tactique : une fois qu'un attaquant a pris pied, il est en terrain hostile et la détection se fera, dans un système correctement défendu, à sa première erreur technique ou organisationnelle.

La LIO offre une grande flexibilité d'emploi par la *diversification de ses effets* qui peuvent être d'ordre matériel, comme la neutralisation d'un système d'arme, la collecte de renseignement, la lutte informationnelle. Le domaine cyber offre un contrôle théorique accru sur les effets, ceux-ci peuvent être temporaires, réversibles ou définitifs. En pratique, estimer et contrôler les effets réels reste une science compliquée et souvent inexacte (Section 2.7). De plus, ils peuvent s'étendre du niveau tactique au niveau stratégique en fonction des besoins. Les actions cyber offensives sont un très bon moyen pour démultiplier les effets d'une opération classique afin d'atteindre un objectif stratégique pour un coût en ressources et une prise de risque faibles. À l'opposé, la surface d'attaque est démultipliée par la taille de l'écosystème numérique d'une Nation, de son avancée technologique et de son ouverture.

La flexibilité de l'emploi et la difficulté à attribuer une attaque permettent d'agir en évitant les pénalités liées au recours à la force armée par un contournement par le bas de l'ordre établi, en restant en dessous du stade de la légitime défense ou en étant par exemple dans la zone grise de l'article 5 de l'OTAN [13]. L'usage de groupes non-étatiques comme proxy permet le déni plausible et donc favorise un usage décomplexé de la force. En prenant en compte sa facilité d'usage et l'avantage écrasant donné à l'offensive, le cyber offre un pouvoir égalisateur (notamment entre puissances étatiques et non étatiques) dans la mesure où les enjeux restent assez faibles, pouvoir qui reste bien inférieur à celui de l'atome. Aujourd'hui le cyber ne peut sanctuariser un territoire face à une puissance conventionnelle ou nucléaire. L'arme cyber [14] permet aux États de remettre en cause l'ordre établi par le biais d'intrusions et de perturbations nuisibles, permanentes et systématiques. Par ailleurs, le système international est affecté par l'émergence d'acteurs non-étatiques qui peuvent s'attaquer à des États voire mettre en jeux leur sécurité nationale. La technologie a un effet nivelant par la facilité de disposer de capacités cyber intermédiaires grâce au développement d'un marché parallèle et du "faible" coût en moyens humains et financiers nécessaires. À l'inverse les technologies militaires essentielles à un affrontement de haute intensité ou à des opérations très ciblées accentuent les déséquilibres dans les rapports de forces entre États [15] en faveur de ceux ayant procédé à un développement capacitaire important au premier rang desquels se trouvent les États-Unis et la Chine.

Les forces occidentales sont de plus en plus *exposées techniquement et informationnellement*. L'évolution des armements et des équipements les rendent plus vulnérables à des perturbations de la connectivité sur un théâtre d'opération. Les UAV (drones) sont les plus exposés, notamment

12. S. Taillat. « Le cyberespace et la conflictualité internationale ». In : *La Cyberdéfense*. U. Paris : Armand Colin, 2018, p. 26-33, p.28.

13. Lors du sommet de l'OTAN du 14 juin 2021, réaffirme dans sa déclaration que le Conseil de l'OTAN peut invoquer l'article 5 suite à une cyberattaque « au cas par cas » (NATO. *Communiqué du sommet de Bruxelles publié par les chefs d'État et de gouvernement participant à la réunion du Conseil de l'Atlantique Nord tenue à Bruxelles le 14 juin 2021*. URL : `http://www.nato.int/cps/fr/natohq/news_185000.htm` [visité le 24/06/2021])

14. L. Kello. *The Virtual Weapon and International Order*. Yale University Press. 22 août 2017.

15. Taillat, loc. cit.

dans le cas de l'U.S. Air Force qui les utilise en Irak, en Syrie ou encore en Afrique depuis l'Europe ou l'Amérique, à la différence des forces françaises qui projettent les pilotes de drones sur le théâtre d'opération. En pratique, opérer des flottes d'UAV à distance nécessite de s'appuyer sur les câbles sous-marins [16] à cause de leurs besoins en terme de latence et de bande passante, ce qui les rend vulnérables. En Décembre 2008, les trois câbles sous-marins centraux reliant l'Italie à l'Égypte ont été endommagés ; cela a entrainé une diminution de près de 80% de la connectivité entre l'Europe et le Moyen -Orient et de près de 95% des communications stratégiques américaines dans la zone, car les armées projetées s'appuient massivement sur l'infrastructure civile perturbant fortement les opérations des 200 000 soldats anglo-américains alors présents en Irak avec par exemple le passage de centaines à quelques dizaines de sorties de drone par jour [17]. La numérisation des armements, commencée dès la fin de la guerre froide, et leur organisation en réseau posent la question de leur maitrise, comme celle de leur plateforme. Seront-ils opérationnels le moment venu ou paralysés par une frappe cyber ? La perturbation de la défense anti-aérienne syrienne en 2007 lors du raid israélien contre la centrale en construction d'Al Kibar en est l'archétype. En 2009, des Rafales et des ordinateurs de la base aérienne 107 de Villacoublay ont été temporairement paralysés par le malware Conficker [18]. Lors du FIC 2019, Florence Parly, alors ministre des Armées, annonce qu'une opération offensive du groupe russophone Turla a ciblé la chaîne de ravitaillement en fuel des navires de la Marine Nationale de fin 2017 à avril 2018 [19]. Les équipements de dernière génération sont encore plus vulnérables, à l'image du F-35 américain. Ses systèmes sont composés de plus de 30 millions de lignes de code. Des failles exploitables ont été mises en évidence dans l'aide à la reconnaissance des cibles, les systèmes de simulation et de maintenance préventive qui pourraient, suite à des interceptions, servir à renseigner l'adversaire ou à compromettre le bon fonctionnement des appareils. Les nouveaux programmes d'armement, principalement à travers les faiblesses cyber de la BITD, sont des cibles de choix pour de l'espionnage stratégique et industriel, par exemple près de 50 téraoctets de données concernant le F-35 ont été dérobés par des groupes proches du pouvoir chinois. La dissipation du brouillard de guerre s'appuie de plus en plus sur la capacité de visualisation mais aussi sur du renseignement d'origine cyber, les deux s'appuyant sur un triptyque [20] acquisition, fusion puis dissémination des données. Cette évolution s'accompagne d'une nouvelle faille, rendant possible l'empoisonnement des modèles d'analyses par des données spécifiquement forgées à cet effet. Des attaques plus classiques visant à perturber les capacités d'acquisition mais aussi l'interconnexion entre les systèmes d'information et les autres plateformes et systèmes d'armes accroissent les dommages potentiels qui peuvent résulter de la pénétration d'un de ses systèmes par latéralisation.

Les *frontières des théâtres d'opérations ne cessent de s'effacer*. Il y a peu, l'éloignement des terrains d'opérations extérieures permettait un certain contrôle des flux d'informations. Aujourd'hui, la contraction des distances et des délais de propagation entrainent une répercussion sur le sol national [21]. Le phénomène a commencé avec le terrorisme des années 1970 mais il est exacerbé par la transition numérique et la montée en puissance des capacités d'influence des acteurs. Pour ces même raisons d'instantanéité, de diversité des effets et d'abstraction des distances, les *niveaux tactiques opératif à stratégique s'écrasent* et se confondent en matière d'opération numérique et d'influence numérique [22]. La conduite des opérations restent similaire entre les différents niveaux, avec une forte centralisation en métropole au sein du COMCYBER en France (ou CyberCom outre-Atlantique), les objectifs et l'exploitation des effets diffèrent.

Enfin, la *frontière entre civils et militaires s'estompe*. La place de la société civile oscille entre

16. R. Sunak et J. Stavridis. *Undersea cables : indispensable, insecure*. Policy Exchange, 2017, p.22.
17. Ibid.
18. H. Leroux. *Cyber guerre : la montée des périls*. url : `https://www.ifri.org/sites/default/files/atoms/files/044_051_cyberguerre-2.pdf` (visité le 17/07/2020).
19. *Un groupe de pirates informatiques russophones a visé la chaîne d'alimentation en carburant de la Marine nationale*. 18 janvier 2019. url : `http://www.opex360.com/2019/01/18/un-groupe-de-pirates-informatiques-russophones-a-vise-la-chaine-dalimentation-en-carburant-de-la-marine-nationale/`.
20. Mise en avant par la LPM 2019-2025.
21. Les campagnes de propagande de DAESH, l'instrumentalisation des pertes et des erreurs de forces occidentales.
22. B. Boyer. « Les opérations sur l'environnement : la nouvelle guerre de l'information ». In : *La Cyberdéfense*. U. Paris : Armand Colin, 2018, p. 209-217, p. 215.

acteur incontournable et victime. Le numérique a opéré un renversement des positions entre monde militaire et civil pour le contrôle, l'utilisation et le développement de la technologie mais aussi de par les attributions traditionnellement régaliennes que s'octroient les société privées dans l'attribution et dans la riposte : l'État ne dispose pas du monopole de l'usage de la force. Un nombre croissant d'entreprises de cybersécurité, disposant d'équipes dédiées au repérage et à l'analyse des menaces cyber, révèle publiquement le contenu de ses recherches [23] fournissant ainsi une attribution technique indépendamment de la position étatique. Par exemple, le piratage ayant touché le parti démocrate en 2016 [24] a été attribué aux APT Fancy Bear et Cozy Bear par l'entreprise américaine de cybersécurité Crowdstrike [25]. Les acteurs privés sont fortement impliqués dans les opérations de hack-back [26] (parfois appelées cyberdéfense active). La défense passive s'appuie largement sur le secteur privé : les fournisseurs d'accès pour sécuriser les réseaux, les plateformes ou les éditeurs de logiciel pour gérer les vulnérabilités. Les positions des États sont assez divergentes sur ces sujets, certains s'opposent à toute forme de hack-back de la part d'acteurs privés, d'autres souhaitent leur laisser la possibilité de répliquer. L'intégration d'acteurs civils dans les opérations cyber (en Occident, en Russie ou en Chine) complique l'application du principe de discrimination du DCA et renforce l'incertitude régnant dans le cyberespace. Ceci pose la question de l'articulation entre puissance publique et puissance privée, mêlant compétition entre acteurs, tentative de régulation étatique mais aussi, de la part d'acteurs privés, construction d'une forme de coopération dans les pays anglo-saxons ou en Israël, voire une forme d'intégration pour les Chinois, les Russes.

A l'inverse, *la société civile est de plus en plus exposée et ciblée*. Les États sont dans l'incapacité de parer les coups portés contre leurs ressortissants et leurs infrastructures. La défense ne peut se faire, sauf à construire un "Great firewall" à la chinoise, à la frontière du réseau national (si tant est que puisse être clairement définie une frontière). L'évolution des pratiques tend à accroitre la vulnérabilité des sociétés, comme par exemple le principe du Bring Your Own Device qui consiste à utiliser des équipements personnels sur le réseau d'une organisation (ordinateur portable, téléphone) ou celui du "Shadow IT", qui correspond au déploiement d'infrastructures et de services au sein d'une organisation sans en informer la direction, sans compter le télétravail parfois déployé dans l'urgence au mépris des règles élémentaires de sécurité. L'exposition est renforcée par une désynchronisation des rythmes entre le développement des menaces et l'évolution des technologies, source de déviance aux règles d'hygiène numérique par méconnaissance ou par nécessité.

2 Le cyber : une arme d'emploi

Le COMCYBER [27] définit trois cadres d'emploi des opérations offensives couvrant à la fois les niveaux tactique et stratégique : l'évaluation des capacités adverses (renseignement d'origine cyber), leur réduction ou leur neutralisation (Lutte informatique offensive) et l'action sur les représentations (opérations militaires d'influence) ou la capacité d'analyse adverse. Ils se déclinent au niveau stratégique et tactique. Des opérations offensives peuvent être menées dans le cadre d'une défense active afin de caractériser une attaque ou faire cesser une agression contre les systèmes. Dans le cas français, de telle opérations ne peuvent être conduites que lorsqu'une attaque vise « exclusivement les capacités opérationnelles des armées ou les chaînes de commandement de la défense » [28]. Dans cette section, nous allons tenter d'apporter des éléments de réponse aux questions suivantes : Comment l'emploi du cyber permet-il d'atteindre l'effet final recherché ? Le cyber est-il l'effecteur principal ou reste-t-il un élément, essentiel, permettant l'exécution de la mission au même titre que la logistique ?

23. Nocetti, op. cit., p. 24.
24. Attaque ayant mené à la divulgation le 22 juillet 2016 de 19 252 emails et 8 034 pièces jointes sur le site internet Wikileaks.
25. CrowdStrike. *Our Work with the DNC : Setting the record straight.* 22 janvier 2020. URL : `https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/` (visité le 16/04/2020).
26. K. Bannelier et T. Christakis. *Cyber-attacks Prevention-Reactions : The Role of States and Private Actors.* Paris, 2017, p. 88, p. 56-80.
27. COMCYBER, op. cit.
28. Ibid.

2.1 L'appui aux forces

Au niveau tactique, l'emploi tient de la stratégie contre-forces. Les frappes cyber permettent la décapitation ou la paralysie de groupes terroristes en attaquant les communications entre insurgés. Sur la période 2007-2008 en Irak, des campagnes d'intoxication utilisant les outils de communication des réseaux ont permis de favoriser leur localisation (donc l'élimination) et de déstabiliser l'organisation des groupes en ciblant les maillons les plus faibles par des actions informationnelles [29]. La LIO peut aussi être utilisée contre les forces d'autres nations en ciblant des systèmes d'armes pour les mettre hors service, par contre rares sont les exemples en sources ouvertes. Un certain nombre d'États, au premier rang desquels se trouvent les États-Unis et la Russie, utilisent des moyens cyber pour soutenir des opérations spéciales voire clandestines [30]. Cela peut permettre de modifier l'environnement d'action des forces en mettant en place une bulle d'exclusion informationnelle autour des unités opérant dans la profondeur, ou encore en perturbant les communications adverses pendant une action afin d'affaiblir les capacités de riposte [31] ou de pouvoir affiner la cartographie des forces en présence en liant opération cyber et guerre électronique.

Au niveau stratégique, la LIO permet de déstabiliser une zone avant, ou pendant, une opération militaire conventionnelle en ciblant des infrastructures privées et militaires. En 2008, des actions russes ébranlent la Géorgie pendant la guerre de l'été [32] : avant l'offensive, les sites institutionnels sont mis hors service comme les systèmes permettant l'organisation d'une potentielle riposte au premier rang desquels les forums des hackers géorgiens. Au fur et à mesure de l'avance russe, les cibles évoluent pour maintenir une bulle de silence médiatique autour des opérations en cours en ciblant les sites web relayant l'avancée des troupes. Elle peut confiner, en la couplant à des mesures de guerre électronique, un territoire en vue de son contrôle comme ce fut le cas lors de la prise de la Crimée en 2014 par les forces russes. L'action offensive peut être utilisée en substitution à une frappe conventionnelle pour éviter les désagréments associés (attribution, riposte, escalade potentielle) comme en 2010 avec l'usage du virus Stuxnet pour saboter les centrifugeuses d'enrichissement d'uranium de Natanz (Iran) ou plus récemment en riposte aux attaques contre les infrastructures pétrolières saoudiennes. Elle sert à user l'adversaire, en frappant ses systèmes critiques et sa légitimité comme lors des opérations en 2015-2016 contre le système de distribution électrique et contre le gouvernement ukrainien. Enfin, face à la multiplication des bulles AD/2D de déni d'accès et interdiction de zone [33], le cyber peut être utilisé comme un mode d'action facilitant l'entrée en premier sur un territoire dans une zone d'interdiction aérienne. Des éléments de lutte électromagnétique ont, d'après les sources ouvertes, été utilisés par l'aviation israélienne en septembre 2007 comme vecteur de transmission d'un malaware ciblant et perturbant des infrastructures radars en Syrie afin de tromper la surveillance de l'espace en soutien à la destruction de la centrale nucléaire en construction d'Al-Kibar

2.2 Modes opératoires dans le spectre de la manœuvre hybride

Le cyber contrôle de zone est intéressant car il combine opérations techniques, contrôle informationnel et renseignement et même des opérations relevant d'autres domaines comme la guerre électronique pour brouiller des portions de territoire. Il peut se pratiquer avec plus ou moins de finesse, et à diverses échelles. Pendant les printemps arabes, l'Égypte coupe tout accès à internet, la Libye entrave fortement l'accès et brouille la réception satellitaire, la Syrie filtre plus finement

29. S. Taillat. « Chapitre 7. Doctrines et dispositifs. Dissuasion et coercition ». In : *La Cyberdéfense*. U. Paris : Armand Colin, 2018, p. 141-149, p. 148.

30. SGDSN, op. cit., p. 52.

31. Intervention de Luc, un ancien agent de la DGSE le 07/11/2019 dans le cadre des conférences de Sécurité/Défense du Magistère de Relations Internationales et Action à l'Étranger (MRIAE) de Paris 1

32. A. Namor. « Les opérations numériques dans les conflits contemporains ». In : *La Cyberdéfense*. U. Paris : Armand Colin, 2018, p. 199-208, p. 204.

33. Le déni d'accès représente les actions mises en œuvre pour interdire l'accès à un théâtre d'opérations tout comme celles visant à empêcher tout déploiement sur ce même théâtre. L'interdiction de zone représente les actions déployées sur le théâtre d'opérations pour restreindre la liberté d'action d'un adversaire à proximité d'une zone donnée.

et laisse un accès restreint aux réseaux sociaux pour faciliter l'action des services de renseignement. En novembre 2019, l'Iran s'est coupé des réseaux mondiaux tout en assurant la continuité de ses services et de ses infrastructures. Le cyber contrôle de zone se heurte à trois limitations : la dégradation de l'image internationale du pays [34], les mesures de confinement qui peuvent être contournées (comme en Libye) et surtout une approche trop stricte s'opposant à des impératifs de renseignement (déportement vers d'autres moyens d'échange). Au delà des conflits internes, il permet de cloisonner un adversaire dans des moyens de communication moins sécurisés ou moins efficaces (Ukraine, Syrie) et il semble particulièrement bien adapté à de brèves phases d'engagement en tirant partie de la réversibilité des actions. Suite aux attaques chimiques de Douma en avril 2018 par les forces loyalistes, la Russie a déployé une stratégie informationnelle tous azimuts visant à désorienter les dirigeants occidentaux et les opinions publiques [35].

L'Ukraine offre un cas d'étude intéressant car elle a été le théâtre de l'application et du test de stratégie mêlant cyber et opérations hybrides. Cartographions la situation de l'Ukraine dans les différentes couches du cyberespace avant le début des hostilités : malgré une bonne connexion au monde extérieur et une densité nationale satisfaisante, le réseau comporte une faiblesse majeure, les IXP [36] ukrainiens sont majoritairement situés dans les zones dites « russophones » d'Ukraine [37]. Dès le début des opérations, les forces présentes aux deux points d'accès terrestres de la Crimée (isthme de Perekop et Flèche Tatare) ont momentanément interrompu le trafic afin d'isoler la presqu'île et pris le contrôle de l'IXP de Simferopol. De plus, plusieurs cyberattaques ont déjà eu lieu depuis le début du mois de mars, visant à perturber la structuration de la riposte. Les premières furent probablement d'origine russe [38], les plus récentes se sont vraisemblablement appuyées sur les infrastructures situées en Crimée, une zone aujourd'hui sous contrôle de l'armée russe.

2.3 Contre-terrorisme et cyber

La NSA et l'U.S. Cyber Command ont mené une vaste opération d'influence, de type cyber-enabled technical influence operations, dans le cadre de la lutte anti-terroriste appelée Glowing Symphogny [39] visant à perturber les moyens de cyber de DAESH, à savoir les communications, les outils de propagande, de communication, de recrutement et de financement. L'un des axes de l'opération, en plus des opérations classiques de LIO visant à rendre inutilisable un service ou une infrastructure, a été de créer une série sans fin de perturbations désorganisant le mode opératoire de l'organisation. L'opération a débuté en novembre 2016 et a été menée par la task force ARES mise sur pied au printemps de la même année [40]. ARES est composée d'experts à la fois de la LIO et du contre-terrorisme mais aussi du comportement. Son objectif est d'exploiter la faille de l'organisation de l'EI, à savoir la forte centralisation de la distribution du contenu. Le cœur de la structure n'était constitué que d'une dizaine de comptes et de serveurs centraux permettant de gérer l'ensemble du réseau médiatique de l'organisation. La compromission initiale se fit, d'après les documents déclassifiés, par une attaque de phishing classique. Puis quelques mois furent consacrés à la latéralisation et la préparation de l'offensive et à de petites actions contre les infrastructures hébergeant le contenu de Daesh afin de démontrer la possibilité de frappes chirurgicales pour ne pas mettre en péril les infrastructures civiles ou critiques attenantes, comme par exemple lorsque du contenu était hébergé sur des serveurs d'hôpitaux. La première phase de l'opération Glowing Symphony débute fin 2016 avec la prise de contrôle des serveurs centraux et comptes de gestion. Ensuite, la deuxième phase fut plus fine, l'objectif étant de ne mettre en œuvre que des actions

34. Si le régime politique est menacé, il est très improbable que cela constitue un frein à l'emploi.

35. J. Nocetti. « Dazed and Confused : Russian "Information Warfare" and the Middle East – The Syria Lessons ». In : (février 2019), p. 12.

36. Ce sont des points d'interconnexion physiques permettant aux fournisseurs d'accès d'échanger du trafic.

37. K. Limonier. *CARTO-UKRAINE. Quelques (cyber)considérations.* Poussières d'empire. URL : `https://villesfermees.hypotheses.org/243` (visité le 10/04/2020).

38. Ibid.

39. H. Lin. « On the Integration of Psychological Operations with Cyber Operations ». In : *Lawfare* (9 janvier 2020). (Visité le 29/05/2020).

40. *USCYBERCOM After Action Assessments of Operation GLOWING SYMPHONY | National Security Archive.* URL : `https://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-01-21/uscybercom-after-action-assessments-operation-glowing-symphony` (visité le 30/05/2020).

pouvant passer pour accidentelles, en ralentissant artificiellement les temps de téléchargement, en perturbant les connexions, en renvoyant de temps en temps des erreurs, en vidant les batteries des téléphones ou en faisant en sorte que les premières tentatives de connexion à un compte échouent. Le tout est de pouvoir opérer sous le radar, de perturber l'organisation et provoquer des tensions internes. Selon l'article de NPR [41], l'opération a été un succès car DAESH a dû changer son modus operandi dans le cyberespace au pied levé, affaiblissant ainsi son organisation.

2.4 Le cyber : le terrain de jeu du renseignement

Dans le cyberespace, l'espionnage est une composante essentielle des opérations numériques ciblées afin de mieux connaitre la cible, de trouver une ou des failles (humaines ou techniques) et mieux appréhender l'organisation cible. La récolte d'information constitue l'un des objectifs récurrents des cyber-attaques étatiques [42] pour s'installer durablement dans les réseaux et systèmes adverses, pour réaliser de l'espionnage industriel, du vol de propriétés intellectuelles ou pour compromettre (ou faire pression sur la cible). Ces différents objectifs peuvent s'entremêler, l'espionnage peut servir de prérequis à la conduite d'une opération de coercition ou d'une action contre des systèmes critiques. La nature de l'action évolue en fonction des opportunités, de l'évolution du contexte opérationnel, stratégique et politique [43].

Dans l'ensemble, les caractéristiques du cyber en font un milieu favorable aux activités d'espionnage. La clandestinité est favorisée par l'opacité provenant des différents moyens d'anonymat, des opérations sous false flag, de la grande difficulté relative à l'attribution. Le cyberespace donne la possibilité de faire faire très facilement, permettant aux services d'opposer un déni plausible, en s'appuyant sur des proxies, sur le marché noir et les services de mercenariat qui se développent ou même sur des prestations d'entreprises privées. Le terme de guerre des courses donne une bonne image des tendances actuelles, avec des acteurs agissant sous l'autorité d'autres. Mais à la différence du parallèle historique, les relations sont plus floues, le nombre d'acteurs plus grand et le champ d'action global touchant le coeur même des sociétés civiles.

Les objectifs de renseignement peuvent s'opposer à des missions de protection ou à des actions offensives. Pour se protéger dans la couche sémantique, une des options explorée est de mettre en place un contrôle de contenus à caractère terroriste ou en faisant l'apologie. Celui-ci a été introduit par la loi du 13 novembre 2014 autorisant le blocage administratif de sites web puis renforcé par le règlement européen relatif à la prévention de la diffusion de contenus à caractère terroriste en ligne de 2019 qui prévoit un retrait dans l'heure des contenus sur les plateformes. Les effets de ces mesures sont duales. D'un côté elles visent à casser la chaine de propagation virale [44] offerte par la structure des plateformes. D'autre part, le risque est d'entrainer un déportement de la propagande vers d'autres moyens de diffusion plus difficiles à contrôler et pouvant passer plus facilement sous les radars, par exemple à travers par des groupes de discussions fermés utilisant des protections techniques simples mais efficaces comme du chiffrement de communication.

Au niveau logique, la tendance est à la démocratisation des techniques de chiffrements pour se protéger contre le vol de données. D'un coté cela renforce l'état moyen de cybersécurité des acteurs, de l'autre, le travail des services de renseignement (cela complique aussi la détection de cyberattaques par analyse du réseau) s'en trouve pertubé. En France, la stratégie est de lutter contre toute idée d'embarquer des backdoors, malgré certaines velléités politiques, car une porte d'entrée peut être utilisée par n'importe qui. Pour permettre aux services de travailler, deux modes d'interactions sont possibles avec les acteurs privés mettant en œuvre des solutions de chiffrement des communications et des contenus. Le premier repose sur la collaboration avec les Over-the-top service (ou offre hors du fournisseur d'accès à l'internet ou service par contournement) (OTT) (service par contournement en français), comme par exemple Whastapp, et avec les opérateurs

41. « How The U.S. Hacked ISIS ». In : *NPR* (26 septembre 2019). (Visité le 30/05/2020).
42. Q. E. Hodgson et al. *Fighting Shadows in the Dark : Understanding and Countering Coercion in Cyberspace*. Santa Monica : CA : RAND Corporation, 2019.
43. Taillat, *Le cyberespace et la conflictualité internationale*, p. 27.
44. La structure d'un réseau social permettant une propagation exponentielle pendant les premiers temps (D. H. Zanette. « Dynamics of rumor propagation on small-world networks ». In : *Physical review E* 65.4 [2002], p. 041908).

de communications électroniques (OCE), comme Orange. L'autre option possible est de se servir, cependant cela nécessite l'emploi de ressources conséquentes car il faut disposer de vulnérabilité zéro-days et de la main d'œuvre nécessaire, le tout face à des opérateurs en pointe dans le monde numérique.

Enfin, chercher à appliquer des effets de manière cyber peut se heurter à des logiques du renseignement : l'utilisation d'un accès dérobé ou d'une faille peut le dévoiler et compromettre de futures opérations en faisant disparaitre une source. Ces frictions sont d'autant plus succeptibles d'apparaitre dans les modèles d'organisation où un service de renseignement concentre la grande majorité des capacités cyber offensive (par exemple la DGSE en France.)

2.5 Le cyber au service d'opérations combinées

Guerre électronique La LIO joue son rôle de démultiplicateur d'effets en tirant partie de la mise en réseau des systèmes militaires et en se combinant aux modes d'actions conventionnels. Elle s'interface très bien avec la guerre électronique [45]. L'heure est à la convergence entre systèmes de guerre électronique et cyberdéfense. L'objectif principal étant d'utiliser des capacités de guerre électronique embarquées sur des avions, des drones (ou autre) afin de fournir un vecteur déporté nécessaire pour mener des opérations cyber contre des systèmes possiblement inaccessible depuis les réseaux classiques.

Prendre pied dans un système d'arme actuel devient particulièrement pertinent à l'heure de l'infovalorisation, des technologies diverses de cloud de combat qui cherchent à mettre en réseau (au moins localement) des plateformes d'armes entre elles. Par exemples, les Etats-Unis modernisent les nacelles de guerre électronique (passage des AN/ALQ-99 aux Next Generation Jammers, la capacité opérationnelle de ces derniers devraint être prononcée en 2022) des EA-18G Growler [46] ce qui leur permettra de mener de opérations cyber offensive. Les satellites sont aussi vulnérables à ce type d'attaques, par exemple les Etats-Unis se sont dotés de systèmes de guerre électronique (terrestres) pour perturber les communications spatiales [47]. De même, il faut s'attendre au déploiment de charge utiles cyber à partir de satellites (comme relais) - qu'ils soient compronis ou conçus pour ce faire.

Plus généralement, au déla de la connectivité physique et des communications électromagnétiques tous les capteurs optroniques sont des portes d'entrées pour des attaques d'origines "cyber". Par exemple, un algorithme de reconnaissance de forme derrière une caméra peut être attaquer en forgeant une séquence d'images qui sera mal interprétée ; cela peut aller d'une mauvaise reconnaissance (une menace étant détectée comme un allié ou bien ouvrir un chemin d'accès potentiel pour une compromission plus avancée du système.)

Opérations d'influence, psyops et cyberespace Les opérations d'influence (aussi appelées information warfare) sont apparues, sous cette dénomination, au sein de l'armée et de la communauté du renseignement américain dans les années 1980. Elles regroupent une grande variété d'activités liées à la guerre psychologique [48], comprenant la collecte d'informations tactiques, la validation d'informations, la propagation ou la désinformation afin de perturber la population ou les forces adverses, ou encore la lutte contre les opérations d'influence adverse. Les opérations d'influence s'articulent avec les activités diplomatiques, les opérations militaires et la contre-ingérence.

L'Occident démarre avec un temps de retard dans la prise en compte de l'importance du cyber comme vecteur d'influence. Son réveil remonte aux années 2015-2016 alors que, dès la construction du cyberespace, le contrôle de l'information et la cyberdéfense technique ont été les deux faces d'une même pièce pour la Russie et la Chine. Par exemple, les unités russes chargées de la cyberdéfense sont le plus souvent rattachées aux organisations en charge de la manipulation de l'information.

45. Utilisation à la fois de frappe cyber et brouillage pour déstabiliser l'Ukraine en 2014

46. M. Pomerleau. *US military to blend electronic warfare with cyber capabilities*. C4ISRNet. 14 avril 2021. URL : `https://www.c4isrnet.com/electronic-warfare/2021/04/14/us-military-to-blend-electronic-warfare-with-cyber-capabilities/` (visité le 13/07/2021).

47. N. Strout. *This is what the Space Force will use to jam enemy satellites*. C4ISRNet. 8 avril 2020. URL : `https://www.c4isrnet.com/electronic-warfare/2020/04/08/this-is-what-the-space-force-will-use-to-jam-enemy-satellites/` (visité le 13/07/2021).

48. A. Kiyuna et L. Conyers. *Cyberwarfare Sourcebook*. Lulu. com, 2015.

Aujourd'hui encore, l'influence reste assujettie à la technique et en soutien aux opérations dans la conception occidentale. Les Américains ont théorisé l'« information warfare » dans le milieu cyber comme l'utilisation de l'avancée technologique au service du contrôle de l'information. En France, le document de prospective stratégique *Action Terrestre Future* de 2016 en fait un facteur de supériorité opérationnelle et les éléments de doctrine du COMCYBER considèrent la sphère informationnelle comme l'un de leur trois terrains d'action.

Les évolutions technologiques et socio-économiques transforment l'environnement informationnel et renforcent la place du cyberespace. La création et la diffusion d'information ne sont plus concentrées entre quelques mains mais largement décentralisées (le contrôle tend à se centraliser dans les mains de quelques plateformes). Dans le même temps, le système médiatique est fragilisé par les choix économiques des médias traditionnels au détriment de l'intégrité et de la correction des informations. Les individus sont eux aussi soumis à une évolution similaire, en partie du fait de l'instantanéité des communications : ils ont perdu l'habitude de vérifier et croiser leurs sources. Cela les rends d'autant plus vulnérables aux campagnes d'influence.

Les objectifs, les cibles et les concepts stratégiques des cyber opérations d'influence (CIO) sont utilisés en dehors de la sphère cyber [49]. La différence se fait au niveau des outils, des acteurs et de l'échelle, du fait des spécificités du cyberespace que sont l'instantanéité de la transmission, la propagation en exponentiel, la grande diversité de plateformes ainsi que la facilité d'automatisation des procédés et l'ubiquité du milieu [50]. Le développement des techniques de publicité ciblées fournit d'excellents outils pour définir les cibles potentielles de campagne d'influence [51].

Les objectifs principaux sont la modification de la motivation et des idées des cibles. Ils peuvent varier en fonction du contexte et inclure par exemple la déstabilisation d'une région ou, dans le cadre d'un conflit armé, s'attaquer à la volonté de se battre des forces adverses. Les cibles se répartissent en trois groupes [52] : les cibles de masse à l'échelle d'une société, souvent utilisées lorsque l'objectif est de s'attaquer à des infrastructures critiques comme un gouvernement ou un système de vote, avec des messages reposant sur les symboles et l'histoire communément partagés par la société ; le ciblage socio-démographique revient à concentrer l'action sur une région, sur une minorité ou sur le personnel militaire dans un conflit avec des messages adaptés au contexte ; le ciblage psychologique correspond à la sélection d'individus en fonction de leur profil et la mise au point d'une communication personnalisée. Les technologies actuelles commencent à permettre le passage à l'échelle du ciblage psychologique en s'appuyant sur des techniques de recommandation, alimentées par les grandes quantités de données personnelles disponibles, pour définir les cibles puis en utilisant des systèmes de synthèse automatique ou semi-automatique (en s'appuyant par exemple sur des unités de "trolls" professionnels).

La large diffusion des technologies cyber, ainsi que leur faible coup d'entrée, permettent à n'importe qui de s'engager dans des opérations d'influence à échelles variables, que ce soit des acteurs étatiques (comme des actions de déstabilisation lors de l'élection présidentielle des États-Unis en 2016 ou lors du référendum du Brexit), des mouvements hacktivistes, des groupes terroristes (à l'image de Daesh), des réseaux criminels ou des individus isolés, ceux-ci pouvant s'entremêler dans une logique de faire faire et d'utilisation de proxy, notamment de la part d'États. La guerre informationnelle repose « bien moins sur des compétences techniques que sur l' informationnel généré par une attaque » [53] que ce soit de la part d'un acteur non étatique ou de la part d'un État . En effet, il suffit de savoir faire de la retouche d'images et utiliser les réseaux sociaux pour pouvoir se lancer dans l'influence. De plus, ces dernières années ont vu se démocratiser les techniques de "deepfake" donnant naissance à des outils faciles et assez puissants d'édition vidéo et audio, tel FaceApp qui permet de changer les visages d'une vidéo afin de faire des faux convaincants. Être

49. *Cyber Influence Operations : An Overview and Comparative Analysis*. Zurich : Center for Security Studies (CSS), ETH Zürich, octobre 2019, p.11.

50. Limitée par certaines mesures techniques comme par exemple les réseaux fermés et soumis à un fort contrôle comme ceux de la Chine ou de l'Iran.

51. Par exemple utilisés par la société Cambridge Analytica dans le but de mener des campagnes d'influence sur Facebook lors de l'élection américaine de 2016 ou lors du référendum concernant le Brexit.

52. J. Pamment, H. Nothhaft et A. Fjällhed. « Countering information influence activities : The state of the art ». In : (2018).

53. Bertrand Boyer dans Boyer, op. cit., p. 210

en mesure de réussir et d'évaluer ces actions est cependant une autre histoire.

Les cyber opérations d'influence (CIO) peuvent être classifiées entre les opérations d'influences techniquement permises par le cyber (CeTIO) et les opérations socialement permises par le cyber (CeSIO). Les premières sont le plus souvent des opérations de Lutte informatique offensive (LIO) en soutien d'actions d'influence [54] afin de perturber la couche logique du cyber, en détruisant ou altérant des informations sur un système cible [55]. Les secondes ne nécessitent pas l'usage de capacité cyber pour altérer les couches physiques ou logiques du cyberespace, elles se concentrent dans la couche sémantique. Elles sont parfois qualifiées de "soft" opérations d'influence. Elles s'appuient sur diverses techniques comme l'achat de publicité sur les plateformes, l'analyse de données en source ouverte, la publication de contenus plus ou moins ciblés sur diverses plateformes et restent légales dans l'ensemble, à la différence des CeTIO. En effet, l'enjeu tactique est de s'adapter aux évolutions des comportements en cours : l'information de masse se transforme en information individuelle et sélective, les utilisateurs sont alors enfermés automatiquement dans des bulles, ce qui nécessite de mener des actions ressemblant au ciblage marketing. Au préalable, il faut analyser l'environnement et comprendre les mécaniques sous-jacentes. Quels sont les principaux acteurs et les enjeux locaux ? Ceci donne toute sa place au renseignement d'intérêt cyber et aux États pouvant s'appuyer sur des plateformes concentrant les contenus et disposant de nombreux utilisateurs [56].

Ces opérations d'influence sont particulièrement profitables car elles permettent de saper la puissance conventionnelle d'un État en ne nécessitant que de faibles ressources et en offrant une grande flexibilité d'action. Le tout en ne prenant que peu de risques car les risques de détection puis d'attribution sont par nature faibles mais surtout parce que les stratégies d'influence restent bien en deçà du seuil d'emploi de la force limitant ainsi l'escalade et les potentielles représailles. Cependant, comme le souligne le rapport de Center for Security Studies [57], déterminer l'efficacité stratégique (directe ou indirecte) d'opérations d'influence est une chose malaisée par la difficulté à en observer les effets. Pour autant, cela ne signifie pas que de telles actions restent sans conséquence surtout si elles produisent des effets stratégiques. L'administration d'Obama a répondu économiquement et diplomatiquement (voire clandestinement) aux ingérences russes de 2016, cependant les démocraties occidentales n'apparaissent que faiblement armées pour y faire face en temps de paix : regardons le temps qu'il a fallu pour coordonner et mener des actions de contre-influence contre Daesh. Les CIO ne sont pas forcément mises en œuvre contre des puissances étrangères mais aussi dans le cadre de conflits internes comme par exemple en Syrie par les forces d'Assad. Les questions qui se posent à ce jour concernent l'évaluation de l'efficacité de ces opérations et leurs coûts réels.

2.6 De l'utilité stratégique des opérations offensives

Étudier l'utilité stratégique des opérations nécessite de se détacher du déroulé des opérations, savoir qu'un outil offensif est bien conçu donne une information sur l'aspect tactique mais non sur les retombées stratégiques. Il faut s'intéresser aux effets (directs ou indirects) de leur usage. Mesurer la valeur de l'offensive cyber peut se faire à différents niveaux : étudier sa capacité à venir en renfort de la stratégie nationale ou alors s'intéresser à la production des effets recherchés sur un conflit [58] (ou sur les relations internationales). Étudier la première va largement dépendre de la stratégie de la Nation , traiter de la seconde revient à se poser la question de comment conduire une opération cyber qui aide à perturber l'issue stratégique d'un conflit ou à éviter (ou retarder) un conflit comme pour l'opération Olympic Game.

54. V. Mariel chef de bataillon. « L'influence militaire pour créer la surprise dans un champ de bataille transparent ? » In : *Lettre d'information du centre de doctrine et d'enseignement du commandement* (février 2019), p.3.

55. P. Brangetto et M. A. Veenendaal. « Influence Cyber Operations : The use of cyberattacks in support of Influence Operations ». In : *2016 8th International Conference on Cyber Conflict (CyCon)*. IEEE. 2016, p. 113-126.

56. Les États-Unis avec les GAFAM, la Chine avec les BATX, la Russie avec les plateformes composant le Runet

57. *Cyber Influence Operations : An Overview and Comparative Analysis*, p. 20.

58. M. Smeets. « The Strategic Promise of Offensive Cyber Operations ». In : *Strategic Studies Quarterly* 12.3 (2018), p. 90-113.

L'emploi offensif du cyber, espionnage exclu, peut être pensé en tant que stratégie contre-forces ou contre-valeurs [59], en suivant un découpage similaire à celui de la réflexion stratégique sur le nucléaire. Le cyber est une arme d'emploi, le nucléaire non. La logique contre-forces dénote du choix de frapper les forces militaires ou les infrastructures opérationnelles (voire possiblement des proxies) d'un opposant. Par exemple, une telle stratégie fut mise en œuvre dans le cas des attaques DDoS contre les réseaux géorgiens au moment de l'entrée des troupes dans la province d'Ossétie du sud, visant à perturber la logistique et le commandement des forces géorgiennes. Celle de contre-valeurs signifie une action contre les sources de la puissance de son adversaire pouvant englober les infrastructures critiques (approvisionnement en eau, télécommunication, secteur de l'énergie ou de la santé) mais aussi l'économie. L'un des exemples emblématiques en est la vague d'attaques menées contre le réseau électrique ukrainien en 2015. Si techniquement la mise en œuvre des logiques est similaire, les capacités et les ressources nécessaires pour développer les deux logiques tendent à diverger. Individuellement, une attaque dans une logique contre-forces peut être moins coûteuse que dans une logique contre-valeurs car il suffit par exemple de perturber temporairement les capacités de communication dans une zone. Cependant, maintenir un système contre-forces dans le temps et à grande échelle nécessite un investissement conséquent en ressources, humaines notamment, dans sa maintenance et son usage car cela nécessite d'être capable de mener des opérations ciblées. En effet, il faut développer des systèmes pour chaque type de forces (et de systèmes) auquel on veut pouvoir s'opposer et les avoir compromis à l'avance, dans une logique de prépositionnement, pour être en capacité de répondre dans la temporalité adéquate. A l'inverse quand une logique contre-valeurs est privilégiée, les capacités mises sur pied peuvent plus facilement être réutilisées d'un conflit à l'autre et d'un adversaire à l'autre, par exemple en développant un arsenal ciblant les systèmes SCADA présents dans la plupart des systèmes critiques et industriels.

Quatre valeurs stratégiques du cyber se dégagent. Premièrement, les capacités offensives cyber donnent plus d'options au décideur comme dans le cas d'Olympic Games qui a permis d'atteindre deux objectifs vitaux, à savoir ralentir le programme iranien et montrer aux Israéliens une voie n'impliquant pas un conflit ouvert avec l'Iran. Pour certains, le domaine cyber offre des options « pre-escalatory » [60], plus généralement des capacités d'action en tout temps : en temps de paix, de guerre ou entre les deux. Deuxièmement, les capacités cyber offensives peuvent être utilisées, dans une logique contre-forces, en conjonction ou soutien d'autres capacités militaires afin de les démultiplier [61] en ne requérant que de faibles investissements par rapport aux autres capacités. L'efficacité dépendra principalement de l'intégration des forces. Dans la première configuration, le cyber et les capacités conventionnelles remplissent des fonctions séparées mais contribuant à un but commun comme en Géorgie et en Ukraine ; dans la deuxième configuration il y a une interdépendance séquentielle, le succès de l'emploi du cyber est nécessaire à la réussite de l'emploi conventionnel qui va suivre, comme lors de la frappe aérienne contre la centrale de Deir ez-Zor en 2007, conditionnée par la mise hors service des capacités adverses de déni d'accès. Troisièmement afin d'obtenir un ascendant psychologique sur l'adversaire, la mise en œuvre cherche le plus souvent des effets (d'humiliation et de perte de confiance en soi) plus subtils que les OMI traditionnelles. Les deux logiques (contre-forces, valeurs) peuvent impliquer des effets psychologiques directs ou indirects. Enfin, les opérations cyber sont réalisables avec peu (ou pas) de pertes [62] et les effets peuvent être réversibles s'ils sont maitrisés. Mener des opérations cyber nécessite une longue préparation ce qui limite leur emploi tactique et entraine *une compression des niveau tactique et stratégique.*

59. Ibid.

60. H. Lin. « Thinking about Nuclear and Cyber Conflict : Same Questions, Different Answers ». In : *presentation, Hoover Institution/Center for International Security and Cooperation* 15 (2015).

61. Smeets, op. cit., p. 98.

62. Des pertes indirectes peuvent être entraînées par des frappes contre les systèmes critiques. Des actions directes sont aussi théoriquement possibles en attaquant certains objets connectés comme des pacemakers ; le Vice Président Dick Cheney a fait désactiver les fonctionnalités de connection de son implant cardiaque dans la crainte d'une tentative d'assassinat.

2.7 Maitriser les effets

La maitrise de l'emploi de la LIO revient à contenir ses effets, prendre garde à la dualité des technologies afin d'éviter une prolifération, contrôler l'arme tout au long de son utilisation pour éviter son détournement ou sa récupération pour une utilisation par d'autres. Il faut durcir les cyber armureries et prendre garde à effacer les traces pour éviter les vols de charges utiles comme ce fut le cas avec ceux de la NSA, à travers APT EquationGroup, qui ont probablement aidé à la mise au point de WannaCry et NotPetya [63]. Après la découverte de la fuite, la NSA aurait activé ses propres sondes pour détecter l'utilisation de ces outils par des parties tierces, notamment les agences chinoises ou russes. Dans le cas général, il faut considérer qu'un outil cyber employé appartient à la communauté.

Les risques inhérents au milieu doivent être pris en compte : immédiateté de l'action, dualité des technologies (à la fois employées dans le monde civil et militaire), hyperconnectivité afin de limiter les propagations incontrôlées et les dommages collatéraux. Dans le cas du traitement d'un objectif par des munitions conventionnelles, les forces savent cibler et choisir l'armement approprié pour obtenir l'effet final recherché tout en estimant et controlant les dommages collatéraux. Dans le cas d'une action informatique offensive, les effets sont plus difficiles à contraindre au risque de toucher un allié voir ses propres systèmes. Borner les actions d'influence est encore plus difficile.

Le corollaire étant la grande difficulté à estimer, en source ouverte à minima, les effets directes (tactiques) d'une opération cyber offensive, des actions informationnelles, et a fortiori les effets stratégiques. Cela empêche de quantifier la portée politique et stratégique d'opérations cyber sur un conflit, tout comme sur la politique d'un Etat. Prenons le dernier point, la littérature semble démontrer un faible succès des opérations de coercition ; cependant les États continuent à en user [64]. Ceci soulève plusieurs questions : de telles opérations restent-elles rentables du fait du faible coût de mise en œuvre ? Y a-t-il une surmédiatisation des échecs, une sous-visibilité des effets pouvant être indirecte ou toucher des intermédiaires ? En effet, la littérature s'appuie sur des sources ouvertes, dans le cas d'une opération réussie la partie ayant cédé révèle-t-elle les pressions subies au risque d'affaiblir son image et, inversement, lorsqu'une tentative échoue la victime dénonce-t-elle l'opération afin d'écorner l'image de l'adversaire ? Ou alors, cela peut n'être qu'une grande répétition car les États considèrent qu'à terme la numérisation de la société et l'évolution des technologies et des usages vont rendre la coercition cyber efficace.

Conclusion

Le recours à l'action offensive dans le cyberespace est techniquement facilité par un état de sécurité insuffisant, par sa complexité et son caractère englobant. Son utilisation offre des facilités opérationnelles importantes : immédiateté des effets (au prix d'une longue préparation), compression des distances et centralisation possible des effecteurs (étatique) sur le sol national. Enfin, la LIO est une arme d'emploi fournissant une souplesse d'utilisation propre à séduire le politique de par l'incertitude qu'elle produit, le contournement de l'ordre établi en restant au-dessous de l'agression armée, le secret qui l'entoure, la diversité des effets proposés et l'absence, pour l'instant, de létalité directe. En contre partie, cela entraine une modification des conditions opérationnelles avec une cyberdéfense omniprésente tant pour la protection des forces que pour le bon déroulement des opérations, qui nécessite une supériorité cyber pontuelle. La LIO est un outil d'appui essentiel des forces, permettant la démultiplication des effets, la supériorité informationnelle et la protection des unités engagées et des infrastructures. Elle transforme la notion de profondeur, affaiblit la séparation entre objectifs civils et militaires et dilue la frontière entre temps de paix et temps de conflit. Les critères de violence atteinte par des cyberattaques sont encore trop faibles pour qu'ils puissent caractériser un conflit armé. « Il n'est pas certain que la guerre puisse s'y gagner, mais il ne fait aucun doute que cet espace fera perdre celui qui n'y aura pas la supériorité, au moins pour

63. S. Biddle. « The NSA Leak Is Real, Snowden Documents Confirm ». In : *The Intercept* (19 août 2016). (Visité le 16/04/2020).

64. Hodgson et al., op. cit.

accomplir ses missions. » [65].

Dans le même temps, les armées sont devenues dépendantes du monde numérique pour leur organisation comme pour la réussite de leurs missions. La Revolution in Military Affaire suivie de la transformation numérique augmentent la surface d'attaque cyber des forces et de l'écosystème de défense. Le fonctionnement en écosystème par la mise en réseau des plateformes d'armes, des capteurs et des organes de commandement augmente la surface d'attaque et réduit le cloisonnement entre les différents composants, facilitant d'autant la latéralisation. Il est nécessaire de conserver un équilibre entre innovation, résilience et rusticité afin que les armées puissent continuer à opérer, même en mode dégradé. Cet équilibre nécessitera d'adapter les méthodes d'innovation issues du secteur civil afin d'apporter des gages de durcissement, de correction et de sécurité.

Si l'introduction du cyber a complexifié les opérations, modifié le contexte et la technologie, l'organisation des armées n'en a été que peu perturbée, les processus de commandement sont restés les mêmes avec un fonctionnement en plateau agrégeant les différentes composantes dans la conduite des opérations, le cyber ayant intégré les moyens d'appuis au même titre que la guerre électronique. Une question se pose : le cyber souffrira-t-il des mêmes affres que la stratégie aérienne en son temps, c'est à dire, l'apparition d'une pensée stratégique considérant que le cyber peut à lui seul gagner des guerres ? Une telle approche risquerait d'entrainer un retard théorique de par le temps perdu à déconstruire cette pensée et un surinvestissement capacitaire. Pour l'instant, le problème n'est pas à l'ordre du jour, le cyber est plutôt utilisé en soutien plutôt que comme une arme de mêlée.

Au delà du risque de rupture technologique, se pose la question d'une rupture stratégique. Actuellement, la nature de la conflictualité dans le cyberespace tient, par analogie avec la stratégie maritime [66], à une forme de guerre de course. Les proxies sont au cyberespace ce que les corsaires étaient à l'espace marin avec une plus grande liberté d'action. Les stratégies de guerre de côtes, appliquer des effets directs dans d'autres milieux (par exemple la destruction d'un drone), et de guerre d'escadre, détruire ou à réduire les forces adverses opérants dans le cyberespace, ne sont pas encore appliquées et ni applicables au cyberespace. Cependant, la possibilité de mener des actions relevant de la guerre de côtes grandit avec la numérisation des systèmes industriels, des systèmes d'armes et plus largement la prolifération d'objects connectés permettant d'appliquer des effets cinétiques à partir du cyberespace. Si aujourd'hui la guerre d'escadre se révèle peut probable, une forme légère pourrait être envisagée en cherchant à paralyser les systèmes d'information permettant la collaboration et la coordination des organes de réponses, en s'appuyant sur des logiques de prépositionnement. Enfin, la neutralisation des capacités cyber peut être envisagée en dehors du cyberespace par des frappes cinétiques contre des infrastructures (satelitte, câbles sous-marins, ...) mais aussi contre des personnels, a minima dans des conflits asymétriques [67].

65. A. Coustillière. « Cyberdéfense militaire : vers une nouvelle composante des armées ». In : *DSI Hors-Série* 52 (mars 2017).

66. M. Motte et al. *La mesure de la force*. Thallandier. Paris, 2018.

67. La première frappe connue a été réalisée en 2015 par les USA, pour neutraliser Junaid Hussain membre du Cyber Caliphate, un groupe de hackers affiliés à DAESH.

Références

Leroux, H. *Cyber guerre : la montée des périls*. URL : https://www.ifri.org/sites/default/files/atoms/files/044_051_cyberguerre-2.pdf (visité le 17/07/2020) (cf. p. 4).

Limonier, K. *CARTO-UKRAINE. Quelques (cyber)considérations*. Poussières d'empire. URL : https://villesfermees.hypotheses.org/243 (visité le 10/04/2020) (cf. p. 7).

NATO. *Communiqué du sommet de Bruxelles publié par les chefs d'État et de gouvernement participant à la réunion du Conseil de l'Atlantique Nord tenue à Bruxelles le 14 juin 2021*. URL : http://www.nato.int/cps/fr/natohq/news_185000.htm (visité le 24/06/2021) (cf. p. 3).

USCYBERCOM After Action Assessments of Operation GLOWING SYMPHONY | National Security Archive. URL : https://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-01-21/uscybercom-after-action-assessments-operation-glowing-symphony (visité le 30/05/2020) (cf. p. 7).

Pomerleau, M. *US military to blend electronic warfare with cyber capabilities*. C4ISRNet. 14 avril 2021. URL : https://www.c4isrnet.com/electronic-warfare/2021/04/14/us-military-to-blend-electronic-warfare-with-cyber-capabilities/ (visité le 13/07/2021) (cf. p. 9).

CrowdStrike. *Our Work with the DNC : Setting the record straight*. 22 janvier 2020. URL : https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/ (visité le 16/04/2020) (cf. p. 5).

Lin, H. « On the Integration of Psychological Operations with Cyber Operations ». In : *Lawfare* (9 janvier 2020). (Visité le 29/05/2020) (cf. p. 7).

Strout, N. *This is what the Space Force will use to jam enemy satellites*. C4ISRNet. 8 avril 2020. URL : https://www.c4isrnet.com/electronic-warfare/2020/04/08/this-is-what-the-space-force-will-use-to-jam-enemy-satellites/ (visité le 13/07/2021) (cf. p. 9).

COMCYBER. *Éléments publics de doctrine militaire de lutte informatique offensive*. Janvier 2019, p. 12 (cf. p. 1, 5).

Cyber Influence Operations : An Overview and Comparative Analysis. Zurich : Center for Security Studies (CSS), ETH Zürich, octobre 2019 (cf. p. 10, 11).

Hodgson, Q. E., L. Ma, K. Marcinek et K. Schwindt. *Fighting Shadows in the Dark : Understanding and Countering Coercion in Cyberspace*. Santa Monica : CA : RAND Corporation, 2019 (cf. p. 8, 13).

« How The U.S. Hacked ISIS ». In : *NPR* (26 septembre 2019). (Visité le 30/05/2020) (cf. p. 8).

Mariel chef de bataillon, V. « L'influence militaire pour créer la surprise dans un champ de bataille transparent ? » In : *Lettre d'information du centre de doctrine et d'enseignement du commandement* (février 2019) (cf. p. 11).

Nocetti, J. « Dazed and Confused : Russian "Information Warfare" and the Middle East – The Syria Lessons ». In : (février 2019), p. 12 (cf. p. 7).

Un groupe de pirates informatiques russophones a visé la chaîne d'alimentation en carburant de la Marine nationale. 18 janvier 2019. URL : http://www.opex360.com/2019/01/18/un-groupe-de-pirates-informatiques-russophones-a-vise-la-chaine-dalimentation-en-carburant-de-la-marine-nationale/ (cf. p. 4).

Bombal, S. et V. Le Bihan. « Planifier et conduire les opérations numériques ». In : *La Cyberdéfense*. U. Paris : Armand Colin, 2018, p. 218-232 (cf. p. 2).

Boyer, B. « Les opérations sur l'environnement : la nouvelle guerre de l'information ». In : *La Cyberdéfense*. U. Paris : Armand Colin, 2018, p. 209-217 (cf. p. 4, 10).

Motte, M., G.-H. Soutou, J. de Lespinois et O. Zajec. *La mesure de la force*. Thallandier. Paris, 2018. 416 p. (cf. p. 14).

Namor, A. « Les opérations numériques dans les conflits contemporains ». In : *La Cyberdéfense*. U. Paris : Armand Colin, 2018, p. 199-208 (cf. p. 6).

Nocetti, J. « Géopolitique de la cyber-conflictualité ». In : *Politique étrangère* Été.2 (2018), p. 15-27 (cf. p. 2, 5).

Pamment, J., H. Nothhaft et A. Fjällhed. « Countering information influence activities : The state of the art ». In : (2018) (cf. p. 10).
SGDSN. *Revue stratégique de cyberdéfense*. 2018 (cf. p. 2, 6).
Smeets, M. « The Strategic Promise of Offensive Cyber Operations ». In : *Strategic Studies Quarterly* 12.3 (2018), p. 90-113 (cf. p. 11, 12).
Taillat, S. « Chapitre 7. Doctrines et dispositifs. Dissuasion et coercition ». In : *La Cyberdéfense*. U. Paris : Armand Colin, 2018, p. 141-149 (cf. p. 6).
— « Le cyberespace et la conflictualité internationale ». In : *La Cyberdéfense*. U. Paris : Armand Colin, 2018, p. 26-33 (cf. p. 3, 8).
Bannelier, K. et T. Christakis. *Cyber-attacks Prevention-Reactions : The Role of States and Private Actors*. Paris, 2017, p. 88 (cf. p. 5).
Coustillière, A. « Cyberdéfense militaire : vers une nouvelle composante des armées ». In : *DSI Hors-Série* 52 (mars 2017) (cf. p. 14).
Kello, L. *The Virtual Weapon and International Order*. Yale University Press. 22 août 2017. 336 p. (cf. p. 3).
Sunak, R. et J. Stavridis. *Undersea cables : indispensable, insecure*. Policy Exchange, 2017. url : `https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf` (cf. p. 4).
Biddle, S. « The NSA Leak Is Real, Snowden Documents Confirm ». In : *The Intercept* (19 août 2016). (Visité le 16/04/2020) (cf. p. 13).
Brangetto, P. et M. A. Veenendaal. « Influence Cyber Operations : The use of cyberattacks in support of Influence Operations ». In : *2016 8th International Conference on Cyber Conflict (CyCon)*. IEEE. 2016, p. 113-126 (cf. p. 11).
Kiyuna, A. et L. Conyers. *Cyberwarfare Sourcebook*. Lulu. com, 2015 (cf. p. 9).
Lin, H. « Thinking about Nuclear and Cyber Conflict : Same Questions, Different Answers ». In : *presentation, Hoover Institution/Center for International Security and Cooperation* 15 (2015) (cf. p. 12).
Bonnemaison, A. et S. Dossé. *Attention : Cyber ! : vers le combat cyber-électronique*. Economica, 2014 (cf. p. 1).
Bockel, J.-M. (*La cyberdéfense : un enjeu mondial, une priorité nationale*. 18 juillet 2012. url : `http://www.senat.fr/rap/r11-681/r11-681_mono.html` (cf. p. 1).
Zanette, D. H. « Dynamics of rumor propagation on small-world networks ». In : *Physical review E* 65.4 (2002), p. 041908 (cf. p. 8).