Les drones et le "cyber" dans la transformation de la guerre

Par Panpi Etcheverry

Il peut paraître à première vue pour le moins insolite et intellectuellement périlleux d'analyser deux sujets aussi vastes, techniques et finalement très différents que sont les drones[1] et, au sens le plus large du terme, le "cyber".[2] En effet, les drones relèvent principalement du domaine aérien, de la robotique et dans une moindre mesure de l'informatique. Les drones MALE (Moyenne Altitude Longue Endurance),[3] actuellement les plus utilisés pour des missions de reconnaissance ou dans le cadre d'actions de force, tels que le *MQ1-Predator B* ou celui que l'on surnomme la "faucheuse", le *MQ-9 Reaper*, sont des engins qui relèvent de la dimension aérienne[4] et dont le déploiement a des conséquences "cinétiques", matérielles et humaines directes dans certains endroits du monde.[5]

La "cyberguerre" n'a encore jamais directement tué personne, même si une cyber-attaque d'envergure contre des réseaux ou des infrastructures vitales (dits aussi "opérateurs d'importance vitale": OIV) pourrait avoir des conséquences humaines potentiellement dramatiques. C'est là une différence majeure qui pourrait un jour ne plus en être une.

---

[1] On devrait normalement parler de "système de drone". On peut le définir de manière générale comme "*un système dont le vecteur, non habité et porteur d'une ou plusieurs charges utiles, opère à une distance plus ou moins éloignée de sa station de contrôle en lui transmettant en temps réel les informations collectées*" : *cf.* D. Mercier (ss.dir.), *Les drones aériens: passé, présent et avenir*, Paris, Documentation Française, 2013, p.27.

[2] Les définitions du cyberespace sont nombreuses. Dans cet article, le cyberespace s'entend comme un "système sociotechnique" composé de plusieurs couches (principalement : 1. *matérielle* – serveurs, câbles sous-marins, et toute infrastructure assurant la communication, le traitement automatisé des données et l'interconnexion mondiale ; 2. *logicielle* – applications, programmes, permettant l'usage des ordinateurs par des personnes dépourvues de maîtrise technique avancée ; et 3. *sémantique* – contenu informationnel, interactions humaines), produisant une interdépendance inédite dans tous les domaines de l'activité humaine, formant à la fois un espace autonome et transversal en termes de sécurité et de défense. Voir les définitions de Daniel Ventre, Amaël Cattaruzza, Olivier Kempf ou Frédérick Douzet.

[3] Ce sont les drones principalement utilisés à l'heure actuelle pour des opérations de reconnaissance, de surveillance ou d'"élimination ciblée". Les États-Unis sont les seuls à opérer (officiellement) des drones militaires pour des frappes aériennes, Israël n'ayant jamais reconnu officiellement leur utilisation. C'est surtout de ce type de drones dont il s'agira dans cet article – ceci bien que l'émergence des nanodrones, ou des drones de combat partiellement ou entièrement autonomes actuellement en expérimentation, pose d'autres questions encore, qui ne pourront être traitées ici qu'à la marge.

[4] Les domaines "traditionnels" de la guerre étaient les dimensions terrestres, maritimes, aériennes et spatiales. Aujourd'hui, le cyberespace est un "nouveau domaine" de la guerre, une sphère où se déroulent des actions qui lui sont propres, mais qui dans le même temps traverse toutes les autres dimensions, ce qui lui procure une très haute sensibilité, et un caractère stratégique fondamental.

[5] De nombreux rapports mettent en cause les frappes de drones dans la mort de civils et la dégradation de leurs conditions de vie : *cf.* International Human Rights & Conflict Resolution (Stanford Law School) & Global Justice Clinic (New York University School of Law), "Living under Drones : Death, Injury and Trauma to Civilians from US Drone Practices in Pakistan", 2012 (http://www.livingunderdrones.org/report/); Columbia Law School's Human Rights Clinic & Center for Civilians in Conflict, "The Civilian Impact of Drones : Unexamined Costs, Unanswered Questions", 2012 (http://civiliansinconflict.org/resources/pub/the-civilian-impact-of-drones). Selon le Bureau of Investigative Journalism, le nombre de tués par des frappes de drones s'étage de 3072 à 4756, dont 556 à 1128 civils au Pakistan, au Yémen et en Somalie.

Publié in ***Res Militaris*** (http://resmilitaris.net), **hors-série** "**Cybersécurité**", **juillet 2015**

Néanmoins, plutôt que de répertorier les différences (trop nombreuses) entre drones et "cyber", il n'est pas inintéressant de se demander ce qu'ils ont en commun : dans quelle mesure ils s'inscrivent bien dans un même mouvement civilisationnel et de mutation de la guerre, dont les maîtres-mots sont information, clandestinité et/ ou irrégularité croissante des actions de force, autonomisation/ automatisation des systèmes. En effet, si l'explosion de l'emploi des drones et l'avènement du cyberespace comme lieu d'affrontement géopolitique, idéologique et militaire sont loin d'être les uniques manifestations d'un changement d'ère dans les relations internationales et stratégiques, il n'en demeure pas moins qu'"*à travers l'histoire, l'évolution des stratégies de guerre a dépendu en grande partie du niveau des technologies à la disposition des combattants et des leaders*".[6]

La guerre, en tant qu'acte de violence déclarée, limitée dans le temps et dans l'espace, semble ainsi se raréfier au profit d'un "état de violence" plus indéterminé, flou, insidieux et permanent. Les drones et le cyber participent de cette impression d'une violence larvée, non officielle, mais non mois réelle. L'avènement de l'"infosphère"[7] participe d'une *diffusion de la puissance*, comme le démontre l'action de l'"État Islamique" (EI) dans le cyberespace aux fins tant de communication que de recrutement,[8] action qui démultiplie sa stratégie de terreur et contribuent à augmenter son influence et son capital humain. De même les drones, qui symbolisent *a priori* l'asymétrie de la position américaine vis-à-vis du reste du monde, en particulier des populations des territoires qu'ils frappent, participent aussi de ce processus de diffusion de la puissance. En 2004, seule une quarantaine d'États possédaient des drones : ils sont 90 une décennie plus tard.[9] Et des mouvements tels que Hamas ou Hezbollah affirment posséder des drones et être capables d'en opérer, de telle sorte que l'on peut désormais parler de "techno-guérilla".[10]

L'un des effets majeurs également induits par la banalisation du recours à des systèmes de drones et des cyberattaques est lié aux bouleversements des perceptions et à la perte de repères et de limites à la fois psychologiques et juridiques des acteurs internationaux et des sociétés pour définir ce qui relève ou ne relève pas d'un acte de guerre. Comme le dit très bien Peter Singer, aujourd'hui…

> Les armées peuvent s'engager dans des actes qu'auparavant on aurait interprétés comme des actes de guerre, mais qui désormais ne sont pas considérés comme tels, soit qu'ils n'affectent pas directement la sécurité des hommes, soit qu'ils sont si rapides – ou si lents, comme dans certains types de sabotage numérique – qu'ils n'entrent pas dans la conception traditionnelle de la guerre.[11]

---

[6] M. Amitav, *Technology and Security in the 21th Century. A Demand-Side Perspective*, Stockholm, SIPRI Research report n°20, 2004, p.11.

[7] C. Malis, *Guerre et stratégie au XXIe siècle*, Paris, Fayard, 2014, p.157.

[8] O. Hertel, "Cyber-terrorisme : un recrutement en 4 phases", *Sciences et Avenir*, 17 mars 2015, http://www.sciencesetavenir.fr/high-tech/20150317.OBS4764/cyber-terrorisme-un-recrutement-en-4-phases.html.

[9] Cette prolifération est suivie de près par la CIA : S. Kreps & M. Zenko, "The Next Drone Wars : Preparing for Proliferation", *Foreign Affairs*, mars-avril 2014: http://www.foreignaffairs.com/articles/140746/sarah-kreps-and-micah-zenko/the-next-drone-wars.

[10] Malis, *op.cit.*, p.229.

[11] *Cf.* "New Technologies and Warfare", *International Review of the Red Cross*, n°886, Summer 2012, p.472.

Il semble que la "*guerre hors-limites*"[12] théorisée par deux colonels chinois dès 1999 s'inscrive pleinement dans les soubresauts de notre époque, et que nombre de pays (États-Unis et reste de l'Occident compris) se soient appropriés ses modes d'action (opérations clandestines,[13] attaques informatiques en premier lieu). Les cyberattaques et le recours à des drones armés hors conflit conventionnel relèvent d'une dérégulation de la guerre de plus en plus patente, car le droit de la guerre a été élaboré à partir de l'expérience européenne de la guerre interétatique et à une époque où le cyberespace tel que nous le connaissons relevait encore de l'impensable. Or, aujourd'hui la guerre interétatique devient l'exception, les acteurs des conflits se démultiplient, et la technologie crée de l'ambivalence : d'un côté, elle asymétrise encore davantage certains conflits, mais procure à certains acteurs des moyens d'action auxquels ils n'avaient pas accès auparavant.

Dans ce contexte mouvant et volatil, que révèlent donc des mutations de la guerre les drones et le cyber, et comment y contribuent-ils ? En quoi peuvent-ils interagir, même s'ils sont bien différents, et s'inscrivent incontestablement dans un rapport ambivalent aux moyens et à la technologie ? Quelles perspectives et quels enjeux géopolitiques et stratégiques font-ils émerger ?

Dans la première partie de cet article, il s'agira de voir comment, chacun à leur manière, les drones et le cyber s'inscrivent dans les mutations actuelles des conflits armés, qui font de l'information une donnée plus que jamais centrale, rendent caduques les frontières et limites classiques de la guerre et, en conférant aux technologies de l'information et de la robotique un poids croissant, renforcent l'influence des acteurs privés.

Dans la seconde partie, il sera nécessaire d'évoquer comment et dans quelle mesure le cyber et les drones peuvent parfois interagir au sein d'une stratégie globale de *full-spectrum dominance* ou de "techno-guérilla". Le domaine de la cyberdéfense comme celui des drones englobe une grande diversité de moyens et de pratiques en constante évolution. Si d'emblée on pourrait penser que l'utilisation des drones est l'apanage des États les plus développés, il n'en est en réalité rien,[14] de même que le cyberespace voit intervenir, à des fins politiques, idéologiques ou stratégiques, toutes sortes d'acteurs, de l'individu isolé à des groupes terroristes, en passant par des groupes autonomes constitués par et pour Internet.

La dernière partie portera sur les bouleversements géostratégiques et les questions juridiques soulevés par les frappes de drones et les opérations hostiles menées via le cyberespace. L'usage des drones à d'autres fins que la seule reconnaissance ainsi que les opérations cyber clandestines posent de graves questions à un droit de la guerre qui, s'il a le mérite d'exister et de fixer certaines limites, paraît aujourd'hui difficilement applicable

---

[12] Q. Liang & W. Xiangsui, *La guerre hors limites*, Paris, Payot et Rivages, 2003.

[13] Voir pour la France le livre de V. Nouzille, *Les tueurs de la République*, Paris, Fayard, 2015, ou pour les États-Unis, N. Turse, *Les nouvelles armes de l'empire américain*, Paris, La Découverte, 2014.

[14] Cela même si seuls les États-Unis ont jusqu'ici opéré des drones à des fins de frappes militaires et/ou d'assassinats ciblés, et disposent de capacités sans commune mesure avec celles d'autres États.

en l'état. De surcroît, l'"opacité structurelle" et le "non-respect des frontières",[15] caractéristiques du cyberespace, fluidifient les logiques d'alliance et donc les relations internationales, tout comme la prolifération des drones pourrait encore renforcer la volatilisation de l'ordre international.

Les ordinateurs, l'environnement dans lequel ils évoluent (le cyberespace) et les robots (dont les drones sont les premiers avatars, encore contrôlés par l'homme, mais probablement pas pour toujours), sont donc de véritables *game changers*.[16] C'est-à-dire qu'ils procurent des capacités nouvelles, inimaginables ne serait-ce qu'une génération auparavant, tout en soulevant de nouvelles questions cruciales pour lesquelles il n'existe pas (encore) de réponses définitives et/ ou satisfaisantes. De plus, si l'on peut avoir l'impression qu'il y a un effet de mode à parler des drones et du cyber, tant les articles journalistiques, universitaires ou les reportages se multiplient, cet engouement lié à la fascination de nos sociétés pour les progrès technologiques s'explique également par un principe de réalité. Cette centralité des drones et du cyber dans les politiques de sécurité et de défense se retrouve dans les pays qui ont une volonté d'exister sur la scène internationale et des ambitions stratégiques. Par exemple, la loi de programmation militaire française telle qu'actualisée en juin 2015 met bel et bien l'accent sur le renforcement des priorités que sont les forces spéciales, les drones, le cyber et le renseignement,[17] et tout ce qui contribue à une amélioration de ce que les militaires appellent l'ISR (intelligence, surveillance et reconnaissance). Les drones et le cyber sont bien vecteurs et protagonistes des mutations actuelles et futures de la guerre.

Les drones et le cyber au cœur des mutations de la guerre et de la "complexité stratégique"[18] de notre époque

La révolution cyber et la "robolution"[19] dans laquelle s'inscrivent les drones interviennent dans un champ conflictuel qui, comme on l'a brièvement évoqué en introduction, connaît de grands bouleversements. La raréfaction des affrontements westphaliens classiques entre États et la banalisation d'une violence plus fragmentée, plus diffuse (terrorisme, criminalité transnationale, cyberattaques, etc.), ont contribué à la confusion entre ce qui relève des affaires intérieures de l'État et ce qui revient à sa politique étrangère et de défense.

---

[15] O. Kempf, *Alliances et mésalliances dans le cyberespace*, Paris, Economica, 2014, p.178.

[16] S. Brimley, B. Fitzgerald, K. Saylor & W.P. Singer, "Game Changers : Disruptive Technology and US Defense Strategy", Disruptive Defense Papers, Center for a New American Security, septembre 2013, http://www.cnas.org/files/documents/publications/CNAS_Gamechangers_BrimleyFitzGeraldSayler_0.pdf.

[17] P. Chapleau, "Inflexion de la LPM : Jean-Yves le Drian veut ouvrir cinq travaux", *Ouest-France*, Blog Lignes de Défense, 11 mars 2015, http://lignesdedefense.blogs.ouest-france.fr/archive/2015/03/10/les-5-travaux-de-jean-yves-le-drian-pour-13651.html.

[18] Kempf, *op.cit.*, p.11.

[19] Néologisme issu de robot et de révolution, emprunté à R. Doaré & H. Hude, *Les robots au cœur du champ de bataille*, Paris, Economica, 2011, p.13.

En dépit du sentiment de perte de contrôle de l'État et d'une "désétatisation" de la guerre, les États conservent un pouvoir de décision et d'action majeur dans ce domaine. En cela, le cyber comme les drones sont à double tranchant dans le rapport ambivalent qu'entretient l'État vis-à-vis de ses capacités à influer sur l'ordre des choses, éventuellement par des actions de force. Le cyber est désormais considéré par les États comme au cœur de leur souveraineté du fait de la nécessité de protéger leurs informations les plus secrètes[20] et des nouvelles marges de manœuvre qu'offrent cet "outil" et ce "milieu" nouveaux. Les drones, quant à eux, offrent de nouvelles possibilités de renseignement en terrain hostile tout en réduisant les coûts économiques et politiques d'une intervention terrestre ou avec des aéronefs habités. Néanmoins, le cyber comme les drones poussent les États à opérer dans l'ombre, et leur utilisation a des effets sur la maîtrise réelle de leurs prérogatives, de leur souveraineté et même de leur légitimité. En effet, une certaine opacité est consubstantielle à ces nouvelles technologies, et l'information (*a fortiori* si elle est confidentielle, stratégique ou économique) est au cœur des usages du cyber comme des drones. Ils participent d'une dérégulation et d'une extension des limites du domaine de la guerre : en effet,

> dès lors que la régulation de la guerre entraîne, pour celui qui la respecte, une réduction de ses marges de manœuvre, le choix de l'irrégularité peut apparaître comme la composante d'une stratégie visant à déstabiliser un adversaire".[21]

Enfin, le recours au cyber comme aux drones pousse les États à faire appel à des acteurs privés, issus du monde de l'entreprise. Ces technologies sont également au cœur d'une "guerre économique"[22] de plus en plus intense que se livrent à la fois les différents États et les entreprises privées.

L'information et le renseignement comme nerf, technique et fin de la guerre

Il faut ici bien distinguer les deux domaines, car si le cyber et les drones sont liés[23] et s'ils ont tous les deux l'information pour raison d'être, leurs usages et les perspectives qu'ils ouvrent sont différents.

Pour les drones, en tout cas ceux qui nous intéressent ici, à savoir les MALE opérés sur des théâtres extérieurs, l'information est essentiellement d'ordre opérationnel, tactique, et transmise en temps réel ; sa quête peut déboucher soit sur de longs vols de renseignement, soit sur une frappe ciblée. Les drones permettent aux militaires de bénéficier d'une *situation awareness*, c'est à dire d'une connaissance en temps réel de la situation jamais atteinte auparavant. Il faut également noter que les drones comme outil de renseignement et de surveillance vont probablement être utilisés de manière croissante par

---

[20] Kempf, *op.cit.*, p.20.

[21] B. Badie & D. Vidal, *Nouvelles guerres : L'état du monde 2015*, Paris, La Découverte, 2014, p.45.

[22] Voir P. Gauchon (ss.dir.), "Nous sommes en guerre économique", Revue *Conflits*, Hors-série n°1, Hiver 2014, ou le numéro 24 des grands dossiers du magazine *Diplomatie*, intitulé "La guerre économique mondiale", décembre 2014-janvier 2015.

[23] Voir *infra* (p.17 *sqq*) la seconde partie du présent article : "Le cyber et les drones : opérabilités, compatibilités, vulnérabilités".

l'ONU après l'expérience-pilote, menée dans le cadre de la MONUSCO en République Démocratique du Congo (RDC), d'un premier vol de drone de surveillance en décembre 2013.[24] En effet, l'organisation internationale se devant d'être impartiale et de bénéficier de la confiance de tous les acteurs, elle n'est pas en mesure d'utiliser les leviers de services de renseignements de type étatique, et doit opérer en toute transparence. La technologie est apparue comme un moyen de pallier les carences dont souffrent les militaires onusiens en termes de renseignement militaire et opérationnel, et les drones de surveillance onusiens risquent de faire leur apparition sur d'autres théâtres dans les années à venir, d'autant plus que les effectifs de casques bleus sont également en flux tendus.

C'est avant tout sur le terrain militaire que les drones (armés ou pas) offrent un avantage tactique considérable, de par la précision et l'actualité de l'information qu'ils font remonter ou bien qu'ils transmettent sur le terrain à d'autres unités ou équipements. À ce titre, l'Afghanistan, l'Irak, la Libye mais aussi les conflits récurrents entre le triptyque Israël-Hamas-Hezbollah "*ont joué récemment le rôle de laboratoires militaires de la robotisation*",[25] en particulier pour ce qui concerne l'opérabilité des drones et leur intégration dans la structure globale des opérations. Ainsi,

> l'US Army généralise l'intégration du système VUIT (*Video From UAV for Interoperability Teaming*) sur ses hélicoptères [...], système qui permet la réception d'images provenant de drones – et de *pods* de désignation de type *Sniper* – au sein de l'hélicoptère et une transmission de ces même images, ainsi que de celles provenant de ses propres capteurs embarqués vers les forces au sol dotées du terminal OSRVT (*One-System Remote Video Terminal*).[26]

Ce dernier est également installé sur les véhicules terrestres de l'armée américaine et permet la réception de données issues des nombreux drones opérés par les États-Unis (*Shadow*, *Hunter*, *Pioneer*, *Raven*, *Predator*, etc.). On le voit donc, sur les théâtres d'opérations de la première des armées postmodernes,[27] le drone "*fonctionne comme un capteur déporté multipliant les performances intrinsèques*"[28] des forces au sol comme des autres appareils aériens,[29] hélicoptères compris.

---

[24] Y. Mens, "L'ONU va aux renseignements", *Alternatives Internationales*, n°63, juin 2014.

[25] Malis, *op.cit.*, p.125.

[26] B. Slaski, "Les drones et la puissance aérienne future. L'exemple américain et ses conséquences", *Notes stratégiques*, Compagnie Européenne d'Intelligence Stratégique (CEIS), mars 2013, p.7.

[27] Une armée postmoderne peut se définir comme celle qui se repose sur les possibilités offertes par la technologie pour mettre à distance la mort du combattant, non seulement parce que celle-ci est de moins en moins acceptée dans les sociétés postmodernes, mais également parce que les soldats sont une "ressource" rare. Le "post-héroïsme", au sens de Luttwak, le vieillissement des populations, la professionnalisation des armées et les progrès technologiques caractérisent donc les armées postmodernes, ou relevant du régime stratégique post-westphalien, au sens de Christian Malis.

[28] Slaski, *op.cit.*, p.8.

[29] "*L'IAF (Israeli Air Force) prétend que toutes les destructions de lance-roquettes courte et moyenne portées ont été exécutées dans un cycle de ciblage de moins de 10 minutes, ce qui accrédite la thèse de l'emploi des drones comme effecteurs en plus de leur mission ISR (lors de l'opération 'Changement de direction' contre le Hezbollah en juillet-août 2006)*" : P. Gros, "Les drones armés israéliens : capacités, bilan de leur emploi et perspectives", Note de la Fondation pour la Recherche Stratégique (FRS), juillet 2013, p.18.

Surveillance, renseignement, ciblage, reconnaissance sont les principales missions des drones et – il faudra y revenir – l'avenir leur appartient. En effet, leur autonomisation croissante, au moins pour les fonctions de vol, de recueil des informations et d'observation, va aller de pair avec leur miniaturisation, ce qui va encore accroître leur importance en matière de renseignement, au-delà de la sphère strictement militaire. En effet, le croisement des progrès des nanotechnologies et de la biomimétique débouchera très probablement sur l'apparition de nano-drones capables "*de missions de reconnaissance et de renseignement au contact*",[30] en se fondant dans le décor, ou en pénétrant dans le dédale des bâtiments.

On a d'ailleurs tendance à oublier trop souvent que nombre de drones américains sont opérés directement par la Central Intelligence Agency, et qu'ils relèvent à ce titre du renseignement et de l'espionnage. Imaginons le potentiel de ces nano-drones en matière de renseignement et peut-être même d'assassinats ciblés. Ils ont d'ailleurs déjà été expérimentés sur le terrain militaire par les soldats britanniques en Afghanistan[31]: ce n'est donc pas de la science-fiction. Or, après le tollé politico-médiatique suscité par les révélations d'Edward Snowden sur le programme d'espionnage américain PRISM,[32] on imagine mal comment l'opinion publique mondiale et les dirigeants de pays alliés (ou pas) des États-Unis réagiraient si ces derniers expérimentaient (avant peut-être de généraliser) le survol de territoires tiers par des drones chargés de les espionner. Car si la CIA n'ira peut-être pas jusque-là, l'armée américaine réfléchit aujourd'hui à l'utilisation à des fins d'espionnage de son immense flotte de drones MALE en dehors de ses zones d'action traditionnelles,[33] par exemple dans le Golfe Persique, en Asie-Pacifique ou dans la zone sahélo-saharienne.

Alors que le recours aux drones a connu une intensification sans précédent durant les dernières phases, contre-insurrectionnelles, des guerres d'Irak et d'Afghanistan, ils sont également déployés sur des théâtres où leur caractère clandestin est primordial. Ainsi, dans le cadre de la "guerre contre le terrorisme", "*le nombre de déploiements de drones a approximativement sextuplé sous la présidence Obama par rapport aux deux autres mandats de George W. Bush*",[34] et leur dotation dans l'armée américaine a été multipliée par 40 entre 2002 et 2010.[35] En Somalie, au Pakistan et au Yémen, les frappes de drones interviennent en dehors de zones de conflit "conventionnelles", dans des "zones grises",[36] afin d'en supprimer les éléments les plus dangereux (les fameuses *high-value targets*) et de contrôler ces territoires en permanence grâce à l'omniprésence permise par les drones. Or,

---

[30] Malis, *op.cit.*, p.241.

[31] L. Lagneau, "L'armée britannique utilise des nano-drones en Afghanistan", *Opex36.com*, 4 février 2013 : http://www.opex360.com/2013/02/04/larmee-britannique-utilise-des-nano-drones-en-afghanistan/.

[32] A.J. Lewis, "Étude préliminaire sur les analyses en cybersécurité : l'Affaire Snowden comme étude de cas" ; L. Petiniaud, "Cartographie de l'affaire Snowden", *Hérodote*, n°152-153, 1er-2e trimestres 2014.

[33] *Cf.* http://stratrisks.com/geostrat/14227.

[34] M. Zapfe, "Les drones américains dans la lutte antiterroriste", *Les analyses du CSS*, CSS ETH Zurich, n°137, juillet 2013, p.2.

[35] Malis, *op.cit.*, p.125.

[36] G. Minassian, *Zones grises. Quand les États perdent le contrôle*, Paris, Autrement, 2011.

cette escalade de la guerre clandestine sans véritable débat public pose de nombreuses questions, notamment "*en termes de risques posés à la stabilité régionale et au droit de la guerre*".[37]

À travers le cyberespace circule une masse sans précédent d'informations sur l'ensemble des activités humaines, dont certaines peuvent avoir une portée économique, politique, socioculturelle, géopolitique ou militaire. La maîtrise et la protection des informations sensibles ou secrètes est là un enjeu décisif, tandis que les opérations hostiles menées via ou dans le cyberespace visent par exemple à l'acquisition de données sensibles, à la perturbation ou à la destruction d'un système adverse, ou bien encore au déni d'accès ou au *défaçage* de sites Internet. Mais les actions hostiles dans le cyberespace n'ont pour seules limites que l'ingéniosité humaine ou la connexion au réseau, et sont favorisées par les vulnérabilités inhérentes aux systèmes (les fameuses "failles") et/ou liées aux négligences humaines.[38] Dans une société fondée sur l'information, les systèmes informatiques revêtent un caractère crucial et une cyberattaque revient toujours, peu ou prou, à endommager l'environnement informationnel de l'ennemi, voire les supports matériels et logiciels qui permettent le bon fonctionnement d'une structure. Les liens entre cyber et information sont abordés ci-dessous dans une perspective de renseignement, d'intelligence économique et de défense, afin de voir comment différents acteurs peuvent exploiter cet environnement.

Comme en témoigne la nouvelle loi sur le renseignement en France, votée en mai 2015,[39] le cyber joue un rôle majeur, qui ne devrait cesser de se renforcer à l'avenir, dans le renseignement et la surveillance : en effet, pour reprendre un jeu de mots, "*les nouveaux espions tissent leur toile*".[40] Si les méthodes traditionnelles des services de renseignement (infiltration, rémunération d'informateurs, écoutes par mouchard, etc.) perdurent, le cyber-espace en tant que réceptacle de toutes les informations et de toutes les rivalités offre des potentialités inédites en termes d'espionnage. L'"outil-milieu" cyber permet de dynamiser le renseignement dit "fermé"[41] aussi bien que le renseignement "au sens élargi",[42] et offre ainsi aux services concernés la possibilité de rechercher plus efficacement des informations protégées (pour des besoins de sécurité, d'appui à la politique nationale, de conduite des opérations militaires), ou de s'assurer une meilleure perception globale de l'environnement (social, économique, sécuritaire, international). Bien entendu, comme les drones d'une autre manière, le cyber se prête parfaitement aux actions clandestines puisque la dépendance

---

[37] L.E. Davis, M.J. McNemey, J. Chow, T. Hamilton, S. Harting & D. Byman, "Armed and Dangerous ? UAVs and US Security", Santa Monica, RAND Corp., 2014: http://www.rand.org/pubs/research_reports/RR449, p.18.

[38] K. Parsons, A. McCormack, M. Butavicius & M. Ferguson, "Human Factors and Information Security : Individual, Culture and Security Environment", Australian Government Department of Defence, Edinburgh, October 2010 : http://www.dtic.mil/dtic/tr/fulltext/u2/a535944.pdf.

[39] P. Alonso & A. Guiton, "Les cinq points-clés du projet de loi sur le renseignement", *Libération*, 17 mars 2015, http://www.liberation.fr/societe/2015/03/17/les-cinq-points-cles-du-projet-de-loi-sur-le-renseignement_1222330.

[40] Titre du dossier du numéro 63 d'*Alternatives Internationales* paru en juin 2014.

[41] Observatoire de la Défense/Orion, "Le renseignement en France. Quelles perspectives ?", Essai, Fondation Jean Jaurés, avril 2012, pp.43-44.

[42] *Ibid.*

envers les systèmes d'information se renforce sans cesse partout, et que la croissance de l'interconnexion va souvent de pair avec une mauvaise sécurisation, ou du moins une multiplication des failles. Les opérations clandestines dans le cyberespace ont un coût globalement très faible et les difficultés chroniques d'attribution d'une action à tel ou tel acteur dans le cyberespace, offre un certain confort pour mener de telles opérations.

Les services spéciaux (DGSE française, Government Communications Headquarters au Royaume-Uni, NSA et CIA américaines, par exemple) recrutent d'ailleurs massivement, mènent à l'évidence des actions offensives,[43] et continueront probablement à se renforcer. Surveillance, espionnage, sabotage sont donc promis à un bel avenir tant la manière dont les luttes de pouvoir et d'influence entre les multiples acteurs de la scène internationale s'y transposent. Le *hacking*, au sens le plus large, est pratiqué par tous les États aujourd'hui, et tous en sont victimes.

Peut-être davantage encore que sur le terrain politico-sécuritaire, c'est bien sur celui de la compétition économique que le cyberespionnage ou la quête d'informations à haute-valeur ajoutée semble en plein essor. En effet, "*la frontière entre sécurité nationale et sécurité économique devient floue dans un monde où les rivalités entre puissances se sont largement déplacées du terrain militaire à celui des affaires*",[44] comme en témoigne la place centrale des cyberattaques chinoises dans le différend diplomatique sino-américain.[45] Les enjeux sont colossaux :

> [L]es entreprises et les services de renseignement de nombreux États se livreraient au pillage en règle de données de leurs concurrents, adversaires ou ennemis, pour s'emparer de leurs secrets, de leur propriété industrielle, des résultats de leurs efforts de recherche et développement, d'informations politique, militaires ou stratégiques.[46]

La Chine est particulièrement agressive dans ce domaine : les cyberattaques qui en émanent visent tous azimuts de nombreux secteurs de l'économie, entre autres américaine. Elle peut compter non seulement sur une unité militaire entièrement dédiée à ce type d'opération (l'unité 61398, dont 5 officiers sont officiellement recherchés par le FBI pour des opérations de cyber-espionnage), mais a probablement à sa disposition de nombreux *hackers* non étatiques, tels ceux qui auraient dérobé des centaines de téraoctets d'informations à pas moins de 141 entreprises dans 20 domaines industriels-clés, aérospatial et défense compris. L'exemple des drones fera prendre la mesure du phénomène. La Chine semble en effet avoir bâti une grande part de ses capacités en matière de drones militaires sur le cyber-espionnage, ce qui n'a pas manqué d'affecter

---

[43] Les exemples ne manquent pas de cyberattaques menées soit par des agences de renseignement, soit par des cybercombattants plus ou moins intégrés à des structures de défense nationale : les dénis de service en Lettonie et en Géorgie en 2007-2008 ; le virus *Stuxnet* contre les centrifugeuses iraniennes, révélé en 2011 ; la cyberattaque *Shamoon* contre l'ARAMCO saoudienne en août 2012 ; et de nombreuses autres...

[44] Y. Mens, "Les nouveaux espions tissent leur toile", *Alternatives Internationales*, n°63, juin 2014, p.27.

[45] D. Ventre, "Cyberespionnage et diplomatie : l'exemple des tensions Chine/ États-Unis", *Diplomatie*, Les grands dossiers, n°23, octobre-novembre 2014.

[46] *Ibid.*, p.17.

gravement les constructeurs de drones américains.[47] Le fait que le drone *Lijian* ressemble énormément au *X-47B*, que le *Chengdu Xianglong* soit presque identique au *RQ-4 Global Hawk*, ou encore que le *Chengdu Pterodactyl 1* soit similaire à l'emblématique *Reaper* montre bien que ce cyber-espionnage a bien des conséquences stratégiques majeures – peut-être l'un des plus grands transferts de richesses de l'histoire de l'Humanité, pour reprendre l'appréciation trouvée sous la plume du général Keith B. Alexander.[48]

Sur le plan purement militaro-sécuritaire, la cyberdéfense s'avère également de plus en plus incontournable. Les Américains ont créé en 2009 un *CyberCom* constitué de quatre sous-commandements spécifiques à chaque armée (Army, Air Force, Navy, Marine Corps), directions qui ont ensuite fusionné pour être confiées au directeur de la NSA[49] afin de favoriser la réactivité de l'ensemble. En France, la prise de conscience de cette menace a conduit la même année à la création de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), organisation interministérielle chargée de la cybersécurité, puis en 2011 à la mise en place d'un commandement opérationnel de cyberdéfense, "*intégré à tous les processus de préparation et de conduite des opérations militaires*"[50] et dirigé par l'officier général (OG) Cyberdéfense à l'État-Major des Armées. La Chine[51] et la Russie ne sont pas en reste. Cette dernière se distingue en ce que les autorités n'y abordent pas la conduite par les forces armées d'opérations militaires offensives via le cyberespace dans le document officiel[52] présentant la cyberstratégie nationale, alors qu'à l'évidence la Russie fait partie des États les plus actifs dans le domaine[53] et utilise le cyberespace dans tous les conflits ou différents où elle est impliquée.

Si les techniques et les cyberarmes sont différentes selon les pays (qui ont chacun une histoire, une culture, un fonctionnement politique, une vision du monde induisant des aspirations, des motivations et des moyens d'action propres),[54] tous cherchent à collecter des données à des fins de renseignement. Concernant le cyber dans la guerre, l'arme cybernétique, déjà centrale, va devenir incontournable, les opérations militaires classiques intégrant brouillage, interceptions, dénis de service, vers sophistiqués pouvant atteindre le

---

[47] E. Wong, "Hacking US Secrets, China Pushes for Drones", *New York Times*, 20 septembre 2013 : http://www.nytimes.com/2013/09/21/world/asia/hacking-us-secrets-china-pushes-for-drones.html?_r=0.

[48] Ventre, "Cyberespionnage et diplomatie : l'exemple des tensions Chine/ États-Unis", *op.cit.*

[49] C.C. Demchak, "Organiser sa défense à l'ère du cyberconflit : un point de vue étatsunien", *Revue Internationale et Stratégique*, n°87, automne 2012, p.106.

[50] A. Coustillière, "La défense française et le cyberespace", *Diplomatie*, Les grands dossiers n°23, octobre-novembre 2014, p.71.

[51] Lire F. Clérot & V. Mayor, "Jeu de Go dans le cyberspace", *Revue Internationale et Stratégique*, n°87, automne 2012.

[52] Министерство обороны Российской Федерации (Ministère de la Défense de la Fédération de Russie), Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве (Points de vue conceptuels sur les activités des forces armées de la Fédération de Russie dans l'espace d'information), 2011, http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle#2.

[53] M. Tual, "L'Ukraine et la Russie au bord de la cyberguerre", *Le Monde*, 13 août 2014.

[54] K. Geers, D. Kindlund, N. Moran & R. Rachwald, "World War C : Understanding Nation-State Motives behind today's advanced cyber attacks", *Fire Eye*, 2014: https://www.fireeye.com/resources/pdfs/fireeye-wwc-report.pdf.

fonctionnement et la viabilité des systèmes d'information adverses, intoxication sur les réseaux sociaux, etc. Les cyberarmes ont également un aspect psychologique fondamental : si une cyberattaque réussit, elle mine la confiance, la crédibilité et l'autorité du régime ou de l'institution qui l'a subie. De même, les cyberarmes instillent le doute et l'incertitude sur les capacités que possède l'adversaire : leur rapport au secret[55] est fondamental. En somme,

> le ravage numérique – nous ne parlons pas du cyberespionnage qui, lui, est en pleine expansion – apparaîtrait plutôt comme un degré dans l'échelle des pressions et avertissements, qui tantôt éviterait la violence ouverte, "cinétique", tantôt en augmenterait l'efficacité par l'anticipation et la précision.[56]

"Ni-ni" : l'abolition des frontières géographiques et temporelles entre paix et guerre

L'"état de violence" évoqué en introduction peut se manifester par des conflits intra-étatiques où règne l'indistinction entre civils et combattants, par des actes terroristes indiscriminés, par des frappes de drones sur des territoires non officiellement en guerre ou dans le cyberespace, ou par une généralisation des attaques malveillantes et des opérations d'espionnage issues tant d'États que d'acteurs privés, avec pour conséquence une volatilisation sans précédent de l'ordre international. La mort simultanée "*de la grande guerre et de la vraie paix*"[57] est liée au fait que les États ne sont plus les seuls acteurs internationaux capables d'influence (ils doivent compter avec les ONG, un secteur privé de plus en plus présent, les organisations internationales, les acteurs armés non étatiques), mais encore aux progrès et à une dissémination technologiques sans précédent. Les drones et les cybertechnologies étendent la portée de la sphère militaire pour ceux qui en ont les moyens (ou pas[58]), et contribuent à abaisser le seuil de recours à la force pour plusieurs raisons.

D'abord, pour des questions de coût, ce qui n'est pas négligeable dans une période où la plupart des pays développés sont confrontés à des difficultés budgétaires et à des impératifs de plus en plus pesants de réduction de leur dette publique. Les drones armés sont bien moins coûteux que les chasseurs habités : "*un drone* Reaper *coûte 10,5 millions de dollars contre 150 millions de dollars pour un avion de chasse F-22*".[59] En fait, leur coût est tellement compétitif que l'armée américaine se permet une certaine attrition de ses forces dronisées. En effet, depuis deux décennies, sur les 269 *Predator* acquis par l'US Air Force, plus de la moitié se sont écrasés, et depuis janvier 2014, ce fut le cas de 14 drones *Predator* et *Reaper*.[60] Concernant le cyberespace, "*la croissance des réseaux offre de*

---

[55] F.-B. Huyghe, "Cyberarmements: les nouvelles logiques", *Revue Internationale et Stratégique*, n°96, hiver 2014, p.110.

[56] *Ibid.*, p.112.

[57] A. Beaufre, *Introduction à la stratégie*, Paris, Fayard, Pluriel, 2012 [1963].

[58] Voir *infra* (p.17 *sqq*), la seconde partie de cet article : "Le cyber et les drones : opérabilités, compatibilités, vulnérabilités".

[59] Badie & Vidal, *op.cit.*, p.117.

[60] *Cf.*, sur le blog d'Édouard Pflimlin, "Quand les drones Predator tombent du ciel", *Le Monde*, 1er avril 2015 : http://robots.blog.lemonde.fr/2015/04/01/quand-les-drones-tombent-du-ciel/.

nouveaux moyens d'action particulièrement puissants, rapides et peu coûteux, qui permettent d'agir à une échelle sans précédent, avec des conséquences d'une ampleur parfois inédite".[61] S'il est difficile d'évaluer le coût ne serait-ce qu'approximatif d'une cyberattaque, il est en outre facile d'affirmer que ce coût sera dans la grande majorité des cas largement inférieur aux dommages causés par la cyberattaque.[62]

Deuxièmement, bien que le débat soit ouvert pour le cyber,[63] il semble au vu des pratiques associées à l'emploi de ces nouvelles armes, qu'elles avantagent les postures offensives plutôt que défensives. En effet, les drones sont pour le moment la forme la plus aboutie de l'extension constante de l'allonge des armes depuis que l'homme fait la guerre : la distance entre l'opérateur du système de drone peut aller du kilomètre à plusieurs milliers de kilomètres selon la catégorie du drone et le théâtre d'opérations. Le fait de pouvoir lancer des opérations de nature militaire, souvent létales, sans risquer de vies du côté de l'attaquant ne peut pousser qu'à davantage d'interventionnisme. Au croisement de la guerre "zéro-mort"[64] et de la guerre "réseau-centrée", le drone permet de ne pas exposer les militaires à certaines missions dangereuses et de perfectionner les systèmes de surveillance, de reconnaissance et de traitement des cibles[65] dans une perspective d'attaque. Les frappes de drones quasi systématisées par B. Obama dans le cadre de la guerre contre le terrorisme sont des opérations purement offensives (sinon préemptives) dont le but est l'élimination d'individus identifiés comme ayant un rôle-clé dans un réseau ("*personality strikes*"), ou d'individus dont l'identité est inconnue mais qui, au vu de leur comportement ou de caractéristiques apparentes, sont des membres présumés d'un réseau terroriste ("*signature strikes*").[66]

Si la force létale ou la nocivité du drone est évidente à bien des égards (le missile *Hellfire* est là pour le rappeler), "*que peut un armement dit 'cyber' dont l'efficacité repose sur l'information et l'action sur l'information via des logiciels ou des algorithmes ?*".[67] Quelle que soit la réponse à cette question, il est clair que les acteurs peuvent être encouragés à attaquer dans le cyberespace car toute attaque est entourée d'incertitude (le brouillard de la guerre cher à Clausewitz y est particulièrement épais) et l'attribution, si elle est possible, demeure extrêmement difficile à déterminer. Un service d'État, un *hacker* isolé ou appartenant à un groupuscule, agissant pour des raisons idéologiques, financières, ou manipulé(s) par un État tiers, un acteur privé, un groupe terroriste : les concepteurs et

---

[61] *Ibid.*, p.115.

[62] "*Si le coût de fabrication d'une cyberarme offensive est évidemment aussi secret que sa nature, il est néanmoins possible de se faire une idée du 'bon marché' relatif de la défense cyber*" : F.-B. Huyghe, "Cyberarmements : les nouvelles logiques", *op.cit.*, p.111.

[63] En effet, une bonne cyberstratégie passe avant tout par un équilibre entre utilisation (ou menace) offensive de cyberarmes et une cyberdéfense bien structurée et réactive.

[64] A. Dumoulin, "Le 'zéro-mort' : entre le slogan et le concept", *Revue Internationale et Stratégique*, n°44, 2001, pp.17-26.

[65] Badie & Vidal, *op.cit.*, p.120.

[66] M. De Groof, "Utilisation des drones armés : Considérations juridiques et pratiques", Note d'analyse, Bruxelles, Groupe de Recherche et d'Information sur la Paix et la Sécurité (GRIP), 24 avril 2014, p.7.

[67] Huyghe, *op.cit.*, p.107.

acteurs potentiels d'une cyberattaque sont extrêmement nombreux et divers. Néanmoins, pour les grandes attaques informatiques relevant d'une véritable cyberguerre, seuls certains États ont la capacité avérée de cibler des systèmes et infrastructures précis et de toucher au cœur stratégique d'autres États. Cette capacité a pu dans certains cas être utilisée afin d'éviter d'avoir recours à des moyens "cinétiques" classiques (par exemple, dans le cas de *Stuxnet*, la destruction des infrastructures nucléaires iraniennes). En cela, la cyberattaque est une action de force, de "diplomatie coercitive", de sabotage, d'espionnage ou de subversion qui présente certains atouts pouvant pousser à l'adoption d'une posture offensive.

Dans un contexte où "*à partir de la guerre du Golfe, l'espace de combat se brouille, le champ de bataille est mouvant et indistinct de l'espace général*"[68]…

> les robots, en particulier les drones permettent de violer la souveraineté sans donner l'impression de le faire, en allant plus loin plus discrètement [...], et la robotisation, surtout dans le cadre de la guerre contre le terrorisme, globale, non-étatique, permet de dé-géographiser le champ de bataille comme la cyberdéfense.[69]

Partant de ce postulat, le cyber et les drones contribuent pleinement à abolir la distinction entre interne et externe (et donc à redéfinir la notion de frontière), et à introduire de nouvelles vulnérabilités. Si le progrès technologique et les flux d'informations semblent procurer un sentiment de pleine maîtrise du monde, de l'environnement et de ses aléas, ils ouvrent également une ère d'incertitudes. Le cyberespace est, au moins en partie, un espace a-territorial, et ce qu'il s'y passe (par exemple, une cyberattaque impliquant deux acteurs) peut avoir des répercussions bien plus larges, par viralité. Pourtant, en dépit d'une fluidité et d'une universalité qui ouvrent considérablement le paysage stratégique et sécuritaire, le cyberespace est parallèlement animé par "*une dynamique géopolitique de territorialisation et même de fragmentation*"[70] (on parle parfois de "balkanisation du cyberespace"). Il est donc difficile de faire la part des choses entre les vulnérabilités globales induites par le cyberespace, qui concernent tout un chacun, et le fait qu'il ait "*engendré ses propres dynamiques sociales et politiques et des jeux d'acteurs nouveaux, qui s'ajoutent et interfèrent avec ceux du 'monde réel' et complexifient l'analyse géopolitique contemporaine*".[71] Les actes hostiles sont permanents dans le cyberespace, émanent d'une grande diversité d'acteurs, et visent aussi bien les particuliers, les entreprises, les organisations de toutes sortes, que les États. Cette instabilité donne le sentiment d'une "guerre[72] de tous contre tous", face à laquelle personne n'est à l'abri, et

---

[68] O. Kempf, *Guerre et économie : de l'économie de guerre à la guerre économique*, Paris, L'Harmattan, 2013, p.65.

[69] P.W. Singer, "La guerre connectée : les implications de la révolution robotique", *Politique Étrangère*, vol.78, 2013, p.86.

[70] Malis, *op.cit.*, p.159.

[71] A. Cattaruzza & D. Danet, *La cyberdéfense. Quel territoire, quel droit ?*, Paris, Economica, Collection Cyberstratégie, 2014, p.32.

[72] Le terme de guerre dans le cyberspace n'est pas toujours le plus adapté, peut-être faudrait-il davantage parler de conflictualité.

qui pose des questions en termes de stabilité internationale, de respect de la vie privée, de liberté d'expression ou de protection des données.[73]

Les drones semblent relever d'une "*conception hyper-technologique de la guerre et du combat qui en font le décalque des dérives et utopies observées en matière sociétale*".[74] Comme ils sont largement utilisés dans le cadre de la guerre contre le terrorisme et que celui-ci relève largement du droit pénal, les drones consacrent le fait que "*le paradigme du maintien de l'ordre vient se greffer à celui de la guerre*".[75] Ils s'inscrivent dans une dérive sécuritaire engendrée par la menace terroriste, qui a mené à une confusion interne/externe, opérations de police/ interventions extérieures, et suscite de lourdes interrogations sur le rapport entre valeurs démocratiques, prévalence du droit et sécurité. Les opérations menées dans le cadre de la guerre contre le terrorisme consistent en effet en une "*exportation des éléments garantissant la sécurité intérieure des États-Unis au-delà de leurs frontières à travers les* covert operations*, l'usage des forces spéciales et l'activité des services de renseignement*".[76]

Cette indifférenciation croissante entre sécurité interne et externe est accrue par la place croissante des robots et/ ou des drones dans le système général de coercition : parallèlement à la confusion qui est de plus en plus souvent de mise entre forces armées, police et sociétés de sécurité privées, les systèmes de robots "*ont tendance à renforcer les capacités de prévention (anticipation, rapidité, réaction) et la surveillance de masse des individus*".[77] La perspective d'une fusion de plus en plus probable entre techno-logies de l'information et robotique fait craindre que ne devienne réalité demain "*la guerre anonyme et universelle à coups de robots tueurs bon marché, accessible à tous, trouvant immanquablement leur cible grâce aux* Big Data*, aux traces numériques que tout individu laisse désormais derrière lui en arpentant la cybersphère*".[78]

Les drones et le cyber comme symptôme du poids croissant du secteur privé et de la technologie dans les politiques de sécurité et de défense des États

Les années 1980 marquent, en termes de politique économique, une rupture majeure avec l'entrée dans l'ère du néo-libéralisme et de la financiarisation croissante de l'économie. Mis en œuvre par des figures telles que M. Thatcher et R. Reagan, ce tournant idéologique et pratique transforme le capitalisme tout comme les États, au détriment de ces derniers, dont les prérogatives et les marges de manœuvre se restreignent. Ce changement majeur de paradigme se retrouve également dans les questions de sécurité, puisque désormais la

---

[73] Cattaruzza & Danet, *op.cit.*, p.49.

[74] C. Galacteros-Luchtenberg, *Manières du monde, manières de guerre*, Paris, Nuvis, 2013, p.89.

[75] T. Randretsa, "Assassinats par drones : un cadre juridique ambigu", *Diploweb*, 21 novembre 2012, http://www.diploweb.com/Assassinats-par-drones-un-cadre.html.

[76] J.-V. Holeindre & I. Testot, *La guerre des origines à nos jours*, Paris, Éditions Sciences Humaines, 2014, p.143.

[77] D. Danet, J.-P. Hanon & G. de Boisboissel (ss.dir.), *La guerre robotisée*, Paris, Economica, 2012, pp.22-23.

[78] Malis, *op.cit.*, p.241.

tendance lourde est que les enjeux financiers sont au moins aussi importants que les enjeux militaires, et que l'externalisation modifie durablement les frontières entre le public et le privé. En effet, après la Guerre froide, l'"*État qui avait été le grand ordonnateur technique pour des questions de puissance a passé la main à l'entreprise privée*".[79]

Les sociétés militaires privées se multiplient et prospèrent alors que les grands acteurs industriels gagnent sans cesse en influence, par leur force de frappe financière colossale et leur capacité à innover, à créer des besoins auprès de certains gouvernements, par une politique de l'offre en matière de matériaux militaires à haute valeur ajoutée technologique. Cette tendance générale se renforce avec la robotisation du champ de bataille, et l'essor des drones participe largement de ce processus de privatisation sécuritaire. D'après Peter Singer, "*les sociétés sous contrat occupent une place énorme dans le pilotage et la maintenance de la flotte de drones armés de la CIA*".[80] De plus, la manne économique représentée par les drones stimule largement la croissance des géants de l'armement américain et leur permet de densifier leur réseau de lobbyistes au Congrès américain (le *drone caucus*). Parallèlement, "*l'écart entre le militaire et le civil n'a cessé de diminuer, ce que confirme aujourd'hui la privatisation croissante qui touche aussi les opérateurs de drones*".[81] En effet, comme le dit très bien le politologue Herfried Münkler,

> la robotisation contribue à la privatisation en renforçant le poids des concepteurs et des fabricants naturels et logiciels dans l'action militaire proprement dite, à la stimulation des sociétés militaires privées, à la dépolitisation potentielle de l'emploi de la force (autonomie croissante des machines) et au renforcement de l'asymétrie par la fuite en avant technologique.[82]

Les grandes entreprises américaines du secteur (Hughes, Raytheon, Lockheed-Martin, Boeing/ McDonnel Douglas, Northrop Grunman, TRW, etc.) dominent le marché mondial de l'exportation d'armements, bien qu'elles soient concurrencées par les firmes israéliennes dans le domaine des drones. Ainsi, "*le recours massif aux drones apparaît ainsi assez largement indissociable du mouvement de privatisation de la défense engagé aux États-Unis. Les acteurs privés en contrôlent une part sans précédent dans l'histoire des armements*".[83]

Les principales entreprises produisant des drones pour le compte du Département de la Défense (DoD) américain sont General Atomics et Northrup Grumman, qui dominent à eux seuls la moitié du marché. Pour l'année 2011, le DoD a eu besoin de 6,1 milliards de dollars pour les achats et le développement de programmes de drones, cette somme devant probablement atteindre 24 milliards entre 2010 et 2015[84] pour l'extension des capacités

---

[79] J.-F. Daguzan, *Guerre et économie*, Paris, Ellipses, 2003, p.38.

[80] Doaré & Hude, *op.cit.*, p.8.

[81] P.W. Singer, "La guerre connectée : les implications de la révolution robotique", *Politique Étrangère*, vol.78, 2013, pp.91-104.

[82] H. Münkler, "Les guerres du XXI° siècle", *Revue Internationale de la Croix Rouge*, 31 mars 2003, pp.7-22.

[83] Danet, Hanon & de Boisboissel, *op.cit.*, p.8.

[84] J. Chesebro, "Unmanned Aircraft Systems": http://www.trade.gov/static/aero_rpt_flight_plan_2011_uas.pdf.

déjà existantes. Le secteur des drones est clairement le plus dynamique dans le domaine de la défense et des technologies aérospatiales. La plupart de ces entreprises font des profits colossaux uniquement grâce aux commandes et aux ventes de drones, bien que certaines aient également des activités aéronautiques plus larges. Par exemple, Boeing, qui n'est pas dans cette liste, a également investi ce marché, en particulier à travers le *Phantom Eye*. General Atomics ou encore Northrop Grunman, qui ont fait des drones militaires leur fonds de commerce, ont des chiffres d'affaires qui oscillent entre plusieurs dizaines et plusieurs centaines de millions de dollars. Leur marché est très largement américain, et donc lié au budget de la défense des États-Unis, mais cela est déjà en train de changer.[85] De plus, il est avéré que les entreprises ne se contentent pas de vendre leur matériel aux militaires américains, mais participent également à leur utilisation en opérations.[86] Cela pose un réel problème de confusion de responsabilités et d'attribution qui participe du flou de la guerre d'aujourd'hui. En effet, le degré de sophistication croissant des équipements militaires, en particulier dans un contexte de robotisation croissante, fait que les compétences nécessaires à leur mise en œuvre seront probablement de plus en plus liées à leurs concepteurs.

Il en va de même pour le cyber qui fait face aux mêmes problèmes de liens "incestueux" entre compagnies privées et administrations publiques de sécurité et de défense. En effet, là encore, l'affaire Edward Snowden a révélé à la face du monde l'ampleur et la profondeur des interactions entre les agences de renseignement américaines et certaines firmes privées : l'intéressé lui-même était un employé de Booz Allen Hamilton (BAH), sous-traitant de la NSA. Au lendemain du 11 septembre 2001, le gouvernement américain a voulu accroître sa capacité à rassembler des informations et surveiller les communications, poussant la NSA et la CIA à massifier la sous-traitance. À titre d'exemple, les bénéfices de BAH entre 2010 et 2013 ont été multipliés par huit, alors que 99% du chiffre d'affaires de l'entreprise proviennent de contrats fédéraux.[87] Mais cela va beaucoup plus loin que le seul cas de BAH : en effet,

> près de 70% du budget de la communauté américaine du renseignement serait consacré à des entreprises privées et l'estimation selon laquelle ces dernières seraient plus de 1900 a fait l'objet d'une validation en haut lieu : parmi elles, 533 (soit1/4) sont nées après le 11 septembre et les autres, qui existaient déjà, ont alors connu un développement rapide.[88]

De plus, le secteur privé a un rôle en tant que cible et conducteur potentiel des cyberattaques,[89] et est largement impliqué dans ce qui relève du cyberconflit beaucoup plus

---

[85] R. Missy, "Obama Administration to allow sales of armed drones to allies", *The Washington Post*, 17 février 2015: http://www.washingtonpost.com/world/national-security/us-cracks-open-door-to-the-export-of-armed-drones-to-allied-nations/2015/02/17/c5595988-b6b2-11e4-9423-f3d0a1ec335c_story.html.

[86] D. Isenberg, "Predator Military Contractors : Privatizing Drones", *Huffington Post*, 18 octobre 2012, http://www.huffingtonpost.com/david-isenberg/contractors-privatizing-the-drones_b_1976650.html.

[87] F. Autran, "Officiers (sous-)traitants", *Alternatives Internationales*, n°63, juin 2014, p.28.

[88] R. Foliard, "La privatisation du renseignement américain", Institut Français d'Analyse Stratégique, 14 février 2011 : http://www.strato-analyse.org/fr/spip.php?article205.

[89] N. Arpagian, "Les entreprises, complices et victimes de la 'cyberguerre' ?", *Revue Internationale et Stratégique*, automne 2012, n°87, pp.65-72.

qu'il ne l'a jamais été dans les conflits cinétiques traditionnels. Comme on vient de le voir, il existe aux États-Unis une interpénétration réciproque entre acteurs militaires et civils, alors que les caractéristiques du cyberespace sont largement construites, opérées et possédées par des entités du secteur privé.

Le cyber et les drones : opérabilités, compatibilités, adaptabilité

Il apparaît donc que si les drones et le cyber sont deux choses bien différentes, ils s'inscrivent tout de même dans un contexte global au sein duquel la révolution technologique "*agit sur toutes les composantes de l'ordre social et donc aussi sur la guerre*".[90] Mais les deux domaines sont liés également sur le plan technique : "*la robotisation s'engrène sur l'informatisation et la numérisation, SIC et réseaux sont en effet l'interface indispensable pour faire circuler et exploiter les données émises par les drones de tout type*".[91] Cyber et drones sont deux domaines marqués par une grande variété de capacités, lesquelles évoluent en permanence. Enfin, si l'on pourrait *a priori* supposer que seuls les États développés sont à même d'utiliser le cyber et les drones dans leurs modes opératoires, l'examen des "manières de guerre" des uns et des autres suggère qu'il n'en est rien. Nombre d'acteurs peuvent y avoir recours avec une efficacité redoutable, en dépit d'un degré de perfectionnement moindre que celui des armes que déploient les États-Unis, par exemple.

Deux composantes d'une même révolution dans les affaires militaires (RAM) et d'un même contexte global

Qu'est-ce qui distingue les drones, les systèmes d'armes autonomes (ou en voie d'autonomisation), les armes "nano" et la cyberguerre des méthodes et moyens classiques utilisés jusqu'à aujourd'hui ? Ce sont essentiellement quatre choses : l'autonomisation/automatisation, la délégation à la machine (ou aux algorithmes), la précision et la résilience, enfin la capacité à user de moins en moins de forces "cinétiques" pour arriver à des effets équivalents ou supérieurs.[92] Si la technologie se démocratise, il est évident que la "Révolution dans les affaires militaires" (RAM, dont on parlait déjà lors de la première guerre du Golfe) et la *network-centric warfare*[93] trouvent leur origine, et doivent beaucoup, aux États-Unis.[94] Cette "technologisation" croissante de la guerre s'est accélérée durant les années 2000,[95] et la tendance semble se confirmer. Elle paraît aller de pair avec la "clandestinisation" de l'usage de la force, décrite plus haut. En effet, après les interventions massives et coûteuses en Irak et en Afghanistan, les États occidentaux, États-Unis en tête,

---

[90] Kempf, *op.cit.*, p.20.

[91] Malis, *op.cit.*, p.129.

[92] "New Technologies and Warfare", *International Review of the Red Cross*, n°886, Summer 2012, p.458.

[93] Conduite des opérations militaires par l'exploitation des capacités des systèmes d'information, dont les drones et le cyber sont des composantes essentielles.

[94] Pour une analyse détaillée de la RAM : *cf.* E. de Durand, "'Révolution dans les affaires militaires'. 'Révolution' ou 'transformation' ?", *Hérodote*, n°109, 2003/2, pp.57-70.

[95] Malis, *op.cit.*, p.125.

ont opté pour une *light footprint strategy*.[96] Drones et cyber font donc partie d'un même substrat stratégique au sein duquel la technologie, ses évolutions et l'interpénétration de ses différentes branches (robotique et informatique, entre autres) jouent un rôle majeur.

Automatisation et numérisation sont les deux piliers de la robotisation, car c'est bien par le biais des systèmes d'information et de communication que sont transmises et exploitées les grandes masses d'informations recueillies, en particulier par les drones. Le drone a donc d'une certaine manière une dimension cyber. C'est d'ailleurs un de ses principaux talons d'Achille puisque, en dépit de leur caractère éminemment stratégique, des cas de drones "*hackés*" ont déjà été répertoriés, en plus des nombreuses pertes dont on ignore l'origine. Ainsi, en 2009, "*des rebelles irakiens sont parvenus à intercepter les liaisons émises par un drone américain, et en 2011, la défense aérienne iranienne a réussi à détourner un drone américain en lançant une cyberattaque contre le système de pilotage*".[97] De même, des rapports récents indiquent que les forces russes ont *hacké* un drone de surveillance américain survolant la Crimée en mars 2014.[98] Si l'on prend en compte les évolutions probables de la révolution "robonumérique"[99] qui s'ouvre à nous, il faut envisager les conséquences d'une cyberattaque sur des…

> essaims de robots de toutes tailles et de niveaux d'autonomie, diversifiés selon les milieux, de capteurs abandonnés, d'avions optionnellement télé-pilotés, de missiles et de bombes qui dépendront pour leur mise en œuvre d'une noosphère sécurisée ultrahaut débit "en nuage".[100]

L'autonomisation et la miniaturisation sont les prochains défis de la révolution qui affecte actuellement la guerre. Elles soulèvent de lourdes questions, dont les principales sont l'avènement de "robots tueurs"[101] partiellement ou intégralement autonomes, et l'exploitation des *Big Data* (données massives agencées par des algorithmes complexes et automatisés) à des fins de sécurité intérieure par exemple,[102] ou... pour mener des opérations d'"assassinats ciblés" à partir de la signature numérique des individus. Faut-il s'attendre à une évolution qui nous dirigerait, en France par exemple, vers une "*République des algorithmes*", selon la formule utilisée par Gilles Babinet[103] afin de d'illustrer le le

---

[96] N. Turse, *Les nouvelles armes de l'empire américain*, Paris, La Découverte, 2012.

[97] Badie & Vidal, *op.cit*. p.122.

[98] R.I. Porche, "Cyberwarfare Goes Wireless", Santa Monica, The RAND Corporation, 7 avril 2014, http://www.rand.org/blog/2014/04/cyberwarfare-goes-wireless.html.

[99] Malis, *op.cit*., p.207.

[100] *Ibid.*

[101] Human Rights Watch, "Mind the Gap: The Lack of Accountability for Killer Robots", USA, April 2014 : http://www.hrw.org/sites/default/files/reports/arms0415_ForUpload_0.pdf.

[102] L'article L. 851-4 du projet de loi français sur le renseignement prévoit que le Premier ministre peut ordonner aux opérateurs de communications électroniques et aux fournisseurs de services de *détecter, par un traitement automatique, une succession suspecte de données de connexion*, dont l'anonymat ne sera levé qu'en cas de menace terroriste avérée: http://standblog.org/dc-blog/public/2015/19.03.2015_dossier_de_presse_-_projet_de_loi_renseignement.pdf.

[103] Gilles Babinet est le représentant de la France pour le numérique auprès de la Commission européenne.

"fait de transmettre un pouvoir régalien aux machines"? L'homme ira-t-il jusqu'à confier "*à une entité non humaine (...) la capacité de choisir des cibles et d'user de la force*"[104] ?

Contre-usages du cyber et des drones : vers leur appropriation par des acteurs armés non-étatiques (AANE) ?

On l'a vu, le cyber et les drones – pour les États-Unis et Israël, les drones *armés* – sont utilisés selon différents degrés et modalités par des pays qui comptent dans le paysage stratégique mondial. Néanmoins, vu le panel capacitaire, les usages extrêmement variés qui peuvent être faits de ces deux technologies, et les coûts déclinants pour y accéder, "*elles sont déjà largement à la portée de nombreux autres États et d'acteurs non étatiques*".[105]

En effet, il n'est pas nécessaire d'être capable d'élaborer un virus aussi complexe que *Stuxnet*, de disposer de capacités aussi dantesques que la NSA ou de disposer d'une armada de drones *Reaper* ou autres, pour infliger des dommages physiques et/ou psychologiques considérables à un adversaire. Ces technologies sont d'ores et déjà appropriées par les différents acteurs internationaux en fonction de leurs intérêts, de leurs capacités et de leur culture stratégique. Il est évident que…

> quand les États cesseront d'avoir le monopole de la technologie de destruction, les armes, grâce à la loi de l'offre et de la demande, finiront forcément entre les mains des terroristes les plus riches et les mieux organisés du marché.[106]

Et comme il est déjà possible de le constater,

> la robotisation pourrait accroître le combat asymétrique sous ses formes les plus extrêmes et les plus inattendues (terrorisme, attaques informatiques, etc.) et renforcer encore davantage la fragmentation des rapports de puissance.[107]

En ce qui concerne les drones, il faut bien voir qu'il existe différentes catégories et différents degrés de perfectionnement, et que même un système relativement rudimentaire et basique, s'il est bien utilisé, peut procurer des avantages tactiques sur le terrain, en termes d'éclairage, de connaissance des forces ennemies, et de leurs mouvements. La techno-guérilla fait des émules de par le monde ; elle est d'ailleurs un facteur majeur de "*transformation des rapports de force militaires*",[108] comme en témoigne la guerre de 2006 entre Israël et le Hezbollah – sans doute la première "non-victoire" militaire de l'État hébreu depuis les débuts de son existence. Le Hezbollah y avait effet combiné des techniques classiques de guérilla avec l'usage de technologies assez avancées (dont des drones et le piratage des drones adverses).

---

[104] M. Wareham, "Pourquoi doit-on interdire les 'robots tueurs'", *Revue Internationale et Stratégique*, n°96, hiver 2014, p.101.

[105] T. Hsia & J. Sperli, "How cyberwarfare and drones have revolutionized warfare", *New York Times*, 17 juin 2013, http://atwar.blogs.nytimes.com/2013/06/17/how-cyberwarfare-and-drones-have-revolutionized-warfare/?_r=0.

[106] B. Ackermann, "Les pouvoirs d'exception à l'âge du terrorisme", *Esprit*, n°327, août-septembre 2006, p.153.

[107] Danet, Hanon & de Boisboissel, *op.cit.*, p.27.

[108] Malis, *op.cit.*, p.229.

En 2012, Hassan Nasrallah, dirigeant du Hezbollah libanais, affirmait avoir fait voler un drone dans l'espace aérien israélien juste après qu'Israël eut annoncé avoir détruit un engin non piloté (UAV).[109] Le Hezbollah aurait, dit-on, une stratégie visant à contrer la supériorité israélienne dans le domaine : en piratant les systèmes adverses, comme il est avéré qu'il a réussi à le faire en 2006, et en se dotant de mini-drones de fabrication iranienne pour tenter d'exploiter cette même arme face à l'ennemi.[110] De fait, des drones *Ababil* et des *Mohajers 4* de fabrication iranienne "*furent utilisés pour faire du repérage et du ciblage d'objectifs militaires israéliens*".[111] Si la "victoire" du Hezbollah ne peut être attribuée à l'utilisation de ces drones ou aux cyberattaques contre les drones israéliens survolant ses combattants, on sait que tactiquement ces moyens ont permis au mouvement chiite de mener des embuscades meurtrières contre les soldats de *Tsahal* ou bien d'avoir un à plusieurs coups d'avance sur ces derniers en visionnant les images piratées émises par les drones adverses.

Plus récemment, les brigades *Ezzedine al-Qassam* ont affirmé dans un communiqué qu'elles avaient envoyé des drones au-dessus du ministère israélien de la Défense à Tel-Aviv, alors que Tsahal reconnaissait avoir abattu un UAV plus au sud.[112] Un communiqué déclarait que "*les ingénieurs des Qassam ont réussi à produire des UAV* Ababil *et fabriqué trois modèles de reconnaissance,* [et] *d'autres* [qui] *peuvent tirer* [des missiles] *ou servir pour des attaques suicides*".[113] S'il est possible que le Hamas ait réussi à se forger des capacités en matière de drones de manière autonome, le fait que le drone ait pour nom *Ababil* (comme le drone iranien livré au Hezbollah) laisse envisager l'hypothèse d'une source d'approvisionnement extérieure.

S'il n'y a pas encore eu d'acte terroriste perpétré à l'aide de drones, de fortes présomptions existent sur le fait que leur potentiel pour en commettre intéresse des individus ou des groupes terroristes, comme en témoignent un certain nombre de faits divers récents. En septembre 2011, Rezwan Ferdaus, étudiant de 27 ans diplômé en physique, a été arrêté puis condamné en 2012 pour terrorisme : il voulait attaquer le Pentagone et le Congrès des États-Unis à l'aide de drones bourrés d'explosifs, des répliques de *F-4* et *F-86*.[114] Bien qu'on ignore à quel stade de préparation en était l'attentat, on voit bien que le drone pourrait constituer le pendant volant, souple, maniable et difficile à contrôler, de la tristement traditionnelle voiture piégée. En juin 2013, en

---

[109] Stratrisks : Observing the Grand Geopolitical Game of Risk, "CIA says 87 nations now possess drones" : http://stratrisks.com/geostrat/16373?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+StratRisks+%28StratRisks%29.

[110] F. Assaf, "Moyen-Orient : un intérêt accru pour les drones", 2 mai 2012 : http://www.mesp.me/2012/05/02/moyen-orient-interet-accru-pour-les-drones.

[111] Malis, *op.cit.*, p.230.

[112] Source : *La Presse* (Montréal). *Cf.* http://www.lapresse.ca/international/dossiers/offensive-israelienne-a-gaza/201407/14/01-4783768-le-hamas-affirme-avoir-envoye-plusieurs-drones-vers-israel.

[113] *Ibid.*

[114] J.-P. Ney, "Drones terroristes : les États prennent des mesures", *Infosdéfense*, 15 octobre 2013. *Cf.* http://www.infosdefense.com/drones-terrristes-les-etats-prennent-des-mesures-32603.

Allemagne, plusieurs étudiants tunisiens en aéronautique ont été arrêtés à Stuttgart, Munich et Dachau afin de démanteler un réseau islamiste mettant au point des drones équipés de missiles.[115]

Si l'idéologie des djihadistes est rétrograde, leur adaptation aux technologies d'aujourd'hui nécessite donc de prendre au sérieux la menace qu'ils représentent. Leur activité sur la toile et dans le cyberespace en général, en particulier celle de *Daech*, est symptomatique de cette appropriation des nouvelles technologies par des acteurs asymétriques. Si l'"État Islamique" n'est pas un État, il a reconnu la dimension hautement stratégique du cyberespace au même titre que les "vrais" États, et l'utilise à la fois comme une ressource (recrutement), comme un outil de communication et de propagande (vidéos d'exactions ou d'exécutions extrêmement travaillées), mais encore et surtout comme un "champ de bataille".[116] Rien ne prouve pour le moment qu'un groupe affilié à *Daech*[117] ait bien perpétré la cyberattaque d'une ampleur inédite qui a touché *TV5 Monde* le 8 avril 2015[118]: à la limite peu importe. Car si ce ne sont pas des combattants directement affiliés à l'organisation terroriste qui l'ont perpétré, cela peut-être un groupe de sympathisants, des "cybercriminels" financés par le groupe terroriste, ou bien une des nombreuses cellules de *hacking* islamiste qui font preuve d'une agressivité particulière depuis quelques années déjà.[119] D'une certaine manière,

> la cyberguerre qui a pour objectif de porter atteinte à la gouvernance d'un pays, attaquer ses données militaires, ses transactions financières ou accomplir d'autres types d'actions ciblées invalidantes ne requiert pas d'investissements ni de moyens importants. Elle correspond en tout point à la stratégie du terrorisme.[120]

Cette cyberattaque pourrait en préfigurer d'autres, moins symboliques et plus cruciales: destruction de données financières, brouillage de communications, attaque contre un opérateur d'importance vitale (OIV), un hôpital voire même un avion ou une centrale nucléaire. Bien entendu, rien n'est moins sûr, et une telle attaque requerrait un degré de perfectionnement encore supérieur, car les OIV font l'objet d'une protection particulière. Néanmoins, en attaquant une chaîne aussi diffusée que *TV5 Monde*, les auteurs de la

---

[115] *Ibid.*

[116] J.-F. Fiorina, "Internet, un espace de jeu géopolitique", CLES, Grenoble École de Management, 5 mars 2015 : http://notes-geopolitiques.com/internet-un-espace-de-jeu-geopolitique/.

[117] En effet, d'après certains médias, les soupçons de l'ANSSI se tourneraient désormais en direction de la Russie, ce qui montre à quel point l'attribution certaine des actions hostiles dans le cyberespace demeure une gageure : voir D. Leloup & M. Untersinger, "Piratage de TV5 Monde : l'enquête s'oriente vers la piste russe", *Le Monde*, 11 juin 2015 : http://www.lemonde.fr/pixels/article/2015/06/09/piratage-de-tv5-monde-l-enquete-s-oriente-vers-la-piste-russe_4650632_4408996.html?xtmc=tv5_monde&xtcr=1.

[118] M. Pinard, "TV5 monde piratée : c'est une cyberattaque d'une ampleur inédite. Une étape a été franchie", *Le Nouvel Observateur*, 9 avril 2015, http://leplus.nouvelobs.com/contribution/1351347-tv5-monde-piratee-c-est-une-cyberattaque-d-une-ampleur-inedite-une-etape-ete-franchie.html.

[119] T. Berthier, "Le *hacking* d'influence, outil d'un activisme musulman", *Diplomatie*, Les grands dossiers n°23, octobre-novembre 2014.

[120] H. Eudeline, *Le dossier noir du terrorisme. La guerre moderne selon Sun Tzu*, Bègles, L'esprit du Temps, 2014, p.115.

cyberattaque ont voulu porter un coup dur à la crédibilité et à l'image de la France dans le monde, et en cela, cette cyberattaque constitue un véritable acte de cyberterrorisme.[121]

Quels enjeux et quelles perspectives géostratégiques sont induits par l'essor du cyber et la prolifération des drones ?

En 2004, seuls 41 États possédaient des drones ; ils sont 76 en 2011.[122] La CIA affirme quant à elle en dénombrer 87. À l'inverse, seulement 15 pays investiraient dans les technologies relatives à la cyberguerre.[123] Ce chiffre est intéressant car il montre bien qu'en matière d'intégration du cyber dans des politiques de défense structurées, crédibles et potentiellement offensives, un fossé demeure entre les pays s'étant emparés de ce défi et y consacrant des moyens conséquents, et les autres. Néanmoins, l'ampleur de la prise de conscience de l'importance de l'enjeu du cyberespace, les évolutions non seulement géopolitiques mais encore technologiques, font qu'il n'y a rien de définitif : que le champ des possibles pour l'avenir du cyber est immense et difficilement cernable. En somme, les drones comme le cyber posent trois questions fondamentales pour l'avenir :

- celle de l'avenir de la gouvernance[124] à l'échelle internationale ;
- celle de l'élaboration d'un cadre juridique pour l'usage des drones armés et du cyber comme arme de guerre ;
- celle de l'influence de ces technologies sur l'ordre ou le désordre international.

Aplanissement stratégique de la planète, ou creusement d'un fossé technologique insurmontable ?

Pour les pays qui possèdent et maîtrisent ces nouvelles technologies, le développement majeur est la possibilité de mener des actes de guerre sans mobiliser de conscrits, sans envoyer de soldats sur le front, sans occuper de territoire, comme c'était le cas durant les grandes guerres du 20e siècle. Le fait est qu'aujourd'hui peu de nations sont capables de contrôler leur développement et de les opérer de manière efficiente, fiable et répétée. Les États "postmodernes", essentiellement occidentaux, ont basculé dans l'ère que Luttwak a nommée "post-héroïque". Le refus de la mort (non seulement celle qu'engendre la guerre, mais en général), la dissolution du lien entre l'État et le citoyen, ou la fin du citoyen-soldat,[125] et la montée en puissance de tout ce qu'il y a autour des *human enhancement technologies*[126] en sont les symptômes civilisationnels.

---

[121] C'est-à-dire que, pour reprendre la définition de R. Aron, son impact psychologique est sans commune mesure avec ses effets physiques.

[122] Kreps & Zenko, "The Next Drone Wars": http://www.cfr.org/drones/next-drone-wars/p32648.

[123] Transcription d'un débat organisé par le *think tank* britannique Chatham House, entre Christopher Coker, Marco Roscini et Deborah Haynes sur le thème "Drones : The Future of War ?", 8 Avril 2013 : www.chathamhouse.org/sites/files/chathamhouse/public/Meetings/Meeting%20Transcripts/080413Drones.pdf.

[124] D. Ventre, "Luttes et enjeux de gouvernance dans le cyberespace mondial", *Diplomatie*, Les grands dossiers n°23, octobre-novembre 2014.

[125] Kempf, *op.cit.*, p.16.

[126] Note d'analyse n°310 du Centre d'Analyse Stratégique (Premier ministre), "Les technologies d'amélioration des capacités humaines", décembre 2012.

Ceci explique le surinvestissement occidental dans la technologie, car comme le dit très bien G. Chaliand,

> les transformations de la guerre au cours des trois dernières décennies ont été impulsées sur le plan technologique, mais la véritable Révolution dans les Affaires Militaires (RAM) concerne avant toute chose la dimension sociale de la stratégie, qui est intimement liée au contexte démographique et à l'évolution des mentalités dans les pays occidentaux".[127]

Face à ces États postmodernes se dresserait un monde prémoderne qui, à l'asymétrie des moyens à laquelle il est confronté, opposerait une asymétrie de l'héroïsme, au sens d'absence de peur de la mort, voire sa recherche active. La plupart des conflits dans lesquels les États occidentaux ont été impliqués après 1991 s'inscrivent dans ce contexte, et ils se sont soldés – en dépit des moyens technologiques considérables mis en œuvre (en Irak, Afghanistan et Libye, par exemple) – par des échecs stratégiques.

Partant de ce constat, il faut se demander si ce fossé technologique qui se creuse entre un petit nombre de pays et l'écrasante majorité des autres va encore s'accentuer ou bien se rééquilibrer progressivement avec, en premier lieu, les modernisations opérées par les armées chinoises ou russes, suivies par d'autres dans un futur plus lointain ? On peut également se demander si, à moyens comparables, les usages des technologies de ces pays seront similaires ou radicalement différents des pratiques occidentales ?

La réponse n'est pas évidente. En matière de drones, la Chine, la Russie, voire l'Iran opèrent une véritable montée en puissance, même si leurs capacités sont bien évidemment difficiles à évaluer, compte tenu du caractère confidentiel de ces programmes. Néanmoins, tous types de drones confondus, la Chine en posséderait environ 900 (du microdrone au drone de combat),[128] alors que Poutine proclamait en juin 2014 en Crimée que "*la Russie développe des armes inédites* [...], *l'armement le plus moderne, de systèmes défensifs et offensifs, dont les autres armées du monde ne disposent pas encore*". L'Iran, plus connu pour son programme nucléaire, n'économise pas ses efforts en matière de drones. Déjà en 2013, la République Islamique dévoilait son *Shahed 123*, un drone d'attaque d'environ 2000 km de rayon d'action et pouvant voler 24 heures sans interruption,[129] alors qu'une récente étude de l'armée américaine a révélé que l'Iran avait développé un drone-suicide qu'il partagerait avec ses alliés du Hamas et du Hezbollah.[130]

En matière de cyber, la problématique est similaire. Après avoir subi une cyberattaque d'ampleur pour freiner l'avancée de son programme nucléaire, l'Iran semble

---

[127] G. Chaliand, *Le nouvel art de la guerre*, Paris, L'Archipel, Paris, 2008.

[128] C. Haress, "The Rise of China's Drone Fleet : Why It May Lead to Increased Tensions in Asia", *International Business Times*, 11 janvier 2014: http://www.ibtimes.com/rise-chinas-drone-fleet-why-it-may-lead-increased-tension-asia-1535718.

[129] R. Scarborough, "Iran Creating 'Suicide' Drones that Threaten Israel", *Washington Times*, 8 avril 2015, http://www.washingtontimes.com/news/2015/apr/8/iran-creating-suicide-drones-us-army-report-warns/.

[130] *Le Nouvel Observateur*, 18 novembre 2013: http://tempsreel.nouvelobs.com/monde/20131118.OBS5840/l-iran-devoile-un-drone-d-attaque-d-une-portee-de-2-000-km.html.

en avoir tiré profit pour renforcer ses capacités dans le domaine, en matière défensive comme en matière offensive.[131] D'après certaines sources, "*l'Iran possède les ressources humaines et technologiques pour transformer le cyberespace en champ de bataille et serait déjà parmi les 5 'cyber-États' avec les États-Unis, la Russie, la Chine et Israël*".[132] La Russie et la Chine sont très actives dans ce domaine, alors qu'une coopération semble émerger entre ces trois pays dans le cyberespace,[133] pour pousser vers une conception plus "stato-centrée" de l'Internet.

On le voit donc, la fracture numérique et technologique ne concerne pas tout le monde. Néanmoins, si "*le futur de l'humanité va dépendre de la bonne gestion des technologies d'une manière à réduire les conflits et favoriser la coopération et la coexistence pacifique*",[134] le 21e siècle ne s'est pas engagé sous les meilleurs auspices.

Enjeux juridiques induits par la "dronisation" et la "cybernétisation" des conflits

Le droit international humanitaire (DIH) ou le droit des conflits armés se trouve profondément interrogé par les évolutions de la conflictualité contemporaine, l'émergence, le développement rapide, et l'usage croissant de nouvelles technologies dans la guerre, cyber et drones en tête. Néanmoins, les interrogations et controverses qu'ils suscitent en matière juridique et éthique sont différentes. Elles ne convergent que sur une seul point, mais il est d'importance, à savoir que…

> L'application de règles juridiques préexistantes à une technologie nouvelle soulève la question de savoir si ces règles sont suffisamment claires au vu des caractéristiques spécifiques – et peut-être sans précédent – de cette technologie, et également au vu de l'impact humanitaire qu'elle peut avoir dans un avenir prévisible.[135]

Quelle légalité et quelle régulation pour les frappes à distance par des drones armés ? Quand et comment appliquer les règles du DIH concernant les cyberattaques lorsqu'on sait l'opacité qui règne dans le cyberespace ? Étant donné la complexité et le volume des enjeux ou des interrogations, ces brefs développements ont modestement vocation à pousser le lecteur à aller plus loin.

Il faut d'abord commencer par rappeler brièvement en quoi consiste le DIH : quel est son esprit et son corpus. Le DIH cherche avant tout à réglementer les méthodes et les moyens de guerre. Un certain nombre de règles doivent être respectées (principes de discrimination, de proportionnalité, d'emploi de la force en dernier recours, etc.) afin que l'action menée soit considérée comme légale. Le DIH se compose également d'accords

---

[131] G. Greenwald, "NSA Claims Iran Learned from Western Cyberattacks", *The Intercept*, 10 février 2015, https://firstlook.org/theintercept/2015/02/10/nsa-iran-developing-sophisticated-cyber-attacks-learning-attacks/.

[132] Open Briefing, the Civil Society Intelligence Agency, "Iran's Cyber Posture", *Intelligence brief*, 18 novembre 2013 : http://www.openbriefing.org/regionaldesks/middleeast/irans-cyber-posture/.

[133] T. Flichy de la Neuville, "Chine-Iran-Russie, la cyberguerre au prisme de la géoculture", *Diplomatie*, Les grands dossiers n°23, octobre-novembre 2014.

[134] A. Mallik, "Technology and Security in the 21st Century", *SIPRI Research Report*, n°20, 2004.

[135] Discours d'ouverture de la XXXIVe Table ronde sur les sujets actuels du droit international humanitaire, par le Président du CICR, M. Jakob Kellenberger, 8 septembre 2011.

internationaux limitant ou interdisant certains types d'armes. Le DIH repose essentiellement sur les quatre Conventions de Genève de 1949, deux protocoles additionnels relatifs à la protection des victimes de conflits armés (1977) et d'autres textes concernant l'interdiction de certaines armes.

Or, si le débat demeure ouvert et extrêmement vif concernant les "robots tueurs autonomes", il semble que les drones comme les cyberarmes ne puissent faire l'objet d'une pareille régulation ou interdiction, faute de consensus international suffisant, et du fait de pratiques répétées de certains États qui jugent certains types d'action comme relevant de la sécurité nationale. Pourtant, les drones comme le cyber ne peuvent être considérés comme hors du champ du DIH, étant donné que l'article 36 du Protocole additionnel I reconnaît explicitement que dans l'étude, la mise au point ou l'adoption d'une nouvelle arme ou d'une nouvelle méthode de guerre, les États parties ont l'obligation de déterminer si l'emploi en serait interdit, dans certaines ou en toutes circonstances, par une règle du droit international qui leur est applicable.

Concernant les drones, la légalité d'une attaque repose sur les mêmes règles que celles qui encadrent d'autres types de frappes, par exemple par des aéronefs habités. C'est-à-dire que la légalité d'une frappe de drone armé est conditionnée par l'existence d'un conflit, international ou non, l'existence de parties clairement identifiées, par le fait que la personne visée soit partie prenante au conflit et qu'elle ait des fonctions militaires ou qu'elle soit un civil combattant, que le lieu de la frappe ait un lien avec la guerre, enfin que cette frappe soit conforme aux principes de nécessité, de distinction, de proportionnalité, de précaution, et ne cause pas de maux superflus.[136] En fait, lorsqu'on interroge la conformité des drones armés avec le DIH, ce n'est pas tant le moyen, ou le vecteur, qui pose question, que l'usage qui en est fait : les États-Unis en arguant que la Guerre contre le terrorisme est un conflit armé d'un nouveau type, justifient leurs frappes de drones comme des actes de légitime défense ou préemptives, qui sont transnationales parce que la menace est transnationale. Or, un conflit armé constant et mondial tel que défini et matérialisé par les États-Unis au travers des attaques de drones armés, remet totalement en question le DIH. À titre d'exemple, on peut affirmer que les *signature strikes* ayant fait des victimes civiles sont *de facto* illégales. Or, dans un contexte de prolifération des drones (voir ci-après), l'extension du raisonnement juridique que les États-Unis appliquent pour justifier leurs frappes de drones fait peser de lourds risques sur la stabilité internationale à moyen terme. En effet, une part non négligeable du DIH reposant également sur du droit coutumier, il faut envisager un monde dans lequel la doctrine américaine de frappes de drones deviendrait une norme par la pratique…

Contrairement à l'opinion très communément admise, "*il n'y a pas de vide juridique dans le cyberespace*"[137] : peut-être même peut-on réalistement parler d'un trop-

[136] M. De Groof, "Utilisation des drones armés. Considérations juridiques et pratiques", Note d'analyse, Bruxelles, GRIP, 24 avril 2014.

[137] B. Louis-Sidney, "La dimension juridique du cyberespace", *Revue Internationale et Stratégique*, Automne 2012, n°87, p.74.

plein.[138] Mais la question fondamentale que pose le cyber au DIH est que la conflictualité qui s'y enracine et les attaques qui en découlent ne s'inscrivent pas forcément, ni même souvent, dans le cadre d'un conflit armé international ou interne. Les cyberattaques peuvent effectivement s'inscrire dans le cadre d'un conflit armé comportant conséquences physiques, cas dans lequel l'applicabilité du DIH est pleine et entière. Néanmoins, lorsque les cyberattaques interviennent en dehors d'un conflit armé et en temps de paix (majorité écrasante des cas de cyberattaques), c'est beaucoup moins évident, et là réside un problème essentiel posé par le cyber. Ce problème-là en englobe en fait plusieurs autres. D'abord, très globalement, du fait de la nature même du cyberespace, la qualification juridique[139] des actes qui s'y déroulent est extrêmement difficile. L'attribution de la responsabilité tout d'abord : la nature du responsable et l'origine géographique de l'attaque peuvent s'avérer impossibles à déterminer. Est-ce un service étatique, ou un groupe travaillant pour le compte d'un État, qui est à l'origine de telle attaque ? Est-ce un groupe terroriste, un *hacker*, ou encore des "cybermercenaires" rémunérés pour porter atteinte à des systèmes d'informations en échange d'importantes sommes d'argent ? Et d'où vient l'attaque ? L'adresse IP ou le serveur peuvent donner des indications, mais l'attaque a pu être lancée par un ou plusieurs *botnets* (ordinateurs zombies) contrôlés à distance.

De même, l'interconnexion des systèmes d'information interroge sur le principe de discrimination appliqué aux actions hostiles dans le cyberespace. Un ver ou un virus peut très bien se propager au-delà de sa cible et toucher, corrompre ou détruire des systèmes et des informations appartenant à des États ou des civils tiers. En l'absence de conflit armé, cela est encore plus complexe, et il faut bien le dire, la majorité des États sont "*réticents à une évolution du cadre juridique des conflits informatiques*"[140] du fait que cela leur permet de conserver des capacités d'opérations clandestines (voir *supra*) et de mener des opérations hostiles, mais pas suffisamment graves au vu de leurs conséquences physiques pour justifier une riposte militaire conventionnelle.

Vers une volatilisation de la scène internationale ?

Environ 473 frappes militaires et/ou assassinats ciblés hors théâtres d'opérations de guerre ont été menés par les États-Unis depuis 2002 ; 98% l'ont été par le biais des drones.[141] Et même depuis 2011 (année où Washington a officiellement déclaré sa préférence pour la capture ou l'arrestation), les faits sont là : 3 arrestations pour 187 frappes de drones.[142] Cette politique d'utilisation des drones, on l'a dit, crée un précédent dangereux à l'heure où les systèmes de drones armés semblent se multiplier partout autour des foyers de crise. En effet, "*si d'autres pays utilisent des drones armés de manière*

---

[138] Cattaruzza & Danet, *op.cit.*, p.154.

[139] Louis-Sidney, *op.cit.*, p.80.

[140] *Ibid.*, p.81.

[141] S. Kreps, "Drone Proliferation : What We Have to Fear", *The Hill*, Washington, DC; 25 juin 2014 : http://thehill.com/blogs/pundits-blog/210109-drone-proliferation-what-we-have-to-fear.

[142] *Ibid.*

similaire, il sera possible de voir des États effectuer des attaques transfrontalières en prenant beaucoup moins de précautions".[143]

Par la facilité avec laquelle on peut observer, surveiller et attaquer avec un drone, le seuil de recours à la force s'abaisse de manière presque inconsciente ou du moins pernicieuse. Or, il est clair que "*le fait que les drones augmentent le potentiel pour des mauvais calculs et des escalades militaires est particulièrement vrai en ce qui concerne les aires maritimes disputées*",[144] par exemple entre la Chine et ses voisins. Il faut également signaler que les trois pays où les frappes de drones ont été les plus importantes, le Pakistan, le Yémen, et la Somalie, sont durablement et profondément déstabilisés, et que le terrorisme qui y était visé s'y est plutôt renforcé qu'atténué.[145]

Cette absence de régulation internationale et la boîte de Pandore[146] ouverte par les États-Unis pourraient encourager des États extrêmement jaloux de leur souveraineté nationale, tels que la Russie ou la Chine, à utiliser les drones armés à l'intérieur de leurs territoires contre celles de leurs populations qui vivent en état de quasi-insurrection, dans le Caucase ou bien au Xinjiang[147] – ou ailleurs. Ainsi, la Chine a récemment bien failli procéder à une frappe ciblée de drone afin de tuer un criminel suspect dans le Myanmar, avant de finalement y renoncer.[148]

Dans un contexte de multipolarisation, de contestation de l'ordre international tel qu'il s'est constitué au lendemain de la Seconde Guerre mondiale, et de multiplication des tensions et conflits régionaux, la prolifération et l'utilisation croissante des drones par des acteurs de plus en plus divers peut être une source supplémentaire de volatilisation de la scène internationale. Une volatilisation qui se manifesterait de deux manières différentes. La première résiderait dans une individualisation ou une personnalisation croissante de l'usage qui peut être fait des drones par les différents acteurs internationaux, rendant de plus en plus illusoire l'élaboration d'un cadre juridique international commun à tous : cela signerait la volatilisation définitive de la notion de "communauté internationale", chacun

---

[143] *Ibid.*

[144] Kreps & Zenko, "The Next Drone Wars", 2014, *op.cit.*

[145] Les illustrations récentes ne manquent pas : attaque des Shebabs somaliens contre le centre commercial de Westgate au Kenya en septembre 2013 (67 morts) ; 141 morts dont 132 enfants tués dans un attentat des talibans pakistanais à Peshawar le 16 décembre 2014 ; attaques de Paris du 7 au 9 janvier 2015 revendiquées le 14 janvier par Al-Qaïda dans la Péninsule Arabique (AQPA), basée au Yémen ; près de 150 morts dans trois attentats contre des mosquées chiites à Sanaa au Yémen le 20 mars 2015 ; attaque de l'université de Garissa (Kenya) par les Shebabs le 2 avril 2015 (147 morts). Cela alors même que la campagne américaine de frappes de drones se poursuit au Pakistan, qu'Ahmed Abdi Godane, chef des Shebabs, a été tué par une frappe de drone en septembre 2014, et qu'au Yémen l'échec américain est désormais patent. *Cf.* http://www.lemonde.fr/idees/article/2015/04/07/une-faillite-americano-saoudienne_4610823_3232.html.

[146] Stuart Casey-Maslen, "Pandora's Box ? Drone Strikes under *jus ad bellum*, *jus in bello*, and International Human Rights Law", *International Review of the Red Cross*, n°886, Summer 2012, pp.597-625.

[147] Cet usage domestique de drones armés pourrait concerner d'autres États encore. Voir M. Zenko & S. Kreps, "Limiting Armed Drones Proliferation", *Council on Foreign Relations*, Council special report n°69, June 2014, p.22.

[148] E. Wong, "Hacking U.S Secrets, China Pushes for Drones", *New York Times*, 20 septembre 2013 : http://www.nytimes.com/2013/09/21/world/asia/hacking-us-secrets-china-pushes-for-drones.html?pagewanted=all&_r=0#.

utilisant un système d'armes porteur de nombreuses dérives comme il l'entend, tant à l'intérieur de ses frontières que dans le cadre d'actions extérieures jugées légitimes par les uns, mais pas par les autres. La seconde consisterait dans l'aggravation d'une instabilité chronique, liée tant au frottement des intérêts nationaux par drones interposés qu'à la multiplication des usages détournés de drones, même rudimentaires. En conséquence, grâce aux drones, les acteurs internationaux désireux d'affirmer leur puissance ou bien de tester l'opposition potentielle, seraient tentés d'opérer dans une sorte de *borderline* perpétuelle, pouvant mener à des escalades sciemment provoquées, ou non maîtrisées. En entrant dans des considérations relevant encore davantage de la prospective, le développement de véritables drones de combat (capables d'attaquer d'autres aéronefs ou de se défendre en cas d'attaque) ayant une autonomie qui va probablement augmenter avec le temps, rend l'occurrence de ces tendances encore plus probable.

Le cyberespace, par l'abolition des distances qu'il engendre et l'opacité qui le caractérise, fait qu'une alliance stratégique avec vos voisins directs perd quelque peu de son sens, mais que de plus "*chacun peut agir contre tous les acteurs*".[149] Cela signifie qu'en dépit de tentatives d'élaboration de projets collectifs autour de la cyberdéfense sur la base d'alliances (OTAN) ou d'institutions communautaires (Union Européenne),[150] le cyberespace favorise assez largement l'émergence "*d'un monde de la lutte de tous contre tous*".[151] Comme les ennemis potentiels ou les adversaires, les alliés constituent des cibles, ainsi que les révélations d'Edward Snowden l'ont crûment exposé aux yeux du monde. Si des possibilités d'alliance existent dans le cyberespace, qu'elles soient interétatiques ou hybrides, leur ambivalence[152] semble plus grande encore que celle qui caractérisait les alliances traditionnelles. En effet, entre menace permanente, multidirectionnelle, multi-forme, et méfiance généralisée en découlant, le cyber complexifie considérablement toute tentative de coopération internationale.[153]

En somme, le cyberespace est équivoque : on peut considérer que les affrontements clandestins généralisés qui s'y déroulent forment finalement une sorte de soupape de sécurité dans les relations internationales,[154] sans pour autant exclure qu'à un moment, ce qui se passe dans le cyberespace demeure éternellement dans le cyberespace...

Conclusion

Les drones comme le cyber sont donc au cœur de mutations considérables dont les conséquences ne sont pas toutes mesurables aujourd'hui. Ils interrogent les normes et les pratiques en vigueur jusqu'à maintenant, le rôle de l'État et du secteur privé, la portée de la

---

[149] Kempf, *op.cit.*, p.58.

[150] O. Kempf, "Union européenne, cyberstratégie et cyberdéfense", *Diplomatie*, Les grands dossiers n°23, octobre-novembre 2014.

[151] Kempf, *op.cit.*, p.60.

[152] Kempf, *op.cit.*, p.26.

[153] Malis, *op.cit.*, p.160.

[154] Malis, *op.cit.*, p.161.

notion de souveraineté et de frontière, et peuvent laisser à penser qu'ils constituent des armes ultimes.[155] Pour autant, il n'en est rien. Les drones armés présentent effectivement des avantages tactiques considérables pour l'État qui a les moyens de les mettre en œuvre. Néanmoins, le drone ne dispense pas d'une réflexion stratégique car la technologie à elle seule, sans vision politique du conflit et des objectifs, est inopérante, sinon contre-productive. Or, le "vide stratégique"[156] et le manque de vision globale de la conflictualité contemporaine semblent être accentués par le recours tactique aux drones armés par les Américains. De plus, cette politique d'élimination ciblée est dangereuse à plus d'un titre. Elle s'avère déstabilisante pour des sociétés et des États qui sont déjà dans une instabilité chronique (Yémen, Pakistan, Somalie) ; elle déprécie le "modèle américain" et les valeurs démocratiques dont les États-Unis sont le chantre, sans véritablement contribuer à affaiblir le terrorisme djihadiste, qui prospère plus que jamais. Elle crée également un dangereux précédent qui pourrait pousser certains pays à adopter un usage similaire des drones armés, avec toutes les conséquences déstabilisantes que cela pourrait avoir pour le système international. D'ailleurs, N. Melzer ne dit pas autre chose :

> L'incertitude qui règne en ce moment quant aux normes juridiques applicables, le développement rapide et la prolifération des drones et des technologies robotiques, et le manque de transparence et de responsabilisation dans les politiques actuelles peuvent polariser la communauté internationale, miner l'État de droit, et à terme déstabiliser le climat international en matière de sécurité.[157]

La perception du cyberespace qu'ont l'ensemble des acteurs qui y évoluent et l'utilisent oscille entre opportunités et vulnérabilités. Les cybermenaces émanent d'une diversité d'acteurs aussi importante que dans le monde réel, et revêtent des formes aussi variées que celles de leurs auteurs. C'est donc un environnement profondément volatil, fruit de l'action de l'homme, et donc absolument indissociable des conflits géopolitiques classiques[158] qui y trouvent un écho et un terrain d'expression inédit. Cela est évident lorsque l'on regarde l'évolution des rapports sino-américains depuis quelques années, évolution qui se caractérise par une augmentation des tensions, matérialisées dans le cyberespace par des opérations hostiles engendrant un durcissement diplomatique bien réel. La guerre des djihadistes de *Daech* trouve également un écho particulier sur le cyberespace. Si pour le moment, la "*guérilla cybernétique endémique mondiale*"[159] n'a pas débordé symétriquement dans les autres sphères de l'activité humaine, et n'a encore engendré directement ni perte de vies humaines, ni importantes destructions physiques, rien ne prouve en l'état actuel des choses que cette tendance soit durable ou inhérente à la nature du cyberespace.

---

[155] Au sens où Douhet l'entendait pour l'aviation.
[156] P. Baumard, *Le vide stratégique*, Paris, CNRS Éditions, 2012.
[157] M. De Groof, Note d'analyse, GRIP, 24 avril 2014, *op.*cit., p.21.
[158] Cattaruzza & Danet, *op.cit.*, p.53.
[159] Malis, *op.cit.*, p.161.