« La guerre cyber »

Biblioveilles- octobre 2022

La Russie mène depuis février 2022 des attaques contre le service Starlink dans le but d'entraver l'accès des Ukrainiens à Internet. Cet exemple d'actualité illustre l'importance que le domaine cyber a pris dans la guerre d'aujourd'hui. Il s'agit d'un domaine de conflictualité au même titre que les espaces terrestre, maritime, aérien et spatial. Ce *Biblioveilles* s'attarde sur des publications récentes qui abordent les diverses modalités de la guerre cyber menée aussi bien en zone euratlantique qu'en Afrique ou en Asie.

MONTENON (de), Philippe. « Cyberespace : la guerre a commencé », ***Revue Défense Nationale***, n°829, 2020/4, (pp. 25-31).

« On peut sans doute résumer les enjeux de l'affrontement dans le cyberespace à cette idée : celui des adversaires qui possédera la supériorité numérique sera désormais en position de briser toute attaque du camp d'en face, voire de le dissuader de toute tentative d'action hostile. »

« L'efficacité de la défense de nos systèmes et la capacité à gagner la supériorité numérique reposent avant tout sur le talent de celles et ceux qui préparent et exécutent les opérations de cyberdéfense. »

Le général Philippe de Montenon expose l'enjeu de souveraineté majeur que constitue la cybersécurité, décrite comme « *une guerre d'aujourd'hui* » (p. 26). Le cyberespace est un nouveau champ de confrontation où défendre ses intérêts. Cette nouvelle réalité stratégique amène à viser la supériorité numérique sur son adversaire quelle que soit sa nature. L'auteur multiple ainsi les références historiques afin de saisir les enjeux nouveaux posés par ce domaine. Il propose une définition claire de ce que représente une attaque cyber : elle repose sur le type d'attaquant, les méthodes et outils employés tout comme sur les effets visés et produits. Ces derniers seraient de trois natures : l'entrave, l'extraction de données et la modification des perceptions.

Dans cet article, l'auteur met la focale sur l'efficacité d'une stratégie de guerre numérique et ses piliers : la connaissance et l'étude de l'adversaire comme du terrain, l'étude des rapports de force et motifs d'actions, et enfin l'élaboration de plans de secours. Cependant, bien que ces facteurs soient proches de ceux des guerres conventionnelles, la guerre cyber a un temps

de préparation long et un temps d'action relativement bref. C'est pourquoi le développement par l'État d'une protection cyber est désormais nécessaire.

CATTARUZZA Amaël. « Vers une géopolitique numérique », ***Constructif***, n°60, 2021/3, (pp. 46-50).

« La multiplication des cyberattaques de grande ampleur illustre cette poussée croissante de vulnérabilité globale. […] cette montée en puissance des technologies numériques dans l'arène internationale implique une transformation importante de la notion même de puissance »

Professeur à l'Institut français de géopolitique et président du Comité national français de géographie, Amaël Cattaruzza tente dans cet article d'esquisser une partie des grandes mutations induites par les technologies numériques, notamment en matière de structuration de la scène internationale. La comparaison de la transformation numérique avec les révolutions industrielles du XIX^{e} siècle met en lumière des conséquences à différentes échelles : politiques, économiques et sociales. Bien que l'ère numérique facilite de multiples décisions, illustrées par l'exemple des *smart cities*, elle développe aussi de nouvelles vulnérabilités exposées lors des attaques de WannaCry ayant touché en 2017 plus de 130 pays en quelques heures. La cyberguerre est donc polymorphe, peut générer des conséquences physiques directes, comme d'autres plus discrètes voire invisibles. Amaël Cattaruzza se réfère ainsi aux attaques de mai 2007 contre l'Estonie ou encore aux révélations d'Edward Snowden.

Une nouvelle forme de compétition se dessine avec le développement numérique : il y a concurrence internationale autour de l'accès internet. Force est de constater l'émergence de nouveaux acteurs privés, dont certains ont une puissance comparable à celle des États, posant ainsi des défis et des questionnements. Cette géopolitique du numérique fait intervenir une analyse à deux échelles : internationale, passant par la conquête de nouveaux marchés et actions souterraines, et amenant à une collaboration entre acteurs publics et privés ; sociétale, afin de répondre tant aux multiples interrogations soulevées par cet espace qu'à la question de la répartition des pouvoirs aujourd'hui à l'œuvre au sein de nos sociétés.

DELEPINE Justin. « Cyberattaques : sommes-nous prêts ? », ***Alternatives économiques***, n°424, juin 2022 (pp. 56-59)

« … plus d'un millier de cyberattaques sur des organisations françaises ont été répertoriées en 2021, un tiers de plus qu'en 2020. Soit en moyenne a minima trois attaques par jour. »

Ce constat inquiétant amène Justin Delépine, journaliste spécialisé dans l'économie d'entreprise, à tirer la sonnette d'alarme sur le manque de moyens dont disposent les organisations françaises – qu'elles soient publiques ou privées – dans le domaine de la cybersécurité. En France, on a répertorié 200 entreprises comme essentielles pour la sécurité de la nation. La liste demeure secrète, mais on sait qu'elles sont amenées à renforcer la sécurité de leurs systèmes numériques, notamment avec le soutien des agences gouvernementales dédiées à cet effet. Cependant, Jules Delépine attire l'attention sur le fait que le danger vient surtout des entreprises de sous-traitance et des PME, moins observantes en ce qui concerne la protection de leurs systèmes d'information. À cause de l'interconnectivité de nos sociétés actuelles, une attaque sur un point fragile d'un réseau peut causer des dégâts sur le réseau entier. Or, un pays voulant mettre à mal ses ennemis n'aura aucun scrupule à viser les infrastructures civiles, ce que Jules Delépine montre à travers l'exemple de la Russie qui a effectué des cyberattaques contre les États qui soutenaient l'Ukraine afin d'infléchir l'aide qu'ils apportaient à Kiev. La cybercriminalité, dont l'objectif n'est pas de déstabiliser un pays mais simplement d'obtenir des gains économiques par des voies illégales, est également un problème auquel sont régulièrement confrontées les entreprises françaises.

La réponse à apporter à ce dernier problème doit être aussi bien nationale qu'européenne. L'émergence de géants européens de la cybersécurité est particulièrement nécessaire afin de créer un écosystème numérique sûr pour les organisations présentes sur le continent. La France, quant à elle, doit investir davantage pour que les *start-up* spécialisées dans la cybersécurité puissent se développer et avoir des moyens suffisants pour mener à bien leurs objectifs. Dans le cas contraire, ces dernières risquent de passer dans le giron américain, ce qui a déjà été le cas pour Sqreen et Alsid en 2021.

CLACK, Timothy ; JOHNSON Robert (dir.). **The world information war, western resilience, campaigning, and cognitive effects**, Londres, Routledge, 2021.

« … the west finds itself in a war it did not want. It is a war it did not realize, until now, which had already broken out. It is a global in its scope and concerns the future shape of the world's governance. It is a war, at the time of writing, the West is losing […]. »

Thimothy Clack et Robert Johnson, enseignants-chercheurs à l'université d'Oxford, ont dirigé un ouvrage qui offre au lecteur un panorama complet de la guerre de l'information, concept qui, selon les auteurs, n'est pas encore suffisamment maîtrisé par les démocraties occidentales alors qu'elles sont les premières visées. Si la guerre de l'information doit être distinguée de la guerre cyber, il n'en reste pas moins que les deux domaines sont inextricablement liés. La guerre de l'information se joue la plupart du temps dans le monde virtuel, notamment sur les réseaux sociaux qui sont de plus en plus le théâtre de campagnes d'influence très agressives. L'ouvrage cite en exemple le cas de Vitaly Bespalov, journaliste au chômage qui a été recruté par le Kremlin pour intégrer les usines à troll visant à donner une image positive de l'annexion de la Crimée en 2014. Pour Bespalov, le poste qui lui était proposé devait seulement consister à informer les lecteurs sur la situation militaire du pays, mais il s'est rapidement rendu compte que Moscou l'utilisait comme propagandiste tout en faisant en sorte qu'il ait l'image d'un journaliste indépendant. Ces procédés sont encore renforcés par l'utilisation des données personnelles pour paramétrer des algorithmes. Leur efficacité est telle qu'ils sont capables d'influencer des communautés de personnes pour qu'elles adhèrent à une opinion déterminée.

Tout en alarmant le lecteur sur le danger que représentent la guerre de l'information et le retard pris par l'Occident dans ce domaine, les auteurs indiquent néanmoins que les démocraties sont parfaitement capables de faire face à des attaques informationnelles. Grâce à des réactions rapides, à une opinion publique faisant confiance aux médias traditionnels et à un contre-discours pertinent développé par les services de communication de l'État, la Finlande est par exemple parvenue à contrer les attaques informationnelles que le pays a subies à plusieurs reprises. Les leçons à tirer de cet exemple sont claires : pour gagner la guerre de l'information, il faut être proactif et réussir à créer un climat de confiance entre la population et les institutions.

BRANTLY, Aaron F. (dir.). **The cyber deterrence problem**, London, Rowman and Littlefield International, 2020.

« By acknowledging the failures and inadequacies of deterrence strategies and the potential places where novel strategies found in other fields are applicable, the intractable problem of cyber deterrence becomes more manageable. »

Aaron F. Brantly, professeur de sciences politiques à la *Virginia Tech*, propose une analyse du concept de dissuasion appliqué au domaine cyber. Très centré sur les États-Unis, l'ouvrage montre comment Washington peut et doit faire face aux attaques cyber qui sont de plus en plus dangereuses pour la sécurité du pays. Tous les contributeurs de l'ouvrage partagent l'idée que les concepts classiques de la dissuasion ne sont pas opérants dans le domaine du cyber. Trop souvent, les attaques cyber causent des dégâts bien inférieurs à ceux qui justifieraient une riposte. De plus, la dissuasion suppose que l'ennemi estime clairement ce qu'il risque en attaquant, ce qui est difficile à évaluer dans le domaine cyber, d'autant qu'il n'est pas toujours aisé d'identifier l'origine d'une agression informatique. Le besoin de mettre en place une cyberdéfense robuste afin de protéger les infrastructures critiques des États-Unis, cibles privilégiées des attaques cyber, appelle à élaborer de nouveaux cadres de pensée et des méthodes adaptées au domaine informatique.

Contrairement à la dissuasion nucléaire, qui veut que toute attaque utilisant l'arme nucléaire appelle une réponse du même type, la dissuasion cyber doit mobiliser plusieurs domaines, qu'ils soient militaires, diplomatiques ou économiques. Pour illustrer son propos, le livre raconte la façon dont les États-Unis ont réagi aux multiples attaques que la Chine effectuait depuis son territoire durant les années 2000. En 2013, la publication du rapport « APT 1 » par la firme privée *Mandiant* a permis au gouvernement américain d'identifier la section de l'Armée populaire de Libération en charge des attaques cyber et de repérer les multiples opérations qu'elle menait. Le Département de la Défense a ensuite pris le relais et a élaboré

toute une série de réponses possibles qui incluaient aussi bien des contre-attaques cyber que des sanctions économiques. Cela a permis à Barack Obama d'envoyer un signal fort à la Chine en lui indiquant que les États-Unis savaient identifier ses opérations cyber et avaient l'intention d'y répondre, ce qui a entrainé une réduction substantielle des pénétrations cyber menées par Pékin. Ainsi, une politique de dissuasion cyber demande de dépasser le seul théâtre du cyber qui présente trop de limites pour élaborer une menace crédible de riposte.

BARICHELLA, Arnault. « **Cybersécurité et protection des données en Europe** », Paris, Institut Jacques Delors, Mars 2022.

« […] compte-tenu de l'accélération de la "révolution numérique", ainsi que de l'augmentation exponentielle du nombre de la sophistication des cyber-attaques touchant pratiquement tous les secteurs, le renforcement des politiques et de la législation de l'UE dans ce domaine devrait constituer une priorité absolue pour les décideurs européens. »

Cet article publié par l'Institut Jacques Delors met l'accent sur la numérisation des infrastructures critiques. Cette « révolution numérique », bien qu'utile, génère également pléthore de menaces et risques cyber. Les attaques cyber permettent un ciblage simultané et menacent d'effondrer un système interconnecté entre secteurs. Ces attaques et violations concernent tous les domaines. Véritable acte de guerre, ces cyber-menaces pèsent sur les dynamiques géopolitiques, y compris européennes.

La seconde partie de cette étude menée par Arnault Barichella s'intéresse aux approches européennes en matière d'IA, de protection des données et de cyber sécurité. L'Union européenne vise à ce que son approche soit définie comme « globale » et « souple ». Il s'agit de faire entrer dans sa législation un volet cybersécurité et de tenter le développement d'une approche européenne concernant l'intelligence artificielle. Cependant, les pays de l'UE n'ont pas tous un cadre national sur le cyber d'une efficacité comparable. Certains considérés comme maillons faibles amènent les autres membres à hésiter à partager des informations classifiées avec eux. Ainsi, face à cette guerre hybride, les membres de l'UE se doivent de renforcer la législation européenne cyber et ses liens avec la PSDC.

VAN WIE DAVIS Elizabeth. **Shadow warfare. Cyberwar Policy in the United States, Russia and China**, Londres, Rowman & Littlefield, 2021.

« Russia agrees with the United States that cyberspace is an incipient battleground. There the agreement ends. »

Cet ouvrage consacré au *shadow warfare* par Elizabeth Van Wie Davis, chercheuse américaine spécialisée en relations internationales, propose plusieurs définitions de la guerre cyber. Elle est caractérisée par sa continuité et son caractère invisible, plongeant les États dans une guerre permanente. La guerre cyber rend difficile la distinction entre adversaires et alliés, et émane de la synthèse entre nouvelles technologies et imagination militaire. Proposant un mélange entre guerre conventionnelle et méthodes hybrides, elle menace d'amplifier les conflits et les violences. Chaque pays propose sa propre vision de ce que représente la guerre cyber et ses enjeux, rendant difficilement imaginable la formalisation de normes universelles autour de cette notion.

Les États-Unis prennent en compte trois aspects pour le développement de leur politique de guerre invisible : les facteurs politiques, sociaux et économiques ayant un impact sur leurs objectifs à long terme, leur administration et ses particularismes, les principes nationaux et idéologiques. La politique de *cyberwarfare* russe repose à la fois sur la réaction à la politique des autres pays et sur une volonté de guider d'autres gouvernements vers la création d'un monde multipolaire. La Chine est à la poursuite d'une stabilité tant nationale qu'internationale, tant politique qu'économique. Ces trois puissances n'emploient donc pas le cyber à des fins équivoques et ne considèrent pas nécessairement les attaques cyber comme élément déclencheur d'une guerre cyber.

JASPER, Scott. **Russian cyber operations: coding the boundaries of conflict**, Georgetown, Georgetown University Press, 2020.

« Cyber operations have become a central aspect of Russian forms of conflict or competition. »

Scott Jasper, maître de conférences à la *Naval Postgraduate School*, propose une analyse de la façon dont la Russie emploie l'outil cyber dans la compétition stratégique qu'elle mène avec l'Occident. Profitant du flou juridique et de la complexité technique liés aux opérations cyber, le Kremlin a souvent recours à ce type de méthodes pour déstabiliser ses adversaires en temps de paix comme de guerre. Étant donné que l'armée russe ne dispose pas des forces nécessaires pour mettre à mal les puissances occidentales de façon frontale, les attaques cyber ont l'avantage de pouvoir causer des dégâts très importants avec des moyens *low-cost*. Ainsi, la Russie peut s'en servir à la fois comme méthode de dissuasion, d'agression ou de soutien à son armée lors d'opérations militaires. L'attaque *NotPetya* contre l'Ukraine en juin 2017 montre l'étendue des dégâts que ce type d'opérations peut causer : un simple logiciel malveillant a supprimé les données de vingt-deux banques, six compagnies d'électricité, quatre hôpitaux, deux aéroports ainsi que de presque toutes les agences fédérales ukrainiennes.

Au vu de l'évolution de la politique étrangère russe et compte tenu du fait que les attaques cyber menées par Moscou seront de plus en plus agressives, l'auteur appelle donc à une meilleure gestion des risques cyber par les pays occidentaux. Cela passe notamment par une législation internationale mettant en place des normes actualisées pour mieux qualifier les agressions cyber, par un fort investissement dans les services publics visant à assurer la cyberdéfense de leur territoire et par des sanctions qui ne soient pas uniquement symboliques.

AMSELLEM, David. « Le cyberespace israélien, un enjeu de puissance », ***Hérodote***, 2020/2, n° 177-178 (pp. 281-296)

« Qu'il s'agisse d'applications civiles ou militaires, Israël est présent dans tous les champs qu'offre le cyber : il est à la fois une vitrine politique du service de l'influence de l'État, un instrument stratégique dans les rivalités avec ses ennemis, un marché incontournable pour acquérir les dernières technologies d'espionnage, et un outil de propagation de contenus informationnels. »

Comment Israël est-il parvenu à s'imposer comme un pays à la pointe de la cybersécurité ? L'article de David Amsellem, docteur à l'Institut français de géopolitique de Paris 8, répond à cette question en montrant comment cette réussite tient à la volonté politique de l'État d'Israël qui a favorisé le développement de ce secteur depuis le début des années 2000. Le cyber constitue en effet une filière particulièrement valorisée et attractive auprès de la population qui a la possibilité d'étudier ce domaine dès le secondaire. Ceux qui choisissent cette voie rejoignent la *Silicon Wadi,* terme qui désigne un espace situé dans un rayon de 20 km autour de Tel-Aviv dans lequel se trouvent la plupart des centres de formation scientifiques et des entreprises *high-tech* spécialisées dans le cyber. Très lié à l'armée israélienne, ce secteur compte environ 450 entreprises et *start-up* qui se sont imposées comme des leaders mondiaux.

C'est ainsi que l'armée israélienne dispose d'importants moyens cyber qu'elle emploie lors de ses conflits avec ses adversaires. L'Iran constitue une cible privilégiée de Jérusalem. Téhéran a notamment vu ses centrifuges endommagées par un virus informatique israélien en 2010 et fait régulièrement l'objet de tentatives d'espionnage de la part de Jérusalem. Cependant, Israël emploie également ses outils cyber dans le cadre de la guerre informationnelle dans le but d'améliorer l'image du pays. Les opérations militaires du *Tsahal* sont souvent accompagnées de publications sur les réseaux sociaux visant à légitimer leurs actions en n'hésitant pas à utiliser le ton de l'ironie qui fait mouche sur internet mais qui singularise la communication de l'État hébreu par rapport à celle des autres pays. Ainsi, l'article de David Amsellem montre comment Israël a parfaitement su s'approprier l'outil cyber dans sa stratégie de puissance.

ALLAIN, Enzo. **La cybersécurité en Afrique de l'Ouest**, Paris, Ed. du Cygne, 2020.

« Les nouvelles cybermenaces en Afrique de l'Ouest sont de deux types : l'hacktivisme et le cyberterrorisme. »

Au travers de ce mémoire de fin d'études en géopolitique et sécurité internationale, Enzo Allain interroge les défis de cybersécurité auxquels les pays d'Afrique de l'Ouest sont confrontés. Cette étude se penche sur le développement numérique de la zone étudiée au sens large, du Sénégal au Nigéria et du Mali au Ghana, avec une attention particulière au Sénégal en dernière partie. L'auteur a fait le choix d'y intégrer certains pays extérieurs se servant de cet espace comme théâtre de conflictualités. Ils cherchent à augmenter leur influence numérique en profitant du manque de cohésion régionale et de l'absence d'une stratégie de cyberdéfense. Trois couches du cyberespace sont présentées : infrastructurelle, logique et cognitive. Et différents aspects sont à prendre en compte : informationnel, humain et géographique.

Force est de constater un niveau d'avancement inégal des pays de la zone quant aux questions cyber, bien qu'une prise de conscience soit en marche. L'Afrique de l'Ouest se doit d'affronter à un déficit de connectivité et d'éducation face aux risques cybernétiques pesant sur les populations. Enfin, des solutions aux problèmes du *hacking* et du cyberterrorisme ont été envisagées au travers des conventions de Budapest (23 novembre 2001) et de Malabo (27 juin 2014), mais n'ont pas débouché sur une résolution effective de ces questions. Il ne faut cependant pas omettre le fait que des législations spécifiques et des infrastructures dédiées sont en cours de développement par les différents pays de cet espace ouest-africain.