La cyberguerre au cœur des secteurs civils critiques : mythe ou réalité ?

Par Emmanuel Meneut

La révolution numérique résulte, entre autres, d'une diminution drastique du coût des communications. L'une de ses conséquences a été la connexion des infrastructures civiles à des réseaux d'information, qui les rend de fait vulnérables à des cyberattaques. On constate, plus précisément, que les auteurs d'agressions sur les infrastructures civiles mettent en œuvre des stratégies de coercition qui visent à délégitimer l'État en déstabilisant la confiance que l'opinion publique lui accorde.

Le propos du présent article est de décrire la réalité des cyberattaques sur ces infrastructures numérisées, notamment au travers des exemples que sont la panne électrique géante au Brésil en 2009 et le vol de données dont *Sony Pictures Entertainment* a été la victime en 2014. On en déduira les caractéristiques du défi stratégique posé aux institutions d'État chargées d'assurer la souveraineté et la sécurité des populations. On s'interrogera en particulier sur le rôle que peuvent jouer les forces armées dans cette configuration comme levier principal de la sécurité nationale.

L'émergence de la puissance numérique : origine et facteurs

Quelques années après le passage de la technologie Internet du domaine militaire au civil, Joseph Nye et Robert Keohane, dans un article de *Foreign Affairs* publié en 1998, décrivaient l'émergence au sein de ce nouvel espace cybernétique d'une "puissance douce" ("*soft power*"), fruit d'un accroissement des flux d'informations. Les auteurs fondaient leur argumentation sur une distinction des types d'information qui circulent dans le cyberespace, et permettent de préciser ses caractéristiques[1] :

- l'information libre : celle que produisent et diffusent des acteurs sans compensation financière. Le gain pour l'émetteur réside dans l'influence qu'il exerce sur la croyance du destinataire en la validité de l'information. On est là dans le registre de la communication politique ou de la propagande, qui ont véritablement explosé avec la diffusion d'Internet ;
- l'information stratégique : celle qui, par dissymétrie, confère un avantage à un acteur qui la possède sur un adversaire qui en est dépourvu. Ce registre est celui de l'espionnage, qui s'est étendu lui aussi d'une façon exponentielle au cyberespace ;
- l'information à valeur économique produite, échangée et utilisée par des entreprises, fondement de l'industrie logicielle, notamment en matière de contrôle/ commande des infrastructures civiles dans les secteurs critiques de l'énergie ou du transport.

[1] Keohane & Nye, 1998.

La diminution du coût des communications a augmenté le volume de tous ces flux d'informations, et le nombre de canaux. L'information gratuite circule plus vite, et plus facilement ; cette capacité devient accessible à des acteurs non étatiques animés par des objectifs politiques, notamment les ONG ou les groupes terroristes. L'information stratégique, quant à elle, liée aux ordinateurs (dès leurs débuts, en 1942) et aux canaux de communication entre eux, fait l'objet d'une traque incessante du renseignement à intercepter. Toute organisation connectée peut être systématiquement espionnée, comme on l'a vu lors de la révélation en 2009 du programme de cyberespionnage chinois *Ghostnet*, ou de son pendant américain (PRISM), divulgué par Edward Snowden en 2013. Selon Keohane et Nye, l'accroissement exponentiel de l'information libre et l'accès à l'information stratégique est la substance même du *soft power*, qui permettrait d'influencer les acteurs de la scène internationale avec autant d'efficacité que les moyens diplomatico-militaires ("*hard power*"). Enfin, l'information aujourd'hui valorisée en termes monétaires via des logiciels, par exemple pour le fonctionnement d'un réseau électrique ou d'une raffinerie, est devenue l'élément critique de la sécurité de ces infrastructures. Selon le cabinet PwC, depuis 2009, le nombre d'incidents augmente de 66% par an.[2] Elle dépend du respect du droit de la propriété intellectuelle et des contrats entre fournisseurs et utilisateurs de logiciels. Cependant, ce droit n'est pratiquement pas appliqué lorsque les enjeux de politique étrangère sont prioritaires, et les entreprises ne savent pas gérer ces situations. Ainsi, la société Siemens a été mise en cause par les Iraniens en 2009, lors de la cyberattaque américaine *Olympic Games*, à propos de ses contrôleurs numériques ("*programmable logic controller*") : elle s'est défendue en invoquant le "nécessaire partage des risques" entre fournisseur et client.[3] Selon la vision néo-réaliste d'un système international anarchique, l'absence de gouvernance du cyberespace permet à ces nouveaux leviers de puissance d'être utilisés quelle que soit la nature des acteurs.[4]

De plus, la facilité d'accès au cyberespace, le nombre considérable de failles des systèmes d'information et le coût exorbitant de la sûreté rendent pratiquement impossible une cyberdéfense efficace de ces actifs stratégiques.[5] Dans le cyberespace, l'avantage est à l'offensive, d'où la "guerre invisible" et permanente entre grandes puissances numériques.[6] Ainsi, la montée exponentielle de tous les flux d'information affecte le concept même de puissance : elle a engendré des puissances numériques, tout comme l'introduction de l'arme atomique avait en son temps créé une nouvelle catégorie : les puissances nucléaires.

La révolution numérique a intensifié toutes les activités de propagande et d'influence, d'espionnage et de vol de données, d'attaque et de prise de contrôle des infrastructures numériques d'une société, qu'elles concernent ses services publics ou son secteur privé. De fait, les dirigeants chargés de la sécurité doivent aborder cette réalité globale et articuler

---

[2] Herjavec, 2015.
[3] Brandstetter, 2010.
[4] Waltz, 2000.
[5] Clarke, 2010.
[6] Vitkine, 2012.

une réponse. Pour cela, la puissance numérique d'un pays doit simultanément être déployée dans les trois secteurs que sont l'influence, l'espionnage, et la sécurisation des infrastructures numériques. Ces trois secteurs de la puissance numérique reposent sur les capacités technologiques. Un acteur puissant dans l'un de ces domaines l'est aussi dans les autres. Or, les dernières décennies ont montré que la mutualisation des moyens de renseignement pour accroître la sécurité internationale est restée un idéal.[7] Ainsi, les perspectives de gouvernance mondiale de cybersécurité sont une utopie. Un État ne partage pas ses moyens de renseignement sur une base d'égalité, comme l'illustre bien l'alliance UKUSA[8] qui gère ECHELON[9] ; c'est encore plus vrai en matière de cyberarmes.[10] Ce contexte de cyberguerre permanente est un défi stratégique et organisationnel pour les forces armées. Si la cyberdéfense des réseaux numériques n'est pas satisfaisante, car trop chère, quelle stratégie offensive faut-il mettre en œuvre pour protéger les infrastructures numériques sans risquer de perdre le contrôle de la montée aux extrêmes ?

Une ébauche de réponse est la mise en place d'un commandement dédié, à l'image du *Cyber Command* créé par décision du Président Obama en 2009, car les capacités décisionnelles sont déterminantes face à une cyberattaque qui se déploie en quelques minutes. Mais pour répondre plus précisément, il est nécessaire de comprendre comment la puissance est affectée par l'ensemble de ces flux d'informations.

La diffusion du pouvoir et l'émergence d'acteurs non étatiques

En 2006, moins d'une décennie après l'article cité, Joseph Nye mettait à jour les caractéristiques de la cyberguerre.[11] La diminution du coût d'accès aux moyens de communication permet une extension mondiale du réseau à l'ensemble des infrastructures des grandes puissances – États-Unis, Chine, Russie, et d'autres – et elle structure désormais leurs rapports de forces.

Tout d'abord, le phénomène de globalisation de la cyberguerre est très rapide. C'est la conséquence de la dynamique que crée une rupture technologique par essence non linéaire. L'augmentation du nombre d'infrastructures critiques connectées au cyberespace, *Smart Grid*, objets connectés, etc., suit la même croissance exponentielle, et elle offre un nombre important de vulnérabilités et de leviers de pouvoir. Il devrait y avoir 50 milliards d'objets connectés d'ici à 2020.[12] Les acteurs sont en permanence sous un voile d'incertitude quant aux menaces qui pèsent sur eux à ce titre, car on ne peut pas observer une cyberarme depuis un satellite espion : on peut tout juste compter le nombre de cyberguerriers d'un adversaire – et encore ! Propagande, cyberespionnage et cyberattaques n'ont

---

[7] Aldrich, 2009.

[8] Alliance nouée en 1946 entre les États-Unis, la Grande-Bretagne, le Canada, l'Australie et la Nouvelle-Zélande.

[9] Le réseau ECHELON désigne le système mondial d'interception des communications privées et publiques (Sigint).

[10] Delesse, 2012.

[11] Nye, 2006.

[12] Bembarron, 2015.

aucune difficulté à atteindre une audience, intercepter des informations secrètes ou paralyser une infrastructure civile, quelle que soit leur localisation, et à toutes les échelles : locale, régionale ou internationale.

Les acteurs de ces activités ne sont plus seulement les États, mais encore les acteurs de la société civile, entreprises et associations. Cette diffusion de la puissance au bénéfice d'acteurs non étatiques est la caractéristique majeure de la cyberguerre, précise Nye en 2006. Ainsi, l'activité de propagande des groupes terroristes s'est développée de façon là encore exponentielle avec l'extension du cyberespace. Elle a permis le développement du mécanisme de franchise entre des groupes éloignés géographiquement et à commandement décentralisé, comme *Al-Qaïda* et ses branches régionales. Lorsque des forces armées participent à des cyberguerres, elles font face à un théâtre d'opérations global et à des ennemis qui ne sont pas nécessairement des forces armées ; il en va de même pour leurs alliés potentiels. Ce sont des menaces très incertaines, portées par des acteurs hétérogènes.

Cependant, cette diffusion de la puissance n'affecte pas tous ces acteurs de manière uniforme. Si une ONG peut toucher une large audience et mobiliser l'opinion publique pour faire inscrire sa cause à l'ordre du jour international, ses capacités d'espionnage sont limitées, et elle est plus souvent la cible de cyberattaques étatiques qu'à l'origine d'attaques contre des États. Si *Reporters Sans Frontière* avait en 2008 la capacité de faire pression sur Pékin à propos des Jeux Olympiques, elle a surtout été victime d'une attaque couronnée de succès de la part de cyberguerriers vraisemblablement chinois, qui ont significativement réduit son audience auprès de l'opinion publique. Les associations sont donc des acteurs périphériques, et il existe une asymétrie fondamentale entre elles et les États. Ces derniers possèdent des moyens classiques de renseignement, prérequis indispensable au succès d'une cyberattaque comme celle menée contre les centrifugeuses du programme d'enrichissement nucléaire iranien en 2009.[13] De plus, ils sont les seuls à disposer de ressources qu'ils peuvent affecter de façon permanente à des activités de conception et de mise en œuvre de cyberarmes pour maintenir une capacité offensive dans un cyberespace en constante évolution technologique. Enfin, ils bénéficient, avec les forces armées, du monopole de la violence légitime, monopole qui leur assure la possibilité avérée de nuire à des associations ou des entreprises considérées comme hostiles.[14]

L'enjeu n'est donc pas celui de l'existence de la souveraineté, mais sa centralité et son fonctionnement tels qu'altérés par la cyberguerre. Le processus d'adaptation change les modalités d'exercice de la souveraineté, son ressort de compétence, et le rôle des acteurs non étatiques. Face à l'impossibilité technologique et financière de garantir la sûreté des infrastructures civiles critiques, l'État doit, de concert avec des entreprises et des associations, parer aux vulnérabilités en exerçant sa puissance numérique par l'influence, l'espionnage et les cyberattaques qu'elle permet. Les capacités de ces trois secteurs reposent sur le capital technologique des entreprises. Ainsi, selon Nye (2006), la puissance

[13] Sanger, 2012.
[14] Sur tous ces points : Nye, 2006.

numérique d'un État est conditionnée par la taille des entreprises et l'ampleur du marché intérieur, des ressources financières dont disposent ces acteurs, et de leurs capacités technologiques :

- La taille importe encore car elle conditionne l'existence d'entreprises avec des capacités globales. Le facteur "taille du marché" est déterminant. Les industries culturelles requièrent un large marché intérieur pour bénéficier d'économies d'échelle avant de partir à la conquête du marché global grâce à des prix réduits. De même, les acteurs des télécommunications doivent atteindre une certaine taille sur le marché domestique afin de se positionner sur le marché global pour bénéficier de l'"effet-parc" qui conduit à un cyberespace unique. L'existence d'un marché intérieur significatif permet de construire des entreprises dont le savoir-faire est un appui dont ne peuvent se passer les forces armées. Les ressources humaines des entreprises et des forces armées constituent le capital de savoir-faire critique. Ce capital est partagé et enrichi mutuellement au travers d'échanges permanents. La hiérarchisation des puissances numériques peut se faire uniquement sur ce critère, mesurable à travers le nombre de cyberguerriers.
- La quête de la domination technologique : le premier conquérant à diffuser une rupture technologique domine le marché. En effet, il est celui qui définit les standards et les architectures. En termes de sécurité, il peut donc peut fixer le niveau de vulnérabilité acceptable. La première position sur le marché le conduit à terme à le dominer autant financièrement que techniquement. Ainsi, la variable technologique impose sa dynamique particulière : la rupture permanente, une forte incertitude sur les moyens de l'adversaire et l'ampleur de la menace. La sécurité doit être au centre de la recherche technologique autant que les perspectives de rentabilité. Les décisions sur les équipements et les infrastructures numériques doivent donc être partagées entre l'État, les militaires et les entreprises. Les logiciels "*on the shelves*" ne sont plus seulement source de réduction des coûts, mais de vulnérabilités.[15]
- Les ressources financières sont toujours des ressources stratégiques critiques. Par exemple, pour continuer de bénéficier de la domination informationnelle et de la surveillance du cyberespace, le gouvernement américain doit dépenser plus de 40 milliards de dollars par an pour la collecte, l'interception et l'analyse d'informations par sa communauté du renseignement.[16]

Ces leviers de la performance économique des entreprises sont aussi les déterminants de la puissance numérique de nature politique et ils doivent se traduire dans les forces armées afin qu'elles puissent efficacement contribuer à l'exercice de la souveraineté. Ainsi, les grands groupes nationaux privés du secteur des technologies de l'information et de la communication doivent établir des relations privilégiées avec les forces armées au travers tant de la circulation des ressources humaines que des possibilités d'accès et de surveillance des réseaux civils. Une part significative du budget public doit alimenter les capacités militaires d'intervention dans le cyberespace, surtout offensives, afin de contribuer à l'équilibre des forces en présence. Enfin, les développements technologiques affectant les cyberarmes doivent être l'objet d'une obsession de la part des

[15] Clarke, 2010.
[16] Russell, 2007.

militaires, afin de maintenir leurs capacités opérationnelles. Ces éléments s'accompagnent d'une doctrine d'emploi et des moyens de commandement afférents.

Le couplage État-entreprise : maillon critique de la sécurisation

La cybersécurité et son rôle constituent un enjeu et un défi stratégiques majeurs pour les forces armées. Plus précisément, peuvent-elles être utilisées en rétorsion contre une cyberattaque sur des infrastructures civiles? Dans l'affirmative, avec quelles cyberarmes et quelle doctrine offensive ? Ce défi est double : il doit répondre à l'anonymat des cyberattaques, et veiller à la proportionnalité de la réponse. Afin d'analyser la nouveauté du défi stratégique introduit par la révolution numérique, il peut être utile et précieux de rappeler une étude de cas révélatrice de l'importance de l'identification de l'origine du dysfonctionnement d'une infrastructure civile comme un réseau d'électrique.

Le mardi 10 novembre 2009, une coupure géante d'électricité plongeait 60 millions de personnes dans le noir pendant plusieurs heures en Amérique du Sud. Au départ, c'était la panne du barrage hydroélectrique d'Itaipu qui avait entraîné une coupure de courant dans 18 États brésiliens sur 26, et une partie du Paraguay. L'origine de la panne était incertaine. Mais la perception d'une cybermenace était réelle pour de nombreux acteurs. Ainsi, l'ancien conseiller à la cybersécurité du Président George W. Bush déclarait au même moment que "*les États-Unis* [n'étaient] *pas à l'abri d'attaques terroristes au vu des incidents qui ont eu lieu au Brésil, lorsque des* hackers *ont réussi à éteindre le courant*".[17] De même, cette menace est toujours présente à l'esprit des responsables français. Le directeur de l'ANSSI, Guillaume Poupard, déclarait au quotidien *Les Échos* en mai 2014 : "*Ma crainte, c'est la panne d'électricité qui plonge la France dans le noir*".

Cette panne a eu des conséquences importantes sur l'image du Brésil. En effet, ce pays est le plus vaste et le plus peuplé d'Amérique latine. De 1990 à 2011, il est passé de la 15e à la 6e place en termes de puissance économique mondiale. Naturellement, il est devenu un acteur de la scène internationale, notamment en accueillant la Coupe du Monde de Football en 2014. Il va organiser les Jeux Olympiques en 2016. À cette occasion, le Comité International Olympique (CIO) a demandé que la ville de Rio de Janeiro soit isolée du système d'alimentation électrique du pays afin d'éviter un nouveau *black-out* face à la faible cybersécurité du pays.[18]

Les conséquences peuvent être encore plus sérieuses au plan politique. Ainsi, au Paraguay, le pays le plus pauvre d'Amérique du sud, la coupure d'électricité géante de 2009 a initié des rumeurs de coup d'État. Le ministre paraguayen de la communication a dû démentir toute forme d'attaque qui aurait eu pour objectif de déstabiliser le pouvoir en place, très fragilisé.

---

[17] Clarke, 2010 : "*We can look forward to the kind of things happening here that happened to Brazil, where hackers successfully brought down the power*".

[18] *Cf.* www.olympic.org/Documents/Reports/FR/fr_report_1469.

Enfin, aux États-Unis, l'utilisation de cet événement pour alimenter le débat public sur les moyens de la cyberdéfense est liée à la conjonction fortuite de facteurs convergents. Trois jours avant cette panne, la chaîne d'information CBS avait diffusé un documentaire dans le cadre de l'émission "*60 minutes*" sur le thème de possibles cyberattaques contre le réseau électrique américain. Ce documentaire relatait deux pannes d'électricité intervenues au Brésil un peu plus tôt (en 2005 et 2007), et attribuées à des cyberattaques de *hackers*. La panne de janvier 2005 avait eu lieu à Rio et celle de septembre 2007 dans l'État d'Esperito Santo, où elle avait touché plus de 3 millions de personnes pendant 48 heures. Interviewé par les auteurs du documentaire de CBS, le Directeur du renseignement de l'époque, Mike McConnell, analysait le risque d'une cyberattaque similaire aux États-Unis. De plus, en 2009, les sites Web de la Maison Blanche, du Département d'État et du Pentagone étaient la cible de cyberattaques virulentes. La perception de cette menace était partagée à la fois par les dirigeants américains et l'opinion publique. Finalement, la même année, le Président Obama annonçait la création d'un *Cyber Command* rattaché à la National Security Agency et au Strategic Air Command, chargés de la cybersécurité, du cyber-espionnage et des attaques informatiques (comme l'opération *Olympic Games* contre le programme nucléaire iranien). Auparavant, dans son discours du 29 mai 2009, le président américain avait déclaré : "*Nous savons que des intrus ont infesté nos réseaux électriques, et dans d'autres pays des cyberattaques ont plongé des villes entières dans le noir*".[19] Les moyens alloués à la Défense au titre de la cybersécurité étaient en 2012 de 8 milliards de dollars, soit 60% du budget fédéral destiné au cyberespace.

Ainsi, une panne électrique très importante dans un pays peut avoir des conséquences politiques déterminantes en termes de légitimité de l'État. Le Brésil, dans un contexte d'émergence d'une grande puissance déjà confrontée à deux cyberattaques sur son réseau électrique, voit sa réputation atteinte au moment d'organiser les Jeux Olympiques. Le Paraguay, pays pauvre, est confronté à un risque de déstabilisation politique. Enfin, les États-Unis, confrontés aux rivalités entre grandes puissances numériques, entreprennent la mobilisation de ressources exceptionnelles avec la création du *Cyber Command*.

Pourtant, l'origine de cette panne, la plus importante jamais observée au Brésil, n'était qu'un court-circuit sur une ligne de transmission, source d'une perte de quelque 14 gigawatts de puissance et l'arrêt des 18 turbines de la plus grande centrale du pays, le barrage Itaipu, pour la première fois en 25 ans de fonctionnement. L'analyse *a posteriori* de ce cas révèle la difficulté à laquelle est confronté l'ensemble des parties prenantes. Selon les autorités brésiliennes, les mauvaises conditions météorologiques ont provoqué la détérioration de trois lignes de transmission qui reçoivent l'énergie de la centrale d'Itaipu, point de départ, au sein du réseau de distribution électrique, d'un "effet domino" qui s'est propagé à travers le Brésil et le Paraguay.

---

[19] Citation originale: "*We know that cyber intruders have probed our electrical grid, and that in other countries cyber attacks have plunged entire cities into darkness*" : http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure, consulté le 13 février 2015.

Lorsqu'une panne a une origine aléatoire, la responsabilité du gouvernement porte sur la rapidité de la remise en marche des infrastructures. Par exemple, l'ouragan Katrina de 2005 dans le sud des États-Unis, qui avait détruit une grande partie du réseau électrique et empêché les raffineries alimentées par les plates-formes du Golfe du Mexique de retrouver leur niveau de fonctionnement nominal pendant longtemps, a conduit le gouvernement à recourir à des moyens exceptionnels d'alimentation du réseau de distribution d'essence.[20] Il fut sévèrement critiqué sur la lenteur de sa réaction.

Au contraire, lorsque l'attaque provient d'un acteur anonyme, la responsabilité n'est plus seulement fonctionnelle. Elle nécessite une réponse politique. Le rôle des forces de sécurité est alors d'identifier l'origine politique ou non du dysfonctionnement des infrastructures numériques. Cette capacité de diagnostic nécessite d'articuler l'action de l'État et celles des entreprises dans une fonction, la maintenance, aujourd'hui régie par le principe économique du coût minimum et le principe juridique de la régulation minimale. La maintenance dépend presque entièrement de la "bonne volonté" des entreprises, c'est-à-dire des clients qui en assument le coût. La défaillance de cette capacité de diagnostic porte le risque d'être vulnérable ou de mobiliser inutilement des ressources en surestimant la menace cybernétique au détriment d'autres risques.

Enfin, les derniers développements de la cyberattaque sur Sony semblent illustrer la seconde tâche : la qualification de l'attaque afin de calibrer la réponse dans les trois registres de la puissance numérique : influence, espionnage et capacité offensive.

En décembre 2014, un groupe de *hackers* qui se fait appeler *Guardians of Peace* (GOP) revendique le piratage des données de *Sony Pictures Entertainment* (SPE). Leur objectif est d'obtenir la suspension de la sortie du film "*The Interview*" qui met en scène un complot fictif de la CIA en vue d'assassiner le leader nord-coréen Kim Jong-Un. Si Pyongyang dément toute implication, le FBI accuse le gouvernement nord-coréen d'être à l'origine de la cyberattaque. En juin, la Corée du Nord avait déjà mis SPE en garde : la stratégie mise en place a été élaborée afin de contraindre le studio à renoncer à la sortie du film.

Non content d'avoir paralysé le système informatique de SPE, le GOP annonçait peu après s'être emparé de 100 Téraoctets de données, désormais irrécupérables. Ces données confidentielles comprenaient des renseignements concernant les 47 000 employés de SPE, et des acteurs hollywoodiens. Certains courriels professionnels étaient potentiellement embarrassants pour la société. Des secrets de propriété financière et intellectuelle, comme le script du prochain *James Bond*, étaient ainsi fragilisés. Le GOP a ensuite diffusé en ligne cinq films de SPE non encore sortis.[21] C'est à la fois une perte de recettes futures et d'investissements déjà réalisés. Puis, le groupe a mis sur Internet, de manière séquencée à sept reprises consécutives, ces informations dérobées, qui ont fait la Une des journaux.

---

[20] Yergin, 2010.

[21] *La Dépêche*, 20 décembre 2014.

Enfin, il a menacé SPE d'une nouvelle parution d'informations encore plus embarrassantes pour l'entreprise. Dans ce contexte, SPE (récemment entrée en négociation avec son assureur sur sa police d'assurance contre les cybercrimes, dont la couverture ne dépasse pas 65 millions de dollars) se trouvait confrontée à une vulnérabilité majeure qui mettait en cause sa capacité à opérer sur le marché de la production de films. Le 16 décembre, le GOP s'attaque aux salles de cinéma qui avaient prévu de projeter le film. Il les menaça en publiant sur *Pastebin*[22] le message suivant : "*Les événements du 11 septembre peuvent toujours se reproduire*". Trois des plus importantes chaînes de cinéma des États-Unis ont paniqué et annulé la projection du film. Dès lors, SPE renonçait à sa sortie, prévue le 19 décembre. Le coût de cette annulation représente une perte d'un demi-milliard de dollars. Sony devait par la suite indiquer que de son point de vue le problème relevait de la sécurité nationale, et que le gouvernement américain devait agir.[23]

Dans un premier temps, la réaction du Président Obama fut vive – il dénonça cet acte de cyberguerre sur la liberté d'expression garantie par le 1er amendement de la Constitution : attaque flagrante contre la souveraineté des États-Unis – avant de la requalifier en termes d'acte de cybervandalisme.[24]

Cette requalification était nécessaire afin de répondre de façon proportionnée à l'attaque subie. Jusque-là, en effet, la doctrine américaine face à un acte de cyberguerre prônait le recours aux forces conventionnelles, ce qui aurait posé un sérieux problème dans l'équilibre des forces de la région. Car si la Corée du Nord est un petit pays, ce n'est pas le cas de son puissant protecteur chinois. Cette doctrine de représailles massives semblait aussi inadéquate aujourd'hui s'agissant de cyberattaques que l'était le recours aux armes atomiques pour défendre Quemoy et Matsu dans les années 1950.

De plus, le rôle de la Chine est une variable essentielle. Parmi les quatre réseaux de type Internet dont dispose la Corée du Nord, tout le routage passe par *China Netcom*, filiale du géant chinois des télécommunications *China Unicom*. La Chine constitue donc l'unique intermédiaire entre le réseau coréen et le reste du monde. Pour lancer cette attaque, la Corée du Nord a dû obtenir le feu vert de son seul allié.

En réponse, la diplomatie américaine envisagea de réinscrire la Corée du Nord sur la liste des États soutenant le terrorisme, dont elle avait été retirée en 2008.[25] De plus, quelques jours après le piratage de SPE, et alors que les États-Unis venaient de qualifier cet acte de cybervandalisme, la Corée du Nord a été victime d'une cyberattaque. Elle a connu neuf heures de perturbations de son accès à Internet, alors même que cet accès reste l'un des rares liens du pays avec le reste du monde.[26]

---

[22] Application web qui permet aux utilisateurs de mettre en ligne des morceaux de textes, habituellement des extraits de code source, pour un affichage public.

[23] *La Dépêche*, 2014, *art.cit.*

[24] *Ibid*.

[25] *Le Point*, 19 décembre 2014.

[26] AFP, 2014.

Conclusion

Cet article a traité de la définition du rôle des forces armées lorsque la légitimité de l'État est mise en cause par une cyberattaque d'origine incertaine sur une infrastructure civile. Les deux composantes de ce défi stratégique, l'anonymat des cyberattaques et la proportionnalité de la réponse, impliquent un acteur non étatique : l'entreprise, tout à la fois cible, acteur de l'identification, et moteur de la réponse. L'articulation de son action avec celle de l'État et des forces armées est donc au centre du défi stratégique. Un "complexe militaro-informationnel" est alors nécessaire pour répondre à une cyberattaque dans les trois registres d'application de la puissance numérique : stratégie d'influence, cyber-espionnage et cyber-offensive.

Or, la coopération du secteur privé est toujours une question ouverte, comme le montre la récente "mauvaise humeur" des entreprises à l'encontre de l'Administration Obama. Plusieurs PDG des industries du cyberespace, *Facebook*, *Yahoo*, *Google*, etc., ont boycotté le sommet sur la cybersécurité organisé en février 2015 par le Président Obama à la suite de la cyberattaque contre SPE, et dont l'objet était la collaboration des entreprises avec les autorités américaines. Ces entreprises sont dans un rapport de forces avec les agences fédérales de renseignement. Elles souhaitent garantir la confidentialité des données de leurs clients, au détriment de la nécessaire visibilité des communications pour la sécurité nationale. Le président a signé un décret qui encourage l'ensemble des entreprises concernées à partager, en matière de cyberattaques, "bonnes pratiques" et informations au bénéfice des organismes chargés de l'analyse de l'information, dont le gouvernement sera un partenaire très actif. Il a ajouté, sans être certain d'avoir été entendu d'elles, que le premier pays capable d'assurer la sécurisation du cyberespace aura un atout majeur dans la compétition mondiale.[27]

Bibliographie

AFP, "Corée du Nord: les connexions internet interrompues par une panne géante", 23 décembre 2014, à l'adresse : http://tempsreel.nouvelobs.com/monde/20141223.OBS8535/la-coree-du-nord-sans-internet-pendant-9h-que-s-est-il-passe.html, consultée le 23 février 2015.

ALDRICH, Richard J., "Beyond the Vigilant State : Globalisation and Intelligence", *Review of International Studies*, vol.35, n°4, 2009, pp.889-902.

BRANDSTETTER, Thomas, *Siemens : Stuxnet*, 2010 : http://www.infracritical.com/papers/siemens-stuxnet-malware.pdf, consulté le 13 février 2015.

BEMBARRON, Elsa, "*L'Internet des objets devient un big business*", *Le Figaro*, 4 juin 2015.

CLARKE, Richard A., *Cyberwar : The Next Threat to National Security and What to Do about It*, New York, Harper Collins Publishers, 2010.

DELESSE, Claude, *ECHELON et le renseignement électronique US*, Rennes, Éditions Ouest-France, 2012.

HERJAVEC, Robert, "State of Cyber Security : A Radical Evolution 30 years in the Making", 10 juin 2015 : *cf.* http://www.robertherjavec.com/state-of-cybersecurity-a-radical-evolution-30-years-in-the-making/.

[27] *Le Monde*, 16 février 2015.

KEOHANE, Robert & Joseph **NYE**, "Power and Interdependence in the Information Age", *Foreign Affairs*, septembre 1998.

LA DÉPÊCHE, "Cyberattaque contre Sony : Obama modère le ton mais va répondre", 20 décembre 2014.

LES ÉCHOS, "Guillaume Poupard : ma crainte c'est la panne d'électricité qui plonge la France dans le noir", 6 mai 2014 : http://www.lesechos.fr/entreprises-secteurs/tech-medias/interview/0203482164962-guillaume-poupard-ma-crainte-c-est-la-panne-d-electricite-qui-plonge-la-france-dans-le-noir-669079.php.

LE MONDE, "Cyber piratage : Obama appelle la Silicon Valley à l'aide", 16 février 2015.

LE POINT, "Sony : Pyongyang prêt à une confrontation avec les États-Unis", 19 décembre 2014.

NYE, Joseph, *Understanding International Conflicts*, 6th ed., New York, Longman, 2006.

RUSSELL, Richard L., *Sharpening Strategic Intelligence*, Cambridge, Cambridge University Press, 2007.

SANGER, David E., "Obama Order Sped Up Wave of Cyberattacks Against Iran", *New York Times*, 1er juin 2012.

VITKINE, Antoine, *La guerre invisible*, Arte, Doc en stock, 2012 : http://boutique.arte.tv/f6678-guerre_invisible.

WALTZ, Kenneth N., "Structural Realism after the Cold War", *International Security*, vol.25, n°1, Summer 2000, pp.5–41.

YERGIN, David, 2010, *The Quest for Energy Security*, New York, Penguin Press, 2010.