Bulletin de l'association de géographes français
Géographies

91-2 | 2014
Les États-Unis en 2014

Géopolitique du cyberespace : La cyberstratégie de l'administration Obama

Geopolitics of cyberspace: the Obama administration's cyberstrategy

Frédérick Douzet

Édition électronique
URL : http://journals.openedition.org/bagf/1837
DOI : 10.4000/bagf.1837
ISSN : 2275-5195

Éditeur
Association AGF

Édition imprimée
Date de publication : 15 juin 2014
Pagination : 138-149
ISSN : 0004-5322

Référence électronique
Frédérick Douzet, « Géopolitique du cyberespace : La cyberstratégie de l'administration Obama », *Bulletin de l'association de géographes français* [En ligne], 91-2 | 2014, mis en ligne le 22 janvier 2018, consulté le 19 avril 2019. URL : http://journals.openedition.org/bagf/1837 ; DOI : 10.4000/bagf.1837

Géopolitique du cyberespace : La cyberstratégie de l'administration Obama

(GEOPOLITICS OF CYBERSPACE :
THE OBAMA ADMINISTRATION'S CYBERSTRATEGY)

Frédérick DOUZET*

RÉSUMÉ – *Le développement exponentiel de l'Internet a engendré de belles crispations territoriales, avec une prolifération des conflits entre une multitude d'acteurs – au premier rang desquels les États-Unis –, à propos de son contrôle et de sa régulation, son utilisation dans les conflits géopolitiques (guerre économique, combats militaires, renseignement, politique d'influence diplomatique et culturelle) et du respect des libertés individuelles. Cet article montre comment l'analyse géopolitique permet d'analyser les enjeux et les stratégies développées par les Etats pour renforcer leur contrôle et leur puissance dans le cyberespace. Il examine l'escalade des discours et des moyens qui caractérisent l'approche de l'administration Obama, dont la cyberstratégie sera l'un des héritages les plus marquants en matière de politique extérieure.*

Mots-clés : *Cyberstratégie – Cyberespace – Géopolitique – États-Unis – Obama*

ABSTRACT – *The exponential growth of the Internet has generated a proliferation of conflicts between multiple stakeholders —most notably the United States— about its control and regulations, its use in geopolitical conflicts (military and economic warfare, intelligence and soft power), and the respect of civil liberties. This paper shows how the geopolitical approach can help analyze the issues raised and strategies developed by States to reinforce their control and power in cyberspace. The Obama administration's approach to cyberstrategy has been characterized by an escalation of means and discourses. It should constitute a significant legacy of President Obama in foreign affairs.*

Keywords: *Cyberstrategy – Cyberspace – Géopolitics – United States – Obama*

* Professeur à l'Institut français de Géopolitique (IFG), Paris 8 – Titulaire de la Chaire Castex de Cyberstratégie (Cercle des Partenaires de l'IHEDN, avec le soutien de la Fondation Airbus Group) – Courriel : fdouzet@gmail.com

Tout à l'euphorie des débuts publics de l'Internet, d'enthousiastes prophètes annonçaient, au milieu des années 1990, « la fin de la géographie » [Virilio 1997]. L'expansion des réseaux de communication a de tout temps suscité l'utopie d'un monde meilleur, portant la promesse d'une démocratisation et d'une pacification du monde par la diffusion des idées et des valeurs démocratiques [Musso 2003, Mattelart 2009], voire l'avènement d'un « village global » [McLuhan 1964]. L'Internet conduirait à une accélération du temps mondial « *dont l'instantanéité efface définitivement la réalité des distances, de ces intervalles géographiques qui organisaient, hier encore, la politique des nations et leurs coalitions* » [Virilio 1997].

Les révélations d'Edward Snowden sur les programmes de surveillance massive de la National Security Agency des États-Unis ont démontré, si d'aucuns en doutaient, à quel point la géographie garde toute sa pertinence pour comprendre les conflits du monde moderne. L'escalade des tensions entre les États-Unis et la Chine à propos des cyberattaques est même qualifiée par le *New York Times* de « cyberguerre froide » [Sanger 2013] et si l'analogie est critiquable, elle est révélatrice des représentations dominantes dans le débat stratégique. David Rothkopf, dans *Foreign Policy*, lui préfère le terme de « guerre cool », pas tout à fait aussi froide que la guerre froide mais « fraîche » et « branchée » (technologique). Il avance ainsi que si la technologie de la guerre froide rendait la guerre impensable, celle de la « guerre cool » la rend « irrésistible » [Rothkopf 2013].

Le développement exponentiel de l'Internet a révolutionné nos modes de vie, démultiplié nos moyens de communication et ouvert bien des horizons. Il a aussi engendré de belles crispations territoriales, avec une prolifération des conflits entre une multitude d'acteurs à propos de son contrôle et sa régulation. Les tensions se cristallisent autour de l'émergence de nouvelles menaces liées à la cybercriminalité ou l'utilisation des réseaux et de cybercapacités dans le cadre de conflits politiques, de combats militaires, de guerre économique, de renseignement ou de politique d'influence diplomatique et culturelle. A l'heure du big data et de l'open data (mise à disposition des données publiques), les débats se multiplient autour des enjeux de respect de la vie privée, la protection de la liberté d'expression et autres libertés individuelles.

Cet article a pour objectif d'expliciter les ressorts et les enjeux de la cyberstratégie des États-Unis, notamment dans sa dynamique de rivalité avec la Chine. Il montrera dans un premier temps en quoi l'analyse géopolitique permet de comprendre les conflits liés au cyberespace, puis analysera les menaces qui conduisent les Etats à développer des stratégies pour renforcer leur contrôle et leur puissance dans le cyberespace. Il abordera enfin l'escalade des discours et des moyens qui caractérisent la stratégie de l'administration Obama, dont la cyberstratégie sera l'un des héritages les plus marquants en matière de politique extérieure.

1. La démarche géopolitique appliquée au cyberespace

La géopolitique est l'étude des rivalités de pouvoir sur des territoires, à différents niveaux d'analyse, impliquant de multiples acteurs, aussi bien au niveau local qu'international. Le territoire est au cœur même de l'analyse puisque la géopolitique rend compte de la dynamique complexe des conflits sur un territoire, des représentations contradictoires des acteurs et de leurs stratégies pour son contrôle, son appropriation et la défense de leurs intérêts au sein de ce territoire. La notion de territoire ne va pas de soi. Le cyberespace est-il une nouvelle forme de territoire ? Et si oui, quelle en serait la matérialité ? Quelles en seraient les frontières ? Quelles seraient les limites de sa souveraineté ?

1.1. Comprendre le cyberespace

Le cyberespace est une réalité difficile à appréhender en raison de son caractère intangible et fortement technique, et d'un grand flou sémantique dans la littérature. Il n'existe en effet pas de définition objective et consensuelle du cyberespace ; on trouve au contraire de multiples définitions en fonction des disciplines, des acteurs et des pays. On peut avancer toutefois que le cyberespace est à la fois l'Internet et l'espace qu'il génère : un espace intangible dans lequel s'opèrent des échanges déterritorialisés entre des citoyens de toutes nations, à une vitesse instantanée qui abolit toute notion de distance.

On trouve parfois une représentation en plusieurs couches [Kempf 2012], qui permet de restituer l'enchevêtrement des différentes dimensions du cyberespace mais aussi des enjeux qui y sont liés.

La première couche est physique et constitue la base de l'Internet, un réseau mondial constitué de réseaux interconnectés dont le cyberespace est le produit. Elle est composée de câbles, de nœuds, de serveurs et d'ordinateurs qui sont des biens matériels, localisés et soumis à des contraintes de géographie physique et politique. Elle a été conçue dans un esprit d'ouverture et de circulation maximale de l'information, sans aucune sécurité intégrée, ce qui explique la très grande facilité avec laquelle il est possible d'aspirer les données qui circulent en clair (sans chiffrement) via les câbles et les routeurs.

La deuxième couche est logique et applicative. Elle comprend les services (applications, logiciels, interfaces, programmes) qui permettent d'assurer la transmission des données entre deux points du réseau, de faire voyager les informations, en petits paquets séparés, de leur expéditeur à leur destinataire. Là encore certains aspects peuvent être géolocalisables (logiciels utilisés, entreprise fournisseur, chemins empruntés, stockage des données, etc…). L'architecture logique repose toutefois sur une base commune, une harmonisation essentielle qui permet à tous les ordinateurs du monde de se

comprendre entre eux, le protocole Internet (TCP/IP).

La troisième couche est cognitive et sémantique, c'est le monde des utilisateurs de la couche logique, le monde de l'information, des réseaux sociaux, des discussions et des échanges en temps réel dans le monde. C'est la couche la plus intangible, la plus difficile à géolocaliser et pourtant pas nécessairement la moins pertinente lorsque l'on arrive à déterminer en quelle langue est la majorité des contenus auxquels accèdent telle ou telle partie de la planète, qui sont les pays les plus « amis » sur Facebook, d'où partent les campagnes de désinformation ou les cabales contre un mouvement, un Etat ou une institution…

Le cyberespace, c'est donc à la fois une réalité matérielle localisable et un espace d'échange intangible complexe à appréhender. Il peut désigner un ensemble de réseaux d'ordinateurs (et tablettes, smartphones, etc..), de réseaux humains, de flux de données et d'information, tout ce qui circule par les réseaux informatiques interconnectés entre eux et qui utilisent un langage commun. Avec le développement de l'Internet des objets, de plus en plus d'appareils de tout type se connectent aux réseaux et la masse des données disponibles est en constante expansion. Selon qui l'utilise et pourquoi, le terme cyberespace peut renvoyer à une réalité ou à un imaginaire totalement différents dans un certain flou conceptuel.

La démarche géopolitique apporte dès lors un outil indispensable à l'appréhension du cyberespace, celui des représentations. Une représentation est « une construction, un ensemble d'idées plus ou moins logiques et cohérentes » qui a une fonction dans les conflits géopolitiques. Elle « décrit, exprime une partie de la réalité, de façon floue ou précise, déformée ou exacte ». Elle se nourrit donc de faits objectifs tout en gardant un caractère profondément subjectif. Les représentations ne sont donc pas neutres, elles façonnent comme elles peuvent servir la stratégie des acteurs, afin de convaincre, inquiéter, enthousiasmer ou mobiliser des acteurs (citoyens, soldats, électeurs…).

1.2. La représentation d'un territoire

Le cyberespace n'est pas un territoire au sens géographique du terme, à savoir « une étendue sur laquelle vit un groupe humain qu'il considère comme sa propriété collective » [Lacoste 2003], ou pour les Etats « une portion de l'espace terrestre délimitée par ses frontières et sur laquelle s'exercent son autorité et sa juridiction » [Lacoste 2003]. Ce n'est pas vraiment un espace géographique non plus. On retrouve pourtant toute une terminologie empruntée au territoire géographique, particulièrement la mer et l'espace. On « navigue », on « surfe », on utilise des « routes », des « passerelles », des « canaux » dans le cyberespace. Parce que si le cyberespace n'est pas un territoire, il est perçu et utilisé par différents acteurs comme la représentation d'un territoire, et pour

des raisons diamétralement opposées.

Le concept de cyberespace est d'abord apparu sous la plume d'un romancier de science-fiction, William Gibson, qui décrit dès 1984 dans *Neuromancer* un espace tri-dimensionnel d'une « infinie complexité », généré électroniquement, dans lequel ses personnages entrent en se connectant par ordinateur. Il offre ainsi une représentation mentale des données et de l'information stockée au cœur des systèmes informatiques de toute l'humanité que s'approprieront des générations d'internautes.

Cette représentation imprègne les discours et l'imaginaire des pionniers du Net. En 1990, alors que l'Internet n'est encore qu'un club de quelques millions d'utilisateurs, l'Electronic Frontier Foundation (EFF) voit le jour. Référence directe au front pionnier qui, selon la thèse de l'historien Frederick Jackson Turner, a formé la démocratie américaine, l'association se bat pour la défense des libertés dans le monde digital. Ses missions reflètent l'esprit dans lequel a été créé le réseau, dans l'ambiance de la contre-culture des années 1960 et 1970 sur les campus californiens, un esprit d'ouverture, de liberté des échanges et de l'expression, d'autogestion qui touche au cœur même de l'architecture de l'Internet. Le réseau est pensé pour échapper au contrôle, décentralisé, pour que l'information puisse toujours contourner le blocage. John Perry Barlow, membre fondateur de l'EFF, publie même en 1996 une « déclaration d'indépendance du cyberespace » dans laquelle il affirme que les lois et la souveraineté des gouvernements ne s'y appliquent pas. Critiqué à l'époque pour son incroyable optimisme, il aurait concédé depuis « on devient tous plus vieux et plus sage ». Nombre d'hacktivistes prennent cependant toujours cette déclaration au pied de la lettre et combattent activement l'ingérence des gouvernements dans la régulation du cyberespace.

À partir du milieu des années 2000, le terme cyberespace réapparaît paradoxalement dans les discours des gouvernements, comme la représentation d'un territoire porteur de menaces, un territoire à contrôler, à surveiller, à conquérir, un territoire sur lequel il faut remettre des frontières et réaffirmer sa souveraineté. Les attaques de 2007 contre l'Estonie qui ont paralysé les serveurs des administrations publiques, banques et autres services de l'Estonie ont suscité une véritable prise de conscience des vulnérabilités que pouvait entraîner la dépendance aux réseaux informatiques pour les Etats. Les attaques contre la Géorgie, l'année suivante, ont montré comment les cyberattaques pouvaient venir en appui des forces militaires dans le cadre d'un conflit armé, confirmant l'entrée dans le domaine politique et stratégique d'une préoccupation restée jusque-là essentiellement entre les mains d'experts et de techniciens.

Le cyberespace est ainsi devenu une question géopolitique ; il est à la fois un enjeu de rivalités de pouvoirs, un théâtre d'affrontement et une arme redoutable dans les conflits géopolitiques.

2. Les Etats contre-attaquent

Les Etats ne sont pas les seuls acteurs des conflits du cyberespace, bien au contraire. À l'exception de quelques-uns, notamment les États-Unis, la Chine ou la Russie, ils ont tardé à développer une cyberstratégie adaptée à l'évolution de la technologie et ses enjeux. Les entrepreneurs, les start-ups, les criminels, les hackers ont su se saisir bien plus vite et plus efficacement de ces nouveaux outils, pour le meilleur et pour le pire.

Avec désormais plus de 2,5 milliards d'Internautes, l'émergence des géants du web, et la multiplication des attaques de plus en plus sophistiquées, les Etats ont été conduits à réévaluer les menaces qui pèsent sur leurs pouvoirs régaliens. Nombre d'entre eux ont fait de la cyberdéfense et de la cybersécurité une priorité stratégique, à commencer par les États-Unis, et reviennent en force dans le cyberespace.

2.1. Risques et opportunités du cyberespace

La croissance exponentielle des réseaux est source de risques comme d'opportunités pour les Etats, et affecte tous les domaines de leurs pouvoirs régaliens. Premièrement, la capacité à assurer la sécurité de la nation et la défense du territoire est perturbée par la difficulté à stopper les cyberattaques. Les gouvernements redoutent notamment le sabotage de leurs infrastructures vitales, avec des conséquences non maîtrisées qui pourraient mettre en danger les populations civiles. Dans le cadre stratégique et opérationnel, la maîtrise de l'information est cruciale. Les cyber-attaques peuvent permettre de perturber les communications, manipuler l'information, obtenir un avantage tactique et plus généralement, affecter les capacités opérationnelles de l'ennemi. Les paradigmes classiques de la stratégie militaire sont mal adaptés en raison des difficultés d'attribution des attaques, de l'impossibilité de tester les armes en condition réelle, des incertitudes sur leur efficacité, ou encore du faible coût et de la forte accessibilité de la technologie qui renforce le pouvoir des petits Etats et des acteurs non étatiques face aux grandes puissances, et donc le potentiel de guerre asymétrique. Les pays les plus dépendants des réseaux sont aussi les plus vulnérables aux attaques. Mais ce sont aussi les plus à même de renforcer la protection et la résilience de leurs réseaux, de développer des capacités offensives et de saisir les nouvelles opportunités offertes par les réseaux pour accroître leur efficacité et leur puissance.

Le maintien de la sécurité intérieure et de l'ordre public se heurte à la criminalité, organisée au non, qui opère via les réseaux. Le défi de l'attribution des attaques (qui est derrière et pourquoi) est alors renforcé par la volatilité de la preuve et la possibilité d'opérer à distance, ce qui rend d'autant plus complexe le processus d'investigation, d'appréhension et de mise en examen du suspect. La cybercriminalité traverse aisément les frontières, via les réseaux,

ce qui n'est pas le cas de forces de l'ordre. Lorsque le criminel, la victime et/ou les systèmes utilisés sont situés dans des pays différents, cela requiert des procédures de coopération internationales au niveau des forces de police et de justice qui sont parfois trop lentes pour être efficaces. Alors que la représentation de la menace augmente, les Etats sont tentés d'utiliser les nouveaux moyens pour accroître la surveillance des activités dans le cyberespace, ce qui peut soulever des inquiétudes en termes de protection des libertés civiles. Pour les régimes autoritaires, la surveillance et le contrôle des contenus des réseaux sont un impératif pour la protection de leur régime politique, la menace étant susceptible de venir de l'intérieur.

2.2. Des enjeux de souveraineté

L'exercice de la souveraineté par les Etats est devenu plus complexe car les limites de juridictions et de souveraineté sont plus floues et entremêlées dans le cyberespace. Il est parfois difficile pour un État de faire respecter ses lois et régulations sur son territoire et par ses citoyens pour des actions qui se déroulent via les réseaux, notamment lorsque le service utilisé est fourni par une compagnie étrangère et les données concernées hébergées dans un autre pays. Par exemple, lorsqu'un utilisateur français poste sous pseudonyme un commentaire antisémite sur un réseau social appartenant à une entreprise américaine, il est plus difficile à la justice française d'obtenir la suppression du commentaire et les coordonnées de l'auteur de l'infraction. Les fameux GAFA (Google, Amazon, Facebook, Apple) ont acquis une telle puissance économique qu'ils ne se soumettent pas si facilement à la législation d'un Etat qui réclame des informations sur un utilisateur ou la suppression de contenus. Les juridictions s'enchevêtrent parfois de façon conflictuelle et ce qui constitue une juridiction est avant tout le produit de rivalités de pouvoir et de rapports de force plutôt que d'une définition juridique consensuelle.

Enfin, la souveraineté économique et financière des Etats est mise au défi par l'accélération considérable par les réseaux des flux financiers qui facilitent l'évasion fiscale, la propagation des crises financières internationales et l'émergence de monnaies virtuelles (bitcoin). L'espionnage industriel et économique, le vol de propriété intellectuelle et de secrets industriels connaissent des proportions sans précédent, au point que les intérêts du secteur privé rejoignent ceux de l'Etat. Il en va de la puissance économique et financière des nations, d'où les tensions internationales croissantes liées aux cyberattaques contre les entreprises.

Nombre de ces menaces ne sont pas nouvelles mais se propagent dans le cyberespace de manière plus diffuse, rapide, puissante et à une échelle inédite. La NSA aspire des masses invraisemblables de données, Bradley Manning ou Edward Snowden ont téléchargé des quantités de fichiers impressionnantes… tout se passe plus vite, plus fort et avec une ampleur plus importante. Et les

spécificités du cyberespace ajoutent leur couche de complexité à ces menaces (difficulté d'identifier leur auteur et leur provenance, difficulté à les anticiper, les prévenir et les stopper, complexité de la riposte…).

Les Etats ont donc tout intérêt à se doter d'une cyberstratégie. Par le cyberespace, ils sont exposés à de nouveaux risques et de nouvelles vulnérabilités mais ils peuvent aussi améliorer leur renseignement, gagner de nouvelles capacités militaires, et accroître leur puissance économique ainsi que leur influence diplomatique et culturelle. Sous l'administration Obama, les États-Unis sont clairement passés à l'offensive et, dans ce domaine comme dans d'autres, s'affirment comme une superpuissance.

3. La cyberstratégie de l'administration Obama

La cyberstratégie des États-Unis s'inscrit dans une logique de rivalité avec la Chine, qui collecte agressivement des données aussi bien militaires et politiques, que technologiques, industrielles et économiques, dans une logique de maîtrise de l'information et de positionnement comme puissance incontournable du cyberespace. Au cours de l'année 2013, l'approche de l'administration Obama a été caractérisée par une escalade des moyens mis en œuvre et des discours, qui se comprennent dans un contexte de rivalités géopolitiques très fortes, à la fois à l'échelle internationale et nationale [Douzet 2013].

3.1. Une escalade des moyens

En l'espace de quelques années, les États-Unis ont considérablement renforcé et réorganisé leurs moyens pour assurer leur cyberdéfense : nomination d'un *Cyber Czar* chargé de la coordination de la cybersécurité auprès de l'administration Obama fin 2009 ; lancement opérationnel de l'US Cybercommand (US Cybercom) en 2010, qui inclut toutes les composantes militaires sous la responsabilité du directeur de la NSA ; publication de la cyberstratégie de la Maison Blanche en 2011, où le cyberespace apparaît comme un nouveau domaine militaire. Et le cyber est désormais intégré dans toute la chaîne stratégique, y compris opérationnelle.

En 2013, malgré un contexte de sévères restrictions avec le *budget sequester*, le budget de la cyberdéfense a augmenté de 800 millions de dollars, alors que celui de l'ensemble du Pentagone diminuait de 3,9 milliards de dollars. Les effectifs du US Cybercom devraient être multipliés par cinq dans les prochaines années, passant de 900 à 4 900 employés. Outre ses missions de protection des infrastructures du département de la défense et des infrastructures vitales, le US Cybercom sera amené à devenir une unité de combat à l'âge Internet, en charge d'aider les forces opérationnelles à planifier et exécuter les attaques.

Les révélations d'Edward Snowden ont mis au jour l'ampleur des programmes développés par la National Security Agency, basés sur l'exploitation des métadonnées et – potentiellement – données des entreprises américaines (contraintes par la loi de coopérer), l'aspiration des données qui circulent en clair dans les réseaux des opérateurs américains, la coopération avec de multiples gouvernements, l'interception des communications, des techniques sophistiquées de décryptage… une véritable pieuvre dont on ne finit plus de découvrir les tentacules.

En 2012, le New York Times révélait les détails du programme *Olympic Games* et le développement expérimental du virus *Stuxnet* par les services américains, en collaboration avec les Israéliens, une arme offensive de troisième voie, entre la diplomatie coercitive et l'agression armée, visant à ralentir le programme nucléaire iranien. D'autres informations ont filtré dans la presse sur l'achat massif par le gouvernement de failles *zero day* et de vulnérabilités sur tous types de supports (systèmes, logiciels, etc…), un marché gris prospère qui interroge sur la valorisation de l'approche offensive.

3.2. Inflation des discours

Côté discours, la représentation de la menace auparavant mise en avant par quelques stratèges envahit désormais toutes les strates de la réflexion stratégique jusqu'au sommet de la hiérarchie militaire, sans pour autant faire consensus. Elle émane aussi du complexe militaro-industriel, d'experts et de responsables politiques, le tout relayé voire dramatisé par les médias. Les cyberattaques chinoises menées contre les grands journaux américains (New York Times, Washington Post, Wall Street Journal) ont amplifié encore la diffusion de la menace.

Les analogies avec le nucléaire alimentent les discours catastrophistes. En janvier 2013, John Kerry déclarait que les « cyberhackers étrangers étaient considérés comme les armes nucléaires du 21ème siècle », alors que Leon Panetta, à l'époque directeur de la CIA, en juin 2012 évoquait un risque de « Pearl Harbor numérique » qui pourrait « paralyser le pays ». À ces menaces répondent des discours musclés de la Maison Blanche, dont la cyberstratégie de 2011 stipule que des cyberattaques massives pourraient être considérées comme un acte de guerre, avec une possibilité de réponse par tous les moyens nécessaires. Et en février 2013, un rapport juridique secret sortait dans la presse, faisant état des pouvoir très étendus du président en matière de riposte aux cyberattaques et même de frappes « préemptives », un concept que l'on pensait disparu avec la fin de l'administration Bush.

Dans ces représentations de la menace, la Chine occupe une place de choix, avec une avalanche de révélations dans les médias sur les cyberattaques chinoises. Très médiatisé, le rapport Mandiant est sorti juste avant la plus grande conférence sur la sécurité informatique aux États-Unis (RSA

Conférence). À l'automne 2012, les représentants des équipementiers Huawei et ZTE avaient été sommés de s'expliquer devant le Sénat sur les risques d'espionnage que comporte leur matériel. Au mois d'avril 2013, le vote d'une résolution budgétaire (*continuing resolution)* interdit à la NSA, au Secrétariat au Commerce, au Département de la Justice et à la National Science Foundation d'utiliser du matériel informatique produit par des entreprises chinoises.

À la veille du sommet avec le Président Xi Jinping, début juin 2013, le Président Obama a explicitement accusé l'armée chinoise de mener des cyberattaques contre les systèmes informatiques du gouvernement américain et des industriels de la défense dans le but de cartographier « les capacités militaires qui pourraient être exploitées en temps de crise ». Les révélations de Snowden en plein sommet n'ont guère modifié le discours des États-Unis, mais ont clairement altéré leur crédibilité dans le rapport de force qui les oppose à la Chine.

3.3. Des rivalités de pouvoir géopolitique

Les ressorts de cette escalade se comprennent dans leur contexte géopolitique. Certes, les cyberattaques sont de plus en plus nombreuses et de plus en plus sophistiquées, c'est une réalité indéniable qui ne fera probablement que s'aggraver dans les années à venir. La logique d'escalade répond aussi et surtout à la rivalité avec la Chine, dans une logique de compétition économique mais aussi de montée en puissance de la représentation de la menace chinoise dans le débat stratégique américain. Si les réponses à apporter varient en fonction des écoles de pensées en relations internationales, le constat est partagé sur les ambitions régionales et internationales de la Chine. Outre la modernisation de l'armée, elle a poussé son avantage en mer de Chine et déploie parallèlement ses forces dans le cyberespace. Outre les attaques de basse intensité contre de multiples pays, elle a effectué quelques démonstrations de force, comme le détournement de 15% du trafic des réseaux militaires et civils américains en 2010.

La Chine impressionne par sa capacité à intégrer la dimension cyber dans tous les domaines stratégiques de sa montée en puissance (Douzet, 2013). Nul doute que l'impératif de survie du régime a stimulé très tôt la réflexion stratégique sur l'information à l'âge de l'Internet (Douzet, 2007). Et le régime s'est montré particulièrement créatif, avec le développement d'une stratégie globale qui s'appuie sur l'art ancestral de la guerre, et la volonté d'acquérir une supériorité informationnelle aussi bien offensive que défensive.

Le cyber peut apparaître aussi comme une troisième voie pour les États-Unis, dans l'impossibilité d'affronter directement la Chine, en raison de l'interdépendance économique très forte entre les deux pays et de l'attrait que constituent les marchés chinois. Ces rivalités de pouvoir s'expriment dans le

cyberespace où les pays se testent et marquent leur territoire. Et la Chine a bien l'intention de démontrer qu'elle a toute sa place dans le cyberespace.

Plus la menace est forte, enfin, plus elle justifie les moyens employés. Or beaucoup s'accordent à dire que le virus Stuxnet pourrait être considéré comme le premier cas de « cyberguerre », ou en tout cas d'utilisation de cyberarmes offensives. L'usage « off limits » des drones est justifié par l'administration par la menace terroriste ; l'usage des cyberarmes par la cybermenace, une menace diffuse qui selon le directeur du renseignement Jim Clapper surpasse le terrorisme comme la menace la plus importante à laquelle font face les États-Unis.

L'inflation de la menace répond aussi à des enjeux internes, dans un contexte de polarisation politique et de rivalités de pouvoir très fortes entre l'administration et le Congrès. L'ampleur de la menace aide à justifier les budgets fédéraux dans des négociations plus que tendues qui ont fini par conduire au *government shutdown* en octobre 2013. La situation est tout aussi conflictuelle au sein même du Congrès, les tentatives de législation sur la cybersécurité (CISPA, SOPA…) ayant pour l'instant échoué. Le Président Obama a fini par faire passer en force un décret présidentiel sur la protection des infrastructures vitales, alors que les journaux sonnaient l'alarme sur les cyberattaques.

Enfin, il ne faut pas perdre de vue que le marché de la cybersécurité est florissant et se développe avec l'accroissement des menaces. Dans son discours d'adieu à la nation, en 1961, le Président Eisenhower mettait en garde contre les dangers du complexe militaro-industriel, les liens étroits entre le Pentagone, les entreprises du secteur de la défense et les élus pouvant conduire à une prolifération inutile des forces armées et des dépenses militaires, et une remise en cause des contre-pouvoirs au sein du processus d'élaboration des politiques.

Conclusion

Le cas des États-Unis montre les enjeux des cybermenaces et la volonté de Washington de réaffirmer sa puissance politique, militaire et économique dans le cyberespace. Le premier point à retenir est que les cyberconflits n'existent pas en dehors des rivalités de pouvoir classiques, ils en sont l'expression. Inversement, les opérations cyber feront partie de la plupart des conflits modernes, parce que l'information est de plus en plus au cœur des opérations militaires mais aussi de la société, et les campagnes d'influence menées sur les réseaux sociaux peuvent affecter le déroulement d'une guerre.

La logique d'escalade que semble emprunter l'administration Obama ne fait pas l'unanimité dans les milieux stratégiques et certains, comme Martin Libicki, mettent en garde contre les déclarations musclées qui induisent une demande d'action de la part du public, même lorsque ce n'est pas la meilleure chose à faire, et engagent la crédibilité des États-Unis dans une logique de

dissuasion. Or, bien des questions restent complexes à régler en raison de la difficulté d'attribution (qui est derrière une attaque et pourquoi), d'imputation (comment le prouver), de riposte (comment mesurer sa réponse lorsqu'il y a des incertitudes sur les effets collatéraux des attaques).

Les États-Unis ont affirmé l'applicabilité du droit international au cyberespace. Mais la question de ce qu'est un acte de guerre dans le cyberespace ne fait pas l'objet d'un consensus et encore moins d'une définition dans le droit international. Quelle est la ligne rouge ? Où commence et où s'arrête la guerre dans le cyberespace ? Comment penser la sécurité collective dans le cyberespace ?

Le débat est ouvert et se pose avec une acuité particulière à la France et l'Europe, suite à l'affaire Snowden. Un débat éminemment géopolitique…

Références bibliographiques

- CATTARUZZA, A. & DOUZET, F. (2013) – « Le cyberespace au cœur de tensions géopolitiques internationales », *DSI,* Hors Série n°32.
- DESFORGES, A. (2013) – « Les frontières du cyberspace », in F. Douzet & B. Giblin (dir.), *Des frontières indépassables ?*, Paris, Armand Colin, pp. 101-112.
- DOUZET, F. (2013) – « Chine, États-Unis : la course aux cyberarmes a commencé », *Sécurité globale*, n° 23, pp. 43-52.
- DOUZET, F. (2013) – « Chine : cyberstratégie, l'art de la guerre revisité »*, Diploweb,* 12 septembre (http://www.diploweb.com/Chine-cyberstrategie-l-art-de-la.html)
- DOUZET, F. (2007) – « Les frontières chinoises de l'Internet », *Hérodote,* n°125, pp. 127-142.
- KEMPF, O. (2012) – *Introduction à la cyberestratégie*, Paris, Economica, 176 p.
- LACOSTE, Y. (dir.) (1993) – *Dictionnaire de géopolitique*, Paris, Flammarion, 1679 p.
- LACOSTE, Y. (2003), *De la géopolitique aux paysages, dictionnaire de la géographie*, Paris, Armand Colin, 413 p.
- MATTELART, A. (2009) – *Histoire de l'utopie planétaire. De la cité prophétique à la société globale*, Paris, La Découverte, 430 p.
- McLUHAN, M. (1964) –*Understanding Media. The Extensions of a Man*, New York, McGraw-Hill, 318 p.
- MUSSO, P. (2003) –*Critique des réseaux*, Paris, PUF, 374 p.
- ROTHKOPF, D. (2013) – « The Cool War », *Foreign Policy*, 20 février.
- SANGER, D. (2013) – « In Cyberspace, New Cold War », *New York Times,* 24 février.
- VIRILIO, P. (1997) – « Un monde surexposé », *Le Monde diplomatique,* août.