UNIVERSITÉ DU QUÉBEC À MONTRÉAL

LA MILITARISATION AMÉRICAINE DU CYBERESPACE : UNE RÉPLIQUE À L'ÉMERGENCE D'UNE MENACE CHINOISE

MÉMOIRE

PRÉSENTÉ

COMME EXIGENCE PARTIELLE

DE LA MAÎTRISE EN SCIENCE POLITIQUE

PAR

NICOLAS PELLERIN-ROY

NOVEMBRE 2016

REMERCIEMENTS

Par la finalisation de ce travail, c'est une véritable étape de ma vie qui se termine. Elle se serait par contre terminée beaucoup plus tôt si ce n'eut été de la confiance que l'on m'a accordée et de l'appui de plusieurs personnes de mon entourage.

Je tiens d'abord à remercier mon codirecteur de maîtrise, Charles-Philippe David, d'avoir cru à mon projet, à mon potentiel et à mes capacités. Par ses bons mots, ses encouragements et ses pistes de réflexion, il a su m'éclairer plus d'une fois. Merci à Élisabeth Vallet, ma codirectrice, pour avoir su réaliser l'exploit de m'aider à structurer ma pensée et mes écrits, pour son écoute exemplaire, sa compréhension et sa grande volonté à vouloir rendre publiques les connaissances et les expertises de ses protégé-e-s. M. David m'a invité à participer aux travaux et à la vie quotidienne de la Chaire Raoul-Dandurand et ce fut pour moi un privilège et un honneur, mais aussi un inestimable lieu de rencontres, où chercheurs et membres du personnel auront toujours su ponctuer mes journées de rires et de discussions plus enrichissantes les unes que les autres. Sans vous, la rédaction de ce mémoire aurait sans doute été beaucoup plus ardue.

Mes derniers mots seront pour deux personnes sans qui rien de tout cela n'aurait été possible et qui auront toujours ma gratitude. D'une part ma conjointe, Nancy, pour avoir su d'abord supporter les aléas de la dynamique des études supérieures pendant 3 ans. Elle m'a longuement et rigoureusement fait confiance, écouté, supporté, encouragé, remis à ma place. Rien de cela n'aurait été possible sans elle. D'autre part, mon fils Théodore, par ses sourires et ses accomplissements qui m'ont quotidiennement rendu si fier, a su éclairer mes journées et me permettre de tout relativiser quand je pouvais croire que tout allait mal. Son arrivée pendant ma maîtrise ne fut pas un obstacle, mais davantage une bénédiction. Merci à vous deux d'être dans ma vie.

TABLE DES MATIÈRES

LISTE DES TABLEAUX ix
LISTE DES ABRÉVIATIONS, SIGLES ET ACRONYMES ix
RÉSUMÉ xiii
INTRODUCTION 1
CHAPITRE I
CADRE THÉORIQUE 17
1.1 Le marché des idées concernant la grande stratégie américaine et sa définition 19
1.1.1 La sécurité coopérative 24
1.1.2 La stratégie de primauté 27
1.2 La grande stratégie de la présidence Obama 32
1.2.1 Un risque de surextension hérité de la *doctrine Bush* 34
1.2.2 Un pas en arrière sur la scène internationale pour mieux avancer: l'engagement sélectif 36
1.2.2.1 Le retranchement américain du système international 37
1.2.2.2 La concentration des efforts sur l'Asie avec la stratégie du *pivot* 40
CHAPITRE II
L'ÉMERGENCE DE LA CYBERMENACE CHINOISE 49
2.1 Une menace initiale pensée essentiellement en termes économiques 51
2.1.1 Des actes de cyberespionnage de plus en plus fréquents 51
2.1.2 Une puissance économique relative menacée 57
2.2 Une menace progressivement abordée en termes offensifs et militaires 64
2.2.1 Les cybercapacités perçues comme favorisant l'offensive 65
2.2.2 Des cyberintrusions chinoises réinterprétées sous le prisme militaire 71

CHAPITRE III
L'ADAPTATION DE LA COMMUNAUTÉ MILITAIRE AMÉRICAINE 83
3.1 La transformation de la structure militaire américaine 85
3.1.1 Des cybercapacités en développement et en quête d'identité 86
3.1.2 Des cybercapacités militarisées et institutionnalisées. 93
3.2 L'implantation d'une cyberdoctrine américaine visant la dissuasion 102
3.2.1 La cyberdissuasion comme instrument de la politique étrangère d'Obama 103
3.2.2 La mutation d'une cyberdoctrine américaine visant la dissuasion 108
3.2.2.1 La défense du territoire américain contre les cyberattaques 109
3.2.2.2 La mise en place d'une capacité crédible de représailles 113
3.2.2.3 La projection de la puissance américaine dans le cyberespace. 118
CONCLUSION 123
ANNEXE A
PROPORTION AMÉRICAINE DU PIB MONDIAL ET SES DÉPENSES MILITAIRES 129
ANNEXE B
BUDGETS MILITAIRES DE PAYS DE LA RÉGION D'ASIE-PACIFIQUE ENTRE 2005 ET 2012 131
ANNEXE C
PROPORTION CHINOISE DU PIB MONDIAL ET SES DÉPENSES MILITAIRES 133
ANNEXE D
PRINCIPAUX POINTS DE LITIGES TERRITORIAUX ET OCÉANIQUES EN MER DE CHINE DU SUD 135
ANNEXE E
TRANSFERT DES FORCES ARMÉES AMÉRICAINES DÉPLOYÉES DANS QUELQUES THÉÂTRES RÉGIONAUX ET DANS LES BASES DE GUAM ET D'HAWAII ENTRE 2009 ET 2014 137
ANNEXE F
L'ÉTENDUE GÉOGRAPHIQUE DU CYBERESPIONNAGE CHINOIS EN SOL AMÉRICAIN 139

ANNEXE G
LES DEUX CHAÎNES D'ÎLES 141
ANNEXE H
LE « COLLIER DE PERLES » CHINOIS 143
BIBLIOGRAPHIE 145

LISTE DES TABLEAUX

Tableau Page

1.1 Les trois grandes stratégies américaines possibles sous Obama.....23

LISTE DES ABRÉVIATIONS, SIGLES ET ACRONYMES

AFCYBER	Air Force Cyber Command
APL	Armée populaire de libération
ASB	Air-Sea Battle
ASEAN	Association of Southeast Asian Nations
BRICS	Brésil, Russie, Inde, Chine et Afrique du Sud.
C2	Commandement et Contrôle
C4ISR	Commandement, contrôle, communications, informatique, renseignement, surveillance et reconnaissance
CBO	Congressionnal Budget Office
CNE	Computer Network Exploitation
DCEO	Defensive Cyber Effects Operations
DHS	Département de la Sécurité nationale
DIRNSA	Directeur de la NSA
DISA	Defense Information Systems Agency
DNI	Directeur des services de renseignement
DoD	Département de la Défense
DPG	Defense Planning Guidance
FBI	Federal Bureau of Investigation
IC	Infrastructure critique
ICANN	Internet Corporation for Assigned Names and Numbers
IISS	International Institute for Strategic Studies
IW	Guerre informationnelle (Information Warfare)
JFCC-NW	Joint Functional Component Command for Network Warfare
JTF-GNO	Joint Task Force-Global Network Operations
NORAD	North American Aerospace Defense Command
NSA	National Security Agency

NSDD-145	National Security Decision Directive-145
NSS	National Security Strategy
OCEO	Offensive Cyber Effects Operations
OI	Organisations internationales
ONU	Organisation des Nations Unies
PCC	Parti communiste chinois
PDD-63	Presidential Decision Directive – 63
QDR	Quadrennial Defense Review
R et D	Recherche et développement
RAM	Révolution dans les affaires militaires
RIMPAC	Rim of the Pacific
SEACAT	Southeast Asia Cooperation and Training
SIGINT	Renseignement d'origine électromagnétique
TAO	Tailored Access Operations
TIC	Technologies de l'information et de la communication
USAF	United States Air Force
USCENTCOM	U.S. Central Command
USCYBERCOM	U.S. Cyber Command
USPACOM	U.S. Pacific Command
USSTRATCOM	United States Strategic Command

RÉSUMÉ

Ce mémoire s'intéresse aux raisons ayant poussé les États-Unis d'Obama à officiellement militariser le cyberespace, cinquième domaine militaire, et aux liens de cet effort avec l'émergence de la Chine en tant que sérieuse concurrente aux États-Unis. La thèse ici défendue est que l'accélération et l'institutionnalisation de la militarisation du cyberespace découlent toutes deux du *pivot vers l'Asie*, élément central de la grande stratégie d'engagement sélectif adoptée par Obama à l'endroit de la Chine. Elle participe à la préservation de la stabilité et de la paix en Asie-Pacifique, objectif considéré indispensable à la protection à long terme des intérêts vitaux américains.

Contraint par une faible légitimité internationale et un lourd fardeau fiscal hérités de la présidence de G.W. Bush, Obama a choisi l'*engagement sélectif* afin de guider sa grande stratégie. Cette stratégie se démarquera par un retranchement de la puissance américaine nécessitant une allocation des rares ressources disponibles aux régions stratégiques clés, dont l'Asie du Sud-Est et son plus grand acteur, la Chine. Cet effort de concentration sera analysé avec le concept d'*équilibre de la menace* de Stephen Walt, où, afin d'assurer sa sécurité, un État cherche principalement à limiter et à rééquilibrer les dangers émanant des États perçus comme menaçants.

Ensuite, la Chine représente dès lors une importante cybermenace pour les États-Unis. Contrairement au monde physique, la distance n'y empêche pas la Chine de nuire aux intérêts américains : elle a plusieurs fois démontré ses capacités à pirater et à infiltrer des systèmes informatiques américains, mettant notamment la main sur une importante quantité de propriétés intellectuelles américaines, clés de sa puissance économique et militaire. De plus, plusieurs écrits militaires et stratégiques chinois décrivent leurs intentions d'utiliser des cyberattaques, conformément à la stratégie dite *anti-access/area-denial*, dans le déclenchement d'un éventuel conflit entre les deux pays. Ce mélange de capacités et d'intentions constitue une menace importante pour les États-Unis.

Finalement, ceux-ci ont entrepris d'équilibrer la cybermenace chinoise en profitant des cybercapacités qui, sur deux décennies, ont été développées et utilisées par l'armée américaine, mais surtout par la *National Security Agency*, agence de renseignement qui deviendra le centre de gravité de la cyberpuissance américaine. Celles-ci seront militairement institutionnalisées par la création du *United States Cyber Command* et serviront à implanter une cyberdoctrine visant autant à dissuader les cyberattaques sur le territoire américain qu'à maintenir la paix et de la stabilité en Asie-Pacifique, en préservant la supériorité militaire américaine en participant à la stratégie du *Air-Sea Battle*.

Mots-clés : cyberespace, relations États-Unis/Chine, politique étrangère, National Security Agency, Barack Obama, engagement sélectif, cyberespionnage, United States Cyber Command (USCYBERCOM), A2/AD

INTRODUCTION

Dans *WarGames*, film de 1983 se déroulant en pleine guerre froide, un jeune garçon infiltrait un superordinateur de la *North American Aerospace Defense Command* (NORAD), agence contrôlant l'arsenal nucléaire américain. Par ce geste, il frôla le pire : le déclenchement d'un conflit nucléaire. Le visionnement de ce film par Ronald Reagan mena à la promulgation de la *National Security Decision Directive-145* (NSDD-145)[1], évoquant déjà la nécessité de protéger les systèmes informatiques américains des acteurs malveillants. Près de 25 ans allaient pourtant s'écouler avant que le sujet soit sérieusement remis à l'ordre du jour sécuritaire. Malgré la grande démocratisation des ordinateurs personnels et d'Internet, les présidences suivantes n'ont jamais réellement fait de cette problématique une priorité, en démontrant plutôt leur méconnaissance ou leur indifférence.[2] Il serait néanmoins malhonnête d'affirmer que les administrations suivantes ne l'aient jamais abordée, l'ayant principalement fait en réaction à des actes terroristes en sol américain. D'entrée de jeu, l'évènement d'Oklahoma City de 1995 poussa Clinton à mettre sur pied la *Commission présidentielle sur la protection des infrastructures critiques,* dont le rapport de 1997 affirmait que

> la prolifération et l'intégration rapide des télécommunications et des systèmes informatiques ont relié les infrastructures en un réseau complexe d'interdépendance. Ces liens réciproques ont créé une nouvelle dimension de vulnérabilité, qui, lorsque combinée à une constellation émergente de menaces, pose un risque national sans précédent.[3]

---

[1] Fred Kaplan. « 'WarGames' and Cybersecurity's Debt to a Hollywood Hack ». *The New York Times*, 19 février 2016. En ligne, <www.nytimes.com/2016/02/21/movies/wargames-and-cybersecuritys-debt-to-a-hollywood-hack.html>. Consulté le 21 février 2016.

[2] Bill Clinton affirme encore faussement aujourd'hui n'avoir envoyé que deux courriels dans sa vie, alors que George W. Bush s'est attiré les moqueries après avoir notamment utilisé les termes « le Google », ainsi que « les Internets ». Adrienne Lafrance. « The Truth About Bill Clinton's Emails ». *The Atlantic*, 12 mars 2015. En ligne, <www.theatlantic.com/technology/archive/2015/03/the-myth-about-bill-clintons-emails/387604/>. Consulté le 24 février 2015; NPR. « President Bush and 'the Google' », *National Public Radio*, 30 octobre 2006. En ligne, <www.npr.org/templates/story/story.php?storyId=6404911>. Consulté le 24 février 2016.

[3] États-Unis, White House. *Critical Foundations – Protecting America's Infrastructures*. Washington D.C. : The White House, 1997, p.ix.

Afin de protéger ces infrastructures critiques (IC), ce rapport mènera à la *Presidential Decision Directive – 63* (PDD-63) visant à éliminer leurs vulnérabilités physiques et cyber[4], mais aussi au *National Plan for Information Systems Protection* de 2000. Toutefois, malgré la technophilie démontrée par le tandem Clinton/Gore, le président « ne se préoccupait pas du cyber et, véritablement, ne l'a jamais été.[5] »

Le 11-septembre remit la problématique à l'ordre du jour, menant à la création, par George W. Bush, du *President's Critical Infrastructure Protection Board* en octobre 2001[6] et à l'adoption de la *National Strategy to Secure Cyberspace* de 2003, une mise à jour de la politique mise en place sous Clinton et laissant au secteur privé une totale liberté en ce qui a trait à leur cybersécurité, un secteur incluant pourtant la majeure partie des IC américaines, qu'elles soient civiles ou militaires[7]. Richard A. Clarke, responsable de ces initiatives sous les deux administrations, déplorait toutefois que la cyberstratégie de défense américaine soit considérée comme une préoccupation de second ordre et traitée comme telle[8]. Lentement mais sûrement, les choses allaient changer.

Dès le début de son mandat, Barack Obama soulignait la menace potentielle à la sécurité nationale que représentait le cyberespace, affirmant que « les technologies nous permettant de créer et de construire davantage sont également celles permettant à ceux qui le veulent de perturber et de détruire tout autant.[9] »

---

[4] États-Unis, White House. *Presidential Decision Directive 63.* Washington D.C. : The White House, 1998. En ligne, <fas.org/irp/offdocs/pdd/pdd-63.htm>. Consulté le 22 février 2016.

[5] Fred Kaplan. *Dark Territory – The Secret History of Cyber War.* New York : Simon & Schuster, 2016, p.89.

[6] États-Unis, Department of Homeland Security. *Executive Order 13231 of October 16, 2001 - Critical Infrastructure Protection in the Information Age.* Washington D.C. : Department of Homeland Security, 2001. PDF en ligne, <www.dhs.gov/xlibrary/assets/executive-order-13231-dated-2001-10-16-initial.pdf>. Consulté le 22 février 2016.

[7] États-Unis, White House. *The National Strategy to Secure Cyberspace*, Washington D.C. : The White House, 2003, 60 p.

[8] Richard A. Clarke et Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It*, New York: Harper Collins, 2009, p.96 – 97.

[9] États-Unis, White House. *Remarks by the President on Securing our Nation's Cyber Infrastructure.* Washington D.C. : The White House, 2009. En ligne, <www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure>. Consulté le 15 janvier 2016.

Rompant avec la passivité des administrations précédentes concernant la cyberdéfense, le cyberespace sera désormais officiellement considéré comme un domaine militaire à part entière, une transformation majeure notamment démontrée par la création, en 2010, du *U.S. Cyber Command* (USCYBERCOM). Cette nouvelle organisation a pour mission de défendre les réseaux informatiques du département de la Défense (DoD), et de mener, au besoin, des opérations offensives. Si l'importance du cyberespace pour la sécurité nationale avait déjà été évoquée, elle n'avait jamais été à ce point prise au sérieux par les autorités gouvernementales.

Cette transformation de l'approche étatique relativement au cyberespace n'est pas fortuite, étant liée à un changement majeur de paradigme, alors que le cyberespace a permis le développement, l'affrontement et la superposition de plusieurs visions depuis sa création en 1969[10]. Pour les utopistes de la première heure, issus de la contre-culture californienne des années 70[11], et les actuels puristes, cet espace virtuel permet de dépasser les barrières géographiques ou sociales par l'absence d'autorité et le libre accès à l'information.[12] Dans les années 90, le vice-président Gore encouragea politiquement l'exploitation des réseaux par le secteur privé et la création d'une *autoroute de l'information*[13] permettant à son tour le développement d'une *économie du savoir.* De communauté égalitaire virtuelle, le cyberespace devenait donc un espace commercial idéal et libre de toutes entraves gouvernementales[14], mais rapidement en proie à de nombreuses nuisances : une cybercriminalité croissante gênait la prospérité d'une industrie en pleine expansion et spoliait ce qui était désormais considéré comme un *bien public* et *mondial.* Pour certains, l'espace marchand mondialisé qu'est Internet devient

---

[10] Elle suit la mise en place d'une connexion reliant les universités de Stanford et le campus de Los Angeles de l'Université de Californie, réseau s'étendant à d'autres universités, comme le MIT.

[11] André Mondoux. Histoire sociale des technologies numériques de 1945 à nos jours. Montréal : Éditions Nota Bene, 2011, p.85 – 93.

[12] Mary McEvoy Manjikian. « From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik », *International Studies Quarterly*, vol.54, no.2, 2010, p.383

[13] P.W. Singer et Allan Friedman. *Cybersecurity and Cyberwar : What Everyone Needs To Know*, New York : Oxford University Press, 2013, p.20

[14] Geoffrey L. Herrera. « Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space ». Dans M. Cavelty, V. Mauer et S.F. Krishna-Hensel (eds.), *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace*, Aldershot; Burlington: Ashgate, 2007, p.76; 79; 82.

porteur de modernisation, de progrès et de pacification du monde, facilitant le commerce et augmentant l'interdépendance des États[15]. Il apparaît aussi comme un nouvel instrument du *soft power*, « plus important à l'âge numérique que jamais auparavant, principalement grâce à l'évolution de multiples canaux mondiaux de communications transcendant facilement les frontières souveraines[16] ». Cette conception perdure encore aujourd'hui, alors que Jane Holl Lute, secrétaire adjointe du département de la Sécurité nationale (DHS), affirma en 2011 que « le cyberespace est fondamentalement un espace civil », rejetant du même coup la vision militariste qui allait progressivement s'imposer dans le débat[17].

Les possibles dangers, longtemps écartés au profit de la prospérité économique, émergeront inévitablement, l'interdépendance des systèmes communicationnels et informationnels mondiaux apparaissant désormais comme une vulnérabilité inquiétante. De plus, alors que le cyberespace rend ténu le concept de *distance* physique et temporelle[18], il permet également aux acteurs non étatiques d'exercer une influence importante à l'échelle mondiale et ce, à faible coût[19]. Apparaît alors une conception *réaliste*, où le cyberespace n'est pas tant « un espace révolutionnaire subvertissant les structures existantes de pouvoir au sein des relations internationales », qu'un espace où se superposent les structures traditionnelles de la puissance étatique[20]. Les fruits de la révolution informationnelle sont donc appelés à être adoptés et contrôlés militairement par l'État, destin habituel des innovations techniques naissantes. Le cyberespace passe donc d'un espace *libre* et anarchique à une extension du territoire national et du champ de bataille de demain.[21]

---

[15] Johan Eriksson et Giampiero Giacomello. « The Information Revolution, Security and International Relations: (IR)relevant Theory? », *International Political Science Review*, vol. 27, no.3, 2006, p.230

[16] *Ibid.*, p.231.

[17] Jane Holl Lute et Bruce McConnell. « Op-Ed : A Civil Perspective on Cybersecurity », *Wired*, 14 février 2011. En ligne, <www.wired.com/2011/02/dhs-op-ed/>. Consulté le 16 mars 2016.

[18] Manjikian, *op.cit.*, p.391

[19] Eriksson et Giacomello, *op.cit.*, p.232.

[20] *Ibid.*, p.385

[21] *Idem.*

Encore aujourd'hui, le cyberespace n'est pas neutre : originalement mis sur pied par le Pentagone, il demeure encore aujourd'hui régi par des organisations principalement basées aux É.-U. De ce lot se trouve l'*Internet Corporation for Assigned Names and Numbers* (ICANN) dépendant informellement du département américain du Commerce : cette situation pourrait toutefois changer avec l'adoption, en mars 2016, d'un projet de réforme voulant implanter un pluripartisme mondial par l'entremise de l'*Internet Assigned Numbers Authority*, plan demeurant néanmoins soumis à l'approbation du gouvernement américain![22] Alors que la dévolution de ce pouvoir américain à de multiples acteurs reflète la mise en place d'un système international que l'on pourrait qualifier de *multipolaire*, la nature du cyberespace est donc intimement liée aux transformations d'un système international dominé par les É.-U.

Si la portée d'Internet explosa durant la période de prospérité post-Guerre froide, marquée par un néolibéralisme économique et politique, des « moments conjoncturels où une impulsion politique suffisante permet de surmonter l'inertie institutionnelle enracinée[23] » ont amorcé la perception sécuritaire et militaire, comme le fut le 11-septembre. Ce traumatisme national a mis en place une véritable obsession pour les enjeux de sécurité nationale, alors que la montée en puissance économique de nouveaux États est venue sérieusement ébranler l'idée d'une prédominance américaine, perturbant une vision libérale[24] d'autant plus ternie par la multiplication des cyberincidents laissant croire à l'imminence d'une attaque cybernétique majeure.

La militarisation des réseaux mondiaux en résultant amène certains auteurs à y voir une version numérique de l'ère westphalienne[25], alors que s'implantent des cyberfrontières nationales permettant de mieux contrôler la population et d'assurer la sécurité du

---

[22] Maria Farrell. « Quietly, symbolically, US control of the internet was just ended ». *The Guardian*, 14 mars 2016. En ligne, <www.theguardian.com/technology/2016/mar/14/icann-internet-control-domain-names-iana>. Consulté le 16 mars 2016.

[23] Herrera, *op.cit.*, p.74-75

[24] Chris Demchak et Peter Dombrowski. « Rise of a Cybered Westphalian Age », *Strategic Studies Quarterly*, vol.5, no.1, 2011, p.35.

[25] *Ibid.*, p.32

territoire[26]. Pour Demchak et Dombrowski, il est habituel, depuis les traités de Westphalie de 1648, que les territoires non gouvernés soient pris d'assaut, autant à l'intérieur d'un État (hors de son contrôle) qu'à sa frontière[27], l'État cherchant à gagner en puissance et à réduire les vulnérabilités menaçant son existence, conditions nécessaires au développement social et économique[28]. Autant par l'émergence d'un *Far Web* regorgeant de criminels et d'acteurs malveillants que par la croissance importante des cas de cyberattaques, la frontière numérique devient une réalité inévitable, cherchant autant à augmenter les coûts éventuels de futures attaques à l'endroit de réseaux situés à l'intérieur d'un État qu'à sabrer les avantages offensifs inhérents au cyberespace[29]. Certains ajoutent que « les frontières physiques sont connues, acceptées et désirées par les citoyens dans les sociétés civiles modernes », et qu'il n'en serait pas « différent concernant la création de frontières dans le cyberespace[30] ». C'est notamment le cas pour les entreprises œuvrant dans les technologies de l'information et de la communication (TIC) et qui, après une période de prospérité importante, ont vu leurs réseaux être infectés, leur parc informatique être endommagé et le fruit de leurs recherches et développement, nerf de la guerre de la compétition économique mondiale, être copié, exporté, utilisé et vendu. Si le secteur privé a longtemps prôné le *laissez-faire* économique dans le cyberespace, désormais « les intérêts gouvernementaux et économiques se confondent et travaillent plus que jamais main dans la main.[31] »

Bien qu'abstraites, les cyberfrontières existent déjà : le *Great Firewall*[32] protège le cyberespace national chinois, tandis que les É.-U. ont emboîté le pas en créant le CYBERCOM. Si elles n'élèvent pas de frontières physiques et tangibles, ces initiatives marquent toutefois « la reconnaissance d'une propriété nationale que l'État [...] protégera

---

[26] *Ibid.*, p.85
[27] Demchak et Dombrowski, *op.cit.*, p.37
[28] *Idem.*
[29] *Ibid.*, p.39
[30] *Ibid.*, p.42
[31] Nicolas Arpagian. « Les entreprises: complices et victimes de la cyberguerre », *Revue internationale et stratégique*, vol.3, no.87, 2013, p.67
[32] Fabienne Clérot et Victoire Mayor. « Jeu de go dans le cyberespace », *Revue internationale et stratégique*, vol.87, no.3, 2012, p.112

en utilisant les ressources disponibles et appropriées, y compris l'application de règlements, du droit et de ses capacités militaires.[33] » Hier encore un espace commercial et/ou libre, le cyberespace a depuis subi un assaut étatique et une militarisation rapide, phénomène désormais répandu aux quatre coins du globe.

Aux É.-U., ce mouvement est aisément observable. Alors qu'au cours des dernières années, les budgets des différents services militaires américains ont stagné, voire diminué à la suite du *Budget Control Act* de 2011, les fonds attribués au cyber ont explosé durant la même période. Entre 2013 et 2014, le budget alloué par le DoD au CYBERCOM a plus que doublé et le Général Keith B. Alexander, simultanément à la tête de la *National Security Agency* (NSA), agence gouvernementale associée à la Défense et spécialisée dans le renseignement d'origine électromagnétique (SIGINT), et du CYBERCOM annonçait que le nombre d'employés y travaillant atteindrait le cap des 6000 en 2016[34]. Cette prévision n'incluait toutefois pas le personnel de la NSA et les entrepreneurs privés qui y sont associés, effectifs militairement nombreux et utiles, autant défensivement qu'offensivement.

Parallèlement à cette militarisation croissante du cyberespace, le nombre de menaces en émanant est également en hausse. Bien qu'une grande variété d'acteurs puisse porter préjudice à la sécurité des É.-U., la Chine demeure toutefois la plus persistante et la plus envahissante, des cyberintrusions furtives ayant été répertoriées dans une quantité innombrable de serveurs gouvernementaux, militaires et d'entreprises privées américaines et menant à d'importants transferts de données. Dès 2005, les soupçons se sont tournés vers le gouvernement chinois, accusé d'être à l'origine de ces opérations, autant par l'entremise de sa branche armée que de divers éléments de sa société civile[35].

---

[33] Demchak et Dombrowski, *op.cit.*, p.48

[34] États-Unis. Department of Defense. *Retirement Ceremony for General Keith Alexander*, 2014. En ligne, <archive.defense.gov/Speeches/Speech.aspx?SpeechID=1837>. Consulté le 25 mars 2015.

[35] Ronald J. Deibert. « Chasing Shadows », dans *Black Code: Inside the Battle for Cyberspace*, Toronto: McClelland & Stewart, 2013, p.23.

Alors que l'administration Obama a de nombreuses fois publiquement pointé du doigt ces agissements, ses accusations ont toujours été reçues avec l'indignation et le déni des autorités chinoises.

Si certains membres de l'administration américaine estimaient en 2008 que 140 pays développaient des cybercapacités militaires[36], cette insistance sur les cyberactivités chinoises n'est toutefois pas fortuite. En pleine émergence, la Chine est aujourd'hui vue par les uns comme une puissance à intégrer dans le système international actuel et par d'autres comme une menace à ce même système, menace nécessitant l'adoption d'une ligne dure afin d'éviter ou de se préparer à un éventuel conflit, position ayant progressivement pris le dessus au sein de l'administration Obama.[37] Depuis la présidence Clinton, les relations sino-américaines s'inscrivaient plutôt dans une perspective libérale: malgré les désaccords autour de la question des droits de l'homme, les liens économiques entre les deux pays ont été renforcés et consacrés par l'entrée de la Chine au sein de l'Organisation mondiale du commerce en 2001. Sous George W. Bush, alors que les relations initiales étaient tendues avec un pays que l'on estimait être un futur rival[38], le 11-septembre et ses suites ont relégué cette problématique au second plan. Avec l'arrivée de Barack Obama, cette perspective de la montée pacifique de la Chine a toutefois été mise à l'épreuve.

Les *libéraux* soutiennent néanmoins que la Chine ne représente pas une menace inévitable pour les É.-U. ou pour l'ordre international actuel. Pour Joseph Nye, la Chine est loin de pouvoir surpasser la première puissance mondiale, autant économiquement que militairement. Dépasser le PIB américain ne suffirait pas à éradiquer les éventuelles inégalités présentes au sein de sa société et représentant un potentiel défi de taille pour

---

[36] Mike McConnell. « Cyber Insecurities : The 21st Century Threatscape ». Dans K.M. Lord et Travis Sharp (eds.), *America's Cyber Future : Security and Prosperity in the Information Age – Volume II*, Washington D.C. : Center for A New American Society, 2011, p.29.

[37] Charles-Philippe David. *Au sein de la Maison-Blanche : de Truman à Obama, la formulation (imprévisible) de la politique étrangère des États-Unis*. Québec: Presses de l'Université Laval, 3e édition, 2015, p.957.

[38] Condoleezza Rice. « Campaign 2000 : Promoting the National Interest », *Foreign Affairs*, vol.79, no.1 (2000), p.56.

le gouvernement chinois. Militairement, Nye juge que même avec des forces armées suffisantes, la Chine ne peut se permettre d'être trop agressive, dépendante des marchés et ressources provenant de l'extérieur, une attitude qui provoquerait la formation d'une coalition adverse. Pour les libéraux, il serait donc possible de convaincre la Chine de participer au système international actuellement en place[39]. Pour ce faire, Ikenberry propose un réengagement américain dans l'ordre mondial mis en place par les É.-U. à la suite de la Seconde Guerre mondiale, une implication misant sur une refonte du multilatéralisme facilitant l'intégration des puissances émergentes, dont la Chine, car « plus les relations économiques et sécuritaires sont multilatérales et englobantes, plus le système global préserve sa cohérence.[40] » Pouvant ainsi joindre l'ordre international actuel et y prospérer pacifiquement, la Chine ne trouverait aucun avantage à s'engager dans une voie tortueuse afin de concurrencer ce système.

Pour sa part, David C. Kang estime que la Chine ne pose pas un véritable défi en Asie de l'Est : la plupart de ses voisins ne craignent pas sa puissance, mais « préfèrent que la Chine soit plus forte que faible, car une Chine forte stabilise la région alors qu'une Chine faible fait en sorte que les autres États sont tentés d'essayer de mettre la main sur le contrôle de la région.[41] » De plus, Kang affirme que les États de la région ne voient pas la Chine d'un œil méfiant, mais davantage comme une opportunité et un État bien intentionné, autant au niveau des relations avec ses voisins, de la santé économique de la région et de la stabilité interne des pays environnants[42]. De plus, les É.-U. et la Chine possèdent des liens économiques étroits qu'il serait difficile de rompre[43].

---

[39] Joseph S. Nye Jr. « The Future of American Power : Dominance and Decline in Perspective », *Foreign Affairs*, vol.89, no.6, 2010, p.4-5

[40] G. John Ikenberry. « The Rise of China and the Future of the West : Can the Liberal System Survive? », *Foreign Affairs*, vol.87, no.1, 2008, p.35

[41] David C. Kang. *China Rising : Peace, Power, and Order in East Asia*. New York : Columbia University Press, 2007, p.4

[42] *Ibid.*, p.198

[43] *Ibid.*, p.189

Devant ce constat, Kang doute de la pertinence d'une tentative d'équilibre de la part des É.-U. qui, en plus de nuire à la situation économique américaine, pourrait être accueillie de manière mitigée dans la région et inciter certains pays à s'aligner avec la Chine.

Le néoréalisme permet de comprendre les perspectives réalistes en vogue aujourd'hui. Kenneth Waltz, dans son livre *Theory of International Politics*, considère la structure politique internationale comme étant l'unique variable pouvant expliquer les relations interétatiques. Cette théorie dite *systémique*, ou *néo-réaliste*, repose sur trois idées : l'anarchie comme principe ordonnateur du système, la similarité des fonctions des États (ou unités) et la différence entre le niveau de puissance de chacun. Aujourd'hui, cette théorie est partagée entre les *réalistes défensifs*, plus près de la conception originelle de Waltz, et les *réalistes offensifs*.

Pour John Mearsheimer, tête d'affiche du *réalisme offensif,* la structure internationale anarchique force les États à maximiser leur puissance et à rechercher l'hégémonie mondiale afin d'assurer leur survie[44]. C'est dans cet esprit que pour certains, la montée actuelle de la Chine laisse entrevoir qu'elle pourrait devenir un hégémon régional en Asie en cherchant à s'approprier la mer de Chine[45] : en débarrassant celle-ci des puissances étrangères, elle en ferait un sanctuaire exclusif lui permettant de projeter sa puissance militaire et de s'imposer en tant que grande puissance sur l'échiquier mondial. Pour plusieurs, cette ambition s'apparente à ce que fut la doctrine Monroe pour les É.-U.[46]

Le risque que s'établisse un hégémon régional chinois nécessiterait donc une intervention américaine, menacé par ce compétiteur et cherchant à garder sa position de puissance prédominante au sein du système international. Mearsheimer met aussi en garde les adeptes de l'*engagement* : « Si la Chine venait à devenir un Hong Kong géant, elle aurait

---

[44] John J. Mearsheimer. *The Tragedy of Great Power Politics*. New York : Norton, 2001, p.402

[45] Robert D. Kaplan. « The Geography of Chinese Power : How Far Can Beijing Reach on Land and at Sea? », *Foreign Affairs*, vol.89, no.3, 2010, p.38

[46] Cette doctrine, initiée par le Président Monroe en 1823, affirmait, en parlant des grandes puissances européennes, que les É.-U. « considèreraient toute tentative de leur part d'étendre leur système sur une portion de cet hémisphère comme étant dangereuse envers notre paix et notre sureté. » Cette initiative mènera à l'expulsion des grandes puissances européennes du continent américain et à l'hégémonie des É.-U. sur celui-ci suite à la guerre hispano-américaine de 1898.

probablement environ quatre fois plus de puissance latente que les É.-U., lui permettant d'acquérir un avantage militaire décisif sur les É.-U. en Asie du Nord-Est[47] ».

Selon l'auteur, cet avantage en ferait un adversaire plus puissant et plus dangereux que les É.-U. dans les prochaines années, mais également plus puissant que les États ayant tenté de changer le *statu quo* lors du XX^e^ siècle, comme le furent l'Allemagne nazie ou l'Union Soviétique. Ces analogies évoquant l'inévitable conflit majeur à venir, auxquelles il est possible d'ajouter l'Allemagne wilhelmienne ou le Japon impérial par la composante maritime de l'expansion stratégique chinoise, connaissent une popularité dans l'entourage du DoD[48]. Le *Defense Policy Board*, un de ses organes consultatifs internes, avance en effet que la Chine, par sa géographie et sa nécessité d'assurer un accès constant à son approvisionnement en ressources, sera expansionniste : elle deviendra à la fois une puissance continentale, en raison de son armée considérable, mais aussi une puissance maritime potentiellement agressive.

Moins fataliste, l'analyse de Stephen Walt, réaliste *défensif*, diffère sur les causes et conséquences de l'émergence chinoise. Selon lui, les États recherchent avant tout la sécurité et la protection de leurs acquis, faisant en sorte qu'un État possédant une trop grande puissance militaire créera des inquiétudes chez les autres États qui se ligueront pour la contrer. Ainsi, si la Chine devenait un jour une menace importante pour ses voisins, les plus faibles entreraient en partenariat avec elle, mais les puissances régionales se tourneraient plutôt vers les É.-U. dans le but d'équilibrer cette menace et ainsi inciter la Chine à la retenue et la coopération[49]. Pour ce faire, Walt prône un retour des É.-U. à leur politique d'*équilibrage à distance* : se concentrer sur quelques régions d'importance stratégique, incluant l'Asie, déléguer le maintien de l'équilibre du pouvoir des différentes régions aux puissances locales, maintenir sur place un minimum de forces armées et

---

[47] Mearsheimer, *op.cit.*, p.401

[48] Jean-Loup Samaan. « Une géographie américaine de la menace chinoise », *Hérodote*, no.140 (2011), p.105; Jean-Loup Samaan. *La Menace chinoise : une invention du Pentagone?*, Paris : Vendémiaire, 2012, pp.22 – 23.

[49] Stephen M. Walt. « Balancing Act (Asian Version) », *Foreign Policy*, 3 mai 2010. En ligne, <foreignpolicy.com/2010/05/03/balancing-act-asian-version/> Consulté le 15 avril 2015

n'intervenir de manière décisive que lorsqu'il est impératif de le faire[50], à l'image de l'implication américaine lors des deux guerres mondiales.

L'objectif central de ce mémoire est donc d'identifier les raisons pour lesquelles les É.-U. ont soudainement institutionnalisé le cyberespace et investi dans sa militarisation alors qu'elle a longtemps été délaissée par les administrations successives, au moment même où le financement des forces armées américaines s'est vu être obligatoirement réduit. Ce travail de recherche vise également à remplir un vide dans la littérature concernant la militarisation américaine du cyberespace. Bien que de nombreux ouvrages évoquent le processus historique de cette militarisation ou discutent de la cybermenace planant au-dessus des É.-U., qu'elle soit générale ou spécifiquement chinoise, peu d'ouvrages ont cherché à faire le pont entre les deux sujets, la mission de ce mémoire.

Il est donc nécessaire de se poser quelques questions afin de comprendre ce qui a pu pousser l'administration Obama à rapidement passer d'une cyberstratégie passive et défensive à une cyberstratégie résolument offensive. **D'abord, quelles menaces représentent les cyberintrusions chinoises pour les É.-U. et comment s'inscrivent-elles au sein de la grande stratégie poursuivie par l'administration Obama? Ensuite, quel rôle joue un cyberespace militarisé au sein de cette même grande stratégie et comment cette exigence stratégique et sécuritaire a-t-elle transformé les forces armées américaines?**

Devant ces questions, ce mémoire défendra la thèse que l'accélération et l'institutionnalisation de la militarisation du cyberespace initiées par l'administration Obama s'inscrivent directement dans la lignée du *pivot vers l'Asie*, élément central de la grande stratégie d'*engagement sélectif* adoptée sous Obama. Elle participe ainsi à l'atteinte de l'objectif américain qu'est la préservation à tout prix de la stabilité et de la paix dans la région de l'Asie-Pacifique, un objectif perçu par le 44e président comme étant central et indispensable à la protection à long terme des intérêts américains.

---

[50] Stephen M. Walt. « Taming American Power », *Foreign Affairs,* vol.84, no.5, 2005, p.118; Stephen M. Walt, « The End of American Era », *The National Interest*, n.116, 2011, p.13

Nous nous attarderons à un cadre temporel s'échelonnant de la deuxième moitié du dernier mandat de George W. Bush, période où le processus de militarisation du cyberespace a été amorcé, jusqu'à la fin du premier mandat de Barack Obama, où cette militarisation s'est institutionnalisée par l'établissement du CYBERCOM. Cette période, s'échelonnant *grosso modo* de 2006 à 2013, est cruciale afin de comprendre l'émergence et l'impact de ce qui est considéré comme une nouvelle menace à la sécurité nationale américaine, problématique qui a également des répercussions sur le plan géopolitique, alors que l'administration Obama amorce un *pivot vers l'Asie*, orienté vers la Chine.

Afin de valider notre hypothèse, une analyse documentaire empirique et théorique sera privilégiée. Beaucoup d'informations étant classifiées, la consultation de documents universitaires ou gouvernementaux déjà existants est nécessaire, autant sur la question du pivot vers l'Asie que de la militarisation du cyberespace : monographies, articles spécialisés, documents, rapports et discours officiels de membres du gouvernement américain, etc. Les documents politiques et stratégiques officiels nous permettront de définir la grande stratégie américaine sous Obama, de découvrir le contenu de sa posture stratégique américaine envers la Chine, mais aussi envers le cyberespace, nouveau champ de bataille dont le contrôle est considéré nécessaire au succès de la grande stratégie d'Obama.

Même si de nombreux documents abordant le cyberespace comme domaine militaire ou concernant les actions prises par la NSA et/ou d'autres entités militaires sont inaccessibles, les sources d'informations sur le sujet demeurent toutefois nombreuses. Les documents révélés par Edward Snowden et les différentes fuites d'informations nous permettent d'avoir un meilleur portrait de la situation, et ce, même s'ils sont davantage portés sur la surveillance et la cueillette de données privées, l'organisation (la NSA) et le *modus operandi* demeurant les mêmes. Malgré l'impossibilité de dresser un portrait entier de la situation, suffisamment de documents existent pour nous permettre d'analyser le sujet étudié sous l'angle des perceptions américaines à l'endroit de la Chine

et de sa montée, mais aussi des menaces provenant du cyberespace, particulièrement chinoises, et les différentes mesures adoptées à Washington.

En plus des documents stratégiques du DoD, un nombre croissant de membres de l'appareil américain de sécurité s'expriment au sujet du cyberespace, autant par l'entremise de commissions du Congrès où sont parfois convoqués des personnalités comme le général Keith B. Alexander, d'articles dans les revues spécialisées, de publications de *think tanks*, de mémoires publiés par des personnes près du pouvoir et qui offrent un regard interne sur les problématiques visées, tout comme un nombre croissant de monographies traitant du sujet. Le cyberespace étant également un sujet quotidien d'actualité, une attention sera portée aux articles de journaux ou de magazines traitant du sujet : de plus en plus de journalistes s'y intéressent et diffusent un bon nombre d'informations s'avérant précieuses. Des journaux ou périodiques comme le *New York Times* ou *Foreign Policy* seront consultés pour obtenir des informations brutes, tout comme les documents rendus publics par Edward Snowden.

Trois chapitres permettront de valider notre thèse. Le premier présentera les théories et concepts utilisés dans le cadre de cette recherche, notamment le concept de *grande stratégie* et les visions concurrentes tentant de s'imposer auprès des décideurs américains dans la formulation de celle des É.-U. Ces visions seront abordées afin de déterminer laquelle correspond à la grande stratégie adoptée par l'administration Obama dès son premier mandat. Ce chapitre démontrera que celle-ci correspond à celle de l'*engagement sélectif*, alors que sous Obama, la politique étrangère américaine s'est partiellement retranchée afin de mieux concentrer ses efforts sur les intérêts nationaux jugés les plus importants. Pour ce faire, les É.-U. cherchent à mettre en place un *équilibre de la menace* dans une région potentiellement déterminante : l'Asie du Sud-Est et son plus grand acteur, la menace potentielle que peut représenter la Chine.

Le second chapitre abordera l'interprétation américaine des cybercapacités chinoises et les inquiétudes qu'elles sèment au sein de la communauté stratégique américaine. La première partie vise à effectuer une étude empirique des nombreux cas référencés de

cyberintrusions attribués à la Chine, permettant d'aborder la première interprétation américaine ayant été faite de ces capacités, soit celle d'une menace principalement économique. Ces cyberattaques chinoises ont ensuite été abordées comme une *menace à la sécurité nationale*, dès lors perçues comme étant offensives par leurs caractéristiques techniques et par l'exploitation potentielle qu'elles font de vulnérabilités présentes dans d'importants systèmes informatiques américains. Ces infiltrations sont aussi considérées comme un prélude plausible à des attaques d'une grande envergure dans un éventuel conflit entre la Chine et les É.-U. ou un de ses alliés. De plus, l'existence d'une littérature stratégique chinoise évoquant l'utilisation de cybercapacités consolide la perception américaine qu'elles représentent une menace crédible nécessitant des mesures importantes de défense, entreprises par un *rééquilibrage interne* des capacités américaines œuvrant dans le domaine du cyberespace.

Le troisième et dernier chapitre abordera la manière dont les É.-U. ont entrepris de rétablir l'équilibre de la menace, équilibre que l'utilisation de cybercapacités avait fait pencher en faveur de la Chine. Il sera tout d'abord question de l'institutionnalisation de cette militarisation, notamment par la renaissance d'une NSA devenue indispensable à l'élaboration d'une cyberdoctrine américaine, et de la mise en place du USCYBERCOM, au sein duquel l'agence de renseignement joue un rôle central et essentiel. Finalement, il sera question de ce que font ces organisations afin d'atteindre le but pour lequel elles ont été créées, mais aussi de la nature et l'articulation de la réplique américaine dans le cyberespace. Cette partie portera principalement sur les deux pans d'une stratégie de dissuasion à l'attention de la Chine : une dissuasion axée sur le renforcement de l'aspect défensif, en étanchéifiant les réseaux afin de rendre possible une dissuasion par *déni de bénéfices*, mais aussi d'une stratégie dissuasive basée sur les *risques de représailles*. Pour atteindre son objectif, cette dernière nécessite l'augmentation de la cyberpuissance américaine, de sa capacité de projection et son apport indispensable au maintien de la puissance relative avantageuse que détiennent les É.-U. au niveau des capacités conventionnelles, notamment par l'entremise de la stratégie du *Air-Sea Battle*.

CHAPITRE I
CADRE THÉORIQUE

> Un pessimiste voit la difficulté dans chaque opportunité, un optimiste voit une opportunité dans chaque difficulté.
>
> Winston Churchill

Peu importe l'époque, toutes les grandes puissances ont des objectifs à atteindre, des avantages stratégiques à préserver ou des intérêts nationaux à défendre. Si l'actualité nous dépeint la politique étrangère d'un État comme étant une succession de problèmes et d'évènements provoquant une réaction et nécessitant une solution rapide, cette même politique étrangère découle tout d'abord d'une *grande stratégie* visant la poursuite et l'atteinte d'un ou plusieurs objectifs nationaux s'échelonnant sur le long terme[51], comme le furent la *realpolitik* d'Otto von Bismarck ou le *containment* de George Kennan. Pour Paul Kennedy, « l'élément central de la grande stratégie réside donc dans les politiques entreprises, c'est-à-dire dans la capacité du chef de la nation à rassembler tous les éléments, aussi bien militaires que non militaires, nécessaires à la préservation et au renforcement, à long terme, des intérêts supérieurs de la nation.[52] » Si ce sont les aspects militaire et diplomatique qui sont traditionnellement associés à ce niveau stratégique, tous les *moyens disponibles*, qu'ils soient par exemple financiers, commerciaux ou éthiques, sont nécessaires à l'avancement des prérogatives d'un État, à l'affaiblissement de la volonté

---

[51] Pour Williamson Murray, « ce qui distingue les dirigeants qui ont tenté de développer et de mettre en œuvre une grande stratégie est leur attention à agir au-delà des demandes du présent. En d'autres mots, ils ont adopté une vision plus grande que de simplement réagir aux évènements quotidiens ». Williamson Murray. « Thoughts on grand strategy » dans Williamson Murray, Richard Hart Sinnreich et James Lacey, *The Shaping of Grand Strategy : Policy, Diplomacy and War*, New York : Cambridge University Press, 2011, p.3

[52] Traduction libre. Paul Kennedy. « Grand Strategy in War and Peace : Toward a Broader Definition » dans Paul Kennedy, *Grand Strategies in War and Peace*, New Haven, London : Yale University Press, 1991, p.5

d'un adversaire et à l'assurance d'être dans la meilleure position possible advenant le déclenchement d'un conflit militaire[53], mais aussi à obtenir une situation de paix plus avantageuse[54]. Il est également nécessaire de considérer des éléments hors du contrôle des dirigeants, mais tout aussi importants : alors que la position géographique d'un État a un impact certain sur l'élaboration historique et sur les modalités possibles de sa grande stratégie[55], il est primordial d'y inclure aussi le facteur national, où les éléments de la politique intérieure peuvent influer sur la formulation de la politique étrangère et faciliter la mise en œuvre de la *grande stratégie* ou y nuire. Pour un dirigeant, il s'agit donc d'articuler cette variété d'outils ou de contraintes afin d'atteindre ses objectifs stratégiques et protéger les intérêts nationaux de son pays.

Évidemment, le nombre d'intérêts pouvant être qualifiés de vitaux varie en fonction des personnes, de leur vision du monde et de leur perception de la place et de la puissance de leur État dans celui-ci. Ainsi, ces grandes stratégies doivent faire l'objet d'un rigoureux effort d'équilibre entre les *résultats* désirés et les *moyens* disponibles pour les obtenir[56], ces derniers étant souvent limités à ce que la capacité économique d'un pays permet de faire, d'où la nécessité, lors de la mise en place d'une *grande stratégie*, d'établir des priorités. Aspect déterminant dans le succès ou l'échec d'une telle entreprise, ce sera finalement la vision du monde des décideurs politiques qui tranchera le débat concernant les intérêts nationaux à défendre et la manière de le faire avec les moyens mis à

---

[53] Basil Liddell Hart, dans Paul Kennedy, *op.cit.*, p.6

[54] Paul Kennedy, *op.cit.*, p.4

[55] Pour Murray, la position géographique d'un État et le contexte historique qui l'accompagne contribuent grandement au développement et à l'articulation d'une grande stratégie. Il affirme que le facteur de « la position géographique a mené les administrations politiques britanniques et américaines à penser à la grande stratégie en termes de projection de la puissance militaire. ». Murray, *op.cit.*, p.12 – 13.

[56] La grande majorité des auteurs traitant de la question souligne l'importance de cet équilibre dans le succès d'une grande stratégie. Paul Kennedy, *op.cit.*, p.5; David S. McDonough. « Beyond Primacy : Hegemony and 'Security Addiction' in U.S. Grand Strategy », *Orbis*, vol.53, no.1, 2009, p.7; Clark Murdock et Kevin Kallmyer. « Applied Grand Strategy : Making Tough Choices in an Era of Limits and Constrait », *Orbis*, vol.55, no.4, 2011, p.547 – 548; Murray, *op.cit.*, p.21; Richard Hart Sinnreich. « Patterns of grand strategy » dans Williamson Murray, Richard Hart Sinnreich et James Lacey, *The Shaping of Grand Strategy : Policy, Diplomacy and War*, New York : Cambridge University Press, 2011, p.263

disposition.[57] Cette première sous-section de notre cadre théorique servira à identifier les *grandes stratégies* à la disposition de l'administration Obama à son arrivée au pouvoir et à déterminer laquelle a été retenue, en observant les décisions et initiatives entreprises essentiellement lors de son premier mandat.

1.1 Le marché des idées concernant la grande stratégie américaine et sa définition

Depuis l'accession des É.-U. dans le cercle privilégié des grandes puissances, les grandes stratégies adoptées ont varié au gré de sa puissance relative, mais aussi de la vision du monde qu'adoptaient ses dirigeants : de l'isolationnisme, tendance dominante jusqu'à l'intervention militaire américaine lors de la Seconde Guerre mondiale, ils sont devenus une superpuissance maximaliste par l'entremise du *containment* de Kennan : la rivalité avec l'URSS mena à une multiplication de ce qui était considéré comme des intérêts nationaux requérant une présence et une participation militaire accrue et étendue afin de les défendre. À la suite de la chute de l'adversaire soviétique, les É.-U. devenaient donc la plus grande puissance du système international, ouvrant un nouveau chapitre de sa politique étrangère. Depuis la fin de la guerre froide, le système international est effectivement marqué par la prééminence des capacités américaines (militaires, économiques, culturelles ou technologiques[58]), menant à une situation d'*unipolarité* divisant les politologues sur les conséquences d'une telle configuration du système international.

D'entrée de jeu, l'unipolarité se définit comme étant « une structure dans laquelle les capacités d'un État s'avèrent trop grandes pour être contrebalancées.[59] » Nombreux sont ceux qui ont salué cette victoire américaine sur l'adversaire soviétique et qui, à l'image de Francis Fukuyama et sa vision de la *fin de l'Histoire*, ont vu dans ce déséquilibre

---

[57] Christopher Layne. « From Preponderance to Offshore Balancing: America's Future Grand Strategy », *International Security*, vol.22, no.1, 1997, p.88; Murray, *op.cit.*, p.8

[58] Stephen G. Brooks et William C. Wohlforth. « American Primacy in Perspective », *Foreign Affairs*, vol.81, no.4, 2002, p.21-23

[59] William C. Wohlforth. « The Stability of Unipolar World ». *International Security*, vol.24, no.1, 1999 p.9

important le début d'une ère de paix, de stabilité et de prospérité dirigée[60] par l'*hégémon bienveillant* que seraient les É.-U., dont la puissance inégalée servirait les intérêts des autres États plutôt que de les menacer[61]. De l'autre côté, ceux adhérant à la théorie néo-réaliste (ou du réalisme structurel) et au principe de l'*équilibre de la puissance* estiment que cette situation de domination américaine n'est ni pérenne ni stabilisatrice du système international.

Pour eux, le *moment unipolaire* n'est qu'un intermède vers un retour à la normalité du système international, soit une situation de *multipolarité* où les grandes puissances rivalisent entre elles. John Mearsheimer affirmera même que l'unipolarité tant annoncée n'en est pas une : les É.-U. seraient plutôt un hégémon régional qui, malgré la prépondérance de leurs capacités, doivent composer avec d'autres grandes puissances pouvant se tirer d'affaire contre le géant américain, comme la Russie ou la Chine[62]. Samuel Huntington en arrive aussi à ces conclusions lorsqu'il parle d'*unimultipolarité*, un monde composé de la superpuissance américaine, dont la puissance a une portée mondiale, mais aussi de plusieurs grandes puissances régionales faisant obstruction à cette dernière, préférant poursuivre leurs propres intérêts que de se soumettre aux volontés des É.-U.[63]

En 1996, Barry Posen et Andrew L. Ross ont répertorié quatre *grandes stratégies* dont on a fait la promotion au sein de la communauté stratégique américaine et qui tentent de s'imposer dans le discours public[64]: le *néo-isolationnisme*, l'*engagement sélectif*, la *sécurité coopérative* et la *primauté*. Dans ce mémoire, le néo-isolationnisme ne sera toutefois pas abordé, car ce discours demeure marginal, principalement représenté par des hommes et femmes politiques à tendance libertaire comme Ron Paul et son fils,

---

[60] *Ibid.*, p. 5-9
[61] Robert Kagan. « The Benevolent Empire », *Foreign Policy*, no.111, 1998, p.26 – 30.
[62] Mearsheimer. *The Tragedy of Great Power Politics*, *op.cit.*, p.381 – 382.
[63] Samuel Huntington. « The Lonely Superpower », *Foreign Affairs*, vol.78, no.2, 1999, p.35 – 37.
[64] Barry R. Posen et Andrew L. Ross. « Competing Visions for U.S. Grand Strategy ». *International Security,* vol.21, no.3, 1996, p.5

Rand.[65] Grande stratégie basée sur l'idée que la puissance américaine ne devrait chercher à défendre que le territoire national et à intervenir minimalement et uniquement pour sceller l'issue d'un conflit, comme ce fut le cas dans les deux guerres mondiales, ses partisans se font rares autant dans l'espace public que dans l'arène politique américaine contemporaine[66]. Alors qu'Obama a poursuivi l'implication américaine dans le monde en maintenant une présence militaire en Afghanistan et en appuyant une attaque sur la Libye, le néo-isolationnisme peut difficilement être considéré comme une piste de réponse à nos questions, bien qu'elle demeure une vision tout à fait légitime.

Par conséquent, les trois autres *grandes stratégies* seront comparées selon cinq indicateurs qui nous permettent de bien les distinguer les unes des autres et de faciliter l'analyse de la politique étrangère américaine d'Obama (tableau 1): ce qu'elles perçoivent comme étant le problème majeur dans la politique internationale; l'ordre mondial qu'elles privilégient; leur conception des intérêts nationaux vitaux que les É.-U. doivent défendre; leur priorité régionale et les moyens que doivent entreprendre les É.-U. afin de régler le principal problème du système international.

Elles seront également abordées selon leur position sur l'unipolarité américaine : deux d'entre elles, la sécurité coopérative et la primauté, estiment que les É.-U. sont une superpuissance bienveillante, possédant des intérêts multiples aux quatre coins du monde et dont le leadership est nécessaire à la stabilité et à la sécurité du système international. Le maintien de cette prééminence devient donc un intérêt en soi et nécessite que les É.-U. s'impliquent à l'échelle planétaire : depuis 1991, de Bush père à G.W. Bush, en

---

[65] Michael A. Cohen. « The World According to Ron Paul », *Foreign Policy*, 23 décembre 2011. En ligne, <foreignpolicy.com/2011/12/23/the-world-according-to-ron-paul/>; Pour Ron Paul, le terme *isolationnisme* est trompeur et il se revendique davantage du *non-interventionnisme*, où les É.-U., malgré leur retrait militaire complet des affaires du monde, maintiendraient néanmoins une ouverture sur le monde par leurs activités diplomatiques et commerciales. CNN. « Ron Paul : I'm no isolationist ». *The Situation Room*, 15 décembre 2011. Vidéo en ligne, <www.youtube.com/watch?v=UNOMmUQYlC4>

[66] Michael Cohen. « The Non-Return of American Isolationism ». *The Atlantic*, 24 juillet 2011. En ligne, <www.theatlantic.com/international/archive/2011/07/the-non-return-of-american-isolationism/241927/>. Consulté le 28 septembre 2015; Colin Dueck. *The Obama Doctrine : American Grand Strategy Today*. Oxford (R.-U.); New York : Oxford University Press, 2015, p.134

passant par Clinton, la politique étrangère américaine reposait sur l'idée que les É.-U. étaient « la nation indispensable[67] ». De son côté, l'*engagement sélectif* ne considère pas que les grandes stratégies basées sur le maintien de l'hégémonie américaine et la protection des intérêts nationaux soient viables. Alors que le système international est marqué par l'émergence de plusieurs États, diminuant donc la puissance relative américaine, une telle grande stratégie s'avère coûteuse, dommageable et provoque inévitablement des réactions hostiles, rendant ainsi difficile la protection des intérêts vitaux américains. Avant son élection, Obama critiquait fortement les décisions de politique étrangère ayant été prises par son prédécesseur[68], propos sous-tendant un changement majeur dans la *grande stratégie* américaine qui serait adoptée par son administration. La changer, oui, mais pour laquelle?

[67] Expression popularisée par Madeleine Albright, ambassadrice américaine à l'ONU de 1993 à 1997.
[68] Barack Obama. « Renewing American Leadership ». *Foreign Affairs*, vol.86, no.4, 2007, p.2

Tableau 1.1 - Les trois grandes stratégies américaines possibles sous Obama

	Sécurité coopérative	**Primauté**	**Engagement sélectif**
Problème majeur en politique internationale	Foyers locaux d'instabilité pouvant menacer la paix mondiale	Émergence d'un concurrent sérieux et la perte de la prépondérance américaine	Conflits entre les grandes puissances.
Ordre mondial privilégié	Interdépendance	Hégémonique	Équilibre de la puissance
Conception des intérêts nationaux	Transnationale	De nature variée et géographiquement étendus	Limitée
Priorités régionales	Le monde entier	Eurasie industrielle et la région d'un potentiel concurrent sérieux	Eurasie industrielle
Moyens de régler le problème	Organisations internationales et accords internationaux dissuadant, contrant et punissant les agressions. Créer une situation d'interdépendance pacificatrice	Maintien d'une supériorité militaire américaine vis-à-vis ses rivaux afin de les dissuader et de maintenir la paix	Alliances traditionnelles et présence militaire suffisante pour permettre une dissuasion et maintenir la paix

Source : Barry R. Posen et Andrew L. Ross. « Competing Visions for U.S. Grand Strategy ». *International Security*, vol.21, no.3, 1996, p.6

1.1.1 La sécurité coopérative

Sur la scène internationale, si certains estiment que les É.-U. devraient se limiter au strict nécessaire en ce qui a trait à leur sécurité, d'autres prônent plutôt une plus grande implication. Ces derniers estiment que la paix mondiale, considérée comme un intérêt national majeur, est universelle et que les sources de menaces pouvant la perturber sont multiples et de nature variée, dépassant ainsi le cadre réaliste s'attardant principalement aux capacités et intentions des autres États. Pour eux, même les turbulences les plus lointaines peuvent perturber la stabilité internationale et, par le fait même, avoir des conséquences importantes sur la sécurité nationale américaine[69].

Pour contrôler et éteindre ces foyers d'instabilité, il est nécessaire pour les É.-U. d'étendre et de préserver l'ordre libéral international qu'ils ont mis en place après la Seconde Guerre mondiale. Basé sur la démocratisation, l'ouverture et la transparence des États, cet ordre vise à faciliter les interactions, à permettre l'ancrage et le respect de règles et d'institutions favorisant à long terme les échanges commerciaux et les gains économiques au détriment du bellicisme, objectifs dont l'atteinte améliorerait fortement la sécurité de tous ses membres[70]. Bien sûr, les É.-U. ne cherchent pas à étendre cet ordre aux seules fins altruistes, celui-ci leur permettant également de modeler le système international conformément à leurs intérêts[71] : gérer et réduire les menaces à la sécurité nationale américaine, maximiser leur propre prospérité économique par l'ouverture et la pacification de marchés, et mettre en place des institutions où les États coopéreront en termes favorables aux intérêts américains[72].

---

[69] Posen et Ross, *op.cit.*, p.23 – 24.

[70] G. John Ikenberry. « The Future of the Liberal World Order : Internationalism After America ». *Foreign Affairs*, vol.90, no.3, 2011, p.62; G. John Ikenberry. *Liberal Leviathan : The Origins, Crisis, and Transformation of the American World Order*. Princeton, New Jersey; Princeton University Press, 2011, p.282

[71] G. John Ikenberry, « An Agenda for Liberal International Renewal ». Dans Michèle Flournoy et Shawn Brimley (eds.). *Finding our Way : Debating American Grand Strategy*, Washington D.C : Center for a New American Century, Solarium Strategy Series, 2008, p.46

[72] Stephen G. Brooks, G. John Ikenberry et William C. Wohlforth, « Don't Come Home, America : The Case Against Retrenchment », *International Security*, vol.37, no.3, 2012, p.11

Contrairement aux grandes stratégies reposant sur une vision *réaliste* des relations internationales, la sécurité coopérative s'appuie sur la théorie libérale et sur le concept d'*interdépendance*, où des situations particulières mènent à des « effets réciproques entre des pays ou entre des acteurs de différents pays.[73] » La sécurité et la vigueur économique d'un État sont donc inextricablement liées à celles des autres. Si l'ouverture des frontières et la facilité des échanges amènent un lot de bénéfices aux acteurs impliqués, les problèmes apparaissant dans un pays ou une région du globe peuvent également avoir des conséquences importantes, directes ou non, sur une multitude d'États. Ainsi, d'un *jeu à somme nulle* que représente le système international pour les réalistes, il devient ici un *jeu à somme absolue*, où « les États se soucient peu des bénéfices que peuvent soutirer leurs rivaux lorsqu'ils font leurs choix politiques, mais tendent au contraire à prioriser leur propre bien-être avant tout.[74] »

Pour en préserver les bienfaits, il est essentiel de limiter les perturbations pouvant ébranler l'ordre libéral, notamment en s'attaquant aux dangers que représentent les conflits interétatiques dits *traditionnels*. Si les perspectives réalistes s'attardent principalement aux dynamiques de rivalités et de tensions interétatiques, la sécurité coopérative cherche à prévenir plutôt qu'à « guérir » *a posteriori* les conflits pouvant se déclencher :

> [...] la sécurité coopérative modifie l'élément central de la planification sécuritaire : au lieu de se préparer à affronter des menaces, il s'agit de prévenir l'émergence de celles-ci – autant en dissuadant les agressions qu'en rendant plus difficile leur préparation.[75]

La protection des intérêts nationaux américains est aussi intimement liée à des problématiques *transnationales*, dépassant le cadre national et touchant plusieurs pays simultanément. Que ce soient les guerres civiles ou intraétatiques, la question des États

---

[73] Traduction libre. Robert Keohane et Joseph S. Nye. *Power and Interdependance : World Politics in Transition*. Boston : Little, Brown, 1977, p.7

[74] Marie-Ève Desrosiers et Justin Massie. « Le néolibéralisme et la synthèse néo-néo » dans Alex Macleod et Dan O'Meara (dir.). *Théorie des relations internationales : contestation et résistance*, Montréal : Athéna Éditions, 2007, p.160

[75] Traduction libre. Ashton B. Carter, William James Perry et John D. Steinbrunner. *A New Concept of Cooperative Security*. Washington D.C. : Brookings Institution, 1992, p. 7

faillis[76], les conséquences du réchauffement climatique, la prolifération nucléaire, la piraterie internationale, le terrorisme djihadiste, la sécurité énergétique ou les pandémies, etc., « chacune de ces menaces peut mettre en danger la vie et le mode de vie des Américains, directement ou indirectement, en déstabilisant le système global dont dépendent la sécurité et la prospérité américaine.[77] » Ces sources de menaces mondialement disséminées créent une situation d'*interdépendance stratégique* incitant les différents États à s'y attaquer collectivement. Dans ce but, les partisans de la *sécurité coopérative* misent sur les organisations internationales (OI), l'*Organisation des Nations Unies* (ONU) en tête, afin de coordonner des actions collectives et multilatérales à entreprendre afin de les contrer : implantation de mécanismes de contrôle des armements et de mesures favorisant la transparence, la confiance interétatique et atténuant les dilemmes de sécurité, dissuasion des agressions par la formation d'une coalition de grandes puissances engagées à intervenir militairement pour les contrer ou la formation de contingents militaires internationaux pouvant mener des interventions humanitaires.[78]

Bien que cette grande stratégie soit principalement axée sur le multilatéralisme et la participation internationale que permettent ces institutions, les É.-U. demeurent toutefois le plus important pôle du système international en raison de leur supériorité militaire et technologique[79]. Ainsi, si la communauté internationale devait mener d'éventuelles interventions humanitaires, punir un État agresseur ou empêcher un État d'obtenir des armes de destructions massives, incluant l'arme nucléaire[80], les É.-U. seraient forcément le ou l'un des meneurs de ces opérations. Par le fait même, les Américains se portent garants de la sécurité et de la stabilité d'un ordre mondial dont ils ont permis l'instauration et qui profitent, en fin de compte, à tous.

---

[76] Posen et Ross, *op.cit.*, p.23; Gareth Evans, « Cooperative Security and Intrastrate Conflict », *Foreign Policy*, no.96, 1994, p.11

[77] G. John Ikenberry. *Liberal Leviathan*, p.295

[78] Posen et Ross, *op.cit.*, p.23 – 26.

[79] *Ibid.*, p.24 ; G. John Ikenberry, Michel Mastanduno et William C. Wohlforth. « Unipolarity, State Behavior, and Systemic Consequences ». *World Politics*, vol.61, no.1, 2009, p.6 – 10.

[80] Posen et Ross, *op.cit.*, p.28, McDonough, *op.cit.*, p.9

1.1.2 La stratégie de primauté

Pour d'autres, les É.-U. devraient adopter une grande stratégie dite de *primauté*, voulant elle aussi préserver la distribution inégale de la puissance post-Guerre froide, mais pour des raisons et par des moyens différents. Pour eux, le maintien de la toute-puissance américaine est primordial, car elle permet de pacifier et de stabiliser un système international en proie aux perturbations inhérentes à la multipolarité, tout en assurant la sécurité des intérêts américains et celle de ses alliés[81].

La plus grande crainte des partisans de la primauté est l'émergence d'un concurrent étatique sérieux pouvant menacer la prépondérance américaine et rendre le système international instable. Il est donc nécessaire pour les É.-U. de continuer à distancer, autant militairement, économiquement que politiquement, tous ses compétiteurs actuels et potentiels. Dès 1992, la *doctrine Wolfowitz,* contenue dans la première mouture du *Defense Planning Guidance* (DPG)[82] abordait particulièrement cet objectif :

> Notre premier objectif est d'éviter la réémergence d'un nouveau rival constituant une menace de l'ampleur de celle qu'était l'Union soviétique. [...] notre stratégie doit se recentrer sur un appui à notre politique de sécurité nationale visant à empêcher le développement d'une quelconque entité hostile potentielle qui pourrait se donner comme objectif une domination régionale ou mondiale et entrer en compétition avec les É.-U. et leurs alliés.[83]

Loin d'être une ambition ponctuelle, celle-ci s'est également manifestée de manière explicite dix ans plus tard au sein de la première mouture de la *National Security Strategy* (NSS) de l'administration G.W. Bush[84].

---

[81] Posen et Ross, *op.cit.*, p.30; William Kristol et Robert Kagan, « Toward a Neo-Reaganite Foreign Policy », *Foreign Affairs*, vol.75, no.4, 1996, p.23; De son côté, Charles Krauthammer ira jusqu'à dire que « l'alternative à l'unipolarité est le chaos », dans « The Unipolar Moment », *Foreign Affairs*, vol.70, no.1, 1990, p.32; Samuel Huntington. « Why International Primacy Matters ». *International Security*, vol.17, no.4, 1993, p.83

[82] Document du département de la Défense explicitant ses grandes orientations.

[83] Traduction libre. États-Unis, Department of Defense. *Defense Planning Guidance, FY 1994-1999.* Washington D.C. : Department of Defense, 1992. PDF en ligne, <www.archives.gov/declassification/iscap/pdf/2008-003-doc18.pdf>, p.2 – 12. Consulté le 3 octobre 2015.

[84] États-Unis, White House. *The National Security Strategy of the United States of America.* Washington D.C. : White House, 2002. PDF en ligne, <nssarchive.us/NSSR/2002.pdf>, p.30. Consulté le 3 octobre 2015

Pour maintenir cet ascendant sur les autres grandes puissances et alliés, il est nécessaire de les convaincre que le maintien de la suprématie américaine demeure le meilleur garant de la protection de leurs intérêts. Constatant que la bienveillance américaine procure sécurité et maintien de l'ordre international, les autres grandes puissances ne peuvent faire autrement que d'arrimer leur politique étrangère à celle des É.-U.[85], profitant également des retombées que procure la *pax americana*. En plus de préserver la prééminence de la puissance américaine, cette supériorité écrasante[86] permet de calmer les tensions existantes entre les grandes puissances, les É.-U. possédant la capacité de faire pencher la balance dans un éventuel conflit[87].

Si la principale priorité géographique des É.-U. est l'Eurasie industrielle, riche en ressources et où l'émergence d'un sérieux concurrent serait la plus risquée, il demeure important pour la superpuissance américaine de s'attaquer à une autre source d'instabilité pouvant survenir dans n'importe quel théâtre régional : la prolifération d'armes nucléaires ou de destruction massive. Souvent entre les mains d'États cherchant à s'opposer et à résister à la puissance américaine[88], ces derniers représentent un danger, car ils « minent la liberté d'action des É.-U. en augmentant les coûts et les risques liés aux interventions militaires américaines à travers le monde.[89] » En limitant la capacité des É.-U. à maintenir l'ordre et la sécurité du système international, les États de second ordre possédant ce type d'armes peuvent non seulement mettre en péril l'équilibre de leur région, mais aussi celle du monde entier.

Ces deux problématiques menaçant les intérêts nationaux américains nécessitent donc de grands moyens. Alors que la sécurité coopérative cherche à faire des É.-U. un partisan et porte-parole d'un multilatéralisme visant à atteindre une situation de paix mondiale par

---

[85] Posen et Ross, *op.cit.*, p.31-32; Krauthammer, *op.cit.*, p.25; Bradley A. Thayer. « In Defense of Primacy », The National Interest, no.86, 2006, p.33; « Excerpts From Pentagon's Plan: 'Prevent the Re-Emergence of a New Rival' », *The New York Times*, 8 mars 1992. En ligne, <www.nytimes.com/1992/03/08/world/excerpts-from-pentagon-s-plan-prevent-the-re-emergence-of-a-new-rival.html?pagewanted=all>. Consulté le 3 octobre 2015.

[86] Kristol et Kagan, *op.cit.*, p.20

[87] Posen et Ross, *op.cit.*, p.30; McDonough, *op.cit.*, p.9; Pour Kristol et Kagan, « plus Washington est capable de clarifier le fait qu'il est futile d'entrer en compétition avec la puissance américaine, que ce soit en terme de la taille de ses forces ou de ses capacités technologiques, moins les chances sont grandes que des pays comme la Chine ou l'Iran caressent l'ambition de bouleverser l'ordre mondial actuel », p.26

[88] Krauthammer, *op.cit.*, p.31; Thayer, *op.cit.*, p.34

[89] Traduction libre. Posen et Ross, *op.cit.*, p.38

la prévention et la résolution de telles perturbations au sein des OI, la grande stratégie de *primauté* mise sur la puissance brute comme force pacificatrice, utilisée selon le principe de l'unilatéralisme : les OI, par leur aspect consensuel et démocratique, sont jugées inefficaces au maintien de la paix et contraignent la volonté américaine à exercer son rôle et à mener à bien son devoir international, que ce soit par elle-même ou par la formation d'une coalition *ad hoc* composée d'alliés. Pour Charles Krauthammer, « l'unilatéralisme ne signifie pas d'agir seul. [...] L'unilatéralisme signifie simplement de ne pas se laisser être l'otage des autres.[90] »

Afin d'instaurer une dynamique de dissuasion et d'intervenir si nécessaire, il est primordial d'avoir des forces armées importantes postées aux quatre coins du monde, exigence nécessitant des investissements colossaux, notamment par l'acquisition et la modernisation technologique constante de ses équipements, un avantage américain devant être préservé afin qu'il demeure insurmontable. Ce recours à la haute technologie permet également de faciliter les interventions en les rendant plus précises, moins risquées et plus efficaces[91]. Même si ces entreprises sont forcément coûteuses, elles sont, pour plusieurs, un mal nécessaire afin d'assurer la protection des intérêts américains. Les partisans de cette approche estiment que les É.-U., première puissance économique, peuvent aisément se payer un tel dispositif de défense, les dépenses de ce secteur particulier n'équivalant qu'à une petite partie de son PIB. Certains désirent même augmenter considérablement ces investissements, le seul obstacle n'étant pas la précarité des ressources, mais bien le manque de volonté politique à s'y investir véritablement[92].

1.1.3 L'engagement sélectif

En revanche, d'autres estiment que les É.-U. doivent restreindre leur activisme international. Sans militer pour le retrait total des É.-U. des affaires mondiales, ils préconisent toutefois une réduction importante des intérêts nationaux considérés comme

---

[90] Traduction libre. Charles Krauthammer. « The Unipolar Moment Revisited », *The National Interest*, no.70, 2003, p.17

[91] Brooks et Wohlforth, *op.cit.*, p.22 – 23.

[92] Robert Kagan et William Kristol. « Burden of Power is Having to Wield It », *The Washington Post*, 19 mars 2000. En ligne, <carnegieendowment.org/2000/03/19/burden-of-power-is-having-to-wield-it/77e>. Consulté le 4 octobre 2015; Posen et Ross, *op.cit.*, p.33; Kagan et Kristol, *op.cit.*, p.23 – 24.

vitaux, ou d'une très grande importance, et dont la protection nécessite un effort proportionnel de défense. Ceux prônant un *engagement sélectif* comme ligne directrice de la politique étrangère américaine, comme Robert J. Art ou Barry Posen, considèrent qu'un trop grand engagement américain risque de mener les É.-U. à une situation de surextension pouvant avoir des conséquences périlleuses[93]. Ainsi

> [...] compte tenu d'un environnement international anarchique, le nombre de menaces possibles est grand, et étant donné les limites inéluctables d'une économie nationale, les ressources se font rares et puisque les ressources sont rares, les moyens militaires les plus appropriés devront être sélectionnés pour atteindre les fins politiques désirées.[94]

Il apparaît donc nécessaire de réviser ou de revoir l'ampleur des priorités de la politique étrangère américaine. L'attention et les ressources étatiques doivent être attribuées spécifiquement aux sources majeures de dangers et la force militaire doit être adaptée à ces réalités budgétaires. Pour Thomas M. Skypek, trois grands piliers servent à définir un intérêt à défendre ou un danger à affronter: ce qui menace « (1) la souveraineté et l'intégrité territoriale des É.-U.; (2) la sécurité et la liberté des citoyens américains et; (3) la capacité à mener des échanges et à se livrer au commerce[95] ».

Malgré tout, les penseurs de l'engagement sélectif divergent sur le nombre et la nature des intérêts nationaux devant être poursuivis, ces piliers pouvant être interprétés de diverses façons et résulter en un nombre variable de menaces à affronter et d'intérêts à protéger[96]. Toutefois, outre la protection du territoire américain, une menace majeure à la sécurité des É.-U. demeure récurrente : le maintien de la paix entre les grandes puissances. L'éventualité d'un conflit majeur représente un danger constant pour les É.-U. pour deux raisons : d'une part, il mettrait en péril les intérêts économiques et commerciaux américains dans le théâtre régional touché et d'autre part, il nécessiterait

---

[93] Posen et Ross, *op.cit.*, p.16; Owen Harries et Tom Switzer. « Leading from Behind : Third Time a Charm », *The American Interest*, vol.8, no.5, 2013, p.14; Robert J. Art. « Selective Engagement After Bush ». Dans Flournoy et Brimley (eds.), *op.cit.*, p.26

[94] Traduction libre. Barry Posen, *The Sources of Military Doctrine*, *op.cit.*, p.13

[95] Thomas M. Skypek. « A Grand Strategy for Rand Paul ». *The National Interest*, 28 mars 2014. En ligne, <nationalinterest.org/commentary/grand-strategy-rand-paul-10147>. Consulté le 22 septembre 2015.

[96] Par exemple, Art évoque six objectifs devant être absolument poursuivis dans l'intérêt des É.-U., alors que, de son côté, Posen n'en privilégie que trois. Barry R. Posen. « Pull Back : The Case for a Less Activist Foreign Policy ». *Foreign Affairs*, vol.92, no.1. 2013, p.123.

de facto l'implication de la puissance américaine dans l'un des camps[97]. Dès lors, les É.-U. doivent agir de sorte à dissuader les grandes puissances de leur déclarer la guerre, directement ou par l'entremise d'un allié, en leur faisant comprendre qu'ils posséderaient, le cas échéant, la puissance militaire suffisante pour empêcher la victoire de l'agresseur et initiateur du conflit[98].

Robert J. Art dira même que « l'engagement sélectif est une stratégie qui cherche à modeler, et non pas à contrôler, l'environnement international.[99]» En détenant une puissance militaire dissuasive et en limitant les escalades de tensions entre compétiteurs régionaux, les É.-U. peuvent donc créer et imposer un équilibre dans chaque région dont l'embrasement représenterait un danger important. La sélectivité de cette grande stratégie oblige également les décideurs à se concentrer sur des régions géographiques précises, d'une plus grande valeur et aux dangers potentiels plus élevés. L'engagement sélectif s'intéresse donc principalement au continent eurasien, plus particulièrement l'Europe et l'Asie de l'Est, régions populeuses, riches et aux enjeux plus nombreux et plus importants pour les É.-U.[100]

Cette intention de pacifier les diverses régions se concrétise par l'établissement et le maintien de partenariats ou d'alliances formelles avec des acteurs régionaux, servant à rendre concrète et plus crédible la volonté américaine d'y maintenir le *statu quo*. En plus de favoriser le dialogue, la transparence et la coopération entre les alliés, diminuant la méfiance et la peur souvent initiatrices de conflits, ces relations particulières permettent également une présence militaire américaine par l'implantation de bases avancées. Celles-ci facilitent la projection de la puissance des É.-U. et renforcent la crédibilité de leur engagement à maintenir le statu quo en dissuadant les conflits ou en y participant de manière décisive s'il devait en survenir un[101]. Au-delà de ces ententes formelles, il est essentiel pour les É.-U. de préserver ce qui leur permettrait de les respecter intégralement,

---

[97] Robert J. Art « Geopolitics Updated : The Strategy of Selective Engagement », *International Security*, vol.23, no.3, 1998, p.29

[98] Posen et Ross, *op.cit.*, p.15 – 16.

[99] Robert J. Art. *Selective Engagement After Bush* , *op.cit.*, p.32

[100] Posen et Ross, *op.cit.*, p.18

[101] Robert J. Art. *Selective Engagement After Bush* , *op.cit.*, p.32 – 34.

c'est-à-dire le contrôle sur les *espaces communs mondiaux*, que ce soit les cieux, les mers, l'espace et, désormais, le cyberespace.

Pour Barry Posen, ce contrôle signifie que les É.-U. peuvent librement utiliser ces espaces communs mondiaux à des fins militaires. Ce libre accès ne rend pas seulement possible tout déplacement de forces armées, mais également de dissuader crédiblement de potentiels adversaires : ce contrôle géographique complet permet aux É.-U. d'en interdire l'accès aux opposants, en limitant les capacités opérationnelles adverses, et d'ainsi leur démontrer que les tentatives d'en empêcher l'accès aux forces militaires américaines résulteraient en une défaite militaire inévitable[102]. Pour les É.-U., cette capacité de pouvoir couper aisément les lignes de communication adverses et de déplacer à tout moment, rapidement et sans encombre les éléments constituant sa puissance militaire s'avère être une nécessité pour un *engagement sélectif* réussi.

Récemment, certains partisans de l'engagement sélectif ont réévalué leur position et ont revu à la baisse ce qu'ils considèrent comme étant des intérêts nationaux à défendre, tout en corrigeant la manière de le faire. Par l'adoption d'une politique de *retenue* ou d'*équilibrage à distance* (*offshore balancing*), des gens comme Barry Posen ou Stephen Walt estiment que la préservation du libre accès américain aux régions-clés et aux espaces communs mondiaux est un aspect essentiel à la sécurité et à la prospérité américaine[103], car

> Les É.-U. se tiendraient toujours prêts à déployer leur puissance à l'encontre de menaces spécifiques à ces intérêts, mais celle-ci n'interviendrait que dans les cas absolument nécessaires où l'équilibre local serait brisé et que des intérêts vitaux américains seraient clairement menacés par des forces hostiles.[104]

Sans ce contrôle des espaces communs mondiaux, la possibilité pour les É.-U. d'agir en véritable arbitre et gardien de la stabilité en Asie-Pacifique deviendrait alors difficile, périlleuse et, si une telle situation était poussée à son paroxysme, devenir impossible.

---

[102] Barry R. Posen. « Command of the Commons : The Military Foundation of U.S. Hegemony ». *International Security*, vol.28, no.1, 2003, p.8

[103] Andrew F. Krepinevich Jr. « Strategy in a Time of Austerity », *Foreign Affairs*, vol.91, no.6, 2012, p.58; Barry Posen. *A Grand Strategy of Restraint*. Dans Flournoy et Brimley (eds.), *op.cit.*, p.94 – 99.

[104] Traduction libre. Walt, *Taming American Power, op.cit.*, p.118

1.2 La grande stratégie de la présidence Obama

Dès la course démocrate de 2007, Obama signifiait son intention de se distancier de la politique étrangère de son prédécesseur[105]. À cet effet, son administration a adopté une grande stratégie correspondant à celle de l'*engagement sélectif*, les autres stratégies possibles ne collant pas à ce qui a été entrepris dès 2009.

Dès le départ, il est possible d'éliminer la *primauté*, correspondant *grosso modo* à la *doctrine Bush*[106] tant critiquée par le nouveau président : Obama a plutôt limité les dépenses en défense et n'a pas cherché pas à résoudre tous les problèmes par la seule puissance militaire. Quant à la *sécurité coopérative,* il est difficile d'affirmer que l'administration Obama en ait adopté les principes, malgré une mise en valeur du multilatéralisme et un rejet de la *politique de la puissance*, soulignée par le prix Nobel de la Paix obtenu par le Président[107]. Malgré l'importante participation américaine aux affaires courantes de l'ONU, il en est autrement du côté du Conseil de sécurité, dont la principale responsabilité est justement de maintenir la paix et la sécurité internationales.

Alors que le changement de présidence pouvait laisser croire à un retour vers un multilatéralisme actif, l'inverse s'est plutôt produit : si l'administration G.W. Bush a été très active au sein du Conseil de sécurité, avec 146 déclarations et résolutions adoptées dans la seule année 2006, ce nombre est passé à 83 lors de la première année de l'ère Obama, « le plus bas total en près de deux décennies[108] ». La politique onusienne sous Obama demeure donc un outil aus service de la politique étrangère américaine, agissant unilatéralement dans de nombreux dossiers et passivement dans celui d'éventuelles

---

[105] Obama. *Renewing American Leadership, op.cit.*, p.2

[106] Stratégie unilatérale optant pour la guerre préventive afin d'éradiquer les menaces potentielles et de la croyance que la légitimité américaine provient de l'acceptation de facto par les autres du devoir de l'hégémon, soit la préservation à tout prix la paix et la stabilité internationale.

[107] Lors de son premier discours en tant que président des É.-U. à l'Assemblée générale de l'ONU, il affirmait notamment qu'« à une époque où notre destinée est partagée, la puissance n'est plus un jeu à somme nulle. Aucun pays ne peut ou ne devrait essayer d'en dominer un autre. Aucun ordre mondial élevant une nation ou un groupe de personnes au-dessus d'une autre ne va réussir. Aucun équilibre de la puissance entre les nations ne tiendra. ». Traduction libre. États-Unis. *Remarks by the President to the United Nations General Assembly*. 23 septembre 2009. En ligne, <www.whitehouse.gov/the-press-office/remarks-president-united-nations-general-assembly>. Consulté le 2 octobre 2015

[108] Traduction libre. David Bosco. « Course Corrections : The Obama Administration at the United Nations », *The Hague Journal of Diplomacy*, vol.6, 2011, p.338

réformes de l'ONU[109]. Visant à mieux refléter la distribution actuelle de la puissance mondiale par l'inclusion de pays émergents, dont ceux du BRICS[110], celles-ci représentent aussi de nouveaux opposants éventuels à des É.-U. dont la puissance ne fait plus l'unanimité[111].

La grande stratégie de Barack Obama repose donc sur le concept de l'*engagement sélectif*, un choix logique lorsqu'est prise en compte la posture internationale malaisée dans laquelle se retrouvent les É.-U. lors de sa prise de pouvoir officielle, en janvier 2009. Héritant d'un État à la légitimité internationale affaiblie et aux finances publiques alourdies par plusieurs années de conflits militaires, Obama n'a toutefois pas été freiné dans son ambition de maintenir autant que possible la supériorité américaine au sein du système international. Alors que la militarisation américaine du cyberespace participe pleinement à la poursuite de cet objectif incontournable, il est utile de d'abord se pencher brièvement sur l'état de la puissance américaine au sortir des huit ans du mandat de G.W. Bush. Ce sera toutefois la réaction d'Obama à cette situation donnée qui permettra de comprendre les conditions et les modalités d'émergence d'une puissante filière cyber au sein de l'appareil militaire américain, un outil incontournable servant les objectifs de sa grande stratégie.

1.2.1 Un risque à la puissance américaine hérité de la *doctrine Bush*

Si les É.-U. pouvaient auparavant se qualifier d'*hégémon bienveillant*, légitime et apprécié sur la scène mondiale, la poursuite par l'administration G.W. Bush d'une grande stratégie de primauté à tendance néoconservatrice[112] a mené à l'affaiblissement de cette image bienveillante. À partir de ce moment, Joseph S. Nye estimera que « la *puissance douce* des É.-U. – sa capacité à attirer les autres par la légitimité des politiques

---

[109] *Ibid.*, p.338 – 340.

[110] Acronyme utilisé pour parler du Brésil, de la Russie, de l'Inde, de la Chine et de l'Afrique du Sud.

[111] Stewart Patrick. « Irresponsible Stakeholders? The Difficulty of Integrating Rising Powers », *Foreign Affairs*, vol.89, no.6, 2010, p.50 – 52.

[112] Justin Vaïsse. « Why Neoconservatism Still Matters », *Brookings Policy Paper*, no.20, 2010. En ligne, <www.brookings.edu/~/media/research/files/papers/2010/4/05%20neoconservatism%20vaisse/05_neoconservatism_vaisse.pdf>. Consulté le 10 octobre 2015. Ici, la légitimité s'est davantage manifestée à travers la puissance militaire américaine que par l'acceptation de ses initiatives par la communauté internationale, appui considéré utile, mais non pas indispensable

américaines et des valeurs à l'origine de celles-ci – était en déclin.[113] » Si cela a limité la marge de manœuvre d'Obama sur la scène internationale, ce dernier a également dû jongler avec des contraintes découlant du gigantesque fardeau financier que lui léguait son prédécesseur. Ce dernier fut d'abord causé par un très coûteux et toujours croissant effort de guerre supportant les interventions américaines en Irak et en Afghanistan[114]: cette tendance marquée s'exécute alors même que dès 2000, la part relative du PIB américain au sein de l'économie mondiale amorçait une baisse importante et constante[115], principalement en raison de l'émergence d'États en intense rattrapage économique, comme les pays du BRICS. Aggravés par une sérieuse crise économique et financière, les problèmes économiques américains ont alors fortement influencé l'administration Obama dans le choix de l'engagement sélectif.

Puisque les performances économiques d'un pays affectent sa puissance militaire potentielle, les difficultés pécuniaires des É.-U. sont donc loin d'être bénignes : pour Paul Kennedy, il y a un « lien très net *à long terme* entre, d'une part, l'ascension et le déclin économiques d'une grande puissance et, d'autre part, sa croissance et son déclin en tant que grande puissance militaire[116] », tandis que pour Ashley Tellis, « la capacité d'un État à protéger sa liberté d'action par la possession de capacités économiques supérieures permet à son tour la production de la puissance militaire nécessaire[117] ». La situation économique pesant sur les épaules de l'administration Obama risquait donc d'entraîner des conséquences importantes sur la grandeur de la puissance américaine et, *in extenso*, sur le maintien de son rôle de leader du système international. Ce risque a poussé l'administration Obama à mener des compressions budgétaires considérables et à imposer un effort de réflexion, de priorisation et de réorganisation au sein de la Défense américaine : le DoD a réduit son personnel et son budget en recherche et développement

---

[113] Traduction libre. Joseph S. Nye Jr. « The Decline of America's Soft Power ». *Foreign Affairs*, vol.83, no.3, 2004, p.16

[114] En date de juillet 2015, le Watson Institute de l'université Brown estimait que la guerre à la terreur avait jusque là coûté 4,4 trillions de dollars au gouvernement américain.

[115] Voir Annexe B

[116] Paul Kennedy. *Naissance et déclin des grandes puissances*. Paris : Éditions Payot, 2004, p.30

[117] Ashley Tellis. *Balancing Without Containment : An American Strategy For Managing China*. Washington D.C. : Carnegie Endowment for International Peace, 2014, p.3. Également, plusieurs estiment que le PIB et les dépenses militaires d'un pays sont de bons indicateurs de sa puissance coercitive. Ikenberry, Mastanduno, Wohlforth – *Unipolarity, State Behavior and Systemic Consequences*, *op.cit.*, p.6

(R et D), suspendu, ou carrément mis fin à des programmes de modernisation d'équipements, etc.[118] Dès la première année son mandat, Obama considérait donc le problème économique américain comme étant un risque stratégique important, et affirmait que « notre prospérité fournit une fondation pour notre puissance. Elle paie pour nos militaires. Elle soutient notre diplomatie.[119] » L'inévitable heure des choix allait suivre, forçant les É.-U. à faire un important ménage au sein de leurs engagements internationaux et se limiter à ceux considérés comme étant primordiaux.

1.2.2 Un pas en arrière sur la scène internationale pour mieux avancer: l'engagement sélectif

À propos du futur de la puissance américaine, Paul Kennedy affirmait que « les dirigeants de Washington sont confrontés durablement à une difficulté embarrassante : les intérêts et les engagements américains dans le monde sont actuellement bien trop lourds pour que les É.-U. puissent les défendre tous simultanément.[120] » C'est à ce déséquilibre que l'administration Obama a voulu s'attaquer, notamment par le désengagement progressif des forces américaines postées en Irak et, après un envoi massif de militaires, en Afghanistan. La grande stratégie d'Obama vise donc un léger, mais réel, retranchement de la puissance américaine. Devant méticuleusement allouer ses ressources aux régions stratégiques névralgiques, cet effort de concentration sera analysé avec le concept d'*équilibre de la menace*, permettant de comprendre pourquoi les efforts américains se sont concentrés davantage envers une région potentiellement déterminante : l'Asie du Sud-Est et son plus grand acteur, la Chine.

---

[118] États-Unis, Department of Defense. *DoD Releases Report on Estimated Sequestration Impacts.* Washington, DC : Department of Defense. 2014. En ligne, <www.defense.gov/news/newsarticle.aspx?id=122065>. Consulté le 29 juillet 2015.

[119] États-Unis, White House. *Remarks by the President in Address to the Nation on the Way Forward in Afghanistan and Pakistan.* Washington D.C. : The White House, 2009. En ligne, <www.whitehouse.gov/the-press-office/remarks-president-address-nation-way-forward-afghanistan-and-pakistan>. Consulté le 15 octobre 2015.

[120] Kennedy, *Naissance et déclin des grandes puissances*, *op.cit.*, p.804 – 805.

1.2.2.1 Le retranchement américain du système international

Alors que les É.-U. se dirigeaient vers une surextension stratégique et risquaient d'aggraver un déclin marqué par un PIB relatif en baisse constante, la décision d'Obama de se retrancher de la scène internationale était inévitable afin d'atteindre ses objectifs. Pour MacDonald et Parent, il y a retranchement lorsqu'une grande puissance

> [...] se rétracte de ses engagements liés à sa grande stratégie en réponse à un déclin au niveau de sa puissance relative. De manière abstraite, cela signifie de réduire les coûts globaux d'une politique étrangère en redistribuant les ressources consacrées aux engagements périphériques vers ceux considérés comme étant centraux.[121]

Bien que plusieurs partisans de la *primauté* qualifient d'erreur l'idée d'un tel recul américain sur la scène internationale[122], MacDonald et Parent estiment que l'abandon de certains engagements secondaires permet de libérer des ressources pouvant être réinvesties dans un secteur où l'on veut démontrer ou renforcer un engagement[123]. Pour ce faire, l'État rationnel, cherchant à survivre dans un système international marqué par l'anarchie, diminue l'ampleur de ses forces armées, évite à tout prix des conflits qui alourdiraient une ardoise déjà bien remplie et cherche à transférer une partie du fardeau de la défense mondiale aux autres États. Il tente aussi de rendre plus efficaces ses forces armées qui tendront *de facto* à diminuer[124]. Outre la diminution des dépenses reliées à sa défense et une tolérance zéro quant à sa participation à un éventuel conflit, un pays en retranchement sera très actif diplomatiquement, formant des liens et trouvant des appuis[125]. De cette manière, un État arrive à se réorganiser et à éviter le pire, sans pour autant montrer d'inquiétants signes de faiblesse.

Le premier pas de cette stratégie d'Obama aura été de retirer assez rapidement les troupes américaines d'Irak, réduisant ainsi considérablement les dépenses militaires américaines[126], mais aussi son effectif militaire. Si des baisses plus draconiennes avaient

---

[121] Traduction libre. Paul K. MacDonald et Joseph M. Parent. « Graceful Decline? The Surprising Success of Great Power Retrenchment », *International Security*, vol.35, no.4, 2011, p.11

[122] Hillary Clinton. « America's Pacific Century », *Foreign Policy*, no.189, 2011, p.57 ; Robert Kagan. « Obama's Year One : Contra ». *World Affairs*, vol.172, no.3, 2010, p.14.

[123] MacDonald et Parent, *op.cit.*, p.15

[124] *Ibid.*, p.20

[125] *Ibid.*, p.27

[126] L'important engagement financier encouru par les conflits en Irak et en Afghanistan a mené à une succession de déficits budgétaires importants et qui a fortement contribué à gonfler la dette publique

eu lieu post-guerre froide, Obama a légèrement sabré le nombre d'hommes en uniformes : alors qu'en 2010, l'effort brusque (la *surge)* en Afghanistan s'entamait, le DoD disposait de 1 430 985 hommes et femmes, dont 566 045 dans l'armée de terre uniquement. En 2014, le nombre total passait à 1 354 054, le plus petit effectif depuis la Seconde Guerre mondiale, une perte d'environ 70 000, dont un peu plus de 50 000 membres de l'infanterie[127]. De son côté, en 2016, la marine militaire américaine était à son plus bas niveau depuis 1917, avec 273 navires actifs[128].

Sous Obama, les É.-U. ont également été très actifs diplomatiquement afin d'apaiser des tensions, que ce soit la tentative mitigée de réinitialisation des relations (le *reset*) avec la Russie (2009) ou le rapprochement avec le Myanmar (2012). Le retranchement s'est également manifesté par la mise en place d'une capacité d'influence discrète (*leading from behind*) qu'a pu exercer l'administration Obama, approche rendue nécessaire par une puissance relative américaine en déclin et le scepticisme croissant de plusieurs pays envers le leadership des É.-U.[129] Elle fut mise en place afin de forcer les autres États à s'impliquer davantage sur la scène internationale. Elle est ainsi décrite par Nelson Mandela, premier utilisateur du concept : « un meneur est un comme un berger. Il reste derrière le troupeau, laisse les plus agiles amorcer la marche, après quoi les autres suivent sans avoir réalisé qu'ils ont été dirigés à partir de l'arrière-scène.[130] » Cette capacité s'est principalement fait sentir lors de l'intervention militaire contre la Libye en 2011 : alors

---

des É.-U., croissant de plus de 307% entre 2001 et 2014, passant de 5,792 à 17,81 milliards. Marc Labonte et Andrew Hanna. *The Impact of Major Legislation on Budget Deficits : 2001 to 2009.* Washington, DC : Congressional Research Service, 2010, p.1. PDF en ligne, <www.fas.org/sgp/crs/misc/R41134.pdf>. Consulté le 25 juillet 2015; U.S. Government Accountability Office. *Financial Audit : Bureau of the Fiscal Service's Fiscal Years 2014 and 2013 Schedules of Federal Debt.* Washington, DC: U.S. Government Accountability Office, 2014. PDF en ligne, <www.gao.gov/assets/670/666824.pdf>. Consulté le 25 juillet 2015.

[127] David G. Coleman. *U.S. Military Personnel 1954-2014.* En ligne, <historyinpieces.com/research/us-military-personnel-1954-2014>. Consulté le 12 novembre 2015.

[128] Bien que véridique et souvent utilisé par diverses personnalités politique afin d'illustrer le déclin de la puissance militaire américaine, certains estiment toutefois que l'énoncé est trompeur, puisque les navires contemporains sont largement plus efficaces que lors de la Première guerre mondiale. Glenn Kessler. « Romney doubling down on debate mistatements », *The Washington Post*, 25 octobre 2012. En ligne, <www.washingtonpost.com/blogs/fact-checker/post/romney-doubling-down-on-debate-mistatements/2012/10/24/c1d34826-1e22-11e2-ba31-3083ca97c314_blog.html>. Consulté le 12 janvier 2016.

[129] Ryan Lizza. « The Consequentialist », *The New Yorker,* 2 mai 2011. En ligne, <www.newyorker.com/magazine/2011/05/02/the-consequentialist>. Consulté le 20 septembre 2015.

[130] Traduction libre. Nelson Mandela, dans Ryan Lizza. « Leading From Behind », *The New Yorker,* 26 avril 2011. En ligne, <www.newyorker.com/news/news-desk/leading-from-behind>. Consulté le 20 septembre 2015.

que les É.-U. avaient réussi à limiter sa participation, cette initiative a plutôt été portée à bout de bras par Nicolas Sarkozy et David Cameron[131]. Résultats : l'utilisation de la puissance militaire américaine, se limitant essentiellement à des frappes aériennes et navales, n'aura coûté *que* 1,1 milliard et aura effectué 16% des sorties aériennes totales[132], approche contrastant énormément avec celle de W. Bush.

Ce retranchement ne mène toutefois pas à une politique étrangère américaine s'apparentant à son isolationnisme de l'entre-deux-guerres. Les É.-U. cherchent plutôt à concentrer leurs efforts de défense sur les menaces jugées comme étant les plus préoccupantes pour leur sécurité. Cette rigoureuse réorganisation des ressources rend donc le conflit davantage possible que probable, les États n'ayant pas à maximiser à tout prix leur puissance afin d'assurer leur sécurité[133], limitant par le fait même les causes et les conséquences du dilemme de sécurité. C'est pourquoi Stephen Walt considère, contrairement à plusieurs membres de l'École réaliste, que la logique d'anarchie et du *self-help* du système international ne poussent pas inévitablement les États à rechercher un *équilibre de la puissance*, mais bien l'*équilibre de la menace* : au lieu d'utiliser la puissance nationale et les jeux d'alliances dans le but d'égaler ou de surpasser les capacités de leurs voisins les plus puissants, les États s'efforcent de limiter et de rééquilibrer les dangers émanant des États considérés comme étant les plus menaçants.

Afin d'évaluer et de hiérarchiser ces éventuelles menaces, Walt propose quatre facteurs nécessitant d'ouvrir les « boîtes noires » que sont les États et de décortiquer la perception des dirigeants, ceux et celles qui auront justement à juger du niveau de menace que représente un autre État[134]. S'il est d'abord nécessaire d'évaluer la puissance totale de

---

[131] Michael Elliott. « Viewpoint: How Libya Became a French and British War », *Time.com*, 19 mars 2011. En ligne, <content.time.com/time/world/article/0,8599,2060412,00.html>. Consulté le 20 septembre 2015; Nathalie Nougayrède. « La guerre de Nicolas Sarkozy », *Le Monde.fr*, 23 septembre 2011. En ligne, <www.lemonde.fr/libye/article/2011/08/23/libye-la-guerre-de-nicolas-sarkozy_1562377_1496980.html>. Consulté le 20 septembre 2015.

[132] Ben Smith. « A victory for 'leading from behind'? ». *Politico.com*, 22 août 2011. En ligne, <www.politico.com/story/2011/08/a-victory-for-leading-from-behind-061849>. Consulté le 25 octobre 2015.

[133] Stephen G. Brooks. « Dueling Realism ». *International Organization*, vol.51, no.3, 1997, p.446; Alex Macleod. « Le néoréalisme ». Dans Macleod et O'Meara, *op.cit.*, p.105

[134] Ce faisant, Walt s'éloigne du néoréalisme de Waltz et Mearsheimer. Pour Taliaferro, l'approche de l'*équilibre de la menace* se situe à mi-chemin entre le néoréalisme et le réalisme néoclassique tel que popularisé par Fareed Zakaria. Voir Jeffrey W. Taliaferro. « Security Seeking under Anarchy : Defensive Realism Revisited », *International Security*, vol.25, no.3, 2001, p.135.

cet État et de prendre en compte sa proximité géographique, il est également primordial de jeter un œil à ses capacités offensives et à ses intentions stratégiques[135]. Un État jugé menaçant en regard à ces critères provoquera contre lui un mouvement international d'*équilibrage externe*, où les États se sentant menacés s'allieront avec une grande puissance adverse afin d'en contrer la montée et de limiter le danger potentiel planant sur leur survie[136]. Néanmoins, cet effort peut également être poursuivi à l'*interne*, une situation où les États « se fient à leurs propres capacités plutôt que sur les capacités des alliés[137] » afin de réduire leur vulnérabilité et, par le fait même, la menace que peut représenter un autre État à leur endroit[138].

1.2.2.2 La concentration des efforts sur l'Asie avec la stratégie du « pivot »

L'administration Obama a dû faire le tri dans les engagements internationaux américains et se limiter aux plus importants : le Moyen-Orient, bien que toujours déterminant à court et à moyen terme, ne représente plus le cœur des intérêts stratégiques américains, celui-ci se déplaçant vers l'Asie du Sud-Est, région que Robert D. Kaplan qualifie carrément de *poudrière asiatique*[139]. Elle est, pour plusieurs, « une des rares régions du monde dans lesquelles la possibilité d'un conflit entre grandes puissances demeure substantielle[140] » : en excluant les grandes puissances de la région (Chine, Corée du Sud, Japon), plusieurs puissances pouvant être considérées comme secondaires ont elles aussi amorcé un véritable équilibrage interne en investissant de manière considérable dans leur puissance militaire, émergeant en même temps que leur PIB[141]. Il en est ainsi principalement parce que la Chine voisine monte rapidement en puissance, aussi bien économiquement que

---

[135] Stephen M. Walt. « Alliance Formation and the Balance of World Power », *International Security*, vol.9, no.4, 1985, p.9

[136] *Ibid.*, p.26

[137] Traduction libre. Kenneth Waltz. *Theory of International Politics*. Reading, Mass : Addison-Wesley, 1979, p.168

[138] Walt, *The Origins of Alliances*, p.263

[139] Un bon portrait des tensions régionales est fait dans Robert D. Kaplan. *Asia's Cauldron : The South China Sea and the End of a Stable Pacific*. New York : Random House, 2014.

[140] Traduction libre. « East Asia » *In* Amos A. Jordan; William J. Taylor Jr.; Michael J. Meese et Suzanne C. Nielsen (eds.). *American National Security*. Baltimore, Maryland : John Hopkins University Press, 6e édition, 2009, p.369

[141] Voir Annexe B

militairement[142]. Selon le concept de Walt explicité ci-haut, la Chine s'avère donc être pour ces pays une menace croissante à contrer impérativement.

La Chine améliorant sans cesse ses capacités navales et aériennes, autant en qualité qu'en quantité[143], ses intentions au niveau régional sont également peu rassurantes : elle n'hésite pas à poursuivre agressivement des revendications territoriales et océaniques fortement contestées, et ce, avec de nombreux États de la région, notamment concernant les archipels convoités des Paracels et des Spratlys. La Chine n'hésite pas non plus à s'approprier certaines îles lui permettant d'étendre son plateau continental à l'intérieur de la *ligne en neuf traits* délimitant ce qu'elle considère être sienne, une ambition territoriale qui n'est pas étrangère au fait que cette zone est considérée comme étant très riche en ressources, tels des hydrocarbures situés en eau profonde ou d'importantes réserves de poissons[144]. Par ses revendications, la Chine viole toutefois les *zones économiques exclusives* de ces différents États, régies par le droit international et considérées comme une extension de leur espace souverain[145].

Ces tensions régionales, en grande partie provoquées par une Chine désirant changer le *statu quo* de la région, pourraient croître jusqu'à l'éclatement d'un conflit en bonne et due forme, menaçant directement les É.-U. Ceux-ci possèdent des intérêts importants dans la région, dont 1) y maintenir un accès économique, 2) empêcher l'émergence d'un hégémon régional, 3) décourager les conflits potentiels et maintenir une stabilité régionale[146], ce à quoi il est possible d'ajouter la défense du droit international[147], dont les violations multiples par plusieurs pays pourraient mener à des frictions plus grandes encore. Ces intérêts, pierres d'assise de l'*engagement sélectif,* expliquent en grande partie la décision de l'administration Obama de concentrer la puissance américaine en Asie-Pacifique, où une simple étincelle suffirait pour déclencher les hostilités. En réponse à

---

[142] Voir Annexe C

[143] Barthélémy Courmont. *La tentation de l'orient : une nouvelle politique américaine en Asie-Pacifique.* Québec : Septentrion, 2009, P.145 – 154.

[144] Bill Hayton. *The South China Sea.* New Haven; Londres : Yale University Press, 2014, p.248 – 253

[145] Voir Annexe D

[146] Jordan et als (eds.). *American National Security, op.cit.,* p.371 – 372

[147] Mark Landler. « Offering to Aid Talks, U.S. Challenges China on Disputed Islands », *The New York Times,* 23 juillet 2010. En ligne, <www.nytimes.com/2010/07/24/world/asia/24diplo.html>. Consulté le 15 juin 2015.

cette instabilité régionale, c'est donc le *pivot vers l'Asie* qui s'amorce, véritable équilibrage externe américain à l'endroit de la Chine.

Si pendant la présidence de G.W. Bush, la problématique asiatique était éclipsée par les engagements militaires américains en Irak et en Afghanistan, la vision du monde de Barack Obama l'a personnellement poussé[148] à tourner son attention vers la région de l'Asie-Pacifique, dont la gigantesque population et la croissance économique en font une charnière stratégique pour les É.-U.[149] Cette importance se situe autant du point de vue économique[150], l'Asie devenant une plaque tournante du commerce international, que stratégique, alors que « maintenir la paix et la sécurité à travers l'Asie-Pacifique s'avère de plus en plus crucial pour le progrès mondial [...][151]». Ce *pivot* agit également comme une solution mitoyenne, cherchant autant à contenir et apaiser la Chine qu'à l'engager et la dissuader, compromis visant à maintenir et à perpétuer la direction mondiale américaine pour le XXI[e] siècle[152]. Même si les architectes de cette stratégie ne l'évoquent pas directement, l'incertitude provoquée par la montée en puissance de la Chine, marquée par son développement militaire et économique, et ses actions futures sur la scène internationale sont les moteurs de cette stratégie[153].

Pour Ashley Tellis, l'engagement sélectif requiert une stratégie qui, au lieu de resserrer l'étau autour de la Chine, chercherait d'abord à favoriser la croissance économique et stratégique des pays redoutant la montée chinoise, « afin de réaliser leur potentiel stratégique et d'augmenter leur coopération mutuelle tout en approfondissant leur partenariat avec les É.-U. » permettant ainsi « la création de contraintes objectives limitant les abus de la puissance chinoise en Asie.[154] » Le projet américain de maîtriser le géant chinois et de renverser le fardeau de la menace s'articule tout d'abord par une

---

[148] Frédérick Douzet et Justin Vaïsse. « Obama, le président du pivot », *Hérodote*, vol.149, no.2, 2013, p.7

[149] Kevin Marsh. « Managing Relative Decline : A Neoclassical Realist Analysis of the 2012 US Defense Strategic Guidance », *Contemporary Security Policy*, vol.33, no.3, 2012, p.494

[150] Clinton, *op.cit.*, p.57. Selon elle, le redressement économique américain « dépendra des exportations et de l'habileté des entreprises américaines à percer le vaste et croissant bassin de consommateurs asiatiques. »

[151] Traduction libre. *Ibid.*, p.57

[152] *Ibid.*, p.58; David A. Beitelman. « America's Pacific Pivot », *International Journal*, vol.67, no.4, 2012 p.1086

[153] *Ibid.*, p.1088

[154] Traduction libre. Ashley Tellis. « Balancing without Containment: A U.S. Strategy for Confronting China's Rise », *The Washington Quarterly*, vol.36, no.4, 2013, p.112

importante implication politique et diplomatique, que ce soit en améliorant les relations avec les divers États de la région ou en y répandant la mondialisation par sa participation croissante au sein d'organisations régionales comme l'*Association of Southeast Asian Nations* (ASEAN). Ce volet cherche essentiellement à promouvoir les intérêts américains dans la région en y établissant des normes et des règles bien ancrées et à y augmenter son influence avant que la Chine ne le fasse[155]. Au lieu de contenir la Chine ouvertement et sans équivoque, l'objectif des É.-U. vise davantage à modeler l'environnement et les modalités de la montée chinoise, d'influencer son comportement et d'obtenir sa participation[156].

La diplomatie est aussi flanquée d'un important volet stratégique et militaire : en plus de fortifier les alliances déjà existantes, les É.-U. multiplient les accords fournissant de l'équipement et de la formation militaire aux États inquiets des agissements de la Chine, comme le sont Singapour, l'Australie ou les Philippines[157], et pour que ces pays puissent, au besoin, accueillir des troupes et navires américains. Même si de fortes contraintes budgétaires forcent l'état-major américain à une diminution draconienne de ses effectifs, Obama a proclamé que « les réductions dans les dépenses américaines du secteur de la défense ne seront pas [...] faites au détriment de l'Asie-Pacifique[158] », affirmation se traduisant notamment par l'importance grandissante des capacités navales et aériennes au détriment de celles de l'armée et des Marines[159]. L'administration Obama, en retirant progressivement les troupes d'Afghanistan et d'Irak, a principalement réaffecté celles-ci sous le contrôle du U.S. Pacific Command (USPACOM)[160] : si les bases et postes militaires américains situés en Corée du Sud ou au Japon ont vu leur effectif augmenter de manière importante, ce sont les bases de Guam et d'Hawaii qui accueillent la majeure partie de ces nouveaux effectifs. Dédiées à la défense et au maintien de la paix dans la

---

[155] Beitelman, *op.cit.*, p.1089.
[156] *Ibid.*, p.1090
[157] Robert Gates. « Helping Others Defend Themselves : The Future of U.S. Security Assistance », *Foreign Affairs*, vol.89, no.3, 2010, p.4; Marsh, *op.cit.*, p.494
[158] Traduction libre. États-Unis, White House. *Remarks By President Obama to the Australian Parliament.* Washington D.C.: The White House. En ligne, <www.whitehouse.gov/the-press-office/2011/11/17/remarks-president-obama-australian-parliament>, 2011. Consulté le 27 juillet 2015.
[159] Jean-Loup Samaan. *La Menace chinoise : une invention du Pentagone?*, *op.cit.*, p.114,
[160] Voir Annexe E

région, ces troupes permettent d'assurer les accès américains au Pacifique et à la mer de Chine, deux zones géographiques stratégiquement cruciales.

Outre leur puissance militaire brute, les É.-U. délèguent davantage de responsabilités à leurs alliés régionaux, ceux-ci possédant désormais les moyens économiques et militaires de le faire. La coopération militaire s'y est aussi énormément renforcée, notamment par des exercices tels que *Rim of the Pacific* (RIMPAC)[161], *Southeast Asia Cooperation and Training* (SEACAT)[162] et *Cobra Gold*, ce dernier réunissant des milliers de soldats et visant une inclusion régionale grandissante alors que des pays comme la Chine, le Laos, le Vietnam ou le Myanmar y participent en tant qu'observateurs[163]. Pour le volet diplomatique, essentiel à un retranchement réussi, des forums régionaux comme l'ASEAN ou les rencontres informelles du *Shangri-La Dialogue* de l'*International Institute for Strategic Studies* (IISS) ont été mis en place. Ces dernières servent « à engendrer un sentiment de communauté parmi les décideurs les plus importants du milieu de la défense et de la sécurité, provenant autant des États régionaux que des grandes puissances possédant des intérêts importants dans la sécurité de l'Asie-Pacifique[164] », sans oublier des acteurs de la société civile.

La Chine apparaît donc rapidement comme étant la plus grande menace au maintien de cette paix. Si les taux de croissance inégaux et l'augmentation importante des dépenses militaires de la Chine peuvent laisser présager que cette dernière détrônera à long terme les É.-U. en tant que plus grande puissance mondiale, il n'en demeure pas moins qu'à court et moyen terme, elle ne possède ni la force militaire, ni un réseau d'alliances suffisant pour s'opposer à la superpuissance américaine et à ses nombreux alliés et partenaires en Asie du Sud-Est[165]. Malgré tout, les tensions et les méfiances profondes

---

[161] Se tenant aux deux ans, le RIMPAC de 2014 réunissait 23 pays, qu'ils soient considérés comme étant dans la région Asie-Pacifique ou y possédant des intérêts, que ce soient la France, la Grande-Bretagne, la Norvège ou des pays américains participant à l'*Asia-Pacific Economic Cooperation* (APEC), comme le Chili, le Canada, le Mexique et le Pérou.

[162] Ces exercices annuels incluent Singapour, le Brunei, l'Indonésie, la Malaisie, les Philippines, la Thaïlande et les É.-U.

[163] Richard S. Ehrlich. « China flexes its muscles in U.S.-led military exercises », *The Washington Times*. 12 février 2014. En ligne, <www.washingtontimes.com/news/2014/feb/12/china-flexes-its-muscles-in-us-led-military-exerci/>. Consulté le 8 novembre 2015.

[164] International Institute for Strategic Studies. Shangri-La Dialogue. *About Shangri-La*. En ligne, <www.iiss.org/en/events/shangri-s-la-s-dialogue/about-shangri-la> Consulté le 7 novembre 2015.

[165] Robert D. Kaplan et Stephen S. Kaplan. « America Primed ». *The National Interest*, no.112, 2011, p.43.

entre les différents pays n'écartent pas le risque d'un accident ou d'une mauvaise interprétation menant tout droit à un conflit.

Les intérêts nationaux à défendre dans le cadre de la grande stratégie d'Obama ne se retrouvent pas seulement outre-mer, mais se situent aussi directement sur le territoire américain. Alors que les É.-U. désirent pallier la menace chinoise dans le théâtre Asie-Pacifique en recourant à un équilibrage externe, objectif conforme à la politique de retranchement, ils doivent également s'attarder aux éléments nationaux permettant à la puissance américaine de l'appliquer convenablement et avec succès. Pour ce faire, l'administration Obama a dû parallèlement effectuer un *équilibrage interne*, le seul entretien de liens diplomatiques, économiques et stratégiques ne suffisant pas au maintien de la stabilité recherchée en Asie-Pacifique. Pour arriver à leurs fins, les É.-U. doivent aussi se concentrer sur leur propre puissance afin de maintenir leur incomparable capacité à la projeter dans le monde entier, de se porter garants de la sécurité et de la prospérité asiatiques, visées centrale du *pivot vers l'Asie*, et de confronter militairement la Chine si nécessaire.

Parallèlement, l'économie croissante de la Chine permet à cette dernière d'injecter des sommes importantes dans la mise sur pied de capacités militaires visant spécifiquement à empêcher les É.-U. d'atteindre ses objectifs stratégiques régionaux et qui, par l'exploitation des faiblesses des forces armées américaines, ont le potentiel d'en limiter la capacité de projection en Asie-Pacifique. Ces capacités, dont des composantes cyber, complexifient donc grandement un déploiement éventuel des forces américaines dans la région. Devant ces initiatives contrecarrant les capacités militaires rendant possible la grande stratégie américaine adoptée par l'administration Obama, celle-ci doit absolument maintenir cette capacité de projection tout en possédant moins de ressources pour le faire. Cette situation budgétaire difficile complique le développement et l'acquisition d'équipements à la fine pointe de la technologie, mais extrêmement coûteux, qui permettraient d'outrepasser les défis imposés par les nouvelles capacités chinoises.

C'est dans cette optique que les É.-U. ont dû amorcer un équilibrage interne passant par deux aspects primordiaux. Dans un premier temps, les É.-U. doivent tout mettre en œuvre afin d'assurer le maintien de la puissance américaine actuelle et de sa capacité stratégique

et opérationnelle à la projeter, c'est-à-dire d'être apte à « déployer des éléments opérationnels avancés capables de procéder à des opérations militaires soutenues contre un opposant, et ce, à travers le monde.[166] » Dans un deuxième temps, à une époque de rigueur budgétaire accrue, il est aussi capital de revitaliser de manière considérable l'économie américaine. Pour Ashley Tellis, cet aspect est primordial, car sans sa réalisation, il estime que les É.-U. seront incapables de mettre en place les différents pans de leur grande stratégie, à la fois externe et interne, que ce soit au niveau du renforcement stratégique et économique des voisins de la Chine que du maintien impératif de la supériorité militaire américaine[167].

1.2.2.3 Le cyberespace au service de la grande stratégie d'Obama

L'engagement sélectif, jumelé à un effort de retranchement sur la scène internationale, apparaît donc comme la seule grande stratégie permettant d'atteindre les objectifs de la politique étrangère d'Obama. Elle permet d'abord de préserver la prééminence stratégique américaine, rendue possible par une réduction des coûts engendrés par les divers engagements américains, mais aussi par la protection et l'accroissement de la vigueur économique nationale. En maintenant sa capacité à jouer le rôle d'arbitre dans l'éventualité d'un conflit majeur, cette consolidation de la puissance des É.-U. rend possible le maintien de la stabilité et de la paix en Asie-Pacifique, indispensable état des choses pour une région jugée économiquement et stratégiquement essentielle aux intérêts américains. La grande stratégie américaine doit par contre également composer avec celle de la Chine : prête à en découdre afin de retrouver sa grandeur et son prestige d'antan, elle ambitionne sérieusement à devenir un acteur incontournable du système international et à remettre en question un leadership américain qu'elle perçoit davantage comme un frein à l'expansion et à l'expression de sa puissance que comme un atout. C'est justement dans ce contexte stratégique que la militarisation américaine du cyberespace gagne ses lettres de noblesse, alors que de part et d'autre du Pacifique, ce nouveau champ de bataille

---

[166] Traduction libre. Tellis. *Balancing without Containment : An American Strategy for Managing China*, *op.cit.*, p.55.
[167] *Ibid.*, p.67.

est et sera abondamment exploité par les deux pays dans la poursuite de leurs objectifs respectifs.

Pour les É.-U., le cyberespace représente un atout de taille dans le déploiement de la grande stratégie d'Obama, l'expansion territoriale et sectorielle de la mondialisation ayant propagé une utilisation accrue des TIC dans une grande partie des sphères sociales. Ainsi, la majeure partie de la planète se retrouve désormais connectée à Internet, formant un grand réseau où tout ce qui y est connecté est potentiellement accessible à partir de n'importe quelles coordonnées géographiques. Militariser le cyberespace permet alors de se doter de la capacité de les dominer afin d'exploiter librement la multiplicité des réseaux et des périphériques y étant connectés et qui forment un véritable champ de bataille numérique. Ils peuvent le faire à distance, et ce dans une relative discrétion et à relativement peu de coûts : dans une perspective d'engagement sélectif et de retranchement, ces nouvelles possibilités offertes par le cyberespace s'avèrent primordiales et la maîtrise de cet espace commun numérique nécessaire afin d'en retirer les bienfaits espérés.

Par contre, la cyberpuissance américaine se bute à celle d'une Chine qui a depuis longtemps fait du cyberespace une pierre angulaire de sa grande stratégie. Comme nous le démontrera le second chapitre, l'utilisation chinoise du cyberespace fait intégralement partie des moyens militaires et non militaires servant autant à perturber l'économie des É.-U., qu'à contrer l'avantage technologique de ses forces militaires. Celles-ci ont principalement été développées en tant qu'outil d'espionnage, mais également comme arme asymétrique permettant de contrer, de repousser, voire d'anéantir la toute-puissance des forces américaines, ce qui permettrait de mettre la main sur les territoires revendiqués par la Chine.

Cette augmentation de la puissance militaire chinoise, notamment sa filière cyber, est également une réponse à l'hégémon imprévisible que sont devenus les É.-U. depuis la présidence de George W. Bush : un comportement stratégique jugé à risque de s'accentuer si la première puissance mondiale devait échouer à stopper son déclin relatif, la poussant à devenir plus impulsive et agressive afin de maintenir son ascendant sur une Chine déterminé à faire sa place. Devant cette incertitude, les États qui, comme la Chine,

s'estiment être des victimes potentielles de cet hégémon semblant hors de contrôle depuis le 11-septembre n'ont d'autres choix que de se préparer au pire et de prendre des mesures leur permettant d'exercer un certain contrôle sur les affaires internationales. Ce faisant, les É.-U. font planer une menace importante sur la Chine, la poussant non pas à abandonner ses intentions, mais à plutôt se braquer davantage devant un hégémon cherchant à préserver à tout prix le statu quo et à étendre son emprise, situation pouvant mener, comme dans le cas irakien, à une guerre préventive. Nuno Munteiro affirme que les États se sentant ainsi menacés réagissent habituellement fortement afin de dissuader ou de mieux se défendre en cas d'invasion. Ils

> essaieront de renforcer leurs défenses conventionnelles, de développer les stratégies asymétriques les plus efficaces possible et, scénario plus probable à l'ère nucléaire, tenter d'acquérir la force de dissuasion ultime – des armes nucléaires capables de survivre à une première attaque.[168]

Aujourd'hui, cette recherche d'une puissance nucléaire pouvant résister à une attaque initiale doit être immanquablement suppléée par une puissance cyber, domaine militaire où l'avance prise par les pirates informatiques chinois a inévitablement poussé l'administration Obama à consacrer beaucoup, et urgemment, de ressources au développement de capacités militaires cyber pouvant rivaliser et surpasser ces rivaux chinois, ceux-ci ayant déjà obtenu et démontré ces cybercapacités depuis longtemps.

De par les risques qu'elle fait planer sur les intérêts américains, la question cyber devient un élément incontournable de la grande stratégie d'engagement sélectif poursuivie par Obama. En effet, la Chine possède, par l'entremise du cyberespace, la capacité de saboter les efforts américains à remettre leur économie sur les rails et de priver les É.-U. de son primordial contrôle des espaces communs mondiaux lui permettant de jouer le rôle d'arbitre international, des capacités lui permettant aussi de caresser des scénarios offensifs hautement déstabilisateurs pour la région et pour le monde.

---

[168] Nuno Monteiro, « Unrest Assured: Why Unipolarity Is Not Peaceful », *International Security,* vol.36, no.3, 2012, p.26

CHAPITRE II
L'ÉMERGENCE DE LA CYBERMENACE CHINOISE

> Lorsque l'ennemi est uni, divisez-le ; et attaquez là où il n'est point préparé, en surgissant lorsqu'il ne vous attend point. Telles sont les clés stratégiques de la victoire, mais prenez garde de ne point les engager par avance.
>
> Sun Tzu, *L'Art de la Guerre*

La réalisation d'une grande stratégie d'*engagement sélectif* nécessite donc que les É.-U. amorcent un équilibrage interne, d'abord par le maintien de leur prépondérance militaire et de leur capacité à la projeter librement, mais ensuite par l'amélioration de leur situation économique rendant cette capacité possible. Bien que des milliers de kilomètres séparent le territoire américain du théâtre régional est-asiatique, la poursuite de ces deux objectifs n'est toutefois nullement à l'abri de perturbations provenant de la Chine. Ces entraves se transportent même du front régional au front national par l'entremise du cyberespace, un nouveau, mais incontournable, champ de bataille. S'éloignant des aspects conventionnels de la sécurité nationale, ce fruit du développement des technologies de l'information et de la communication (TIC) relie directement les É.-U. au reste du monde, en rendant certaines composantes aisément accessibles à tous, et joue le rôle de colonne vertébrale d'une société s'appuyant plus que jamais sur l'accessibilité à une grande quantité d'informations. Bien qu'intangible, cet espace virtuel engendre donc inévitablement des conséquences sur le monde réel, qu'elles soient positives ou négatives. Suscitant un intérêt grandissant par la diversification des sources de dangers et de vulnérabilités qu'il a rendues possible, le cyberespace demeure toutefois complexe par sa technicité rendant difficile une évaluation juste et précise des risques et menaces en émanant et augmentant le sentiment national d'urgence à son endroit.

Alors en proie à « des débats interminables sur le niveau de priorité et d'immédiateté devant lui être accordé[169] », les perturbations politiques, sociales ou économiques ayant résulté d'incidents cybernétiques ont fourni à la communauté stratégique et politique américaine un aperçu des possibles répercussions d'une cyberattaque et rendu concrets et plausibles les scénarios où celle-ci pourrait paralyser la société américaine en atteignant ses IC. C'est en prenant connaissance de la dangerosité latente du cyberespace que l'idée d'une menace cybernétique chinoise s'est imposée dans l'ordre du jour sécuritaire américain. Ce présent chapitre cherchera donc à définir la nature de cette menace précise, tout en abordant son impact sur la grande stratégie américaine entreprise par Obama.

D'abord, l'évaluation de cette menace se fera en utilisant la grille d'évaluation de Stephen Walt précédemment évoquée et se concentrera sur les *capacités offensives* et *intentions perçues*, la question de la puissance globale chinoise et de sa proximité ayant déjà été réglée lors du précédent chapitre. Si la Chine représente une menace aux intérêts américains dans leur ensemble, la même formule s'applique aux différents théâtres d'opérations, dont le cyberespace. Toutefois, cette menace prend plusieurs formes : de nombreuses infiltrations informatiques répertoriées au fil des années et attribuées à la Chine ont été qualifiées d'actes ciblés de cyberespionnage et inquiètent par la menace économique qu'elle représente pour les É.-U. et son impact sur l'avantage relatif américain en matière de puissance militaire. Ces opérations, de plus en plus fréquentes, permettent alors à la Chine d'accélérer drastiquement sa croissance économique au détriment des É.-U., « l'économie la plus technologiquement puissante sur la scène mondiale[170] ». Ne se limitant pas aux gains économiques potentiels, ce même espionnage permet également à la Chine de s'approprier plusieurs technologies militaires développées à l'étranger, facilitant ainsi son effort soutenu de modernisation de ses forces armées.

---

[169] Traduction libre. Barry Buzan. *Peoples, States & Fear*, Colchester (UK): ECPR Press, 2007, p.121

[170] Traduction libre. Central Intelligence Agency. « Economy », *The World Factbook*, 5 janvier 2016. En ligne, <www.cia.gov/library/publications/the-world-factbook/geos/us.html>. Consulté le 15 janvier 2016

L'implication directe des autorités chinoises dans ces opérations à l'encontre des É.-U. soulève aussi la question d'une *cybermenace militaire et stratégique*. Dans le but de dissuader une intervention américaine en Asie-Pacifique, plusieurs considèrent la Chine prête à utiliser asymétriquement des cyberattaques envers la clé de voûte de l'efficacité de forces armées américaines actuelles, soit son importante et étendue utilisation des TIC. Ne s'appliquant pas seulement aux points de vue tactique et opérationnel, une telle initiative pourrait également avoir des conséquences stratégiques importantes alors que de plus en plus d'IC sont connectées au cyberespace, une situation faisant aussi craindre les cyberattaques sur le front national. Pour le Pentagone et de nombreux *think tanks*, cette manière potentielle de procéder apparaît conforme à la littérature stratégique chinoise en vogue depuis l'opération *Desert Storm*, laissant transparaître, selon le camp américain, des intentions offensives claires à son endroit.

2.1 Une menace initiale pensée essentiellement en termes économique

Cette section brossera un portrait des capacités chinoises de cyberespionnage et des intentions qui y sont rattachées, paramètres permettant d'établir que la Chine apparaît effectivement comme une menace à l'économie américaine. D'entrée de jeu, un aperçu de différentes opérations chinoises de cyberespionnage ayant eu lieu depuis près de quinze ans permettra de démontrer l'ampleur des *capacités* chinoises, notamment par les cas de *Titan Rain*, *GhostNet* et *Operation Aurora*. Ensuite, il sera question des *intentions* et visées attribuées à ces infiltrations multiples et répétées à l'encontre des É.-U. et qui en font une véritable menace économique.

2.1.1 Des actes de cyberespionnage de plus en plus fréquents

En 2004, un employé de *Sandia National Laboratories*, associé au département de l'Énergie et au programme nucléaire américain, constatait des activités suspectes dans les réseaux informatiques de l'organisation[171]. Un an plus tard, les autorités américaines

[171] Nathan Thornburgh. « The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them) », *Time*, vol.166, no.10, 5 septembre 2005. En ligne, <courses.cs.washington.edu/courses/csep590/05au/readings/titan.rain.htm>. Consulté le 12 décembre 2015.

confirmaient qu'elles faisaient partie d'une importante opération chinoise de cyberespionnage surnommée *Titan Rain*, en place depuis 2003[172] et la première connue à atteindre cette ampleur[173]. Si de multiples agences gouvernementales et entreprises américaines furent touchées, le secteur militaire fut également lourdement affecté : de nombreuses bases militaires et différents fournisseurs gouvernementaux œuvrant dans l'armement ayant été touchés[174]. Selon le major général William T. Lord, les *hackers* auraient réussi à extraire entre 10 et 20 téraoctets de données provenant du *NIPRNet*[175], réseau interne du DoD hébergeant des informations sensibles, mais non classifiées, une quantité d'informations qui, dans le monde physique, aurait difficilement pu être dévalisée incognito[176].

Ces cyberattaques utilisent un *modus operandi* récurrent afin de pénétrer un système ou un réseau informatique ciblé : les assaillants utilisent l'ingénierie sociale et exploitent principalement l'individu, considéré comme le maillon faible du réseau[177]. L'ouverture d'une pièce jointe malveillante ou l'insertion d'une clé USB infectée dans un ordinateur relié au réseau ciblé est suffisante pour en compromettre entièrement la sécurité informatique. Le virus ainsi implanté, il est possible d'accéder à distance et furtivement à ces éléments infectés, d'en extirper des informations et d'assister en temps réel à ce qui s'y passe. La tête de pont mise en place, les pirates informatiques peuvent donc y revenir afin d'atteindre leur objectif en transférant le maximum de données, et ce jusqu'à ce que leurs activités soient éventuellement repérées et bloquées.[178]

---

[172] Nathan Thornburgh. « Inside the Chinese Hack Attack », *Time.com*, 25 août 2005. En ligne, <content.time.com/time/nation/article/0,8599,1098371,00.html>. Consulté le 12 décembre 2015.

[173] Thornburgh. *The Invasion of the Chinese Cyberspies*, *op.cit.*

[174] *Ibid.*; Ethan Gutmann, « Hacker Nation : China's Cyber Assault », *World Affairs*, vol.173, no.1, 2010, p.76.

[175] Major-Général William T. Lord, cité dans Dawn S. Onley et Patience Wait. « Red Storm Rising: DoD's Efforts to Stave Off Nation- State Cyber Attacks Begin with China », *Government Computer News*, 17 août 2006, p.1. En ligne, <gcn.com/Articles/2006/08/17/Red-storm-rising.aspx?Page=1>. Consulté le 12 décembre 2015.

[176] Joel Brenner. *American the Vulnerable : Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. New York : Penguin Press, 2011, p.77

[177] Hannes Holm, Waldo Rocha Flores et Göran Ericsson. 2013. « Cyber Security for a Smart Grid – What About Phishing? », *2013 4th IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe)*, Copenhague (Danemark), 6 au 9 octobre, p.4

[178] Thornburgh. *The Invasion of the Chinese Cyberspies*, *op.cit.*; William C. Hannas, James Mulvenon et Anna B. Puglisi. *Chinese Industrial Espionage : Technology Acquisition and Military Modernisation.* Londres; New York: Routledge, coll. *Asian Security Studies*, p.351

Un scénario comme *Titan Rain* n'est pourtant pas inédit pour le gouvernement américain. Dès 1998, l'administration Clinton était mise au courant que des cyberattaques avaient infiltré à répétition des serveurs gouvernementaux, certaines provenant de la Chine[179], alors que d'autres, regroupées sous le nom de *Moonlight Maze* par le *Federal Bureau of Investigation* (FBI), ont été attribuées à la Russie[180]. La découverte de telles opérations démontra que ce type d'incidents devait dorénavant être considéré comme la nouvelle norme du monde de l'espionnage et du renseignement : plus efficaces, elles permettent aussi d'œuvrer sur de plus longues périodes, et ce, sans risque. Bien que *Titan Rain* provienne du territoire chinois, plusieurs personnes au sein du Pentagone ont d'abord considéré que la Chine pouvait n'être qu'un espace transitoire utilisé par des pirates informatiques étrangers afin de camoufler leurs traces, possédant elle-même un vaste ensemble de réseaux informatiques hautement vulnérables[181].

Le déni systématique des autorités chinoises concernant leur participation dans ces cyberattaques[182] empêchait les É.-U. de blâmer ces dernières, désirant aussi préserver une relation diplomatique qui, après le 11-septembre, s'était sensiblement améliorée. De plus, la non-implication gouvernementale chinoise demeurait tout à fait plausible, les preuves étant ténues et étant reconnu que la Chine comptait, et compte encore aujourd'hui, de nombreux groupes de *pirates informatiques* patriotiques exprimant leur nationalisme en s'attaquant de manière autonome à ce qu'ils considèrent être des ennemis du pays, que ce soient les É.-U., Taïwan, le Japon, etc.[183]

---

[179] Jeff Gerth et James Risen. « 1998 Report Told of Lag Breaches and China Threat », *The New York Times*, 2 mai 1999. En ligne, <www.nytimes.com/1999/05/02/world/1998-report-told-of-lab-breaches-and-china-threat.html?pagewanted=all&src=pm>. Consulté le 13 décembre 2015.

[180] « Significant Cyberattack Incidents : Moonlight Maze, 1998-1999 ». *RealClearPolitics.com*, 26 février 2013. En ligne, <www.realclearpolitics.com/lists/cyber_attacks/moonlight_maze.html>. Consulté le 14 décembre 2015; James Adams. « Testimony of James Adams, Chief Executive Officer Infrastructure Defense, Inc. ». Audition devant le *Committee on Governmental Affairs* du 106e Congrès du Sénat américain, 2 mars 2000. En ligne, <fas.org/irp/congress/2000_hr/030200_adams.htm>. Consulté le 14 décembre 2015; Alexander Klimburg. « Mobilising Cyber Power », Survival, vol.53, no.1, 2011, p.48 – 50

[181] James A. Lewis. « Computer Espionage, Titan Rain and China », *Center for Strategic and International Studies*, 14 décembre 2015. PDF en ligne, <csis.org/files/media/csis/pubs/051214_china_titan_rain.pdf>. Consulté le 15 décembre 2015; Bradley Graham. «Hackers Attack Via Chinese Web Sites ». *The Washington Post*, 25 août 2005. En ligne, <www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318.html>. Consulté le 15 décembre 2015.

[182] Paulo Shakarian, Jane Shakarian et Andrew Ruef. *Introduction to Cyber-Warfare: A Multidisciplinary Approach*. Amsterdam : Morgan Kaufmann Publishers, 2013, p.127.

[183] Mara Hvistendahl. « Hackers : The China Syndrome ». *Popular Science*, 23 avril 2009. En ligne, <www.popsci.com/scitech/article/2009-04/hackers-china-syndrome>. Consulté le 8 janvier 2016;

L'implication de l'un n'empêchant pas celle des autres, les autorités américaines « [...] soupçonnaient fortement qu'elle était orchestrée par des pirates informatiques basés en Chine, faisant les basses besognes de leur gouvernement[184] » et préservant un lien étroit avec le pouvoir central[185]. Ce sont donc des dizaines de millions de pirates[186] qui se rendent disponibles aux autorités chinoises afin d'effectuer certaines missions et formant un important bassin de recrutement gouvernemental, autant pour la surveillance informatique interne que l'espionnage économique et industriel ici observé[187]. Le flou qu'instaure l'utilisation d'une force civile soulève un important problème d'attribution puisque l'identification d'un mandataire et de son mandant s'avère être une tâche titanesque permettant à un acteur d'invoquer aisément le *déni plausible* concernant son rôle. À cet effet, le ministre chinois de la Défense affirmait, en 2011, qu'il était « non professionnel et sans fondement d'accuser l'armée chinoise de lancer des cyberattaques sans avoir de preuve concluante.[188] » Bien que toujours présente, cette ambiguïté s'est toutefois fortement estompée au même moment où d'autres opérations majeures de cyberespionnage ont été découvertes et décortiquées, permettant de renforcer l'hypothèse initiale qu'au-delà des simples pirates, les autorités politiques chinoises en sont aussi grandement responsables. *Titan Rain* ne se sera avéré qu'être la pointe de l'iceberg.

En 2009, des chercheurs de l'Université de Toronto ont publié un rapport décrivant les activités d'un réseau d'espionnage nommé *GhostNet*, touchant 103 pays, 1295 ordinateurs[189] et « ciblant des emplacements pouvant contenir des informations de grande

---

Shannon Van Sant. « China's freelance hackers : For love of country (and proof that propaganda works). *CBS News*, 15 juillet 2013. En ligne, <www.cbsnews.com/news/chinas-freelance-hackers-for-love-of-country-and-proof-that-propaganda-works-57592999>. Consulté le 10 janvier 2016.

[184] Traduction libre. Ronald J. Deibert. *Black Code: Inside the Battle for Cyberspace*, Toronto: McClelland & Stewart, 2013, p.23.

[185] La Chine a peu d'avantages à les stopper, car en plus de voir ses adversaires internationaux être malmenés sans qu'elle ne soit officiellement impliquée, elle canalise ainsi les éléments subversifs nationaux en les détournant d'une potentielle contestation interne. Klimburg, *op.cit.*, p.48

[186] *Ibid.*, p.46

[187] *Ibid.;* George Patterson Manson. « Cyberwar : The United States and China Prepare For the Next Generation of Conflict », *Comparative Strategy*, vol.30, no.2, 2011, p.122

[188] Traduction libre. Craig Timberg et Ellen Nakashima. « Chinese hackers suspected in attack on The Post's computers », *The Washington Post*, 1 février 2013. En ligne, <www.washingtonpost.com/business/technology/chinese-hackers-suspected-in-attack-on-the-posts-computers/2013/02/01/d5a44fde-6cb1-11e2-bd36-c0fe61a205f6_story.html>. Consulté le 9 janvier 2016.

[189] Ronald Deibert, Arnav Manchanda, Rafal Rohozinski, Nart Villeneuve et Greg Walton. *Tracking Ghostnet : Investigating a Cyber Espionage Network*. 2009, p.40. PDF en ligne, <www.f-secure.com/weblog/archives/ghostnet.pdf>. Consulté le 30 août 2015.

valeur, qu'elles soient politiques, économiques et médiatiques.[190] » Selon eux, tout indique que ces cyberattaques aient été commanditées par l'État chinois à des fins militaires et stratégiques[191], leurs recherches permettant de déterminer que ces attaques provenaient de l'île d'Hainan, siège d'une importante section du renseignement électromagnétique chinois, mais aussi du Troisième département technique de l'Armée populaire de libération (APL)[192]. Ils soulignent ensuite que :

> [...] plusieurs des cibles [...] sont clairement liées à la politique étrangère et de défense chinoise, plus particulièrement en ce qui concerne l'Asie du Sud et du Sud-Est. [...], il y a un arc de nœuds infectés partant de l'Inde, du Bhoutan, du Bangladesh et du Vietnam et se rendant jusqu'au Laos, Brunei, les Philippines, Hong Kong et Taïwan.[193]

Du côté américain, 2010 marquera un changement de ton envers les cyberactivités attribuées à la Chine. Dès janvier, Google dénonça publiquement des cyberattaques chinoises visant entre autres, selon l'entreprise, à accéder aux comptes *Gmail* de défenseurs chinois des droits de l'Homme[194], mais réussissant aussi à mettre la main sur un système important de mots de passe utilisé par l'entreprise[195]. *Operation Aurora*, ainsi nommée par la compagnie McAfee qui en soulignera aussi la complexité inédite[196], a compromis les serveurs informatiques de plus de 34 entreprises américaines œuvrant dans différents secteurs de pointe. Outre Google, la liste de celles qui ont vu leur PI être dévalisée compte notamment Adobe, Yahoo!, Northrop Grumman, Symantec et Dow Chemicals[197]. Après une enquête de l'administration Obama sur les accusations faites par

---

[190] Traduction libre. *Ibid.*, p.47

[191] *Ibid.*, p.52

[192] Deibert. *Black Code*, *op.cit.*, p.24

[193] Traduction libre. Deibert, Manchanda, Rohozinski, Villeneuve et Walton. *Tracking Ghostnet*, *op.cit.*, p.52

[194] Google. « A new approach to China ». *Google Official Blog*, 12 janvier 2010. En ligne, <googleblog.blogspot.ca/2010/01/new-approach-to-china.html>. Consulté le 15 décembre 2015. À la suite de cette sortie, Google déménagea son siège social chinois à Hong Kong, cessa la censure de son moteur de recherche qui sera finalement interdit en Chine continentale. Cette sortie publique poussera même Hillary Clinton, alors secrétaire d'État, à confronter directement Beijing au sujet de ces actions.

[195] John Markoff. « Cyberattack on Google Said to Hit Password System ». *The New York Times*, 19 avril 2010. En ligne, <www.nytimes.com/2010/04/20/technology/20google.html>. Consulté le 15 février 2016.

[196] Dmitri Alperovitch, cité dans Kim Zetter. « Google Hack Attack Was Ultra Sophisticated, New Details Show », *Wired*, 14 janvier 1010. En ligne, <www.wired.com/2010/01/operation-aurora/>. Consulté le 20 décembre 2015.

[197] En plus de celles-ci, les pirates chinois ont également attaqué Juniper Networks, Disney, Sony, Johnson & Johnson, General Electric, General Dynamics et DuPont. Adam Segal. « The Code not Taken: China,

Google, la NSA désigna deux universités chinoises comme étant les responsables de ces intrusions, possédant toutes deux des départements d'informatique avancée et des liens avec l'APL[198].

En 2013, l'entreprise de cybersécurité Mandiant révélait les activités de APT-1 (*Advanced Persistent Threat*), entité chinoise « capable de mener une campagne de cyberespionnage étendue et de longue durée en grande partie parce qu'elle reçoit l'appui direct du gouvernement.[199] » Le rapport déterminera aussi que la responsabilité incombe à l'Unité 61398 de l'APL[200], confirmant donc l'implication chinoise dans les multiples cyberattaques menées en territoire américain. Mandiant a également pu observer qu'en sept ans, APT-1 avait amassé des centaines de téraoctets de données provenant d'au moins 141 organisations[201], pillant régulièrement[202] :

> un lot important de propriétés intellectuelles, incluant des plans technologiques, des procédés de fabrication exclusifs, des résultats de tests et d'essais, des plans d'affaires, des documents de tarification, des ententes de partenariats et les courriels et listes de contacts des dirigeants des organisations touchées.[203]

En 2014, faisant suite aux conclusions de ce rapport, le département de la Justice américaine procédait à la mise en accusation de cinq hauts gradés militaires chinois[204].

Les exemples ici amenés ne sont qu'une partie d'un réseau chinois de cyberespionnage géographiquement étendu et très actif dans sa quête d'informations à valeur ajoutée. Il n'en demeure pas moins que la Chine, par l'entremise de pirates informatiques chevronnés, aussi bien civils que militaires, s'en prend directement et massivement à des

---

the United States and the Future of Cyber Espionage », *Bulletin of the Atomic Scientist*, vol.69, no.5, 2013, p.41.

[198] John Markoff et David Barboza. « 2 China Schools Said to Be Tied to Online Attacks », *The New York Times*, 18 février 2010. En ligne, <www.nytimes.com/2010/02/19/technology/19china.html>. Consulté le 22 mars 2015.

[199] Mandiant. *APT1 : Exposing One of China's Cyber Espionage Units*, 2013, p.2. PDF en ligne, <intelreport.mandiant.com/Mandiant_APT1_Report.pdf>. Consulté le 25 novembre 2015.

[200] *Ibid.*

[201] *Ibid.*, p.3

[202] *Ibid.* Selon Mandiant, APT1 a même eu accès aux serveurs d'une de ces organisations pendant près de cinq ans.

[203] Traduction libre. *Ibid.*

[204] Michael S. Schmidt et David Sanger. « 5 in China Army Face U.S. Charges of Cyberattacks ». *The New York Times.* 19 mai 2014. En ligne, <www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html>. Consulté le 5 janvier 2016.

fleurons américains dominant les différents secteurs auxquels ils appartiennent, qu'ils soient industriels, militaires, scientifiques, technologiques ou économiques.

2.1.2 Une puissance économique relative menacée

Par leur cautionnement du vol massif d'informations provenant des serveurs d'entreprises ou d'agences gouvernementales américaines, les autorités chinoises s'adonnent donc à de l'*espionnage économique*, phénomène en croissance depuis l'avènement d'une mondialisation donnant lieu à l'intensification et à l'expansion géographique de la concurrence dans tous les secteurs industriels[205]. Selon *l'Economic Espionage Act* américain de 1996, un espion économique est « quiconque effectue sciemment le ciblage ou l'acquisition de secrets commerciaux afin d'en faire profiter tout gouvernement étranger, entité politique ou agent dépendant de ce dernier.[206] » Si l'espionnage économique n'est pas l'apanage de la Chine[207], en plus d'être pratiqué par l'Occident depuis plusieurs siècles[208], le vol de PI d'origine chinoise constitue dorénavant un véritable problème de sécurité nationale pour les É.-U.[209].

En s'attaquant ainsi à la puissance économique relative américaine, avantage qui lui permet encore aujourd'hui de soutenir son rôle de première puissance mondiale, la Chine est donc considérée comme ayant ouvertement des intentions nuisibles à l'encontre des É.-U. Par ce type d'activités, elle affecte la vigueur économique américaine, l'un des plus importants aspects de la puissance étatique à une époque où la performance économique est la base du statut relatif d'un État. Dans cette optique, le FBI affirmera même que « la

---

[205] Hadieh Nasheri. *Economic Espionage and Industrial Spying*. Cambridge (U.K.); New York : Cambridge University Press, 2005, p.31.

[206] Traduction libre. États-Unis, U.S. Congress. « Economic Espionage Act of 1996 », *U.S. Code*, 1996, p.3489. PDF en ligne, <www.gpo.gov/fdsys/pkg/PLAW-104publ294/pdf/PLAW-104publ294.pdf>. Consulté le 12 janvier 2016.

[207] En 2014, Robert Gates, Secrétaire à la Défense américain de 2006 à 2011, estimait que la France était particulièrement agressive dans son utilisation d'espionnage économique. « Russian and Chinese Assertiveness Poses New Foreign Policy Challenges : A Conversation With Robert M. Gates », *Council on Foreign Relations*, 21 mai 2014. En ligne, <www.cfr.org/defense-and-security/russian-chinese-assertiveness-poses-new-foreign-policy-challenges/p35645>. Consulté le 11 janvier 2016.

[208] Stephen Mihm. « China Didn't Invent Industrial Espionage ». *Bloomberg View*, 26 mai 2015. En ligne, <www.bloombergview.com/articles/2015-05-26/china-didn-t-invent-industrial-espionage>. Consulté le 15 janvier 2016.

[209] National Bureau of Asian Research. *The Report of the Commission on the Theft of American Intellectual Property*. 2013, p.10. PDF en ligne, <www.ipcommission.org/report/IP_Commission_Report_052213.pdf>. Consulté le 2 janvier 2016

guerre froide n'est pas terminée, elle s'est seulement déplacée dans une nouvelle arène : le marché mondial[210] », car si la force militaire demeure aujourd'hui un facteur déterminant pour un État désirant atteindre ses buts et ambitions, elle n'est plus le moyen privilégié pour y arriver, les conflits armés nationaux allant à l'encontre des normes et des valeurs du système international actuel[211]. Désormais, c'est la performance économique d'un État qui lui permet de s'élever dans la hiérarchie mondiale : pour Michael J. Mazarr, « la puissance nationale dérive de l'habileté d'un État à attirer des investissements et à générer des communautés innovantes, productives et créatives[212] », renforçant autant sa position sur l'échiquier mondial que sa stabilité interne, les performances économiques servant également à assurer le bien-être et la satisfaction des citoyens[213].

C'est cette place centrale de l'économie dans le système international que Deng Xiaoping, important leader chinois, avait compris. Alors que la Chine entrait dans une période post-Mao, plusieurs réformes économiques ont été initiées afin de répondre aux besoins immédiats d'une population montrant des signes de fatigue à l'endroit des politiques maoïstes; pour le Parti communiste chinois (PCC), c'est la préservation de son pouvoir qui en dépendait[214]. Dans le cas chinois, l'écart à combler était très grand puisque la stature économique du pays avait précédemment été durement éprouvée sous Mao, autant par la *Révolution culturelle* que par le *Grand Bond en avant*. En 1986, pour pallier ce retard, Deng a notamment mis en œuvre le *Programme national de recherche et développement de hautes technologies*, ou *Programme 863*, visant à faire profiter la Chine des révolutions technologiques prenant place dans plusieurs domaines, dont la biologie, les vols spatiaux, les télécommunications, les lasers, l'automatisation, l'énergie, les nouveaux matériaux et l'océanographie, etc., « chacun étant un élément-clé dans le plan de la Chine visant à mettre sur pied des capacités de classe mondiale[215]». Ces

---

[210] Traduction libre. États-Unis, Federal Bureau of Investigation. « Focus on Economic Espionage », s.d. En ligne, <www2.fbi.gov/hq/ci/economic.htm#intro>. Consulté le 25 janvier 2016.

[211] Michael J. Mazarr. « Rivalry's New Face », *Survival*, vol. 54, no.4, 2012, p.89

[212] Traduction libre. *Ibid.*, p.91

[213] *Ibid.*, p.90

[214] Charles Burton. « China's Post-Mao Transition: The Role of the Party and Ideology in the "New Period ». *Pacific Affairs*, vol.60, no.3, 1987, p.434 – 435. Mazarr, *op.cit.*, p.89

[215] Traduction libre. Hannas, Mulvenon et Puglisi. *Chinese Industrial Espionage*, *op.*cit, p.11 – 12; Selon Mandiant, l'opération APT1 visait des industries que la Chine avait identifiées comme étant stratégiques à sa croissance dans son 12e plan quinquennal, dans Mandiant, *op.cit.*, p.4.

développements dans des secteurs de pointe permettent également à la Chine de se libérer de sa coûteuse dépendance aux technologies étrangères, plus particulièrement envers les É.-U. et le Japon[216]. Plus encore, le *Plan à moyen et à long terme du développement des Sciences et Technologies* de 2006 a comme objectif, par l'innovation nationale, de positionner la Chine comme « une société orientée vers l'innovation d'ici 2020 et se situant parmi les leaders scientifiques et technologiques mondiaux d'ici 2050[217] », objectif dont la poursuite s'effectue notamment par l'espionnage, aussi bien humain que cyber. S'appuyant d'abord sur un effort national interne, le programme mise sur la collecte de renseignements scientifiques et technologiques étrangers afin d'accélérer son propre développement économique national[218].

En ciblant prioritairement le secteur privé américain, chef de file de plusieurs secteurs visés par le *Programme 863* et joueur central dans les réseaux financiers et commerciaux mondiaux, les pirates informatiques accaparent la PI de nombreuses entreprises[219] et s'en servent afin d'avantager l'industrie chinoise. Plus précisément, ils encouragent les *championnes nationales*, entreprises jouissant d'un appui important de la part du gouvernement chinois par l'octroi de « subventions et de politiques préférentielles, tout en utilisant le pouvoir de marché chinois afin de s'approprier des technologies étrangères, les peaufiner et ainsi créer des *innovations nationales* [...][220] ».

Soupçonnés d'être sous le contrôle direct du gouvernement central chinois[221], ces conglomérats cherchent à concurrencer et à surpasser leurs rivaux étrangers en s'emparant de leurs parts de marché, autant sur le territoire chinois que dans les divers

---

[216] Jamil Anderlini, et al. « Industrial espionage: Data out of the door », *Financial Times*, 1er février 2011. En ligne, <www.ft.com/cms/s/0/ba6c82c0-2e44-11e0-8733-00144feabdc0.html>. Consulté le 2 janvier 2016.

[217] Traduction libre. Adam Segal. Déclaration à la *House of the Representatives*, Committee on Foreign Affairs. *Communist Chinese Cyber-attacks, Cyber-Espionage and Theft of American Technology.* 15 avril 2011. PDF en ligne, <fas.org/irp/congress/2011_hr/china-cyber.pdf>, p.35. Consulté le 8 janvier 2016.

[218] Nigel Inkster. « Chinese Intelligence in the Cyber Age », *Survival*, vol.55, no.1, 2013, p.50

[219] Segal, *The Code Not Taken*, *op.cit.*, p.41

[220] Traduction libre. James McGregor. « Time to rethink U.S.-China trade relations », *The Washington Post*, 19 mai 2010. En ligne, <www.washingtonpost.com/wp-dyn/content/article/2010/05/13/AR2010051303551.html>. Consulté le 3 janvier 2016.

[221] Andrew Szamosszegi et Cole Kyle. *An Analysis of State-owned Enterprises and State. Capitalism in China.* Washington D.C. : U.S.-China Economic and Security Review Commission. 2011, p.2. PDF en ligne,<www.uscc.gov/sites/default/files/Research/10_26_11_CapitalTradeSOEStudy.pdf>. Consulté le 3 janvier 2015

marchés mondiaux[222]. En plus de dévoiler les stratégies de négociations et les informations financières de leurs compétiteurs, facilitant la prise de décisions stratégiques[223], les informations illégalement amassées peuvent aider à battre des compétiteurs dans leur propre marché national, en offrant à bas prix des produits pour lesquels ils n'ont pas investi en R et D, une étape aux coûts très élevés[224]. Alors que le retour sur l'investissement s'avère avantageux et les obstacles relativement peu nombreux[225], la Chine « [...] a maintenant une mesure incitative puissante pour utiliser tous les moyens possibles lui permettant de grimper dans la chaîne de valeur économique et d'éviter le piège du revenu intermédiaire[226] », aspects essentiels à la protection de ses intérêts économiques et politiques, dont intérieurs, et pour lesquels le cyberespionnage s'avère fort utile[227]. Dirigées envers des organisations aidant les É.-U. à préserver leur prédominance économique, ces cyberattaques représentent donc une menace réelle, autant à l'endroit de la prospérité économique que de la supériorité militaire des É.-U.[228]

Qualifiée du « plus grand transfert de richesse par l'entremise du vol et du piratage de l'histoire de l'humanité[229] » par le général Keith B. Alexander[230], cette situation a rapidement soulevé les inquiétudes à Washington : Barack Obama a affirmé craindre qu'elles affaiblissent économiquement les É.-U.[231], alors que Tom Donilon[232] dira publiquement que les vols de PI et de secrets commerciaux, éléments « essentiels à l'innovation et à la croissance économique [...], sont passés au premier plan de notre

---

[222] John Lee. « Cyber Kleptomaniacs : Why China Steals Our Secrets », *World Affairs*, vol.176, no.3, 2013, p.79; Amy Chang. *Warring States : China's Cybersecurity Strategy*. Washington D.C. : Center for a New American Century, 2014, p.21.

[223] Segal, *The Code Not Taken, op.cit.*, p.41; Adam Segal. « Chinese Computer Games : Keeping Sage in Cyberspace », *Foreign Affairs*, 1 mars 2012. En ligne, <www.foreignaffairs.com/articles/china/2012-03-01/chinese-computer-games>. Consulté le 10 janvier 2016.

[224] Michael Chertoff, William Lynn et Mike McConnell. « China's Cyber Thievery Is National Policy—And Must Be Challenged », *The Wall Street Journal*, 27 janvier 2012. En ligne, <www.wsj.com/articles/SB10001424052970203718504577178832338032176>. Consulté le 4 janvier 2016.

[225] Bryan Krekel. *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network*. Washington D.C. : The US-China Economic and Security Review Commission, 2009, p.51.

[226] Traduction libre. *Ibid.*, p.60

[227] Chang, *op.cit.*, p.22.

[228] États-Unis, Office of the National Counterintelligence Executive. *Foreign Spies Stealing U.S.Economic Secrets in Cyberespace*. Washington D.C. : Office of the Director of National Intelligence, 2011, p.i

[229] Traduction libre. Gen. Keith B. Alexander « Building a New Command in Cyberspace », *Strategic Studies Quarterly*, vol.5, no.2, 2011, p.6

[230] Directeur de la NSA de 2005 à 2014 et commandant du USCYBERCOM de 2009 à 2014.

[231] Segal, *The Code Not Taken, op.cit.*, p.38

[232] Conseiller pour la sécurité nationale d'Obama de 2010 à 2013.

ordre du jour.[233] » Une carte provenant de la NSA et dévoilée par Snowden démontre qu'entre 2009 et 2014, 600 entreprises ont été victimes d'une opération réussie de cyberespionnage[234]. Diverses estimations faites par des instances gouvernementales américaines indiquent un impact certain, bien que difficile à définir, sur les intérêts économiques américains. En 2012, au moment où l'économie américaine cherchait encore à se sortir de la crise de 2007, le général Alexander estimait que le vol de PI, d'origine chinoise ou non, faisait perdre environ 250 milliards de dollars annuellement aux entreprises américaines[235]. Alors qu'entre 2009 et 2012, le taux de chômage américain demeurait supérieur à 8%, atteignant même le cap du 10% en octobre 2009, ces pertes de revenus nuisent donc à la création et à la préservation d'emplois basés aux É.-U.[236]. Si le secteur industriel des PI soutenait à lui seul 40 millions d'emplois en 2010, soit 27,7% de toute la main d'œuvre américaine[237], une étude de 2011 de la *United States International Trade Commission* estimait que le respect par la Chine des lois protégeant la PI pourrait créer plus de 2 millions d'emplois à temps plein aux É.-U.[238].

Au-delà des chiffres, ces cyberactivités, s'appropriant la PI développée à gros prix par des firmes américaines, s'attaquent également à l'idée de l'innovation américaine, le moteur historique de son développement économique et de son ascension vers la place de plus grande puissance mondiale. En 2010, les entreprises œuvrant spécifiquement dans le domaine de l'innovation, s'affairant principalement à la recherche, au brevetage et à l'exploitation exclusive de PI, représentaient 34,8% du PIB américain[239]. Par leur

---

[233] Traduction libre. Liz Flora. « Complete Transcript: Thomas Donilon at Asia Society New York ». *Asia Society*, 11 mars 2013. En ligne, <asiasociety.org/new-york/complete-transcript-thomas-donilon-asia-society-new-york>. Consulté le 10 janvier 2016.

[234] Voir Annexe F

[235] Josh Rogin. « NSA Chief: NSA Chief: Cybercrime constitutes the "greatest transfer of wealth in history" », *Foreign Policy*, 9 juillet 2012. En ligne, <foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/>. Consulté le 15 décembre 2015.

[236] National Bureau of Asian Research, *op.cit.*, p.9-10

[237] États-Unis, Economics and Statistics Administration et United States Patent and Trademark Office. *Intellectual Property and the U.S. Economy: Industries in Focus*. Washington D.C. : U.S. Department of Commerce, mars 2012, p.43. PDF en ligne, <www.uspto.gov/sites/default/files/news/publications/IP_Report_March_2012.pdf>. Consulté le 12 janvier 2016.

[238] États-Unis, United States International Trade Commission. *China: Effects of Intellectual Property Infringement and Indigenous Innovation Policies on the U.S. Economy*. Washington D.C. : United States International Trade Commission, 2011, p.xx. PDF en ligne, <www.usitc.gov/publications/332/pub4226.pdf>. Consulté le 8 janvier 2016.

[239] Economics and Statistics Administration et United States Patent and Trademark Office, *op.cit.*, p.3

ampleur, elles revêtent donc une importance capitale au sein de l'économie américaine et nécessitent d'être protégées, car « personne ne veut créer de nouvelles idées s'il y a de fortes probabilités que celles-ci soient volées, utilisées et vendues par des compétiteurs[240] ». Aux É.-U., alors que ces craintes sont matérialisées et facilitées par l'avènement de l'espionnage dit cyber, un calcul coût-bénéfice désavantageux cause une diminution autant de l'innovation que de l'entrepreneuriat l'accompagnant, deux éléments pourtant indispensables au développement économique à long terme, aussi bien sur le plan national que mondial[241].

Outre la compétitivité accrue des entreprises chinoises sur les marchés mondiaux, la Chine cherche aussi à rivaliser le plus rapidement possible avec les É.-U. sur le plan militaire, intense processus de modernisation profitant de l'espionnage pour lui procurer un avantage substantiel, notamment par l'élimination des coûts de R et D et du temps nécessaire à la conception de plans[242] . Par l'accaparement de technologies étrangères,

> l'objectif à long terme de Beijing est de créer une industrie nationale de défense capable de répondre aux besoins de l'APL en matière de modernisation et de rivaliser en tant que producteur de premier plan dans le commerce mondial de l'armement.[243]

En ce sens, la mise en service prochaine des avions de chasse chinois de type J-20 et J-31 démontre toute l'ampleur de cette politique. Du côté américain, plusieurs les considèrent comme étant fortement apparentés à des appareils américains de cinquième génération[244], respectivement le *F-22 Raptor* et le *F-35 Joint Strike Fighter*. La conception de ce dernier a coûté jusqu'à maintenant plus de 400 milliards de dollars, le plus dispendieux dans l'histoire du Pentagone[245]. Ces soupçons sont alimentés par le fait

---

[240] Traduction libre. Nasheri, *op.cit.*, p.62

[241] Darrell M. West. *Technology and the Innovation Economy*. Washington D.C. : Brookings Institution Press, 2011, p.1. PDF en ligne, <www.brookings.edu/~/media/research/files/papers/2011/10/19-technology-innovation-west/1019_technology_innovation_west.pdf>. Consulté le 9 janvier 2016; Economics and Statistics Administration et United States Patent and Trademark Office, *op.cit.*, p.9-10

[242] The Wall Street Journal. « China's Cyber-Theft Jet Fighter ». *The Wall Street Journal*, 12 novembre 2014. En ligne, <www.wsj.com/articles/chinas-cyber-theft-jet-fighter-1415838777>. Consulté le 20 décembre 2015.

[243] Traduction libre. États-Unis, Office of the Secretary of Defense. *Military Power of the People's Republic of China 2009*, Washington D.C.: Department of Defense, 2009, p.31.

[244] Brendan McGarry. « Lawmaker: Chinese J-31, J-20 'Mirror' American F-35, F-22 ». *DefenseTech*, 8 janvier 2016. En ligne, <defensetech.org/2015/09/29/lawmaker-chinese-j-31-j-20-mirror-american-f-35-f-22/>. Consulté le 9 janvier 2016.

[245] The Wall Street Journal. « China's Cyber-Theft Jet Fighter », *op.cit.*

que des cyberattaques répétées contre les réseaux informatiques reliés à son élaboration ont eu lieu, menant entre autres à des intrusions chez Lockheed Martin[246] et BAE Systems[247], deux fournisseurs associés au projet, d'où sera effectué un transfert de « plusieurs téraoctets de données relatives à sa conception et à ses systèmes électroniques [...], rendant potentiellement plus facile la défense contre cet appareil.[248] » En créant ainsi de potentielles vulnérabilités dans le système du F-35, contenant 7,5 millions lignes de code informatique[249], ce vol d'informations repoussa d'un an le projet et provoqua une augmentation de ses coûts de 50%[250].

Cette tendance pourrait s'être reproduite notamment avec les drones, secteur où la Chine « a intensifié la recherche au cours des dernières années, et ce plus rapidement que tout autre pays[251] », tendance pouvant s'expliquer par le cyberespionnage, alors que le drone chinois CH-4, qui a fait ses premières sorties en Irak en décembre 2015[252], ressemblerait énormément au *Reaper* américain[253] et le *Wing Loong*, au *Predator*[254]. Alors que le marché mondial du drone militaire pourrait dépasser le 10 milliards en 2024[255], cet accaparement technologique s'avérerait avantageux pour la Chine. Certains craignent également que des cyberattaques chinoises aient pillé sur une période de trois ans les

---

[246] *Ibid.*

[247] Sydney J. Freedberg. « Top Official Admits F-35 Stealth Fighter Secrets Stolen ». *Breaking Defense*, 20 juin 2013. En ligne, <breakingdefense.com/2013/06/top-official-admits-f-35-stealth-fighter-secrets-stolen/>. Consulté le 9 janvier 2016.

[248] Traduction libre. The Wall Street Journal. « China's Cyber-Theft Jet Fighter », *op.cit.*

[249] Siobhan Gorman, August Cole et Yochi Dreazen. « Computer Spies Breach Fighter-Jet Project ». *The Wall Street Journal*, 21 avril 2009. En ligne, <www.wsj.com/articles/SB124027491029837401>. Consulté le 10 janvier 2016.

[250] Shane Harris. *@War : The Rise of the Military-Internet Complex*. New York : Houghton Mifflin Harcourt, 2014, p. xvii.

[251] Traduction libre. États-Unis, Defense Science Board. *Task Force Report : The Role of Autonomy in DoD Systems*. Washington D.C. : Department of Defense, p.69. PDF en ligne, <www.acq.osd.mil/dsb/reports/AutonomyReport.pdf>. Consulté le 8 janvier 2016.

[252] Patrick Boehler et Gerry Doyle. « Use by Iraqi Military May Be a Boon for China-Made Drones ». *The New York Times*, 17 décembre 2015. En ligne, <www.nytimes.com/2015/12/18/business/international/china-drone-export-iraq.html>. Consulté le 15 janvier 2016.

[253] Bill Gertz. « China's armed drones appear built from stolen data from US cyber intrusions ». *Asia Times*, 29 décembre 2015. En ligne, <atimes.com/2015/12/chinas-armed-drones-appear-built-from-stolen-data-from-us-cyber-intrusions/>. Consulté le 15 janvier 2016.

[254] Adam Rawnsley. « Meet China's Killer Drones ». *Foreign Policy*, 14 janvier 2016. En ligne, <foreignpolicy.com/2016/01/14/meet-chinas-killer-drones/>. Consulté le 15 janvier 2016.

[255] Agence France-Presse. « Experts: Drone market to hit $10 billion by 2024 ». *DefenseNews*, 3 octobre 2015. En ligne, <www.defensenews.com/story/defense/air-space/2015/10/03/experts-drone-market-hit-10-billion-2024/73282590/>. Consulté le 19 janvier 2016.

données de la filiale américaine de QinetiQ, une entreprise britannique se spécialisant dans la robotique militaire. Ces infiltrations pourraient avoir fourni à la Chine la capacité de reproduire certains des robots utilisés par les forces armées américaines et de rattraper rapidement et à un coût moindre l'avantage technologique que les É.-U. cherchent à obtenir[256].

Finalement, cette capacité chinoise à infiltrer les réseaux et systèmes informatiques américains représente un véritable problème, car « comme la puissance militaire d'un État dépend en définitive de sa vitalité économique, les pertes soutenues de propriété intellectuelle pourraient éroder autant l'efficacité militaire des É.-U. que sa compétitivité dans l'économie globale.[257] »Si elles affectent certainement l'économie américaine, elles permettent aussi à la Chine de faire d'immenses progrès dans les domaines économiques et militaires, autant en copiant ce qui est fait ailleurs dans le monde, qu'en lui permettant d'investir grandement dans la modernisation de ses forces armées, une initiative encouragée par la croissance annuelle du PIB chinois, franchissant souvent les 10%. C'est ainsi que le cyberespionnage économique et industriel, un aspect spécifique d'une menace économique chinoise globale, réduit la marge de manœuvre d'Obama concernant la mise en place d'investissements militaires lui donnant les moyens d'atteindre les objectifs de sa grande stratégie.

2.2 Une menace progressivement abordée en termes offensifs et militaires

À la suite des *cyberincidents* se manifestant aux quatre coins du monde, la crainte que soulève le cyberespionnage, tentaculaire et constaté avec impuissance, s'est déplacée vers celle des cyberattaques de plus grande envergure, où cette même fragilité sous-tend désormais des conséquences potentielles d'un tout autre niveau. Cette section abordera la nature et les impacts du nouveau visage de la cybermenace chinoise, dépassant maintenant les simples vols de données. Il sera d'abord question d'une conception nouvelle des cybercapacités, vision offensive et abordée sous les aspects sécuritaires,

---

[256] Aliya Sternstein. « US Hiring Researchers to See if China's Military Robots Originiate from Hacked Designs ». *DefenseOne*, 15 janvier 2016. En ligne, <www.defenseone.com/technology/2016/01/us-thinks-china-may-have-stolen-military-robot-designs/125168/>. Consulté le 15 janvier 2016.

[257] William J. Lynn III. « Defending a New Domain: The Pentagon's Cyberstrategy », *Foreign Affairs*, vol.89, no.5, 2010, p.100

militaires et stratégiques. Des opérations comme *Stuxnet* donneront également un avant-goût inquiétant des vulnérabilités américaines, notamment concernant les IC, structures responsables du bon fonctionnement de la société, mais aussi de plus en plus dépendantes du cyberespace.

Ensuite, les cybercapacités chinoises, désormais considérées comme facilitatrices de potentielles agressions armées, s'entremêlent avec des intentions offensives rapportées par une littérature stratégique chinoise nombreuse. Cette dernière prône l'utilisation de ces cybercapacités dans divers scénarios militaires afin de limiter la capacité et la volonté de la puissance américaine d'intervenir en mer de Chine afin de contrer ou de contenir ses ambitions territoriales. L'utilisation militaire des cybercapacités chinoises menace donc directement la capacité américaine à projeter sa puissance où et quand les É.-U. le désirent, un élément que requiert pourtant la grande stratégie d'engagement sélectif prônée par Obama.

2.2.1 Les cybercapacités perçues comme favorisant l'offensive

Dès 2007, un visage plus inquiétant de la menace cybernétique est apparu : des cyberattaques d'origine russe[258] paralysaient les sociétés estoniennes et, un an plus tard, géorgiennes[259], *Anonymous* rendait inaccessibles des sites internet ciblés en guise de protestation et l'aviation israélienne pénétrait en Syrie afin d'y raser *incognito* une centrale nucléaire après avoir piraté les défenses antiaériennes syriennes[260]. En 2010, la donne changea véritablement avec la découverte de Stuxnet, virus dont l'objectif tactique était de rendre inutilisables les centrifugeuses de la centrale nucléaire iranienne de Natanz, un site présumé d'enrichissement d'uranium à des fins militaires. Malgré l'échec de sa visée stratégique (mettre un terme au programme nucléaire iranien), cette opération a tout de même repoussé les limites de ce qui avait été jusqu'à maintenant qualifié de cyberattaque par le bris de plusieurs centrifugeuses. Alors qu'une capacité destructrice à

---

[258] Singer et Friedman. *Cybersecurity and Cyberwar*, *op.cit.*, p.110 – 111; Jeffrey Carr. *Inside Cyber Warfare : Mapping the Cyber Underworld*. Sebastopol, California : O'Reilly Media, 2012, p.17 – 18

[259] Respectivement en 2007 et en 2008. Dans le cas de la Géorgie, les cyberattaques sont effectuées parallèlement à l'invasion russe de la Géorgie, elle-même intervenue en Ossétie du Sud.

[260] Pierre Razoux. « Israël frappe la Syrie : un raid mystérieux », *Politique étrangère*, vol.73, n.1, 2008, pp.9 – 22

l'encontre d'une IC avait désormais été atteinte par une arme cybernétique, l'opérationnalisation d'un nouveau champ de bataille se mettait en branle. Opération issue d'une collaboration israélo-américaine[261], la mise au jour de Stuxnet provoqua de fortes réactions aux É.-U., une situation aggravée par la propagation du virus aux quatre coins du monde et par la divulgation de son architecture complexe.

Pourtant, les dangers du cyberespace étaient déjà évoqués bien avant Stuxnet: en 2010, Mike McConnell[262] n'hésitait pas à proclamer que « les cyberattaques ont le potentiel de mettre en danger notre mode de vie d'une manière aussi dévastatrice qu'une arme nucléaire[263] », le sénateur américain Carl Levin affirmait quant à lui que leurs effets se rapprochaient de ceux des armes de destruction massive[264], tandis qu'en 2009, Obama les qualifiait de potentielles « armes de perturbation massive[265] ». Deux ans plus tard, Leon E. Panetta[266] prononçait un discours alarmiste démontrant l'ampleur des craintes post-Stuxnet que certains décideurs pouvaient désormais ressentir au sujet du cyberespace :

> Une cyberattaque perpétrée par des États ou des groupes extrémistes violents pourrait être aussi destructrice que les attaques terroristes du 11-septembre. Une telle cyberattaque terroriste pourrait virtuellement paralyser le pays. [...] Nous savons que ces cyber acteurs étrangers examinent les réseaux des IC des É.-U. [...] ils cherchent à créer des outils avancés pour attaquer ces systèmes et ainsi causer panique, destruction et pertes de vies. [...] Le résultat collectif de ces types d'attaques pourrait être un cyber Pearl Harbor, paralysant et bouleversant la nation et créant un nouveau et profond sens de vulnérabilité.[267]

---

[261] David E. Sanger. *Confront and Conceal : Obama's Secret Wars and Surprising Use of American Power*. New York : Broadway Paperbacks, 2012, p.207

[262] Directeur des services de renseignement américain de 2007 à 2009 et directeur de la NSA entre 1992 et 1996.

[263] Traduction libre. Mike McConnell. « Cyberwar is the New Atomic Age », *New Perspectives Quarterly*, vol.26, no.3, 2009, p.75

[264] Sen. Carl Levin, cité dans Jerry Brito et Tate Watkins. 2011. « Loving the Cyber Bomb: The Dangers of Threat Inflation in Cybersecurity Policy », *Harvard National Security Journal*, vol.3, no.1, 2011, p.39 – 40.

[265] États-Unis, White House. *Remarks by the President on Securing our Nation's Cyber Infrastructure*. Washington D.C. : The White House, 2009. En ligne, <www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure>. Consulté le 20 février 2016.

[266] Secrétaire à la Défense des É.-U. entre 2011 et 2013.

[267] Traduction libre. États-Unis, Department of Defense. *Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security*. Washington: Department of Defense, 2012. En ligne, <www.defense.gov/transcripts/transcript.aspx?transcriptid=5136>. Consulté le 12 janvier 2016.

Bien que plusieurs contestent cette surenchère[268], l'utilisation de ces différentes analogies démontre que plusieurs comparent Stuxnet à l'ouverture d'une boîte de Pandore exacerbant les risques qu'une cyberattaque majeure n'atteigne les É.-U. Un sentiment d'urgence depuis répandu, car en 2014, une étude du *Pew Research Center* affirmait que 61% des 1,642 répondants sondés, provenant de différents milieux pertinents, estimaient qu'« une attaque majeure causant des dommages à grande échelle pourrait se produire d'ici 2025.[269] » Pour William J. Lynn III et autres cyberpessimistes, la nature du cyberespace met en place trois conditions augmentant le risque latent d'une telle éventualité: 1) le bas prix relatif des cybercapacités permet la création d'une asymétrie militaire, 2) la notion d'anonymat complexifiant la mise en place de mesures dissuasives et finalement, 3) l'architecture d'Internet permettant un avantage offensif considérable[270].

Le général William T. Lord[271] affirmait en 2009 qu'un ordinateur et une connexion à Internet, deux éléments facilement accessibles, suffisaient pour mener une cyberattaque majeure[272]. Selon lui, un peu de savoir-faire et de recherche dans les profondeurs du Web suffirait pour mettre la main sur les outils nécessaires à une attaque qui ne serait plus soumise aux contraintes géographiques[273]. Si le budget de 300 millions de dollars consacré à l'élaboration de Stuxnet[274] a néanmoins démontré qu'une cyberattaque majeure nécessitait des moyens favorisant les entités riches[275], cette importante somme peut toutefois être relativisée. Même si le secteur de la sécurité nationale américaine

---

[268] De plus en plus de voix discordantes, celles des « cybersceptiques », dénoncent l'ampleur prise par les enjeux entourant la cybersécurité et la dangerosité d'éventuelles cyberattaques. Des chercheurs tels Erik Gartzke et Thomas Rid remettent ainsi en question cette vision du cyberespace, celle d'une source de menaces imminentes, pour en relativiser les dangers et l'avantage offensif sans limite. Voir notamment Thomas Rid. *Cyberwar Will Not Take Place.* Londres : Hurst & Company, 2013; Erik Gartzke. « The Myth of Cyberwar : Bringing War in Cyberspace Back Down to Earth ». *International Security*, vol.38, no.2, 2013.

[269] Traduction libre. Lee Rainie, Janna Anderson et Jennifer Connolly. « Cyber Attacks Likely to Increase ». *Pew Research Center*, 29 octobre 2014. En ligne, <www.pewinternet.org/2014/10/29/cyber-attacks-likely-to-increase/>. Consulté le 5 janvier 2016.

[270] Lynn III. *Defending New Domain, op.cit.*, p.98 – 99

[271] Commandant du Air Force Cyberspace Command de 2007 à 2009.

[272] Glenn Derene. « The Coming Cyberwar: Inside the Pentagon's Plan to Fight Back » *Popular Mechanics*, 1er octobre 2009. En ligne. <www.popularmechanics.com/technology/military/4277463>. Consultée le 11 décembre 2013

[273] Adam P. Liff. « Cyberwar: A New 'Absolute Weapon'? ». *The Journal of Strategic Studies*, vol.35, no.3, 2012, p.410

[274] Jon R. Lindsay. « Stuxnet and the Limits of Cyber Warfare », *Security Studies*, vol.22, no.3, 2013, p.388

[275] David Betz. « Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed », *Journal of Strategic Studies*, vol.35, no.5, 2012, p.696

estime que les États demeurent la source de menaces principale envers les É.-U. dans le cyberespace[276], « le bas coût des périphériques informatiques signifie que les adversaires des É.-U. n'ont pas à fabriquer des armes dispendieuses, telles que des chasseurs furtifs ou des porte-avions, afin de représenter une menace importante envers les capacités militaires américaines.[277] » Bien qu'un équipement informatique rudimentaire ne soit pas suffisant en soi pour mener des cyberattaques de grande ampleur, la mise en place de cybercapacités représente, pour un État placé en situation d'infériorité, une solution alternative et rentable au développement de capacités dites conventionnelles, ce qui lui permet de se doter d'une force asymétrique aux effets potentiels comparables, comme dans le cas chinois, ici abordé.

Selon eux, le cyberespace fournit également un avantage considérable aux potentiels utilisateurs malintentionnés : l'anonymat. La grande difficulté à détecter et à retracer l'origine exacte d'une attaque dans un délai raisonnable est accentuée par la capacité des attaquants à camoufler leur emplacement géographique réel. De plus, même si un soupçon concernant un potentiel suspect se manifeste, mener des représailles s'avère complexe. En plus de devoir distinguer clairement si l'attaque provient d'acteurs étatiques ou civils, des règles différentes s'appliquant à chacun des groupes, une éventuelle réplique devrait aussi respecter le principe de *discrimination* tel que convenu au niveau du droit international, devant « distinguer les objectifs militaires, qui peuvent être attaqués, des populations et des biens civils qui ne doivent pas faire l'objet d'aucune attaque volontaire.[278] » Les réseaux militaires reposant en partie sur des infrastructures civiles et des cyberattaques pouvant avoir des comportements imprévus[279], il est donc difficile de s'assurer qu'une riposte cyber serait limitée au niveau de sa portée et de ses effets, même si le défendeur parvient à identifier précisément celui ou celle qu'il doit punir[280]. Alors

---

[276] McConnell, *Cyber Insecurities*, *op.cit.*, pp.27 – 39, Washington D.C. : Center for A New American Society, 2011, p.29.

[277] Traduction libre. Lynn III, *Defending New Domain*, *op.cit.*, p.98

[278] France, Ministère de la Défense. Droit des conflits armés, 16 novembre 2011. En ligne, <www.defense.gouv.fr/sga/le-sga-en-action/droit-et-defense/droit-des-conflits-armes/droit-des-conflits-armes>. Consulté le 2 février 2016.

[279] Dans le cas de Stuxnet, le virus s'est échappé de sa cible initiale pour ensuite se répandre aux quatre coins du monde.

[280] John Markoff, David E. Sanger et Thom Shanker. « In Digital Combat, U.S. Finds No Easy Deterrent », The New York Times, 25 janvier 2010. En ligne, <www.nytimes.com/2010/01/26/world/26cyber.html?pagewanted=all>. Consulté le 10 janvier 2016.

que l'attaquant semble profiter d'une certaine impunité provoquant un sentiment d'impuissance chez la victime, un État attaqué ne peut non plus compter sur sa force dissuasive, même nucléaire, afin de menacer à son tour un adversaire de représailles en cas de comportement inadéquat. Les coûts éventuels d'une attaque s'avèrent donc minimes comparativement aux bénéfices qu'il est possible d'en retirer[281]. Ainsi, pour Martin Libicki, « une posture claire de dissuasion confrontée à une cyberattaque aux effets manifestes, mais à l'origine floue, crée un douloureux dilemme : répondre et risquer de se tromper ou s'abstenir et voir ses autres moyens de dissuasion perdre leur crédibilité.[282] »

Finalement, puisque les puissances industrielles doivent défendre un front informatique décentralisé et étendu, conséquence même de leur ascendant technologique[283], les cyberattaques peuvent être réalisées avec une certaine facilité et en fournissant un avantage majeur à l'attaquant, autant du point de vue technique que stratégique. Avec l'élargissement constant de l'*Internet des objets*, qui pourrait, en 2020, inclure plus de 50 milliards d'éléments[284] disséminés dans toutes les sphères de la société, les points d'entrée potentiels se multiplient pour ceux désirant les exploiter. Cette malveillance est de plus facilitée par la présence fréquente de graves lacunes au niveau de leur sécurité informatique[285]. Cette situation rend pratiquement vain un effort défensif coûteux[286] puisque les failles d'un système sont imperceptibles jusqu'à ce qu'une attaque permette de les découvrir et de les colmater, celles-ci pouvant même être implantées directement dans les composantes physiques d'un système informatique[287]. Pour Lynn III, « les É.-U. ne peuvent pas retraiter derrière une ligne Maginot de pare-feu ou ils risquent d'être envahis. La cyberguerre est comme une guerre de manœuvre, où ce sont la vitesse et

---

[281] Kello, *op.cit.*, p.33.

[282] Traduction libre. Martin C. Libicki. *Cyberdeterrence and Cyberwar*. Santa Monica, CA : RAND, 2009, p.xvi.

[283] La cyberdéfense nationale mise effectivement plutôt sur la collaboration d'acteurs divers et hétéroclites, tels les autorités gouvernementales, le secteur industriel et commercial, sans oublier les particuliers

[284] Cisco. « The Internet of Things ». *Cisco Visualisation*. s.d. En ligne, <share.cisco.com/internet-of-things.html>. Consulté le 7 janvier 2016.

[285] La sécurité informatique est souvent reléguée au second plan au profit de la convivialité, de la facilité d'utilisation et de la profitabilité financière. Voir Ijeoma Onyeji, Morgan Bazilian et Chris Bronk. 2014. « Cyber Security and Critical Energy Infrastructure ». *The Electricity Journal*, vol. 27, no 2, p. 56.

[286] Lucas Kello. « The Meaning of the Cyber Revolution : Perils to Theory and Statecraft ». *International Security*, vol. 38, no.2, 2013, p.27

[287] Kello, *op.cit.*, p.27; Lynn III, *Defending a New Domain*, *op.cit.*, p.101

l'agilité qui comptent le plus.[288] » Tout comme la *Wermacht* nazie a franchi les Ardennes, point faible de la ligne Maginot, pour envahir la France en un temps record, le cyberespace pourrait être lui aussi à l'origine d'un nouveau type de *blitzkrieg*, une opération militaire rapide et décisive ne laissant aucune chance à la victime.

Une telle interprétation offensive des cybercapacités a un impact sur l'*équilibre entre l'attaque et la défense*, un concept influençant le regard que les chefs d'État peuvent porter sur les acteurs étatiques les détenant. Pour Charles Glaser, quand l'attaque possède un avantage marqué, ou semble la posséder[289], que ce soit par des facteurs géographiques ou technologiques, les tensions internationales risquent davantage de se transformer en véritables conflits militaires parce qu'ils :

> [...] seront rapides et décisifs, donc profitables, rendant la guerre plus attirante pour les États cupides. Les États se sentiront moins en sécurité, augmentant la valeur de l'expansion, alors que ceux recherchant d'abord la sécurité trouveront la guerre plus attirante. L'avantage de la première frappe s'accroît avec l'avantage offensif, augmentant la probabilité que des crises escaladent par l'entremise d'attaques préventives ou d'accidents.[290]

A contrario, quand la défense a ou semble avoir le dessus, le *statu quo* est plus facilement maintenu et la coopération plus courante, car lancer un assaut nécessiterait un plus grand investissement afin d'en retirer des bénéfices incertains et/ou plus faibles[291]. Un autre point important de l'équilibre attaque-défense influence la réaction d'un État devant faire face à un adversaire possédant de telles capacités, soit la possibilité de différencier clairement une arme défensive d'une arme offensive. En effet, « les États accordent une attention spéciale aux actions qu'ils considèrent comme n'étant pas celles entreprises par un État prônant le *statu quo*, estimant que ceux démontrant un tel comportement sont agressifs.[292] » Cette caractéristique fait en sorte que si l'éventualité d'un conflit est plus grande, le niveau de tolérance des hommes d'État sera quant à lui au plus bas, percevant

---

[288] Traduction libre. Lynn III, *Defending a New Domain, op.cit.*, p.99

[289] Pour Stephen Van Evera, les risques sont les mêmes lorsque l'avantage est perçu plutôt que réel, mais les conséquences peuvent être désastreuses, comme a pu le démontrer la première Guerre mondiale. Stephen Van Evera. « Offense, Defense, and the Causes of War ». *International Security,* vol.22, no.4, 1998, p.6.

[290] Traduction libre. Charles L. Glaser et Chairn Kaufmann. « What Is the Offense-Defense Balance and How Can We Measure It? ». *International Security,* vol.22, no.4, 1998, p.48

[291] Robert Jervis. « Cooperation under the Security Dilemma ». *World Politics*, vol.30, no.2, 1978, p.190

[292] *Ibid.*, p.200

plus aisément les autres pays comme étant potentiellement agressifs, voire même prêts, comme l'indique Glaser, à attaquer préventivement[293]. Appliqués au cyberespace, les facteurs favorisant l'offensive inquiètent donc forcément les É.-U., eux qui, par l'entremise des opérations de cyberespionnage, estiment n'avoir vu que la pointe de l'iceberg.

2.2.2 Des cyberintrusions chinoises réinterprétées sous le prisme militaire

La possibilité que la Chine se serve préventivement de ses capacités cybernétiques, désormais perçues comme étant résolument offensives, soulève des craintes aux fondements bien réels pour les É.-U. S'il survenait, un tel évènement pourrait avoir des conséquences majeures sur la capacité américaine à projeter sa puissance dans le monde entier et à intervenir militairement et librement afin de maintenir la paix et la stabilité en Asie-Pacifique. L'ampleur de l'arsenal cybernétique chinois demeurant inconnue, l'idée que des cyberattaques surprises soient lancées au cours d'une potentielle offensive militaire gagne en crédibilité et en intensité lorsqu'elle est analysée à travers le prisme d'une littérature stratégique chinoise évoquant justement cette éventualité en cas de conflit avec les É.-U. Pour le Pentagone, cette attribution d'intentions claires, précises et offensives laisse entrevoir une menace potentielle nécessitant une attention particulière : le véritable culte du secret mis en place du côté chinois, situation souvent dénoncée par les É.-U.[294] fait en sorte que « même si la posture militaire de l'autre est actuellement pacifique, elle pourrait développer des intentions agressives dans le futur.[295] »

Lors de la guerre du Golfe, les É.-U., alors sur le point de devenir *de facto* la plus grande puissance mondiale, ont démontré leur avantage militaire relatif obtenu par l'entremise d'une nouvelle *Révolution dans les affaires militaires* (RAM) qui, par de profonds changements techniques, organisationnels et doctrinaires[296] rendait possible :

---

[293] *Ibid.*, p.189 – 190.
[294] Jonathan D. Pollack. « Chinese Military Power : What Vexes the United States and Why? », *Orbis*, vol.51, no.4, 2007, p.647
[295] Jervis, *op.cit.*, p.199
[296] James K. Morningstar. « Technologies, Doctrine, and Organization for RMA », *Joint Forces Quarterly*, no.15, 1997, p.37

> l'application de forces militaires précises contre des infrastructures de communications et de commandement ennemies, l'accélération du déroulement des opérations militaires et la domination sur le plan de la manœuvre et de l'information guidant le combat dans la totalité de l'espace[297].

Ces changements considérables découlent de l'information, désormais recueillie en très grande quantité et rapidement traitée grâce au développement des secteurs des TIC associés au C4ISR (commandement, contrôle, communications, informatique, renseignement, surveillance et reconnaissance). Cette capacité informationnelle permet donc d'obtenir une supériorité militaire par la connaissance de l'espace de combat[298] (*Dominant Battlespace Knowledge)*, « améliorant la conscience situationnelle, réduisant le temps de réponse et rendant l'espace de combat considérablement plus transparent à ceux l'atteignant[299] ». L'atteinte de cette connaissance permet conséquemment l'augmentation de la vitesse, de la portée et de la précision atteignables par l'entremise de la violence létale.[300] Entre la guerre du Golfe et les déboires américains en Irak et en Afghanistan, cette capacité informationnelle exceptionnelle, jumelée à un réseau de bases avancées disséminées aux quatre coins du monde, a permis aux É.-U. de contrôler sans équivoque les espaces communs mondiaux et de projeter leur puissance sans entraves, lui permettant de s'impliquer de manière décisive dans certains scénarios militaires régionaux durant les années 90[301] [302].

Ces démonstrations du potentiel militaire de la RAM ont également poussé les stratèges chinois à se pencher sur son impact sur les guerres à venir, notamment par le recours massif à l'information, à la réorganisation et à la centralisation de son commandement,

---

[297] Andrew Latham, cité dans Charles-Philippe David. *La guerre et la paix – Approches et enjeux de la sécurité et de la stratégie*, Paris : Presses de Sciences Po, 3e édition, 2013, p.214

[298] Amiral William A. Owens. « The Emerging U.S. System-of-systems », *Strategic Forum*, no.64, 1996, p.2

[299] États-Unis, Joint Chief of Staff. *Joint Vision 2010*. Washington D.C. : Joint Chief of Staff, 1995, p.13

[300] Joseph S. Nye et William A. Owens. « America's Information Edge », *Foreign Affairs,* vol.75, no.2, 1996, p.23; William J. Perry, qui allait devenir secrétaire à la Défense sous Clinton, affirmait en 1991 « qu'une armée avec une telle technologie détient un avantage écrasant sur une armée qui ne l'a pas, tout comme une armée équipée de chars d'assaut écraserait une armée détenant une cavalerie montée. » William J. Perry. « Desert Storm and Deterrence ». *Foreign Affairs*, vol.70, no.4, 1991, p.66.

[301] Parmi celles-ci, comptons l'Irak (1991), l'ex-Yougoslavie (Bosnie en 1995 et Kosovo en 1999), ainsi que dans les phases initiales des interventions en Afghanistan (2001) et encore une fois en Irak (2003). David, *op.cit*, p.218 – 219.

[302] David W. Kearn Jr. « Air-Sea Battle, the Challenge of Access, and U.S. National Security Strategy », *American Foreign Policy Interest*, vol.36, no.1, 2014, p.34

aspects faisant dire aux auteurs de *La Guerre hors limite*[303] qu'avec ces innovations, « il devenait possible d'être à la hauteur de la situation dans n'importe quel affrontement armé.[304] » En plus de prendre conscience de la désuétude de ses capacités conventionnelles[305], la Chine devait d'autant plus se méfier de cette capacité américaine à atteindre et intervenir décisivement partout sur la planète, plusieurs décideurs chinois considérant les É.-U. comme étant une puissance révisionniste[306] cherchant à étouffer l'émergence de la puissance chinoise et à la contenir derrière la *première chaîne d'îles (ligne en neuf traits)*[307], « une ligne bien organisée d'alliés américains agissant comme une tour de garde afin de surveiller et possiblement bloquer les accès de la Chine à l'océan Pacifique[308] ».

Ceci s'avère être une limitation contraignante pour la Chine, car, outre le règlement en sa faveur du contentieux taïwanais, la défense de ses intérêts nécessite également le contrôle de l'espace maritime situé en deçà de la deuxième chaîne d'îles[309] et la protection de ses voies commerciales maritimes. Ces dernières sont effectivement indispensables à son économie, sa stabilité politique et à son approvisionnement en ressources naturelles et énergétiques[310]. Des enjeux de cette importance nécessitent donc de préserver à tout prix l'accès au détroit de Malacca[311] et à ce que les observateurs étrangers surnomment le *collier de perles*[312], une série de bases chinoises situées sur le pourtour de l'océan Indien

---

[303] Ce traité stratégique chinois, écrit par deux généraux de l'APL, avait fait grand bruit au début des années 2000 par sa promotion de l'utilisation de moyens non militaires et non conventionnels pour arriver à ses fins.

[304] Qiao Liang et Wang Xiangsui. *La Guerre hors limites*. Paris : Payot et Rivages, Coll. Rivages poche, 2006, p.108

[305] Manson, *op.cit.*, p.121

[306] Andrew J. Nathan et Andrew Scobell. « How China Sees America : The Sum of Beijing's Fears », *Foreign Affairs,* vol.91, no.1, 2012, p.33

[307] Voir Annexe G

[308] Robert Kaplan, « The Geography of Chinese Power : How Far Can Beijing Reach on Land and at Sea? », *Foreign Affairs*, vol.89, no.3, 2010, p.33

[309] *Ibid.*, p.34; Ashley J. Tellis. « U.S.-China Relations in a Realist World ». Dans David Shambaugh. *Tangled Titans : The United States and China*, Lanham (Maryland) : Rowman & Littlefield Publishers, 2013, p.88

[310] Christopher I. Pehrson. *String of pearls : meeting the challenge of China's rising power across the Asian littoral.* Carlisle, PA : Strategic Studies Institute, U.S. Army War College, 2006, p.5

[311] Pour la Chine se pose la question du « dilemme de Malacca », où le fait d'être aussi dépendant du détroit pour ses approvisionnements énergétiques alors qu'il est notamment sous protection américaine, crée une énorme vulnérabilité stratégique. Voir Marc Lanteigne. « China's Maritime Security and the "Malacca Dilemma" ». *Asian Security*, vol.4, no.2, 2008.

[312] Voir Annexe H

et reliant la mer de Chine du Sud à l'Afrique et le Moyen-Orient, deux sources importantes de matières premières.[313]

Alors que tous ces scénarios impliquent une potentielle intervention militaire américaine, Qiao et Wang affirmaient également que « tout pays espérant gagner une guerre au XXI[e] siècle devra inévitablement affronter ce choix : « se réorganiser » ou être battu[314] ». C'est avec cette intention que la Chine a entrepris une modernisation militaire se préparant à ces éventualités et qui, par le développement croissant de ses forces navales et aériennes, a cherché à répondre à l'« encerclement » que représente la maîtrise américaine des mers asiatiques[315]. Cette impression de vulnérabilité a été aggravée en 1996, lorsque le président Clinton a « ordonné la plus grande démonstration de la puissance militaire américaine depuis la guerre du Vietnam en envoyant des navires dans le détroit de Taïwan[316] », en représailles à une série de mesures offensives chinoises cherchant à intimider l'île qu'elle revendique[317].

Observant la facilité avec laquelle les É.-U. sont intervenus dans la région, la Chine a réagi en investissant massivement dans des capacités visant à empêcher qu'une telle situation ne se reproduise[318] et rendant possible une posture de « défense active à distance » (*offshore active defense*), une stratégie inspirée de la stratégie militaire maoïste qui affirme que si « [...] une nation peut assumer une posture stratégique défensive, elle doit néanmoins utiliser des moyens offensifs pour atteindre des objectifs défensifs.[319] » Bref, selon Mao, la meilleure défense demeure sans conteste l'attaque.

Afin de pouvoir contrer la première puissance militaire mondiale en mer de Chine, elle investit donc dans des capacités navales et aériennes servant à projeter sa puissance autant

---

[313] Pehrson, *op.cit.*, p.5-6

[314] Liang et Xiangsui. *La Guerre hors limites*, *op.cit.*, p.108

[315] Toshi Yoshihara et James R. Holmes. *Red Star over the Pacific : China's Rise and the Challenge to U.S. Maritime Strategy*. Annapolis, MD : Naval Institute Press, 2010, p.129

[316] BBC. « Taiwan Flashpoint – US Role », *BBC News*, s.d. En ligne, <news.bbc.co.uk/2/shared/spl/hi/asia_pac/04/taiwan_flashpoint/html/us_role.stm>. Consulté le 10 février 2016.

[317] Andrew Scobell. « Show of Force: Chinese Soldiers, Statesmen, and the 1995-1996 Taiwan Strait Crisis », *Political Science Quarterly*, vol.115, no.2, 2000, p.227 – 228.

[318] Hayton, *The South China Sea*, *op.cit.*, p.224

[319] Taylor Fravel. « The Evolution of China's Military Strategy : Comparing the 1987 and 1999 Editions of Zhanlüexue ». Dans David Finkelstein et James Mulvenon (eds.), *China's Revolution in Doctrinal Affairs : Emerging Trends in the Operational Art of the Chinese People's Liberation Army*. Alexandria, VA : CNA Corporation, 2005, p.86

à Taïwan qu'au-delà de l'île[320], mais à permettre également une stratégie dite de déni d'accès[321] (*anti-access/area-denial* ou A2/AD) mettant en place les composantes de cette défense active. Pour Thomas P. Ehrhard et Robert O. Work, la stratégie d'A2 repose sur

> des actions initiées afin de nier aux forces américaines la capacité de se déployer dans une position au sein du théâtre à partir duquel ils peuvent mener des opérations efficaces à l'encontre des forces chinoises. Elles incluent des actions politiques chinoises cherchant à contraindre les pays régionaux d'empêcher les forces américaines d'accéder à leurs bases opérationnelles, mais également des attaques opérationnelles à l'encontre de bases régionales américaines déjà existantes ou de forces navales profondément déployées.[322]

Pour ce qui est de la portion AD, ils la définissent comme étant « les actions entreprises à l'intérieur du théâtre d'opérations du Pacifique visant à nier aux forces américaines ayant réussi à s'y déployer l'habileté à conduire des opérations efficaces dans les environs de Taïwan et de la Chine continentale.[323] » Il se forme alors ce que Barry Posen appelle une zone contestée (*contested zones*), des « arènes d'action militaire[324] » permettant à des adversaires plus faibles de causer des dommages importants aux forces américaines, celles-ci y perdant leur suprématie et les avantages que cette dernière procure[325]. C'est pour accomplir cette stratégie de déni d'accès que la Chine s'est concentrée sur le développement de capacités asymétriques pouvant exploiter les faiblesses de la puissance américaine[326], intentions que le Pentagone de Donald Rumsfeld mentionne dès 2004 dans son rapport annuel sur la puissance militaire chinoise[327] et qui prend une importance inédite sous son successeur. En effet, Robert Gates affirmait en 2009 que les investissements chinois en ce sens « pourraient menacer les principaux moyens qu'ont

---

[320] Mark Cozad. « China's Regional Power Projection Prospects for Future Missions in the South and East China Seas ». Dans Roy Kamphausen (ed.), David Lai et Andrew Scobell. *Beyond the Strait: PLA Missions Other Than Taiwan.* Carlisle, PA : Strategic Studies Institute, 2009, p.287 – 325.

[321] Yoshihara et Holmes, *op.cit.*, p.17

[322] Thomas P. Ehrhard et Robert O. Work, *Range, Persistence, Stealth, and Networking: The Case for a Carrier-Based Unmanned Combat System.* Washington, D.C.: Center for Strategic and Budgetary Assessments (CSBA), 2008, p.137.

[323] *Ibid.*, p.137 – 138

[324] Barry Posen. « Command of the Commons : The Military Foundation of U.S. Hegemony », *International Security*, vol.28, no.1, 2003, p.7

[325] *Ibid.*, p.22

[326] *Ibid.*, p.23

[327] États-Unis, Department of Defense. *FY04 Report to Congress On PRC Military Power.* Washington D.C. : Department of Defense, 2004, p.14. PDF en ligne, <www.globalsecurity.org/military/library/report/2004/d20040528prc.pdf>. Consulté le 10 février 2016.

les É.-U. pour projeter sa puissance et aider ses alliés dans le Pacifique : ses bases, ses ressources navales et aériennes et les réseaux qui les soutiennent[328] », une vision du déni d'accès que l'on retrouve aussi dans le *Quadrennial Defense Review* (QDR) de 2010[329].

Cette stratégie repose d'entrée de jeu sur des capacités militaires conventionnelles permettant de causer d'importants dommages aux forces navales et aériennes américaines. Sachant qu'elle ne peut pas se battre à forces égales, la Chine s'est spécialisée dans des capacités permettant de contrer l'armement américain et ceux de ses alliés. Près de ses côtes, la Chine compte des sous-marins diesel et des avions équipés de missiles de croisière, tandis que ces mêmes missiles surface-air sont fournis à une flotte nombreuse de petits bateaux rapides prêts à se lancer sur les navires s'approchant trop près[330]. Elle peut aussi attaquer sur une longue distance grâce à des missiles balistiques de courte portée, la mise en place de champs de mines étendus cherchant à empêcher le mouvement des navires américains ou à leur causer des dommages importants[331] et avec le Dong-Feng-21D, un nouveau missile balistique antinavire qui, « avec une portée de plus de 1500 kilomètres et la capacité de manœuvrer lors de sa descente [...], pourrait théoriquement frapper de grands navires à partir de bases situées sur le continent.[332] »

Si de telles capacités peuvent rendre difficiles et pénibles les interventions militaires américaines, elles ne permettent toutefois pas de dissuader totalement les É.-U. d'entreprendre des manœuvres offensives. Pour maximiser l'efficacité et l'impact des capacités nommées ci-dessus, la Chine s'est aussi tournée vers le concept de *guerre informationnelle* se déroulant en majeure partie dans le nouveau domaine militaire qu'est le cyberespace.

Depuis les années 90[333], l'APL œuvre à développer des capacités qui lui permettraient d'obtenir l'ascendant asymétrique ultime sur des capacités militaires américaines à la fine

---

[328] Traduction libre. Robert Gates. « A Balanced Strategy : Reprogramming the Pentagon for a New Age ». *Foreign Affairs*, vol.88, no.1, 2009, p.33.

[329] États-Unis, Department of Defense. *Quadrennial Defense Review Report 2010.* Washington D.C. : Department of Defense, 2010, p.31

[330] Christopher P. Twomey, « The Military-Security Relationship ». Dans David Shambaugh, *op.cit.*, p.240 – 241.

[331] Andrew S. Erickson, Lyle J. Goldstein et William S. Murray. *Chinese Mine Warfare – A PLA Navy 'Assassin's Mace' Capability.* Newport (RI) : China Maritime Studies Institute, U.S. Naval War College, 2009, p.1

[332] Traduction libre. Hayton, *op.cit.*, p.225

[333] Desmond Ball. « China's Cyber Warfare Capabilities », *Security Challenges*, vol.7, no.2, 2011, p.81

pointe de la technologie, soit en ciblant précisément sa dépendance accrue et grandissante aux TIC et en exploitant les domaines électromagnétiques et cybernétiques qu'elle considère comme étant une facette incontournable de la guerre de demain[334]. Le but premier est donc de rapidement mettre fin à la suprématie informationnelle de l'adversaire, tout en préservant la sienne, et d'ainsi l'*aveugler*, autant au point de vue opérationnel, tactique que stratégique, afin de le paralyser et de permettre de contre-attaquer plus efficacement[335], une tactique tirée encore une fois de Sun Tzu et de la stratégie maoïste :

> Il nous faut boucher de la manière la plus complète les yeux et les oreilles de l'ennemi, pour qu'il devienne aveugle et sourd. Il nous faut, autant que possible, créer la confusion dans l'esprit de ses chefs, de façon à ce qu'ils perdent complètement la tête, et en profiter pour emporter la victoire[336].

L'éventuelle mise en œuvre de cette stratégie représente un risque énorme pour les É.-U., considérant que la grande puissance de ses forces armées dépend directement de l'accès et du traitement de l'information permettant à son tour des frappes de précision de longue portée. Perdre cet avantage serait donc un inconvénient majeur dans un éventuel scénario offensif en Asie-Pacifique. Cette importante vulnérabilité a été abondamment abordée dans les cercles militaires américains et a même été au cœur de l'édition 2010 de la simulation militaire Schriever, où un scénario se déroulant en 2022 et mettant aux prises les É.-U. à un « adversaire régional dans le Pacifique[337] » faisant office d'« équipe rouge », démontra aux participants l'impact que des cyberattaques pouvaient avoir sur leurs opérations. Dès les premiers instants, « l'adversaire s'est immédiatement concentré à exploiter et à priver les Américains et leurs alliés de leurs accès aux éléments facilitateurs spatiaux et cyber, lançant une action préventive modelant l'environnement opérationnel[338] », des éléments essentiels qui rendent notamment possible les capacités dites de C4ISR et l'envoi d'ordres sur le champ de bataille. En plus de démontrer la

---

[334] Lei, *op.cit.*, p.147

[335] États-Unis, Office of the Secretary of Defense. *Military and Security Developments Involving the People's Republic of China 2013*, *op.cit.*, p.36

[336] Mao Zedong. *De la guerre prolongée.* PDF en ligne, <maozedong.fr/documents/guerreprolongee.pdf>, p.111. Consulté le 5 février 2016.

[337] Traduction libre. Harris, *op.cit.*, p.49

[338] États-Unis, Air Force Space Command. « Schriever Wargame 2010 », *High Frontier : The Journal for Space and Cyberspace Professional*, vol.7, no.1, 2010, p.32

difficulté que représente l'instauration d'une dynamique de dissuasion dans ce nouveau domaine militaire, cet exercice a également « renforcé la disposition naturelle de l'armée envers la guerre. Il a aussi convaincu les militaires de haut rang et les dirigeants du Pentagone que si une cyber guerre devait survenir, elle se déroulerait à la 'vitesse de la lumière' et pratiquement sans aucun avertissement[339] ».

Pour ce faire, les forces chinoises cherchent à cibler autant les divers éléments informatiques composant les systèmes d'information que les infrastructures satellitaires adverses, indispensables pour sa transmission rapide et précise[340] (en 2007, la Chine a réussi un test capable de détruire un de ses satellites par le biais de missiles[341]). Alors que matériellement, ces ambitions sont facilitées par une industrie chinoise des TIC très performante depuis le début du XXIe siècle[342], elles sont également appuyées par plusieurs écrits militaires, notamment *La science de la stratégie militaire*, où s'ancre l'idée que la *guerre informationnelle* est essentielle contre un adversaire plus fort que soi : « dans la guerre de l'information, le système de commandement et de contrôle est le cœur de la cueillette, du contrôle et de l'application de l'information sur le champ de bataille, dont il est aussi le système nerveux.[343]», une stratégie s'enseignant même dans les académies militaires chinoises et ayant droit à une division de la PLA dédiée et très active[344].

Par ces acquisitions, ces doctrines et cette littérature, il existe donc pour les É.-U. une possibilité que son complexe informationnel s'effondre dans un moment crucial, laissant ses forces à la merci de contre-attaques auxquelles la Chine semble s'être bien préparée et équipée en conséquence[345].

---

[339] Harris, *op.cit.*, p.52

[340] Lei, *op.cit.*, p.148.

[341] États-Unis, Office of the Secretary of Defense. *Military and Security Developments Involving the People's Republic of China 2011*, Washington D.C.: Department of Defense, 2011, p.37

[342] Nina Hachigian. « China's Cyber-Strategy », *Foreign Affairs*, vol.80, no.2. 2001, p.120 – 122.

[343] Passage de *The Science of Military Strategy*, un traité militaire écrit par deux généraux chinois près du pouvoir du Parti, cité dans États-Unis, Office of the Secretary of Defense. *Military and Security Developments Involving the People's Republic of China 2013*, *op.cit.*, p.37.

[344] Barrington Barrett Jr. « Information Warfare: China's Response to U.S. Technological Advantages », *International Journal of Intelligence and Counterintelligence*, vol.18, no.4, 2005, p.688 – 689.

[345] Jon Brickey, Jacob Cox, John Nelson et Gregory Conti. « The Case for Cyber », *Small Wars Journal*, 2012. En ligne, <smallwarsjournal.com/jrnl/art/the-case-for-cyber>. Selon eux, « si ces réseaux critiques commencent à faillir, nous ne sommes pas une force de combat du XXIe siècle; nous sommes une armée des années 1980. »

En semant le doute dans l'esprit des dirigeants américains, leurs équivalents chinois cherchent à dissuader une éventuelle intervention américaine[346], conformément à un des principes centraux de Sun Tzu, utilisant la *guerre informationnelle* « pour détruire la volonté de l'ennemi de se battre en attaquant sa connaissance situationnelle et ses convictions, le poussant ultimement à se rendre[347] » ou pour carrément l'inciter à laisser tomber ses desseins belliqueux[348]. Afin d'obtenir cette supériorité informationnelle tant désirée, les soldats-*hackers* agissent de la même manière que pour l'espionnage : ils pénètrent les réseaux adverses dans le but d'obtenir des accès permettant d'attaquer au moment désiré les éléments constituant l'infrastructure informationnelle américaine. Cet accès fait aussi craindre des cyberoffensives en sol américain, créant par la bande un effet de dissuasion encore plus grand et plus contraignant pour les É.-U., car « les États doivent être préparés au pire quand ils ne connaissent pas la force réelle de leurs rivaux potentiels.[349] » Devant être utilisées de manière inattendue pour être efficaces[350], ces cyberattaques pourraient aussi atteindre directement la société américaine, les réseaux militaires s'appuyant énormément sur leurs contreparties civiles, que ce soit au niveau de la logistique, des communications, mais surtout des IC dont les forces armées dépendent pour leurs activités quotidiennes. Pour les plus alarmistes, cette capacité chinoise à infiltrer les réseaux américains « pourrait causer d'importants dommages à divers secteurs américains, qu'ils soient l'économie, les télécommunications, le transport d'électricité, les données financières et d'autres infrastructures vitales.[351]»

Déjà, Clarke et Knake estiment que le réseau électrique américain est parsemé de « bombes logiques »[352], tandis que des membres d'agences de renseignements américaines soupçonnent l'armée chinoise d'être à l'origine d'une panne électrique majeure en 2003[353] et d'une deuxième en 2008 où un soldat de l'APL aurait été trop

---

[346] Magnus Hjortdal. « China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence », *Journal of Strategic Security*, vol.4, no.2, 2011, p.14

[347] Barrett, *op.cit.*, p.685.

[348] *Idem.*

[349] Hjortdal, *op.cit.*, p.4

[350] Ball, *op.cit.*, p.102

[351] John J Tkacik Jr. « Trojan Dragon: China's Cyber Threat », *Backgrounder*, no.2106, 2008. En ligne, <www.heritage.org/research/reports/2008/02/trojan-dragon-chinas-cyber-threat>. Consulté le 15 novembre 2015.

[352] Clarke et Knake, *op.cit.*, p.54

[353] En faisant sombrer de grandes villes comme New York ou Toronto dans le noir, c'est près de 50 millions de personnes qui auront été touchées et des estimations font état de pertes financières se situant entre 4

téméraire au sein d'un réseau électrique de la Floride[354]. De son côté, Barack Obama affirmait en 2009 que des « cyber intrus avaient sondé notre réseau électrique et que dans d'autres pays, des cyberattaques avaient plongé des villes entières dans l'obscurité.[355] » En faisant ainsi planer une telle épée de Damoclès au-dessus de la tête des dirigeants américains, ceux-ci devront désormais mener un sérieux exercice de réflexion avant de commander un déploiement militaire majeur en Asie-Pacifique. La Chine va plus loin que de simplement empêcher les É.-U. de projeter au besoin sa puissance en mer de Chine, elle cherche à les inciter fortement, par la crainte, à ne pas agir du tout contre elle[356]. Cette éventualité d'une attaque-surprise sur le territoire national, à la Pearl Harbor, inquiète, surtout quand la défense s'avère si difficile.

Finalement, deux hauts gradés chinois proclamaient, en 2011, que « tout comme la guerre nucléaire fut la guerre stratégique de l'ère industrielle, la cyberguerre est devenue la guerre stratégique de l'ère informationnelle : une forme de bataille massivement destructrice et concernant la vie et la mort des nations.[357] » Une telle déclaration peut difficilement être prise à la légère et c'est justement à travers ce prisme d'interprétation que la communauté de sécurité américaine estime désormais que la Chine cherche à s'attaquer directement aux deux éléments primordiaux de cette nécessité stratégique qu'est l'équilibrage interne américain. D'abord, si la Chine empêche, par l'entremise du cyberespionnage, une relance économique américaine optimale, elle en bénéficie grandement elle-même. Ensuite, elle menace, par ses capacités d'A2/AD, de mettre à mal la capacité américaine à projeter sa puissance en Asie-Pacifique. Plusieurs estiment donc que la Chine pourrait utiliser le cyberespace afin de perturber l'utilisation américaine soutenue des TIC à des fins militaires, apport technologique qui a justement permis à la puissance militaire américaine d'être si efficace depuis la première Guerre du Golfe.

---

et 10 milliards de dollars, aux É.-U. seulement. U.S.-Canada Power System Outage Task Force. *Final Report on the August 14, 2003 Blackout in United States and Canada: Causes and Recommendations*. 2004. En ligne, <energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf>. Consulté le 15 décembre 2015, p.1.

[354] Harris, *op.cit.*, p.52

[355] États-Unis, White House. *Remarks by the President on Securing our Nation's Cyber Infrastructure*, *op.cit.*

[356] Segal. « The Code not Taken », *op.cit.*, p.40

[357] Reuters. « China PLA officers call Internet key battleground ». *Reuters*, 3 juin 2011. En ligne, <www.reuters.com/article/us-china-internet-google-idUSTRE7520OV20110603>. Consulté le 15 mars 2016.

Empêcher les forces armées américaines d'agir en temps et lieu et autant de fois que le Commandant en Chef peut l'exiger, c'est également les rendre inutiles aux yeux de leurs alliés, une situation pouvant réduire considérablement l'influence américaine dans la région de l'Asie-Pacifique. C'est donc à ces utilisations perturbatrices du cyberespace par un rival chinois proactif que chercheront à s'attaquer les É.-U., démarches qui seront explicitées dans le prochain chapitre.

CHAPITRE III
L'ADAPTATION DE LA COMMUNAUTÉ MILITAIRE AMÉRICAINE

> Malheureusement, nous devons mener la guerre comme il se doit, et non comme nous le voudrions.
>
> M[al] Horatio Herbert Kitchener

La Chine ne représente évidemment pas la *seule* cybermenace que doivent affronter les É.-U. : Le cyberespace est rempli d'acteurs représentant des menaces potentielles à sa sécurité nationale: pirates informatiques, *hacktivistes*, lanceurs d'alertes, organisations criminelles ou terroristes, États, etc. La Chine demeure toutefois la plus préoccupante, en raison de ses capacités et intentions offensives crédibles s'inscrivant dans une dynamique stratégique internationale potentiellement conflictuelle. Les É.-U. sont donc confrontés à ce que Ken Booth et Nicholas Wheeler ont qualifié, partant du concept de *dilemme de sécurité* de Robert Jervis, de *paradoxe sécuritaire*, où « l'insurmontable incertitude dans l'esprit des acteurs pourrait générer une plus grande insécurité, même si aucune des parties ne le désire[358] ». Ainsi, l'augmentation de la capacité d'un État (la Chine) à se défendre et à assurer sa survie rendra malgré lui un autre État anxieux et tenté par sa propre militarisation (les É.-U.).[359] Pour les auteurs, ce paradoxe se compose de deux dilemmes distincts. D'une part, celui *d'interprétation*, où les dirigeants doivent prendre connaissance des mouvements stratégiques d'autrui, y trouver un sens et y accoler une intention. Dans le cas ici abordé, l'opacité des intentions stratégiques chinoises à l'endroit des É.-U., aussi bien « virtuelles » que « réelles », amène les dirigeants américains à craindre le pire et à vouloir se préparer militairement à une éventuelle offensive, sentiment exacerbé par l'idée que le cyberespace favorise largement l'attaque.

---

[358] Ken Booth et Nicholas J. Wheeler. *The Security Dilemma : Fear, Cooperation and Trust in World Politics*. Basingstoke (Angleterre); New York : Palgrave Macmillan, 2008, p.28

[359] *Ibid.*, p.22

Ce chapitre s'intéressera au dilemme *de réponse*, où les dirigeants doivent décider s'ils vont réassurer un adversaire craintif ou opter pour une posture de confrontation. Devant des cyberactions chinoises interprétées comme menaçantes, les É.-U. ont opté pour une réponse dissuasive visant le maintien de leur suprématie militaire, d'abord par une réorganisation de leurs capacités cybernétiques déjà existantes, suivie d'une forte augmentation de celles-ci. Possédant une puissance militaire plus imposante, cet effort américain ne cherche pas à équilibrer celle de la Chine, mais bien à rétablir la menace qu'elle peut représenter par l'entremise du cyberespace. Pour le gouvernement américain, les cybercapacités chinoises représentent une menace à la sécurité du territoire américain et à sa population : en mettant ainsi en péril sa supériorité technologique et militaire, elles empêcheraient les É.-U. d'assurer le respect de ses alliances, mais aussi de maintenir la paix et de la stabilité en Asie-Pacifique, élément indispensable du *pivot vers l'Asie*. Un *rééquilibrage interne* a donc été mis en place, une initiative stratégique que Kenneth Waltz définit comme l'ensemble des « manœuvres menées afin d'augmenter sa capacité économique, sa force militaire et/ou de développer des stratégies innovantes[360] ».

Ce chapitre abordera la réaction américaine aux cyberactivités chinoises, un enjeu longtemps sous-estimé, mais désormais traité comme une priorité stratégique nationale. La première partie traitera de l'évolution de la place des cybercapacités au sein de l'appareil militaire américain : après leur éclosion au sein de l'armée de l'air, elles sont devenues indispensables à la collecte de renseignements d'une NSA renouvelée. Certains membres de la communauté du renseignement et du DoD ont ensuite voulu exploiter le potentiel militaire et stratégique de ces capacités, d'abord en les intégrant dans un rôle actif sur les champs de bataille irakiens, mais surtout par la création, en 2010, du USCYBERCOM, sous-commandement militaire dédié au contrôle et à la domination de ce nouveau domaine.

---

[360] Traduction libre. Waltz. *Theory of International Politics*, *op.cit.*, p.118

Finalement, il sera question des intentions américaines derrières ces capacités, concrétisées par une cyberstratégie américaine de dissuasion encadrant l'utilisation de ces capacités et cherchant à contrer la menace chinoise, autant sur le plan cybernétique que stratégique. Si beaucoup d'efforts furent d'abord consacrés à la défense des réseaux critiques nationaux, la mise en place d'une contrepartie offensive fût considérée comme nécessaire à l'instauration de cette dynamique recherchée de dissuasion. Finalement, ces capacités ont également été intégrées au sein de la doctrine militaire américaine du *Air-Sea Battle* (ASB), une réponse directe à la stratégie chinoise d'A2/AD. La domination militaire américaine du cyberespace est alors considérée comme un élément stratégique préalable indispensable au succès de futures opérations navales et aériennes, elles-mêmes essentielles à la réalisation de la grande stratégie d'Obama.

3.1 La transformation de la structure militaire américaine

Cette première section dressera un aperçu historique de l'évolution des capacités cybernétiques américaines, afin d'en connaître l'état et le niveau d'avancement lorsque l'administration Obama a décidé d'y avoir recours afin de mener à bien sa grande stratégie envers la Chine et ce, plus particulièrement au sein de la NSA. En plus de son rôle important au sein de la communauté du renseignement américain post-11-septembre, mettant la main sur des informations difficiles d'accès, l'agence de renseignement a adopté un important volet offensif qui en fera la pierre d'assise du USCYBERCOM. Ce sous-commandement unifiant toutes les entités militaires cyber permet non seulement de défendre les réseaux militaires nationaux, mais également de rendre possible et plus aisée la projection de la puissance des forces armées américaines, plus particulièrement en Asie-Pacifique.

3.1.1 Des cybercapacités en développement et en quête d'identité.

Les cybercapacités militaires mises à profit par l'administration Obama n'ont pas été établies spécialement pour répondre aux besoins de sa politique étrangère, leur développement étant l'aboutissement d'un processus historique et bureaucratique bien amorcé.

Dans les années 90, la *United States Air Force* (USAF) considérait déjà le cyberespace comme un domaine militaire[361] qu'elle a teinté de sa culture stratégique inspirée de Giulio Douhet, théoricien militaire italien. Pour ce dernier, de violentes attaques sur les cibles industrielles et civiles de l'adversaire permettent de diminuer sa capacité de résilience militaire et sociale et d'accélérer la résolution des conflits[362], tout en soulignant « que la seule manière de défendre efficacement son propre territoire d'une attaque par les airs est de détruire la puissance aérienne de l'ennemi avec la plus grande rapidité possible.[363] » Pour Douhet, la défense est caduque devant des attaques aériennes, rendant l'adoption d'une posture défensive inutile et coûteuse[364]. Aujourd'hui encore, comme nous le verrons plus loin, la cyberstratégie américaine est fortement influencée par les travaux du stratège italien. [365] En 1996, Libicki et Szafranski écrivaient que le cyber était un domaine de prédilection pour l'USAF, permettant cette *vision d'ensemble* nécessaire aux frappes aériennes ciblées :

> [...] le terrain le plus élevé n'est plus en lui-même l'espace aérien, mais le cyberespace. Compris dans son sens le plus large, le cyberespace est le grand confluent des tous les différents flux d'information et d'octets qui, mis ensemble, génère une « vue en hauteur » stratégique préalablement nécessaire à la victoire.[366]

---

[361] États-Unis, 24th Air Force Office of History. *History of HQ Twenty-Fourth Air Force and 624th Operations Center*, 2014. En ligne, <www.24af.af.mil/shared/media/document/AFD-140429-035.pdf>. Consulté le 4 avril 2016.

[362] Giulio Douhet. *The Command of the Air*. Washington D.C. : Air Force History and Museums Program, 1998, pp.58 – 60.

[363] Traduction libre. *Ibid.*, p.110 – 111.

[364] W. Alexander Vacca. « Military Culture and Cyber Security », *Survival,* vol.53, no.6, 2012, p.166

[365] Gen. Michael V. Hayden. *Playing to the Edge : American Intelligence in the Age of Terror*, New York : Penguin Press, 2016,

[366] Traduction libre. Richard Szafranski et Martin C. Libicki. « " . . . Or Go Down in Flame?" : Toward an Airpower Manifesto for the Twenty-First Century ». *Air Power Journal*, vol.10, no.3, 1996, p.66.

Le cyberespace était alors considéré comme une composante de la *guerre informationnelle* (*information warfare* ou IW), soit « toutes les actions prises pour nier, exploiter, corrompre ou détruire l'information de l'ennemi et les fonctions qu'elle accomplit, tout en se protégeant contre ces actions afin d'exploiter les fonctions de sa propre information militaire » afin de « dégrader sa volonté ou sa capacité à se battre »[367]. Alors que l'information est aujourd'hui omniprésente et socialement indispensable, de sérieux questionnements ont été soulevés quant à la vulnérabilité informationnelle des forces armées américaines: lors de l'exercice militaire *Eligible Receiver*, la NSA, « équipe rouge », a réussi à infiltrer les réseaux électriques et systèmes d'urgence de neuf grandes villes américaines, en plus de prendre le contrôle des ordinateurs du USPACOM.[368] En 2003, John Hamre, alors secrétaire adjoint de la Défense, affirmait qu'*Eligible Receiver* avait véritablement conscientisé le DoD à la vulnérabilité que représentait le cyberespace pour les É.-U., au même titre que, pour lui, le 11-septembre avait mis en lumière leurs vulnérabilités aériennes[369]. L'efficacité du *commandement et contrôle* (C2), « l'exercice de l'autorité et de la direction d'un commandant dûment désigné sur des forces assignées et rattachées dans l'accomplissement d'une mission[370] », demeure aujourd'hui dépendante de la disponibilité et de la qualité de l'information. Elle représente donc une cible de choix[371], car l'introduction d'informations inexactes dans le processus cognitif du C2 affecterait la confiance envers le système, instaurant ainsi une variante du *brouillard de guerre*, obstacle opérationnel que la RAM cherchait justement à surpasser.

---

[367] Traduction libre. États-Unis, Department of Air Force. *Cornerstones of Information Warfare.* Washington D.C. : Department of Air Force, 1995. En ligne, <www.csse.monash.edu.au/courseware/cse468/2006/cornerstones-iw.html>. Consulté le 15 février 2016.

[368] PBS. « The Warnings ». *Frontline : Cyberwar!*, 24 avril 2003. En ligne, <www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/>. Consulté le 1er avril 2016.

[369] PBS. « Interview : John Hamre ». *Frontline : Cyberwar!*, 24 avril 2003. En ligne, <www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/hamre.html>. Consulté le 1er avril 2016.

[370] Traduction libre. États-Unis, Department of Defense. « Department of Defense Dictionary of Military and Associated Terms ». Washington D.C. : Department of Defense, 2010 (mise à jour 2016), p.40. En ligne, <www.dtic.mil/doctrine/new_pubs/jp1_02.pdf>. Consulté le 29 mars 2016.

[371] Kaplan, *op.cit.*, p.93

Cette vulnérabilité représente toutefois une opportunité équivalente. Si pendant la guerre du Kosovo de 1999, des considérations légales et humanitaires ont poussé les É.-U. à ne pas employer ses cybercapacités[372], les Balkans furent, deux ans plus tôt, le théâtre d'une des premières utilisations à des fins militaires, où différents groupes, dont la NSA, ont mené des opérations d'IW, dont la mise hors service des défenses antiaériennes serbes. En infiltrant et en cartographiant le système téléphonique national, un accès direct à ces défenses antiaériennes a été découvert et exploité afin d'y injecter « de fausses informations laissant croire aux écrans radars que les avions provenaient de l'ouest, alors qu'en fait, ils provenaient du nord-ouest », facilitant ainsi les bombardements de l'OTAN.[373] En plus de ces démonstrations offensives et défensives, des attaques majeures comme *Solar Sunrise* (1998)[374] et *Moonlight Maze* (1999) ont semé la panique au sein du DoD[375] et contribué à imposer le cyber comme un secteur stratégique incontournable. Rapidement, d'autres organisations ont mis sur pied des entités dédiées[376], un bon moyen d'obtenir du financement dans une période où les forces armées américaines font les frais de ce que plusieurs appelaient alors les *dividendes de la paix*[377]. Bien que l'USAF ait fait figure de pionnière en opérant très tôt dans le cyberespace, l'épicentre de la révolution cyber se déplacera à Fort Meade, Maryland, quartier général de la NSA, pour qui le cyberespace allait devenir un atout majeur.

---

[372] Julian Borger. « Pentagon kept the lid on cyberwar in Kosovo ». *The Guardian*, 9 novembre 1999. En ligne, <www.theguardian.com/world/1999/nov/09/balkans>. Consulté le 2 avril 2016.

[373] Traduction libre. Kaplan, *op.cit.*, p.96

[374] Attaque informatique survenant en février 1998. Si le gouvernement irakien était originalement suspecté, ce sont finalement trois adolescents, deux Américains et un Isrélien, qui seront à l'origine de cette attaque. Keven Poulsen. « Solar Sunrise hacker 'Analyzer' escapes jail : Community service for terrifying US Army ». *The Register*, 15 juin 2001. En ligne, <www.theregister.co.uk/2001/06/15/solar_sunrise_hacker_analyzer_escapes/>. Consulté le 14 avril 2016.

[375] John Hamre aurait qualifié *Solar Sunrise* « des premiers coups de feu d'une véritable cyber guerre » et de ce qui était jusqu'alors « l'attaque la plus organisée et systématique à l'encontre des systèmes de défense américain. » Traduction libre. Kaplan, *op.cit.*, pp.65 – 76.

[376] Dans la foulée, chaque service mit en place son propre centre de IW. Au *Air Force Information Warfare Center* de l'armée de l'air s'ajoute le *Land Information Warfare Activity* de l'infanterie, le *Naval Information Warfare Activity* de la marine ou le *Computer Network Defense Unit* du corps des fusilliers marins.

[377] Hayden, *op.cit.*, p.104

La décennie post-guerre froide fut pourtant difficile pour l'agence de renseignement, alors que les effets d'une gestion déficiente et d'une inertie bureaucratique se sont ajoutés à une grande perte de ressources humaines et financières[378] : entre 1991 et 1996, elle a perdu le « tiers de son personnel et son budget a été réduit de 35%, passant de 5,2 milliards de dollars à moins de 3,5 milliards.[379] » En 1999, la nomination du général Michael V. Hayden[380] à sa tête posa toutefois les fondations de sa future cyberpuissance et ce, malgré qu'il ait hérité d'une NSA technologiquement inefficiente et victime de l'explosion rapide des communications numériques[381], situation menant à la diminution de la qualité et de la quantité d'informations fournies par l'agence[382]. Cette désuétude technologique touche aussi ses équipements: en 2000, une panne du système informatique chargé d'analyser les informations amassées perturba pendant quatre jours la transmission de renseignements provenant du SIGINT au Président, une grande partie de l'exposé présidentiel quotidien[383]. Souvent considérée comme « la plus importante et la plus coûteuse des agences de renseignement dans toute l'histoire de la civilisation occidentale[384] », la NSA n'était plus l'ombre d'elle-même[385].

Pour Hayden, une nécessaire modernisation de l'agence[386] passait notamment par le développement d'un nouveau volet de son rôle historique de SIGINT, où, depuis sa création, elle se consacrait à l'interception et au décryptage des signaux adverses afin d'en soutirer du renseignement. Il a donc attribué un plus grand rôle au SIGINT dit actif,

---

[378] Matthew M. Aid. « Prometheus Embattled : A Post-9/11 Report Card on the National Security Agency ». Dans Loch K. Johnson (ed.). *Strategic Intelligence vol.2 - The Intelligence Cycle : The Flow of Secret Information from Overseas to the Highest Councils of Gouvernment.* Westport (CT) : Praeger Security International, 2007, p.42.

[379] Traduction libre. *Idem.*

[380] Général 4 étoiles désormais à la retraite. Il a par la suite occupé les postes de directeur de la NSA, directeur adjoint du Renseignement national et finalement celui de directeur de la CIA.

[381] Pierre-Louis Malfatto. *Quand l'intelligence fait défaut : les services de renseignements américains à l'épreuve des attentats du 11 septembre 2001.* Paris : L'Harmattan, Coll. Raoul-Dandurand, 2009, p.111.

[382] Aid, *Prometheus Embattled, op.cit.*, p.42.

[383] Matthew M. Aid, *The Secret Sentry : The Untold History of the National Security Agency.* New York : Bloomsbury Press, 2009, p.236

[384] Traduction libre. Loch K. Johnson. *Secret Agencies : U.S. Intelligence in a Hostile World.* New Haven : Yale University Press, 1996, p.125

[385] Aid, *The Secret Sentry, op.cit.*, p.241

[386] Aid, *Prometheus Embattled, op.cit.*, p.43

dont le *modus operandi* est « de se rendre à la cible et d'en extraire de l'information, plutôt que d'espérer qu'une transmission soit interceptée par le SIGINT passif traditionnel.[387] »

C'est ainsi que les capacités liées au piratage informatique sont devenues une priorité d'acquisition : celles-ci permettent l'exploitation de réseaux et de systèmes informatiques (*computer network exploitation* ou CNE), opérations qui, selon le *Field Manual 3-13*, rendent possible « [...] une collecte de renseignements visant à recueillir les données des systèmes automatisés d'information ou des réseaux de la cible ou de l'adversaire[388] », indépendamment de leur emplacement géographique. En 2000, c'est dans ce but qu'a été mise sur pied une unité constituée de l'élite des *hackers* de la NSA, soit le *Tailored Access Operations* (TAO). Ceux-ci n'ont qu'une mission : trouver un moyen, peu importe lequel, d'infiltrer les réseaux adverses. [389]

Après le 11-septembre, cette collecte agressive de renseignements croîtra et jouera un rôle central dans l'éventuelle militarisation du cyberespace, alors que l'échec de la communauté du renseignement à prévenir les attaques terroristes la força à prendre les mesures correctives nécessaires. En effet, la NSA devait obtenir du renseignement permettant une meilleure attribution d'un financement limité devant être alloué aux menaces les plus urgentes[390], son rôle étant d'obtenir et de redistribuer le renseignement[391]. Cette mission eut recours à l'accroissement de ses capacités de CNE, devant désormais se rendre d'elle-même aux informations pouvant ainsi éviter un autre traumatisme national. Pour la NSA, le 11-septembre représente donc une augmentation importante de ses ressources humaines et financières[392] : alors qu'entre 2004 et 2013, son

---

[387] Traduction libre. Hayden, *op.cit.*, p.129

[388] Traduction libre. États-Unis, Department of the Army. *Field Manual 3-13 : Information Operations: Doctrine, Tactics, Techniques, and Procedures*. Washington D.C. : Department of Defense, 2003, p.2-11.

[389] Pour ce faire, « ils volent ou cassent les mots de passe, implantent des espiogiciels, installent des portes dérobées et travaillent avec le réseau d'espions humains de la NSA, tout cela dans le but d'obtenir de l'information. » Traduction libre. Harris, *op.cit.*, p.70

[390] Hugo Hanne. « Amérique, défendre le territoire », *Géoéconomie*, vol.66, no.3, 2013, p.140

[391] Malfatto, *op.cit.*, p.51

[392] Aid, *Prometheus Embattled*, *op.cit.*, p.47; Hayden, *op.cit.*, p.130

budget passe d'un peu plus de 6 milliards à près de 11 milliards, une augmentation de 53%[393], c'est le TAO qui connaîtra la plus forte croissance de personnel de l'agence, bénéficiant :

> [...] de l'éclatement de la bulle Internet et de l'augmentation massive du patriotisme après les attaques terroristes du 11-septembre. [...] l'incroyable cohorte de spécialistes en SIGINT que nous avons obtenu était jeune, techniquement talentueuse, innovante et aventureuse. [...] leur mentalité faisait en sorte qu'aucune cible n'était impossible à pénétrer [...][394].

En 2005, le général Keith B. Alexander prit ainsi les commandes d'une NSA mieux fournie et en meilleure santé financière[395], accélérant du même coup le mouvement de modernisation. Alexander a une devise personnelle, « Collect It All »[396], traduisant son désir de sans cesse accroître la capacité de l'agence à intercepter, entreposer et analyser des informations et d'étendre géographiquement ses capacités informationnelles. L'accumulation et l'analyse d'un maximum d'informations ainsi interceptées permettraient de mieux contrer de potentiels acteurs malveillants[397]. Avec son zèle, qui lui vaudra le surnom du « cowboy de la NSA »[398], cette ambition fera de la NSA « le plus important centre d'expertise cyber du monde.[399]»

Outre la capacité à accéder aux données d'individus par le biais d'entreprises de télécommunications américaines, avec des programmes comme PRISM ou XKeyscore[400], le TAO a pu établir sa présence dans 89 pays en s'octroyant un accès direct

---

[393] Wilson Andrews et Todd Lindeman. « The Black Budget ». *The Washington Post*, 29 août 2013. En ligne, <www.washingtonpost.com/wp-srv/special/national/black-budget/>. Consulté le 2 février 2016.

[394] Traduction libre. Hayden, *op.cit.*, p.130

[395] Aid, *The Secret Sentry*, *op.cit.*, p.332

[396] Glenn Greenwald. *No Place to Hide : Edward Snowden, the NSA, and the U.S. Surveillance State*. New York : Metropolitan Books/Henry Holt, 2014, p.95

[397] *Ibid.*, p.96.

[398] Shane Harris. « The Cowboy of the NSA », *Foreign Policy,* 9 septembre 2013. En ligne, <www.foreignpolicy.com/articles/2013/09/08/the_cowboy_of_the_nsa_keith_alexander>. Consulté le 10 août 2014.

[399] Traduction libre. Clarke et Knake, *op.cit.*, p.37

[400] Benjamin Ferran. « XKeyscore et Prism, anatomie de la machine à espionner américaine ». *LeFigaro.fr,* 2 août 2013. En ligne, <www.lefigaro.fr/secteur/high-tech/2013/08/02/32001-20130802ARTFIG00313-xkeyscore-et-prism-anatomie-de-la-machine-a-espionner-americaine.php>. Consulté le 4 avril 2016.

à de nombreux systèmes informatiques, accès dont le nombre oscille entre 85 000 et 100 000[401]. C'est par ce moyen que l'agence pouvait notamment espionner les téléphones portables de plusieurs dirigeant-e-s mondiaux[402]. La Chine n'est pas en reste : principale cible de la surveillance de la NSA[403], le TAO « a pénétré avec succès les systèmes informatiques et de télécommunications du territoire chinois pendant presque 15 ans, générant ainsi les meilleurs et les plus fiables renseignements sur ce qui se passait à l'intérieur de la République populaire de Chine.[404] » Parmi les cibles se trouvent deux importants réseaux cellulaires chinois ayant permis de déceler les positionnements géographiques d'importantes unités militaires, mais aussi ceux des lieux de travail de nombreux dirigeants chinois[405]. Elle a également réussi à accéder aux réseaux de Huawei, un géant chinois des télécommunications affirmant connecter le tiers de la planète[406], rendant possible l'accès à de nombreuses institutions chinoises[407], mais aussi aux télécommunications des pays achetant ses équipements. Par cet accès, la NSA élargissait non seulement la portée de son réseau de surveillance, mais aussi celle de potentielles cyberattaques américaines[408].

---

[401] Harris, *@War*, *op.cit.*, p.71; David E. Sanger et Thom Shanker. « N.S.A. Devises Radio Pathway Into Computers ». *The New York Times*, 14 janvier 2014. En ligne, <www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html>. Consulté le 15 mars 2016.

[402] Parmi les victimes, comptons la chancelière allemande Angela Merkel et plusieurs présidents français. Voir Kevin Rawlinson. « NSA surveillance: Merkel's phone may have been monitored 'for over 10 years' », *The Guardian,* 26 octobre 2013. En ligne, <www.theguardian.com/world/2013/oct/26/nsa-surveillance-brazil-germany-un-resolution>. Consulté le 4 avril 2016; Amaelle Guitton et al. « WikiLeaks - Chirac, Sarkozy et Hollande : trois présidents sur écoute ». *Libération.fr*, 23 juin 2015. En ligne, <www.liberation.fr/planete/2015/06/23/chirac-sarkozy-et-hollande-trois-presidents-sur-ecoute_1335767>. Consulté le 4 avril 2016.

[403] Harris, *@War*, *op.cit.*, p.71

[404] Matthew M. Aid. « Inside the NSA's Ultra-Secret China Hacking Group ». *Foreign Policy*, 10 juin 2013. En ligne, <foreignpolicy.com/2013/06/10/inside-the-nsas-ultra-secret-china-hacking-group/> Consulté le 17 mars 2016.

[405] *Idem.*

[406] Martin Pengelly. « NSA targeted Chinese telecoms giant Huawei – report ». *The Guardian*, 22 mars 2014. En ligne, <www.theguardian.com/world/2014/mar/22/nsa-huawei-china-telecoms-times-spiegel>. Consulté le 4 avril 2016.

[407] De ce lot, notons les universités offrant des cursus avancés en informatique et suspectés d'être des pépinières à talent du gouvernement chinois Harris ou les groupes de pirates informatiques. *@War*, *op.cit.*, p.72

[408] David E. Sanger et Nicole Perlroth. « N.S.A. Breached Chinese Servers Seen as Security Threat ». *The New York Times*, 22 mars 2014. En ligne, <www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html?hp>. Consulté le 6 avril 2016.

Sans surprise, les autorités chinoises ont à leur tour dénoncé ces cyberactivités américaines[409], car tout comme l'espionnage chinois fût interprété comme une menace militaire et stratégique par les É.-U, les cybercapacités américaines inquiètent la Chine, même si selon Alexander, elles ne sont que défensives, utilisées dans le seul but d'amasser du « renseignement contribuant à la protection du pays et garantissant que nous prenons les meilleures décisions stratégiques possibles.[410] Loin de se résorber, cette préoccupation sera même accentuée par la mise en place prochaine du USCYBERCOM, dont les fonctions offensives seront bien définies.

3.1.2 Des cybercapacités militarisées et institutionnalisées.

Alors que le SIGINT dit actif permet d'accroître et d'étendre géographiquement les capacités informationnelles de la NSA, l'arrivée d'Alexander accélérera leur transformation en cybercapacités militaires. Ce processus profite aussi de l'esprit d'initiative de personnalités politiques considérant elles aussi le cyberespace comme un élément central de la sécurité nationale américaine, dont le vice-amiral Michael McConnell[411], nommé en 2007 au poste de directeur des services de renseignement (DNI). Il réussira, avec l'aide de la puissance bureaucratique de Robert Gates, secrétaire à la Défense de l'époque, et des exploits techniques d'Alexander, à inscrire durablement la question du cyber dans les agendas présidentiels de W. Bush et d'Obama et de faciliter la mise sur pied du USCYBERCOM.

---

[409] Terril Yue Jones. « China has 'mountains of data' about U.S. cyber attacks: official ». *Reuters*, 5 juin 2013. En ligne, <www.reuters.com/article/us-china-usa-hacking-idUSBRE95404L20130605>. Consulté le 5 avril 2016.

[410] Christopher Joye. « Interview transcript: former head of the NSA and commander of the US cyber command, General Keith Alexander ». *The Australia Financial Review*, 8 mai 2014. En ligne, <www.afr.com/technology/web/security/interview-transcriptformer-head-of-the-nsa-and-commander-of-the-us-cyber-command-general-keith-alexander-20140507-itzhw>. Consulté le 15 avril 2016.

[411] Directeur de la NSA de 1992 à 1996, il est ensuite devenu, jusqu'en 2006, vice-président chez Booz Allen Hamilton, un contractant privé faisant des affaires lucratives dans le secteur de la défense. En 2007, il revient au sein de l'appareil gouvernemental comme Director of National Intelligence, position qu'il a occupée jusqu'au début du mandat d'Obama.

Avant même l'arrivée d'Alexander, les forces armées américaines considéraient déjà le cyberespace comme un important domaine stratégique. Reconnu par la *National Defense Strategy* de 2005 comme un nouveau théâtre d'opérations[412], le chef d'État-major des armées affirmera quant à lui dans la *National Military Strategy* américaine de 2004, que « les Forces armées doivent avoir la possibilité d'opérer à travers tous les domaines de l'espace de combat : air, terre, mer, espace et cyberespace[413] ». Deux ans plus tard, il affirmait que « la prospérité et la sécurité de notre nation compte sur le cyberespace afin d'obtenir un avantage stratégique et de renforcer les instruments de la puissance nationale.[414] »

Le principal objectif stratégique du cyberespace n'est donc plus d'influer sur les processus cognitifs de l'adversaire dans une perspective de dissuasion, mais d'y nier sa liberté d'action en attaquant « [...] le personnel, les installations ou les équipements afin de dégrader, neutraliser ou détruire les capacités de combat de l'ennemi, tout en protégeant les nôtres.[415] » Pour ce faire, opérer dans le cyberespace nécessiterait une supériorité stratégique permise par une puissance de feu qui, encadrée par une doctrine, lui accorderait un rôle opérationnel à la hauteur de sa valeur stratégique. Tout comme la puissance aérienne américaine était, dans l'entre-deux-guerres, assujettie à l'autorité de l'Armée et à ses objectifs stratégiques propres, le cyber était dans une période où son potentiel militaire n'était pas reconnu à sa juste valeur. Selon Alexander, « nous ne pouvons pas nous permettre le luxe d'attendre 20 ans afin de développer une stratégie, des tactiques et une doctrine afin de faire face à cette révolution et ainsi maintenir la supériorité américaine dans cet environnement changeant rapidement.[416] » Il n'aura pas à attendre bien longtemps, car le vice-amiral Michael McConnell prendra ce dossier à bras-

---

[412] États-Unis, Department of Defense. *The National Defense Strategy of the United States of America.* Washington D.C. : Department of Defense, 2005, p.16

[413] États-Unis, Joint Chief of Staff. *The National Military Strategy of the United States of America.* Washington D.C. : Joint Chief of Staff, 2004, p.18.

[414] États-Unis, Joint Chief of Staff. *The National Miliary Strategy for Cyberspace Operations.* Washington D.C. : Joint Chief of Staff, 2006, p.1

[415] Gen. Keith B. Alexander. « Warfighting in Cyberspace ». *Joint Forces Quarterly*, no.47, 2007, p.60

[416] *Ibid.*, p.61

le-corps et deviendra un véritable entrepreneur de la prise de décision, des individus que Michael Mazarr définit comme

> [...] des partisans déterminés, pour une raison ou une autre, à combattre l'inertie, la bureaucratie, les intérêts divergents, et tout ce qui se trouve sur leur voie qui les empêche de promouvoir leurs idées, afin que celles-ci profitent des fenêtres d'opportunité et aboutissent à l'adoption de lois ou de politiques.[417]

Lui-même directeur de la NSA (DIRNSA) entre 1992 et 1996, il considérait déjà à l'époque le cyberespace comme un enjeu stratégique important dans une société de plus en plus interconnectée[418], un intérêt qu'il entretiendra au cours de sa carrière chez Booz Allen Hamilton, un contractant privé oeuvrant dans le milieu de la défense. S'il a accepté le poste de DNI, c'est notamment parce que celui-ci lui permettrait d'inscrire le cyber dans les priorités présidentielles en l'évoquant auprès de personnes-clés[419]: par exemple, lors d'une séance d'information quotidienne donnée au président et à certains conseillers, McConnell avisa G.W. Bush que « si les auteurs du 11-septembre s'étaient concentrés sur une seule banque américaine par l'entremise d'une cyberattaque réussie, cela aurait eu un plus grand impact sur l'économie des É.-U.[420] ». Préoccupant énormément le président[421], ce scénario catastrophe a réussi à capter son attention sur les conséquences que pouvait entraîner une cyberattaque, une véritable opportunité permettant à McConnell de convaincre W. Bush d'y consacrer davantage d'importance et de moyens.

Cette influence de McConnell se fait aussi sentir en 2007 dans le cadre du *sursaut* en Irak. Si, en 2004, le général Abizaid avait sans succès tenté de convaincre W. Bush d'autoriser l'emploi de cyberopérations offensives afin d'appuyer les efforts militaires américains

---

[417] Michael Mazarr, dans David, *Au sein de la Maison-Blanche*, *op.cit.*, p.62.

[418] Tim Shorrock. *Spies for Hire : The Secret World of Intelligence Outsourcing*. New York : Simon & Schuster, 2009, p.49

[419] Kaplan, *op.cit.*, p.141.

[420] Mike McConnell, cité dans Shane Harris. « China's Cyber-Militia ». *National Journal*, 31 mai 2008. En ligne, <www.nationaljournal.com/magazine/china-s-cyber-militia-20080531>. Consulté le 15 février 2016; Kaplan, *op.cit.*, p.142 – 144.

[421] Shane Harris. *The Watchers : The Rise of America's Surveillance State*. New York : Penguin Group, 2011, p.328

contre l'insurrection irakienne[422], McConnell le convaincra, trois ans plus tard, d'envoyer des équipes de la NSA sur le champ de bataille[423] pour une mission reposant « sur des techniques et outils de piratage, incluant des virus informatiques malveillants, alors considérés comme étant parmi les plus innovantes et imprévisibles armes de l'arsenal américain[424] ». L'objectif de ce contingent, atteignant 6000 hommes et femmes oeuvrant en Irak et en Afghanistan[425], était de créer un lien direct entre les services de renseignement et les troupes sur le terrain, d'accélérer la transmission d'informations-clés et de combattre plus efficacement les forces insurrectionnelles irakiennes.

Les capacités informationnelles de la NSA y jouaient d'abord un rôle plus traditionnel, captant des signaux locaux, collectant et analysant les informations, afin de découvrir rapidement de nouvelles pistes et d'obtenir une meilleure compréhension du terrain et des forces en présence[426]. Par le passé, l'agence faisait ce travail à distance, mais avec de longs délais : en oeuvrant directement sur le champ de bataille, « le temps de latence entre la collecte du renseignement et l'action en résultant est passé de 16 heures à une seule minute[427] », un gain en efficacité permettant à la NSA de démontrer la potentialité du cyber en contexte militaire, sans toutefois se limiter au rôle de SIGINT passif. En effet, les pirates informatiques de l'agence sont également passés à l'attaque : l'accès à *Obelisk*, réseau central et véritable C2 d'Al-Qaeda, a permis d'implanter « [...] des programmes malveillants dans les forums djihadistes, incitant leurs utilisateurs à cliquer sur des liens installant des espiogiciels sur leurs ordinateurs. Obelisk donnait donc aux espions un accès aux secrets d'Al-Qaeda et des moyens pour infiltrer ses rangs[428] ». En plus de rendre hors service certains serveurs informatiques de l'organisation, de faux rendez-vous étaient donnés aux insurgés, où les attendront des forces spéciales américaines ou l'œil

[422] Kaplan, *op.cit.*, p.125
[423] Harris, *@War*, *op.cit.*, p.7
[424] *Ibid., p.8*
[425] Kaplan, *op.cit.*, p.132
[426] Harris, *@War*, *op.cit.*, p.13
[427] Kaplan, *op.cit.*, p.132
[428] Harris, *@War*, *op.cit.*, p.19

averti d'un drone[429]. Le mariage entre les secteurs militaires et du renseignement sur le champ de bataille était consommé.

Ne souhaitant pas laisser le champ libre à la NSA, l'USAF mettra sur pied le *Air Force Cyber Command* (AFCYBER) et se proclamera la meilleure option militaire pour le cyberespace[430] où elle adoptera sa posture offensive douhétienne. Malgré les initiatives rivales, la tourmente autour de la découverte du virus *agent.btz* au sein de serveurs classifiés du *U.S. Central Command* (USCENTCOM) consacrera la NSA comme principale responsable de la cybersécurité des É.-U. Sur une base militaire américaine au Moyen-Orient, l'insertion d'une clé USB infectée dans un ordinateur relié aux serveurs touchés a permis à un virus, considéré comme la plus importante violation des systèmes informatiques militaires américains, d'y accéder et de probablement y exfiltrer des données[431], œuvre potentielle d'un service de renseignement étranger.[432] Devant un tel évènement, « aucune entité, civile ou militaire, avait une idée à propos de qui avait fait ça, comment l'arrêter et quoi faire par la suite, excepté l'agence avec l'argent, la technologie et le talent suffisant pour faire face à de telles questions : la NSA.[433] » En vingt-quatre heures, Alexander et son équipe de *whiz kids* mettront en place l'opération *Buckshot Yankee*, localisant et analysant le virus afin d'en tirer un programme nettoyant les ordinateurs touchés[434], une opération qui dura 14 mois[435]. Alexander a donc su habilement exploiter l'opportunité s'offrant soudainement à lui, la réactivité de la NSA marquant les esprits au Pentagone. En se présentant ainsi comme indispensable, l'agence porta un coup fatal à la concurrence.

---

[429] *Ibid.*, p.18 – 19; Kaplan, *op.cit.*, p.133 – 134.
[430] William T. Lord. « USAF Cyber Command : To Fly and Fight in Cyberspace ». *Strategic Studies Quarterly*, automne 2008, p.11.
[431] Kaplan, *op.cit.*, p.150
[432] Lynn III. *Defending New Domain*, *op.cit.*, p.97
[433] Kaplan, *op.cit.*, p.151
[434] *Ibid.*, p.150
[435] Noah Shachtman. « Insiders Doubt 2008 Pentagon Hack Was Foreign Spy Attack (Updated) ». *Wired.com*, 25 août 2010. En ligne, <www.wired.com/2010/08/insiders-doubt-2008-pentagon-hack-was-foreign-spy-attack/>. Consulté le 10 avril 2016.

En 2010, Lynn III écrivait que *Buckshot Yankee* avait été une véritable prise de conscience et un tournant dans la stratégie américaine de cyberdéfense[436], faisant de la cybersécurité une priorité au sein des forces armées[437]. Si de nombreuses réflexions du genre étaient finalement tombées dans l'oubli par le passé, le triptyque Alexander/Gates/McConnell[438] a su surfer la vague, profitant également du fait que l'Estonie et la Géorgie venaient elles aussi de subir, en 2007 et 2008 respectivement, d'importantes cyberattaques d'origine russes. Les astres s'alignaient pour que le cyber prenne une place durable dans l'appareil militaire.

Si avant cet épisode, McConnell avait déjà évoqué à Robert Gates la nécessité de créer un commandement militaire dédié au cyber[439], une idée n'aboutissant pas, mais que Gates trouvait intéressante[440], *Buckshot Yankee* allait toutefois en faire une réalité. Fidèle à la NSA, McConnell militait pour que ce commandement ne dédouble pas les capacités développées par l'agence, conseillant plutôt d'en faire l'élément central.[441] De son côté, Gates, ancien directeur de la CIA, tendait justement à favoriser les organisations civiles et à défendre la perspective du secteur du renseignement, en plus de faire preuve de pragmatisme en allant au-delà des luttes bureaucratiques prenant place au sein du DoD[442]. Le projet survivra à l'élection de 2008, McConnell ayant convaincu Obama du sérieux de la menace cyber[443], ce dernier y étant, par son âge, plus sensible, alors que Gates insistera auprès du nouveau président pour que l'on adopte le projet d'un commandement cyber[444]. C'est ainsi qu'en mai 2010 fut officiellement mis en place le USCYBERCOM, faisant d'Alexander à la fois son commandant et DIRNSA.

---

[436] Lynn III, *Defending a New Domain*, *op.cit.*, p.97
[437] Shachtman, *op.cit.*
[438] Il est important de noter que les trois s'estimaient également beaucoup. Alors que Gates et McConnell ont travaillé ensemble sous H.W. Bush, Gates qualifia Alexander « d'un des meilleurs et des plus intelligents officiers que je n'ai jamais rencontrés. »; Gates, op.cit., p.450; Lawrence Wright. « The Spymaster ». *The New Yorker*, 21 janvier 2008. En ligne, <www.newyorker.com/magazine/2008/01/21/the-spymaster>. Consulté le 10 avril 2016
[439] Robert M. Gates. *Duty : Memoirs of a Secretart at War*. New York : Alfred A. Knopf, 2014, p.449
[440] Kaplan, *op.cit.*, p.152
[441] Clarke et Knake, *op.cit.* p.38
[442] *Ibid.*, p.39.
[443] Kaplan, *op.cit.* p.162
[444] *Ibid.*, p.153.

Loin de séparer les deux responsabilités, la NSA représentera la clé du succès du CYBERCOM[445], exploitant « son expertise en renseignement, en analyse et en protection de l'information, tout en épargnant aux É.-U. les ressources, la sécurité et les opportunités impliquées dans la duplication des capacités utilisées par les décideurs tactiques, stratégiques et opérationnels[446] ». Le CYBERCOM fait également partie du *United States Strategic Command* (USSTRATCOM), dont la mission est de conduire « des opérations globales afin de dissuader et de détecter les attaques stratégiques envers les É.-U. et ses alliés, et il est préparé à défendre la nation de la manière appropriée.[447] » Objectif auquel, comme nous le verrons, participera pleinement le cyberespace.

Fort Meade se transformera dès lors en un pôle de la cyberpuissance américaine. En plus de la NSA, il verra s'y installer le CYBERCOM, entraînant avec lui la quasi-entièreté des unités militaires cyber et la *Defense Information Systems Agency* (DISA), une unité de support de combat chargée de soutenir le réseau de TIC du Pentagone, incluant les composantes du C4ISR[448]. À la suite de cette réorganisation, c'est près de 60 000 employés qui seront désormais placés sous l'autorité du CYBERCOM.[449] Le gouvernement américain ne lésine pas quand vient le temps d'investir dans la défense du pays contre les cyberattaques : alors qu'entre 2010 et 2015, le financement gouvernemental consacré au CYBERCOM passait de 120 millions de dollars à près de 510 millions[450], les investissements du DoD dans les cyberopérations ont quant à eux

---

[445] États-Unis, United States Cyber Command. «Beyond the Build - Delivering Outcomes through Cyberspace ». Washington D.C. : Department of Defense, p.9

[446] *Ibid.*, p.4

[447] États-Unis, United States Strategic Command Public Affairs. « U.S. Strategic Command to Conduct Exercise Global Lightning ». *U.S. Strategic Command*, 22 avril 2016. En ligne, <www.stratcom.mil/news/2016/608/US_Strategic_Command_to_Conduct_Exercise_Global_Lightning/>. Consulté le 15 avril 2016.

[448] États-Unis, Department of Defense. *Directive Number 5105.19*. Washington D.C. : Department of Defense, 2006, p.2

[449] Singer, *op.cit.*, p.134

[450] Adam Segal. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. Philadelphie : PublicAffairs, 2016, p.237

passé de 2,3 milliards de dollars en 2012[451] à 5,1 milliards en 2015.[452] Cette importante concentration de ressources financières a aussi permis d'attirer de nombreuses entreprises, bénéficiant de près de 70% de ce budget annuel[453], dans ce qui deviendra une *Silicon Valley* de la cybersécurité[454], où les jeunes entreprises flairant l'opportunité que représente ce secteur en forte croissance[455] côtoient les multinationales se spécialisant dans la défense, comme Northrop Grumman, Boeing ou Lockheed Martin. Alors que le Pentagone réduira progressivement, mais considérablement, ses commandes d'armements conventionnels, ces dernières s'intéresseront progressivement au secteur lucratif qu'est le cyber[456].

L'établissement du CYBERCOM résout un problème rencontré par la NSA en ce qui a trait aux potentialités offensives de ses cybercapacités informationnelles. D'abord, les opérations de CNE mené par la NSA afin d'obtenir des renseignements par la voie du piratage représentent, pour Hayden, l'étape la plus difficile: il faut pénétrer un système et s'y mouvoir sans se faire détecter, un travail encore plus périlleux quand vient le temps d'exfiltrer de l'information[457]. Alors que ses *hackers* pourraient alors y mener des attaques ou des opérations de défense dite active (*active defense*), elle n'est pas autorisée à le faire. En effet, « la loi américaine est très claire à propos de la distinction entre l'espionnage et les missions de combat. L'espionnage est contrôlé par le Title 50 du Code des É.-U. et supervisé par les comités sur le renseignement du Congrès. Le combat relève du Title 10 et des comités des forces armées.[458] » Une fois l'agent du renseignement à

---

[451] États-Unis. Department of Defense. *Summary of the DoD Fiscal 2012 Budget Proposal.* PDF en ligne, <www.defense.gov/pdf/SUMMARY_OF_THE_DOD_FISCAL_2012_BUDGET_PROPOSAL_(3).pdf>. Consulté le 15 mars 2015

[452] États-Unis. Department of Defense. *DoD Releases Fiscal 2015 Budget Proposal and 2014 QDR.* En ligne, <www.defense.gov/releases/release.aspx?releaseid=16567>. Consulté le 15 mars 2015

[453] Greenwald, *op.cit*, p.101

[454] Jamie Smith Hopkins. « Sourcefire founder: Cisco deal is 'a good match' ». *The Baltimore Sun*, 28 juillet 2013. En ligne, <www.baltimoresun.com/business/bs-bz-sourcefire-martin-roesch-qa-20130728-story.html> Consulté le 16 avril 2016

[455] Nishad Majmudar. « Fort Meade as Cyber Hub Turns Maryland Into a Startup Hot Spot ». *Bloomberg.com*, 30 janvier 2012. En ligne, <www.bloomberg.com/news/articles/2012-01-30/fort-meade-as-cyber-hub-turns-maryland-into-a-startup-hot-spot>. Consulté le 15 avril 2016.

[456] Harris, *@War*, *op.cit.*, p.122

[457] Hayden, *op.cit.*, p.132

[458] *Idem.*

l'intérieur du système informatique d'une cible, seul le personnel militaire est autorisé à y faire feu.

Lorsque G.W. Bush et Dick Cheney incitaient Alexander à privilégier une posture offensive et à développer l'équivalent cyber du *Manhattan Project*[459] ou quand la NSA participait à l'opération *Olympic Games* en développant le virus Stuxnet[460], elle le faisait à travers le *Joint Functional Component Command for Network Warfare* (JFCC-NW), alors une composante du STRATCOM. Quand la NSA accédait à une cible et y faisait de la reconnaissance, c'est le commandant du STRATCOM qui donnait l'ordre final, conformément au *Title 10*, afin que soient menées des opérations de destruction ou de manipulation d'informations[461]. Bien que possible et fonctionnel, ce type d'arrangement devait également être pris pour les mesures défensives par l'entremise du *Joint Task Force-Global Network Operations* (JTF-GNO), des dédoublements administratifs peu efficaces qui seront supprimés par l'intégration de ces deux entités au sein du CYBERCOM[462].

Ce nouveau sous-commandement exauce le souhait d'Alexander de faire du cyberespace un véritable domaine stratégique opérationnel, et d'avoir une organisation pouvant réellement s'impliquer dans tous ses aspects, comme en témoigne sa mission qui est de

> planifier, coordonner, intégrer, synchroniser et conduire les activités dirigeant les opérations de défense des réseaux d'informations indiqués du DoD et d'être prêt à conduire des opérations militaires dans l'entièreté du spectre du cyberespace afin de permettre les initiatives dans tous les domaines, d'assurer aux É.-U. et à ses alliés leur liberté d'action dans le cyberespace, et de nier celle de nos adversaires.[463]

---

[459] James Bamford. *The Shadow Factory : The Ultra-Secret NSA from 9/11 to the Eavesdropping on America*. New York : Doubleday, 2008, p.333

[460] Sanger, *op.cit.*, p.191-193

[461] Hayden, *op.cit.*, p.137 – 138.

[462] Paul Walker. « Organizing for Cyberspace : Operations: Selected Issues ». *International Law Studies*, vol.89, no,341, 2013, p.342

[463] Alexander. *Building a New Command in Cyberspace*, *op.cit.*, p.4

Cette synchronisation des efforts cyber interarmées est régie par une autorité centralisée, utilisant plus efficacement le financement disponible pour le cyber[464] et contrôlant mieux l'utilisation de cyberopérations pouvant avoir des répercussions dommageables pour les É.-U. et pour le monde entier. Le CYBERCOM permet d'abord d'éviter qu'une unité indépendante, comme l'était l'AFCYBER, n'utilise une cyberarme à ses propres fins stratégiques, ayant comme conséquence de la gâcher, son utilisation permettant à la victime, ainsi qu'au monde entier, d'éventuellement mieux s'en défendre[465]. Puisqu'une cyberattaque peut également avoir des conséquences potentielles graves et inattendues et affecter des réseaux civils au passage, la décision d'en faire usage doit rigoureuse et soumise, à l'instar du nucléaire, à un calcul coûts/bénéfices soigneusement effectué[466].

Fortes de la réorganisation de ces cybercapacités et de leur implantation durable dans l'organigramme militaire, les É.-U. développeront pour le cyberespace une doctrine militaire visant la dissuasion, dont l'objectif est d'inciter un adversaire au calme et au respect du *statu quo*, tout en utilisant le moins possible ses atouts offensifs. Alors qu'en 2010, Lynn III affirmait que « l'élément clé du CYBERCOM est le fait qu'il réunisse, sous un même toit, le renseignement, l'attaque et la défense[467] », c'est exactement cette polyvalence opérationnelle qui permettra au cyberespace de prendre la place stratégique qui lui revient et de finalement la mettre en action.

3.2 L'implantation d'une cyberdoctrine américaine visant la dissuasion

Un an après son arrivée au pouvoir, Barack Obama obtenait un nouvel instrument lui permettant d'atteindre ses objectifs de politique étrangère, et ce, conformément à son désir à la fois de retrancher les É.-U. du système international et d'y rendre leur empreinte plus légère, délaissant rapidement les options militaires afin de privilégier les opérations

---

[464] David M. Hollis. « USCYBERCOM : The Need for a Combatant Command versus a Subunified Command », *Joint Force Quarterly*, vol.58, no.3, 2010, p.53

[465] *Ibid.*, p.51

[466] *Idem.*

[467] États-Unis, Department of Defense. *Deputy Secretary of Defense Speech - Remarks at Stratcom Cyber Symposium*. Washington D.C. : Department of Defense, 26 mai 2010. En ligne, <archive.defense.gov/speeches/speech.aspx?speechid=1477>. Consulté le 25 avril 2016.

spéciales, l'utilisation étendue de drones ou l'expertise des diverses agences de renseignements . Outre la CIA, la NSA, un des organes les plus secrets du renseignement américain et l'un des éléments centraux du CYBERCOM, participera activement à cette posture, notamment en retraçant et localisant des cibles en sol irakien ou afghan ensuite pris en chasse par les opérations spéciales ou les drones ou, tel que mentionné plus tôt, en attaquant informatiquement le programme nucléaire iranien. C'est dans cet esprit d'actions clandestines que la mise en place du USCYBERCOM s'arrimera et contribuera à la grande stratégie d'Obama que représente le pivot vers l'Asie. Par contre, tout comme l'analyse des cyberactivités chinoises le démontra lors du chapitre précédent, l'existence de cybercapacités américaines puissantes et imposantes, longtemps méconnues, mais désormais mieux documentées grâce à Snowden, soulève également la question des intentions américaines quant à leur utilisation éventuelle.

3.2.1 La cyberdissuasion comme instrument de la politique étrangère d'Obama

Pourtant, malgré le fait que le cyberespionnage chinois à l'encontre des É.-U. ait été interprété comme une menace claire à la sécurité nationale américaine, la solution au *dilemme de réponse* américain variera selon les tons adoptés par l'administration Obama. Si la posture cyber américaine apparaît aujourd'hui portée sur l'offensive, le président accorda plutôt, dès son entrée en poste, une grande importance à la protection du cyberespace, parallèlement à la brève période où son administration perpétuait la politique d'accommodement de G.W. Bush à l'endroit de la Chine[468].

Voulant éviter de provoquer ou d'inquiéter ses homologues chinois, préciser la véritable nature de cette cybermenace aurait été inopportun. Un an plus tard, la position américaine avait toutefois drastiquement changé. À l'heure où le potentiel rival chinois devenait de plus en plus téméraire avec des revendications maritimes agressivement menées au détriment de ses voisins, Hillary Clinton déclarera, au sommet de l'ASEAN de 2010, que « les É.-U., comme toutes les autres nations, ont comme intérêt national la liberté de

[468] David, *Au sein de la Maison-Blanche, op.cit.*, p.956.

navigation, le libre-accès au bien commun maritime de l'Asie et le respect du droit international dans la mer de Chine du Sud.[469] » C'est donc la vision des *faucons*, principalement défendue par Hillary Clinton et Robert Gates, qui prendra le dessus, une posture malgré tout tempérée par un Obama prudent et ne désirant pas provoquer inutilement la Chine.[470] Comme démontré dans le premier chapitre, cette attitude de confrontation mènera à un rééquilibrage externe proactif en Asie-Pacifique, marqué par des ententes diplomatiques et commerciales avec des pays est-asiatiques, une plus grande présence militaire américaine dans la région et une aide militaire importante apportée aux alliés, notamment auprès de Taïwan qui a reçu, en 2010 et 2011 uniquement, près de 12 milliards de dollars en équipements militaires divers.[471]

Le cyberespace ne sera pas en reste dans cette approche plus musclée envers la Chine, car comme l'affirme Richard L. Kugler, « la perspective de cyberattaques majeures ne devrait pas être considérée de manière isolée, mais dans le contexte de sécurité international[472] ». Afin d'atteindre les objectifs de la grande stratégie d'Obama qu'est le maintien de la suprématie américaine, du *statu quo* international et de la stabilité de la région stratégique qu'est l'Asie-Pacifique, les ressources américaines se faisant plus rares, il était donc nécessaire d'adopter les moyens militaires appropriés afin de les atteindre[473]. Grâce à leur discrétion et à leur coût relatif moins élevé, les cybercapacités américaines seront mises à contribution afin de stopper l'hémorragie économique, technologique et militaire que représente le vol de PI par la Chine, mais également pour contrer les risques d'une éventuelle escalade de tensions régionales pouvant entraîner un conflit militaire majeur. C'est dans cette optique que sera mise en place une doctrine

---

[469] États-Unis, Department of State. *Comments by Secretary Clinton in Hanoi, Vietnam.* En ligne, <iipdigital.usembassy.gov/st/english/texttrans/2010/07/20100723164658su0.4912989.html>. Consulté le 15 avril 2016.

[470] David, *Au sein de la Maison-Blanche, op.cit.*, p.957; Langler, *How Hillary..., op.cit.*

[471] Shirley A. Kan. *Taiwan: Major U.S. Arms Sales Since 1990.* Washington D.C. : Congressional Research Services, 2014, p. 45 – 46. PDF en ligne, <www.fas.org/sgp/crs/weapons/RL30957.pdf>. Consulté le 15 avril 2016.

[472] Richard L. Kugler. « Chapter 13 : Deterrence of Cyber Attacks » dans Franklin D. Kramer, Stuart H. Starr et Larry K. Wentz, *Cyberpower and National Security*, Washington D.C : National Defence University Press; Potomac Books, 2009, p.310

[473] Posen, *The Sources of Military Doctrine, op.cit.*, p.13.

militaire propre au cyberespace, c'est-à-dire des « principes fondamentaux selon lesquelles les forces militaires ou des éléments de ceux-ci guident leurs actions afin d'appuyer des objectifs nationaux[474] » et qui représente « la réponse étatique aux contraintes et incitatifs du monde externe, mais comprenant des moyens qui sont détenus par des organisations militaires.[475] » Cette cyberdoctrine sera donc le résultat d'une rencontre entre, d'un côté, une cybermenace chinoise persistante et s'attaquant à des points sensibles de la puissance nationale américaine et de l'autre, d'importantes cybercapacités américaines éprouvées et désormais techniquement et militairement rationalisées.

Celles-ci serviront non seulement à atteindre les objectifs politiques américains établis pour le cyberespace, mais contribueront également à l'effort national visant à freiner les visées expansionnistes chinoises, potentiel point de rupture géopolitique, notamment au sein de la stratégie d'*Air-Sea Battle*. La *PPD-20* qu'Obama promulgua en 2012 permet de mieux comprendre la forme que cette doctrine prendra, celle-ci affirmant que

> les É.-U. ont un intérêt constant à développer et maintenir l'utilisation du cyberespace comme partie intégrale des capacités nationales américaines afin d'amasser du renseignement, mais également afin de ***dissuader***, ***nier*** ou ***défaire*** n'importe quel adversaire qui chercherait à mettre à mal les intérêts nationaux américains que ce soit en temps de paix, de crise ou de guerre.[476]

En réponse à ces actions interprétées comme étant résolument hostiles, les É.-U. augmenteront de manière importante leurs capacités militaires défensives et offensives, conformément au principe de l'*équilibrage interne*, afin de mettre sur pied une doctrine visant la dissuasion. Selon le DoD,

> les opérations de dissuasion cherchent à convaincre les adversaires de ne pas prendre de mesures pouvant menacer les intérêts vitaux américains, et ce, au moyen d'une influence déterminante sur leur prise de décision. Cette influence est obtenue en les menaçant de manière crédible de leur refuser les bénéfices et/ou de lui

---

[474] États-Unis, Deparment of Defense. « Doctrine ». Dans *DoD Dictionary of Military Terms*, s.d. En ligne, <www.dtic.mil/doctrine/dod_dictionary/data/d/3840.html>. Consulté le 15 avril 2016.

[475] Posen, *The Sources of Military Doctrine*, *op.cit.*, p.38

[476] États-Unis, White House. *Presidential Policy Directive 20.* Washington D.C.: The White House. PDF en ligne, <fas.org/irp/offdocs/ppd/ppd-20.pdf>, 2012, p.4

> imposer des coûts, tout en encourageant la retenue en convainquant l'acteur que la modération se traduira par des résultats acceptables.[477]

Elle permettrait à la fois de limiter la capacité ou la volonté chinoise à mener des cyberopérations, que ce soit au niveau de l'espionnage, domaine où elle est passée maître, mais aussi de potentielles cyberattaques sur des composantes informatiques essentielles au bon fonctionnement des capacités militaires américaines. L'augmentation des tensions entre la Chine et les É.-U. joue donc un grand rôle dans l'adoption de cette posture particulière. Pour Charles Glaser, une stratégie de dissuasion s'applique optimalement à un État qu'il qualifie d'*avare et se sentant en sécurité*, défini comme étant « [...] prêt à encourir des coûts ou des risques pour une expansion non reliée à sa sécurité[478] », qui « [...] reconnaît que le défenseur souhaite seulement protéger le *statu quo* et qu'il utiliserait ses capacités militaires seulement en réponse à une agression.[479] » Du point de vue américain, cette définition peut s'appliquer à la Chine, perçue comme une puissance expansionniste et révisionniste, attitudes incompréhensibles pour ceux qui la considèrent, de par sa force, son emplacement géographique et son environnement stratégique, particulièrement en sécurité au sein du système international actuel.

Même si le chapitre précédent a abordé plusieurs inquiétudes amenant la Chine à militariser ses abords maritimes, Christopher Twomey estime qu'il est difficile de comprendre les raisons la poussant à investir autant dans ses capacités militaires : ses frontières terrestres sont pacifiées, elle est libérée d'une guerre froide qui la prenait en étau entre les É.-U. et l'URSS, elle est pleinement intégrée au sein d'un ordre libéral international dont elle profite amplement et les relations sino-taïwanaises, sans être au

---

[477] États-Unis, Department of Defense. *Deterrence Operations - Joint Operating Concept*. Washington D.C. : Department of Defense, 2006, p.8

[478] Par *éléments non-reliés à la sécurité et à la survie d'un État*, Glaser inclut l'agrandissement de sa richesse, de son territoire ou de son prestige. Charles L. Glaser. « Political Consequences of Military Strategy : Expanding and Refining the Spiral and Deterrence Models », *World Politics*, vol.44, no.4, 1992, p.501.

[479] *Ibid.*, p.502

beau fixe, se réchauffent peu à peu[480]. Selon Robert Jervis, il est donc nécessaire d'agir devant ce type de comportement, car

> de grands dangers surgissent si un agresseur croit que les puissances prônant le statu quo sont faibles, autant en capacités qu'en détermination. Cette croyance va mener la première à tester ses adversaires, débutant habituellement par un petit enjeu d'importance moindre. Si les puissances prônant le statu quo retraitent, ils ne vont pas simplement perdre l'enjeu spécifique alors en jeu, mais, plus important,vont aussi encourager l'agresseur à mettre davantage de pression à long terme.[481]

Confronté à un adversaire de cette nature, il est donc nécessaire de répondre en se montrant crédible et combatif, de lui signaler qu'un éventuel conflit serait coûteux et inévitablement désavantageux. En fin de compte, il s'agit de convaincre les États désireux de perturber la stabilité internationale que la coopération et la retenue sont préférables aux conséquences qu'un comportement considéré comme hostile peut entraîner[482]. Pour y arriver, Van Evera considère qu'un avantage offensif facilitant l'agression et le conflit peut également faciliter les tentatives de dissuasion :

> Les capacités offensives dans les mains de puissances défendant le *statu quo* peuvent fournir plus d'effets dissuasifs que provocants si l'État agresseur sait qu'il a provoqué l'hostilité de la puissance du statu quo, s'il sait que cette dernière n'a pas d'intentions agressives à la base, et s'il ne peut se défaire, par la force, de la menace offensive de la puissance défendant le *statu quo*.[483]

Le concept de la *dissuasion* permet alors d'attribuer une intention claire à la militarisation américaine du cyberespace, car en considérant officiellement ce dernier comme un domaine militaire que les É.-U. doivent maîtriser, la mise en place du USCYBERCOM permet la poursuite de cette suprématie. Cette organisation rend également possible, grâce à ces importantes cybercapacités défensives et offensives, le rétablissement de l'équilibre de la menace qui favorisait jusqu'alors une Chine exploitant impunément un cyberespace

---

[480] Christopher Twomey et Xu Hui. « Military Developments ». Dans Nina Hachigian (ed), *Debating China : The U.S. – China Relationship in Ten Conversations*. New York : Oxford University Press, 2014, p.156

[481] Robert Jervis, « Deterrence, the Spiral Model and the Intentions of the Adversary ». Dans *Perception and Misperception in International Politics*. Princeton (N.J.) : Princeton University Press, 1976, p.58

[482] *Ibid.*, p.60

[483] Van Evera, *op.cit.*, p.16

longtemps délaissé par les Américains, de contrecarrer l'incertitude entourant ses intentions considérées comme potentiellement hostiles et d'y maintenir le *statu quo* régional ainsi menacé. Optant originalement pour des mesures défensives, cette dissuasion cherchera par la suite à exploiter l'avantage offensif attribué au cyberespace afin de forcer la Chine à la retenue. Ne se limitant pas à agir dans son seul domaine, cette cyberdissuasion se retrouvera aussi au sein de la stratégie américaine du *Air-Sea Battle*, visant à contrecarrer une stratégie chinoise de A2/AD accordant une grande importance à l'apport stratégique du cyberespace.

3.2.2 La mutation d'une cyberdoctrine américaine visant la dissuasion

Le concept de cyberdissuasion évoluera rapidement au sein des initiatives gouvernementales et militaires entreprises afin de protéger le cyberespace : au cours du premier mandat du président G.W. Bush, il apparaissait alors impensable de dissuader efficacement les multiples acteurs menaçants d'attaquer les réseaux américains, tout comme il semblait inconcevable que les É.-U. puissent réagir à de telles attaques. La *National Strategy to Secure Cyberspace* de 2003 démontrait qu'une stratégie de cyberdissuasion était encore loin d'être mise en place, affirmant que « nous devons aller de l'avant dans notre compréhension du fait qu'il y a des ennemis qui cherchent à infliger des dommages à notre mode de vie.[484] » Responsable de la cybersécurité américaine, c'est au DHS qu'incombait de mettre en place une stratégie axée sur la protection des réseaux gouvernementaux. Devant prévenir les attaques contre les IC américaines et détecter les cybervulnérabilités de l'appareil étatique américain, le DHS devait également se préparer au pire. Alors que les É.-U. se sentaient très impuissants devant les nombreuses cybermenaces, le DHS devait donc se tenir prêt à réduire les dommages que provoquerait une cyberattaque majeure et à développer une certaine capacité de résilience[485].

---

[484] États-Unis, White House. *The National Strategy to Secure Cyberspace. op.cit,* p.5
[485] *Ibid.*, p.19 – 20

Pendant le premier mandat de G.W. Bush, la question de la cybersécurité n'ira pas au-delà de cet objectif défensif et limité dans sa portée.Trois ans plus tard, le QDR de 2006 réitérait l'aspect défensif en prônant l'obtention de capacités en mesure de défendre le cyberespace et le développement d'un C2 pouvant survivre à une cyberattaque. Par contre, en intégrant le cyberespace à la préoccupation qu'étaient alors les *armes de destruction massive*, le DoD affirmera également qu'il

> maintiendra une posture dissuasive afin de convaincre les agresseurs potentiels que leurs objectifs offensifs seraient niés et que toutes attaques sur le territoire, la population, les IC (notamment par l'entremise du cyberespace) ou les forces américaines pourraient mener à une réponse écrasante.[486]

Plus récemment, dans la lignée de cette volonté américaine de dissuader les cyberattaques, la *International Strategy for Cyberspace* de 2011 affirmait que « les É.-U. veilleront à ce que les risques associés à l'attaque ou à l'exploitation de nos réseaux l'emportent considérablement sur les avantages potentiels.[487] » C'est ainsi qu'après de longues années à discuter de l'éventualité d'une cyberdissuasion, les capacités informatiques de la NSA, dont l'ampleur technique a notamment été mise au jour par les révélations d'Edward Snowden, et la mise en place du CYBERCOM rendront la chose possible.

3.2.2.1 La défense du territoire américain contre les cyberattaques

Quotidiennement, les réseaux civils et militaires américains sont sondés des milliers de fois et scannés des millions d'autres[488], rendant leur défense complexe. En 2010, le DoD « opérait plus de 15 000 réseaux informatiques différents au sein de 4000 installations militaires à travers le monde. Tous les jours, plus de sept millions d'ordinateurs et d'outils de télécommunications du DoD sont utilisés dans 88 pays et permettent de mener des

---

[486] États-Unis, Department of Defense. *Quadrennial Defense Review Report 2006*. Washington D.C. : Deparment of Defense, 2006, p.25

[487] États-Unis, White House. *International Strategy for Cyberspace : Prosperity, Security and Openness in a Networked World*. Washington D.C. : The White House, 2011, p.13

[488] Lynn III, *op.cit.*, p.97

applications de soutien et de combat[489]. » Un tel front, constitué d'autant de portes d'entrée, est donc très vulnérable à des intrusions menant autant à de l'espionnage qu'à de potentielles cyberattaques plus dommageables. Tel qu'abordé plus tôt, l'aspect défensif demeure lourdement défavorisé comparativement à l'attaque, mais dans une logique de dissuasion, il est néanmoins nécessaire de s'y attarder et d'étanchéifier le plus possible le dispositif américain. Cet effort défensif permettra d'instaurer ce qu'on appelle une dissuasion par interdiction (*deterrence by denial*), impliquant de faire croire à l'attaquant qu'une cyberattaque n'atteindrait ni les objectifs fixés ni les gains recherchés. Il s'avérerait donc inutile pour l'attaquant de poursuivre son opération, qu'il croirait vouée à l'échec.[490]

Ce pan de la doctrine de dissuasion profite tout d'abord d'une refonte et d'un effort considérable à la base même de l'organisation, souvent le maillon le plus faible. En plus d'embaucher une main-d'œuvre hautement qualifiée en informatique et en réseautique[491], il est d'abord essentiel de sensibiliser les employés aux bonnes pratiques et aux bonnes utilisations des systèmes informatiques : ce sont ces pratiques déficientes qui permettent aux tentatives d'hameçonnage d'atteindre leur objectif, soit d'obtenir un accès au système, accès permettant de corrompre et d'accéder à l'entièreté du réseau.[492] La simple négligence peut aussi mettre en place des vulnérabilités pourtant facilement évitables et menant à l'affaiblissement du volet défensif de la dissuasion : pour Alexander,

> des correctifs de logiciel qui ne sont pas appliqués, des pare-feu laissés sans surveillance et des antivirus jamais mis à jour, même au sein de l'armée américaine, cela nous cause beaucoup de problèmes, particulièrement quand un risque pour l'un est partagé par tous[493].

---

[489] États-Unis, Department of Defense. *Quadrennial Defense Review 2010*. Washington D.C. : Department of Defense, 2010, p.37

[490] Traduction libre. Kugler, *op.cit.*, p.327

[491] États-Unis, Department of Defense. *Strategy for Operating in Cyberspace*, *op.cit.*, p.10

[492] Massoud Amin et Anthony M. Giacomoni. 2012. « Smart Grid – Safe, Secure, Self-Healing : Challenges and Opportunities in Power System Security, Resiliency, and Privacy », *IEEE Power & Energy Magazine*, janvier/février 2012, p. 35.

[493] Alexander. *Building a New Command in Cyberspace*, *op.cit.*, p.6

Si le risque est mis en commun, la *Comprehensive National Cybersecurity Initiative* de 2008, un programme initié par W. Bush sous la recommandation de McConnell, perpétué par Obama et bénéficiant d'un budget de 17,3 milliards de dollars dès sa première année, permettra de créer le *Federal Entreprise Network*, une supra-agence regroupant les serveurs gouvernementaux disséminés et limitant les points d'accès pouvant être utilisés par des acteurs malveillants : de 4000, la quantité de passage possible est passée à 50[494]. En réduisant considérablement les points d'accès à surveiller, la détection et les mesures défensives sont ainsi plus faciles à mener. Si le DHS est officiellement responsable de ce projet, c'est sans aucune surprise la NSA qui s'en chargera techniquement, étant la seule organisation apte à porter ce projet à bout de bras, raison pour laquelle elle héritera de la majeure partie du budget alloué.

Encore en vigueur aujourd'hui, un des principaux buts de ce programme est de mettre en commun la connaissance situationnelle des diverses entités du gouvernement, permettant à tous de mieux se défendre par le partage des vulnérabilités, des techniques utilisées par les acteurs malveillants, etc. Ce partage d'informations est également fait auprès du secteur privé, alors probablement la plus grande victime des cyberattaques, tout en étant la moins efficace défensivement. Si la *National Strategy to Secure Cyberspace* évitait de se mêler de la sécurité du secteur privé au nom du principe de la libre entreprise[495], le *Defense Industrial Base Initiative*, un projet piloté par la NSA, inclut plus d'une centaine d'entreprises du milieu de la défense, comptant parmi celles les plus largement touchées par le cyberespionnage chinois[496]. L'agence espère éventuellement incorporer d'autres types d'industries, ce qui lui permettrait d'assurer une cyberdéfense globale et optimale pour l'ensemble des É.-U., couvrant autant le secteur civil, militaire, industriel qu'économique. Le secteur privé lui sert alors de paratonnerre et d'éclaireur, car en informant la NSA des attaques subies et de leur *modus operandi*, ces entreprises lui

---

[494] Kaplan, *op.cit.*, p.146
[495] États-Unis, White House. *The National Strategy to Secure Cyberspace. op.cit,* p.14 – 15.
[496] Harris, *@War*, *op.cit.*, p.xix

permettent d'accroître considérablement sa connaissance situationnelle du cyberespace[497].

Le DHS et la NSA auront une approche défensive différente, aspect déterminant pour la suite des choses. Le premier mise plutôt sur une défense passive par l'entremise de son programme EINSTEIN, détectant, identifiant et bloquant les menaces avant qu'elles puissent s'infiltrer trop profondément[498]. Ce programme connaît pourtant un succès mitigé : en février 2016, un rapport du *Government Accountability Office* affirmait que la dernière mouture d'EINSTEIN échouerait à détecter 94% des menaces transitant par des logiciels populaires, telle la suite Office[499]. En 2014, c'est ce même système de surveillance qui a permis l'intrusion chinoise ayant dérobé les données d'autorisation de sécurité de près 21,5 millions d'employés fédéraux dans les serveurs de l'*Office of Personnel Management*.[500] Pour Alexander, ce type de défense passive est une véritable ligne Maginot des temps modernes qui, tout en se proclamant infranchissable, peut rapidement être contournée et s'avérer finalement inutile[501]. La NSA, qui s'est depuis longtemps retirée de ce projet, a préféré opter pour une défense dite *active*, s'appuyant sur l'idée que :

> la défense des réseaux militaires américains dépend de la connaissance que l'on a des cyberactivités de ceux qui nous voudraient du mal, connaissance qui à son tour dépend du renseignement produit par la NSA et les autres membres de la communauté du renseignement au sujet des intentions et des capacités des adversaires.[502]

---

[497] *Ibid.*, p.158

[498] États-Unis, Department of Homeland Security. « EINSTEIN ». Dans *Securing Federal Networks*, 14 décmbre 2015. En ligne, <www.dhs.gov/einstein>. Consulté le 26 avril 2016.

[499] États-Unis, Government Accountability Office. *Information Security - DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System.* Washington D.C. : Government Accountability Office, p.22

[500] Marina Koren. « About Those Fingerprints Stolen in the OPM Hack ». *The Atlantic*, 23 septembre 2015. En ligne, <www.theatlantic.com/technology/archive/2015/09/opm-hack-fingerprints/406900/>. Consulté le 27 avril 2016.

[501] Jennifer Valentino-De Vries et Julia Angwin. « Defenses Against Hackers Are Like the 'Maginot Line,' NSA Chief Says ». *The Wall Street Journal*, 13 janvier 2012. En ligne, <blogs.wsj.com/digits/2012/01/13/u-s-business-defenses-against-hackers-are-like-the-maginot-line-nsa-chief-says/>. Consulté le 27 avril 2016.

[502] États-Unis, Department of Defense. *Statement of General Keith B. Alexander, Commander of United States Cyber Command, Director of National Security Agency, Chief of Central Security Service, Before*

Préférant prévenir plutôt que d'encaisser les coups, la NSA exploite donc la portée géographique permise par ses cybercapacités afin d'observer les attaques qu'un adversaire présumé planifie mettre à exécution. Avant même qu'il puisse frapper, la NSA cherchera à éradiquer à la source la menace qu'il représente, posture défensive finissant aisément par se confondre avec une posture offensive.[503]. Selon le PPD-20, ce sont des *Defensive Cyber Effects Operations* (DCEO) dont le but est de

> permettre ou de produire des effets cyber à l'extérieur des réseaux du gouvernement américain dans le but de se défendre ou de se protéger contre des menaces imminentes, des attaques en cours ou des activités malveillantes allant à l'encontre des intérêts nationaux américains, qu'elles se trouvent à l'intérieur ou à l'extérieur du cyberespace.[504]

3.2.2.2 La mise en place d'une capacité crédible de représailles

Bien qu'essentielle, la dissuasion par déni de bénéfices, misant sur une posture défensive à la fois passive et active, a toutefois d'importantes limitations imposées par la nature même du cyberespace, perçue comme favorisant grandement l'attaque. Ce faisant, « chaque État préoccupé par le domaine cyber dans une perspective de sécurité mondiale est tout aussi déficient et vulnérable à une attaque. Par conséquent, les systèmes se consacrant à la cyberdéfense sont susceptibles de demeurer relativement impuissants, et ce, de manière généralisée.[505] » L'inefficacité proclamée de la cyberdéfense n'est pas sans rappeler celle de Giulio Douhet, véritable maître à penser de l'USAF. Pour pallier ces vulnérabilités béantes, une doctrine de cyberdissuasion doit également s'appuyer sur un volet offensif pouvant imposer des coûts, impliquant de « menacer de manière crédible d'imposer des coûts, des pertes et des risques trop pénibles à accepter, convaincants ainsi

---

the Senate Committee on Appropriations ''Cybersecurity : Preparing for and Responding to the Enduring Threat''. Washington D.C. : Department of Defense, 2013, p.2

[503] Kaplan, *op.cit.*, p.148.

[504] États-Unis, *White House. Presidential Policy Directive 20, op.cit,* p.3

[505] Traduction libre. Matthew D. Crosston. « World Gone Cyber MAD – How "Mutually Assured Debilitation" Is the Best Hope for Cyber Deterrence ». *Strategic Studies Quarterly*, vol.5, no.1, 2011, p.100

l'adversaire que la punition l'emporterait sur le succès espéré.[506] » Pour Warner et Good, plusieurs moyens peuvent augmenter ces coûts : améliorer notre capacité à attribuer les attaques à son responsable, démontrer volonté et capacité à répliquer dans le cyberespace, entreprendre des représailles diplomatiques ou économiques ou bien augmenter sa capacité à mener des opérations offensives. [507]

Avant même de penser à répliquer, à imposer des coûts ou à entamer des représailles à l'encontre d'un adversaire, il est nécessaire de régler le problème de l'attribution et de pouvoir déterminer exactement qui est derrière une attaque donnée. Au-delà du fait d'être techniquement capable ou non, il est important de laisser croire, afin d'être crédible dans notre menace de représailles, que l'on possède les capacités permettant de correctement identifier les attaquants. Pour plusieurs, cette étape demeure toutefois un obstacle majeur au succès d'une cyberdissuasion, un éventuel attaquant pouvant faire transiter ses cyberactivités par d'autres ordinateurs et masquer sa véritable identité ou localisation géographique. Les incertitudes soulevées par le processus d'attribution pourraient empêcher les autorités américaines de mettre en oeuvre une dissuasion en bonne et due forme, une réplique menée à l'encontre de la mauvaise cible ayant potentiellement des conséquences internationales importantes et gênantes[508]. C'est à ce moment qu'entre en jeu la portion « renseignement », car « plus grande sera la maîtrise technique du gouvernement, le bassin de talent et de compétences à sa disposition, plus grande sera la capacité de cet État à cacher ses opérations secrètes, à en découvrir d'autres et à réagir en conséquence.[509] » C'est dans cette optique que le rôle central de la NSA au sein du CYBERCOM se justifie, car si Leon Panetta, ancien secrétaire à la Défense, semblait à première vue bluffer en affirmant que les É.-U. avaient la capacité de retracer et de tenir

---

[506] Kugler. *op.cit.*, p.327

[507] Michael Warner et Michael Good. « Notes on Deterrence in Cyberspace ». Dans *Georgetown Journal of International Affairs – International Engagement on Cyber III : State Building on a New Frontier.* Washington D.C. : Edmund A. Walsh School of Foreign Service, 2013, p.70

[508] Markoff, Sanger et Shanker, *op.cit.*

[509] Traduction libre. Thomas Rid et Ben Buchanan. « Attributing Cyber Attacks ». *Journal of Strategic Studies*, vol.38, no.1 – 2, 2015, p.28 – 29.

responsable de potentiels agresseurs[510], les documents publiés ultérieurement par Snowden ont toutefois permis de renforcer la crédibilité américaine à pouvoir attribuer avec exactitude d'éventuelles cyberattaques à l'encontre des É.-U.

Après avoir déterminé le responsable de l'attaque, il reste à régler l'épineux problème des représailles, deuxième pilier de la dynamique de dissuasion. Les divers épisodes d'espionnage chinois ont démontré qu'il était possible de mener des représailles d'ordre diplomatique et économique dans le but de limiter ce comportement qui, bien qu'affectant grandement la sécurité nationale à long terme, ne représente pas le même niveau de danger qu'une cyberattaque sur les IC nationales. Dans le cas de la Chine, ce type de représailles s'est notamment matérialisé par la mise en accusation de cinq hauts gradés militaires[511] ou par l'échec politiquement influencé de la percée commerciale d'Huawei en sol américain[512]. Ces représailles ont tout tout de même donné lieu, en 2015, à un accord sino-américain visant à stopper la poursuite d'activités de cyberespionnage économique et industriel[513]. Les plus gros enjeux nécessitent toutefois des réponses plus considérables.

Tout comme les bombes atomiques de Hiroshima et de Nagasaki ont très clairement démontré les effets de la puissance nucléaire et, par le fait même, considérablement renforcé l'effet psychologique nécessaire au succès de la dissuasion nucléaire, certains estiment que les É.-U. devraient faire usage de leur cyberpuissance, et des effets punitifs qu'elle rend possibles, afin de démontrer au monde entier la détermination américaine à utiliser le cyberespace s'il est attaqué et d'ainsi instiller la crainte. Sans pour autant délaisser ses cyberopérations secrètes, Crosston estime qu'une utilisation explicite des

---

[510] États-Unis, Department of Defense. *Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security*. Washington: The White House, 2012. En ligne, <www.defense.gov/transcripts/transcript.aspx?transcriptid=5136>. Consulté le 25 avril 2016.

[511] Schmidt et Sanger, *op.cit.*

[512] Adam W. Goldberg et Joshua P. Galper. « Where Huawei Went Wrong in America ». *The Wall Street Journal*, 3 mars 2011. En ligne, <www.wsj.com/articles/SB10001424052748703559604576175692598333556>. Consulté le 25 avril 2016.

[513] Kim Zetter. « US and China Reach Historic Agreement on Economic Espionage ». *Wired*, 25 septembre 2015. En ligne, <www.wired.com/2015/09/us-china-reach-historic-agreement-economic-espionage/>. Consulté le 25 avril 2016.

cybercapacités offensives nationales « [...] rendrait plus probable une dissuasion proactive par la peur et donnerait l'impression d'une supériorité décisionnelle et informationnelle.[514] » Dans la même veine, le colonel Charles W. Williamson III proposait de lancer des attaques DDoS massives et débilitantes à l'encontre des serveurs adverses, affirmant que « les É.-U. requièrent la capacité de larguer un tapis de bombes dans le cyberespace afin de créer la force de dissuasion dont nous manquons.[515] »

Cependant, un acteur étatique se trouvant dans une situation d'interdépendance économique, s'appuyant beaucoup sur le cyberespace et sur la structure informationnelle de la société, comme les É.-U., a peu de chance de vouloir se lancer dans des cybereprésailles. Pour un attaquant, la possibilité de devoir affronter des conséquences imprévues et pouvant même se retourner contre lui peut suffire à pousser à la retenue ces États possédant de fortes capacités cybernétiques[516]. La situation de la cyberdissuasion actuelle s'apparente à celle qui serait peut-être survenue avec la puissance nucléaire si Harry Truman n'avait pas lancé *Little Boy* et *Fat Man* sur le Japon en 1945 : si l'on peut depuis objectivement craindre les armes nucléaires par les immenses dégâts qu'elles ont causés par le passé, le cyber est au contraire « incapable d'induire une peur réelle, mais elle est capable de soulever le spectre du doute et de l'incertitude.[517] » Puisque chaque système informatique possède des vulnérabilités encore inconnues et qu'il est difficile de savoir s'il n'a pas déjà été compromis, infecté ou exploité, un État pourra vraisemblablement imposer une forme de dissuasion par le doute qu'il sème chez ses adversaires. Pour Martin Libicki, « la cible d'une attaque n'est pas tant un système informatique, mais la *confiance* en celui-ci ou dans tous les autres systèmes informatiques[518]». Étant impossible d'assurer qu'une cyberattaque initiale puisse rendre

---

[514] Traduction libre. Matthew Crosston. « Virtual Patriots and a New American Cyber Strategy : Changing the Zero-Sum Game ». *Strategic Studies Quarterly*, vol.6, no.4, 2012, p.107

[515] Traduction libre. Colonel Charles Williamson, cité dans Jean-Loup Samaan. « Beyond the Rift in Cyber Strategy: a Middle Ground for the US Military Posture in Cyberspace », *Strategic Insights*, vol.10, no.1, 2011, p.6 – 7.

[516] Kevin Chilton et Greg Weaver, 'Waging Deterrence in the Twenty-First Century', *Strategic Studies Quarterly*, vol.1, no.3, 2009, p.40; Alexander, *Building a New Command in Cyberspace*, *op.cit.*, p.7

[517] Martin C. Libicki. « Cyberwar as a Confidence Game », *Strategic Studies Quarterly*, vol. 5, no 1, 2011, p.137

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

les capacités adverses totalement inutilisables et ainsi d'empêcher des représailles sévères ou des contrecoups inattendus, ce doute pousse donc tout le monde à la retenue limitant le risque qu'une attaque vienne perturber de manière importante le cours normal de la société.

Toutefois, malgré cette imprévisibilité paralysante, les É.-U. ne se sont pas limités à espérer que l'incertitude inhérente à l'architecture complexe du cyberespace fasse son œuvre. En ce sens, l'*International Strategy for Cyberespace* de 2011 affirmait que

> lorsque cela serait justifié, les É.-U. répondraient aux actes hostiles entrepris dans le cyberespace comme nous le ferions pour toute autre menace envers notre pays. Nous nous réservons le droit d'utiliser tous les moyens nécessaires - diplomatiques, informationnels, militaire, et économique – le cas échéant [...] afin de défendre notre nation, nos alliés, nos partenaires et nos intérêts.[519]

À cet effet, les révélations d'Edward Snowden ont mis au jour des informations permettant d'avancer que la doctrine de cyberdissuasion américaine est également basée sur une importante force de frappe qui, jumelée à l'étendue de son réseau de surveillance et d'accès informatiques secrets, exploite et approfondit sérieusement le dilemme des autres États quant à la confiance qu'ils peuvent porter envers leur propre système informatique. Alors qu'un catalogue de 50 pages répertorie les techniques ou outils de piratage mis à la disposition de la NSA[520], le PPD-20 explique ce que sont les *Offensive Cyber Effects Operations* (OCEO), « soit des capacités uniques et non conventionnelles permettant de faire avancer les objectifs nationaux américains autour du monde, n'offrant peu ou pas d'avertissements à l'adversaire ou à la cible et ayant des effets potentiels allant de subtils à gravement dommageable. [...][521] ». Alors que sont développées des cybercapacités prêtes à être utilisées pour la politique étrangère des présidents américains, « le gouvernement américain doit identifier de potentielles cibles d'importance nationale

---

[519] États-Unis, White House. *International Strategy for Cyberspace*, *op.cit.*, p.14

[520] Jacob Appelbaum, Judith Horchert et Christian Stöcker. « Shopping for Spy Gear: Catalog Advertises NSA Toolbox ». *Der Spiegel*, 29 décembre 2013. En ligne, <www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html> Consulté le 26 avril 2016.

[521] États-Unis, *White House. Presidential Policy Directive 20*, *op.cit,* p.9

où les OCEO peuvent offrir un avantageux équilibre d'efficacité et de risque par rapport aux autres instruments de la puissance nationale [...][522] ».

3.2.2.3 La projection de la puissance américaine dans le cyberespace

La cyberdissuasion américaine ne se limite pas seulement à empêcher l'avènement de cyberattaques à l'encontre de cibles américaines, mais aussi à participer pleinement à la défense et au maintien de la projection de la puissance militaire des É.-U. Les capacités offensives et défensives que la NSA et le CYBERCOM ont su développer et fédérer sous sa gouverne se retrouvent désormais pleinement intégrées dans une doctrine interarmées, soit « les principes fondamentaux guidant l'utilisation des forces militaires américaines dans une action coordonnée vers un objectif commun[523] », celle-ci incluant toutes les composantes de la puissance militaire américaine. Puisque par l'entremise de sa stratégie de A2/AD, la Chine représente un défi considérable pour la supériorité et l'accès militaire américain à la région de l'Asie-Pacifique, élément central de la grande stratégie d'Obama, les forces armées américaines ont dû répondre et s'adapter à cette menace croissante.

Cette réponse fut la mise en place du *Air-Sea Battle,* doctrine voulant contrecarrer les effets recherchés par la stratégie chinoise de déni d'accès et à maintenir les capacités cruciales que sont la projection de la puissance et la domination des espaces communs[524]. D'entrée de jeu, l'objectif de cette stratégie n'est pas de permettre à coup sûr la victoire du camp américain, mais bien de démontrer aux alliés et partenaires de la région d'Asie-Pacifique que la puissance américaine, porteuse de stabilité et de prospérité, demeure présente, fonctionnelle et prête à leur éviter une possible *finlandisation*[525]. Pour Van Tol,

---

[522] *Idem.*

[523] États-Unis, Deparment of Defense. « Joint Doctrine ». Dans *DoD Dictionary of Military Terms*, s.d. En ligne, <www.dtic.mil/doctrine/dod_dictionary/data/j/5003.html >. Consulté le 15 avril 2016.

[524] Andrew F. Krepinevich. *Why AirSea Battle?*. Washington D.C. : Center for Strategic and Budgetary Assessments, 2010, p.2

[525] Jan Van Tol *et al. AirSea Battle : A Point-of-Departure Operational Concept*. Washington D.C. : Center for Strategic and Budgetary Assessments, 2010, p.9

elle vise « simplement à compenser le renforcement militaire injustifié de l'APL[526] ». C'est dans ce cadre qu'elle doit être :

> considérée comme aidant à définir les conditions au niveau des opérations militaires, afin de maintenir un équilibre militaire conventionnel stable et favorable dans la région du Pacifique occidental. Cela signifie le maintien d'une capacité pouvant dissuader la Chine d'y mener des actes d'agression ou de coercition et, si nécessaire, de pouvoir répondre à un évènement si la dissuasion devait échouer.[527]

Afin de bien comprendre le rôle éventuel du cyber dans cette doctrine, il est nécessaire de comprendre les présupposés entourant une potentielle initiative chinoise en mer de Chine, à l'encontre des É.-U. et de ses alliés. Dans ce scénario, il est attendu que l'adversaire s'attaque à la supériorité qu'ont les É.-U. dans tous les domaines (espace, cyberespace, cieux, mers et terre), qu'il lance les hostilités sans prévenir, notamment à l'encontre de troupes américaines ou alliées présentes dans la zone couverte par les capacités d'A2/AD, mais aussi envers les infrastructures de support. Outre les systèmes satellitaires, ces infrastructures incluent également celles permettant l'accès au cyberespace[528] et contre lesquelles une attaque s'avérerait problématique pour le DoD qui les utilise à des fins multiples: amasser et transmettre du renseignement, rendre possible le transport et le déplacement de personnel ou permettre le C2 lorsque vient le temps de mener des opérations militaires sur l'ensemble du spectre.[529] Pour Alexander, la présence du cyberespace au sein des domaines militaires à intégrer dans ce type de doctrine interarmées n'est donc pas fortuite, car pour les É.-U., « la liberté d'action dans le cyberespace [...] est cruciale afin d'employer efficacement ses forces dans tous les domaines. La perte de cette liberté pourrait porter grandement atteinte aux capacités que nous avons mises sur pied dans tous les autres domaines.[530] »

---

[526] *Ibid.*, p.x
[527] *Ibid.*, p.10
[528] États-Unis, Air-Sea Battle Office. *Air-Sea Battle : Service Collaboration to Address Anti-Access & Area Denial.* Washington D.C. : Air-Sea Battle Office, 2013, p.3 – 4.
[529] États-Unis, Department of Defense. *Strategy for Operating in Cyberspace, op.cit.*, p.1
[530] États-Unis, Department of Defense. *Statement of General Keith B. Alexander, Commander of United States Cyber Command Before the House Committee on Armed Service.* Washington D.C. : The White House, 2010, p.4

Distribuant l'effort exigé à l'entièreté des forces militaires impliquées, cette doctrine contient un volet visant à assurer la supériorité américaine dans le cyberespace, c'est-à-dire « le degré de domination du cyberespace par une force permettant la conduite fiable et sécuritaire de ses opérations, ainsi qu'aux forces terrestres, maritimes et spatiales y étant associées, à un moment et une sphère d'opérations donnée, et ce, sans interférences prohibitives[531] ». Cette supériorité permet d'y limiter et d'y contrecarrer les effets d'une première frappe chinoise, prérequis exigeant un appareil défensif étanche et réactif protégeant les cybercapacités offensives qui entreront dès lors en jeu. Comme l'affirme Libicki, « si l'objectif de posséder une armée est d'avoir la capacité d'exercer un pouvoir militaire, le but de la cyberdéfense est de préserver cette capacité en cas d'attaque.[532] » La première vague d'attaques terminée, celles-ci doivent donc être aptes à contre-attaquer décisivement et en profondeur afin de rendre hors service les éléments permettant le bon fonctionnement du commandement militaire chinois. Cette étape facilitera une riposte conventionnelle des forces armées américaines et de ses alliés dans la région[533]. Il s'agit alors de résister aux assauts afin de mieux répliquer, et ce, de manière décisive, mais aussi de maintenir l'efficacité de l'ensemble des outils technologiques rendant possible la puissance militaire américaine[534]. Pour ce faire,

> les forces armées américaines doivent impérativement maintenir l'intégrité de leurs réseaux afin de s'assurer qu'ils soient en mesure de fournir de manière continue et ininterrompue une connaissance situationnelle aux commandants des théâtres impliqués et de contribuer à saisir l'initiative en les alimentant d'informations opportunes sur les cibles ennemies afin de pouvoir mener des opérations offensives.[535]

---

[531] États-Unis, Department of Defense. *Joint Operational Access Concept*. Washington D.C. : Department of Defense, 2012, p.15

[532] Libicki, *Cyberwar and Cyberdeterrence*, *op.cit.*, p.161 – 162

[533] Van Tol, *op.cit.*, p.67

[534] David W. Kearn Jr. *Air-Sea Battle and China's Anti-Access and Area Denial Challenge. Orbis*, vol.58, no.1, 2013, p.136 – 137

[535] David W. Kearn Jr. *Air-Sea Battle, the Challenge of Access, and U.S. National Security Strategy*, *op.cit.*, p.38

Alors qu'elle prône l'utilisation préventive de cyberattaques pour désarmer les É.-U., la Chine se retrouve toutefois devant un important paradoxe. Alors qu'elle se targue de pouvoir exploiter les vulnérabilités inhérentes à la grande dépendance militaire américaine envers les systèmes informatiques, la Chine est progressivement en proie au même mal, conséquence de la modernisation de ses armées. En les équipant de capacités de C4ISR destinées à rendre son complexe militaire de déni d'accès plus précis, plus efficace, mais aussi plus dissuasif auprès d'adversaires potentiels[536], la Chine a toutefois exposé ses forces armées à de potentielles brèches et vulnérabilités informationnelles.

Avec la NSA, les cybercapacités américaines semblent donc avoir informatiquement leur entrée partout, incluant de nombreux réseaux chinois d'importance. Alors que le CYBERCOM y mène des missions de renseignement pouvant déboucher sur des opérations de défense active, il est possible de croire que la Chine ne soit pas réellement tentée par une cyberattaque envers les É.-U., seul ou dans la poursuite de ses objectifs stratégiques en Asie-Pacifique. Alors que la stratégie américaine d'ASB accorde une grande importance au cyberespace, que les É.-U. semblent y avoir une suprématie militaire et que les documents révélés pas Snowden ont démontré que les réseaux et ordinateurs chinois n'étaient pas à l'abri des capacités informationnelles de la NSA, il semblerait que ce que Libicki appelle la *dissuasion par manque de confiance* s'applique au cas ici traité. Alors que le CYBERCOM ne pourrait être qu'à un doigt de pouvoir semer le chaos dans l'écosystème informatique chinois, l'inaction vaut son pesant d'or, surtout lorsque l'on ignore les conséquences qu'une telle initiative pourrait avoir.

Comme le disait Thomas Schelling dans *Arms and Influence*, « c'est un paradoxe de la dissuasion qu'en menaçant de blesser quelqu'un s'il se comporte mal, il n'est pas nécessaire de distinguer à quel point elle vous nuirait aussi – *si* vous pouvez lui faire croire à cette menace.[537] »

---

[536] Pour Tellis, le but est de convaincre les forces maritimes et aériennes américaines de se tenir à distance et, idéalement, à l'extérieur de sa zone d'influence. Tellis, *Balancing Without Containment : An American Strategy For Managing China*, *op.cit.*, p.61

[537] Thomas Schelling. *Arms and Influence*. New Haven (N.J.); Londres : Yale University Press, 2008, p.36

CONCLUSION

Depuis près de dix ans, l'actualité fait la part belle aux menaces émanant du cyberespace, couvrant fréquemment les nombreux cyberincidents que rend désormais possibles et plus fréquents l'effervescence grandissante de la *société de l'information* et l'incorporation croissante des TIC dans notre quotidien. Pour plusieurs, ces cyberactivités jugées illicites et indésirables apparaissent aujourd'hui comme de véritables menaces à l'endroit de notre société et de ses individus. Les données virtuelles intangibles qu'elles mettent en danger, souvent stockées dans des endroits hors de notre portée et de notre contrôle, sont dorénavant légion, centrales à nos vies quotidiennes et paraissent hautement vulnérables devant la malveillance d'acteurs inconnus se terrant dans les profondeurs du Web. De l'*hacktivisme* du groupe Anonymous à la cybercriminalité, du cyberterrorisme qui tarde à réellement se matérialiser aux divulgations massives d'informations qui n'auraient normalement pas dû se retrouver dans l'espace public, leur grand nombre rend inévitablement difficile et confuse la compréhension des efforts menés par le gouvernement américain afin de militariser le cyberespace. Si ces initiatives américaines peuvent sembler être dirigées envers ces diverses sources d'incidents, ces dernières, sans être bénignes, demeurent toutefois loin d'être la cybermenace nécessitant le plus d'être contrée militairement.

Afin de bien comprendre l'objectif de cette initiative, surprenante parce qu'elle mettait fin à près de deux décennies d'un profond désengagement gouvernemental et présidentiel, un éclaircissement était nécessaire et pertinent afin de bien faire ressortir ce qui constituait la principale menace justifiant une entreprise militaire d'une telle ampleur dans le cyberespace. À la lumière de l'analyse faite dans ce mémoire, il est désormais possible de répondre adéquatement aux questions de recherche formulées en début de travail, c'est-à-dire de découvrir les raisons ayant incité l'administration Obama à militariser le cyberespace, notamment par l'entremise du USCYBERCOM, à déceler la grande stratégie guidant l'utilisation des cybercapacités américaine, à mettre le doigt sur l'origine

de la menace ayant mené à ce chamboulement organisationnel et, finalement, à définir la nature, la forme et les usages de la réponse américaine à cette menace.

Comme le stipule l'hypothèse de ce travail, l'institutionnalisation de la militarisation du cyberespace, rapidement initiée par l'administration Obama, doit être observée comme une partie intégrante de la grande stratégie du *pivot vers l'Asie*. Celle-ci, Obama en premier lieu, considère que pour défendre leurs intérêts vitaux à long terme, les É.-U. doivent se positionner favorablement dans la région de l'Asie-Pacifique, une région souvent considérée comme le futur point névralgique de la géopolitique mondiale, et agir de sorte à y maintenir la stabilité et un climat de paix relativement fragile. Prenant la relève de la présidence de G.W. Bush, où plusieurs années de guerre et une crise économique ont laissé en héritage un imposant fardeau fiscal, Obama s'est vu contraint de rompre avec les grandes stratégies de ses prédécesseurs, autant la *primauté*, où la grandeur des É.-U. leur permettait de dicter par la force des règles du jeu les avantageant, que celle de *sécurité coopérative*, où l'amélioration de la sécurité américaine passait par un processus multilatéral de pacification du monde.

La situation américaine actuelle ne permettant pas de telles ambitions maximalistes, il a opté pour l'*engagement sélectif*, une stratégie plus modeste permettant toutefois d'éviter le piège de la surextension stratégique, symptôme souvent précurseur de la chute des empires voulant militairement s'impliquer partout. Afin d'éviter de perdre brusquement leur statut de superpuissance acquis au lendemain de la Seconde Guerre mondiale, les É.-U. ont donc dû réduire considérablement la liste de leurs intérêts nationaux considérés comme vitaux afin de consacrer les ressources se faisant rares aux objectifs stratégiques primordiaux.

Pour Robert G. Kaufman, Barack Obama a accepté avec grâce le déclin de la puissance américaine[538] et c'est avec cette relative sérénité qu'il a amorcé un retranchement des É.-U. du système international : il a rapidement mis fin aux conflits irakiens et afghans, réduit la quantité des troupes disponibles dans les différents corps militaires et considérablement dégraissé le budget du Pentagone, aidé par un Congrès fiscalement conservateur. Cette réduction des moyens militaires disponibles à l'accomplissement des objectifs américains de politique étrangère ne change finalement pas grand-chose alors que la liste des intérêts à défendre s'est dégarnie elle aussi. Parmi les incontournables, la Chine, dont l'importante puissance économique s'accompagnant d'une rapide militarisation dirigée vers la mer de Chine, témoigne d'une ambition inquiétant, à tort ou à raison, plusieurs de ses voisins immédiats, incluant des alliés américains comme le Japon ou la Corée du Sud. Puisque pour les É.-U., les enjeux prenant place dans cette région sont grands, il est donc nécessaire 1) d'y préserver la paix afin de ne pas être impliqué dans une guerre potentiellement très prenante et 2) d'y maintenir une stabilité lui permettant de profiter au maximum du potentiel économique de cette région où vivent 4 milliards de personnes, soit 60% de la population mondiale, un nombre qui devrait atteindre les 6 milliards en 2050[539]. C'est justement à cet effet que de nombreux liens diplomatiques et économiques régionaux ont été tissés ou renforcés sous Obama.

Ce retranchement mènera à un effort de réaffectation des ressources qui touchera directement le cyberespace et son éventuelle militarisation. Si la Chine est physiquement éloignée du territoire américain, ce n'est pas le cas dans le cyberespace, un espace « permettant d'équilibrer la balance entre une force largement supérieure et toutes les autres nations[540] », où elle saura se présenter comme une menace, autant par les capacités qu'elle démontre que les intentions militaires offensives dont elle semble caresser

---

[538] Robert G. Kaufman. « Prudence and the Obama Doctrine ». *Orbis*, vol.58, no.3, 2014, p.446

[539] Silvany Pasaribu. « Asia-Pacific Population Growth and the UN Post-2015 Development Agenda ». *The Diplomat*, 18 juin 2015. En ligne, <thediplomat.com/2015/06/asia-pacific-population-growth-and-the-un-post-2015-development-agenda/>. Consulté le 27 avril 2016.

[540] Jeffrey Carr, cité dans Mac Slocum. « Cyber warfare: don't inflate it, don't underestimate it ». *Radar*, 11 février 2010. En ligne, <radar.oreilly.com/2010/02/cyber-warfare-dont-inflate-it.html>. Consulté le 27 avril 2016.

l'utilisation dans l'éventualité d'un conflit avec les É.-U. La Chine n'est donc désormais plus si éloignée. Avec l'arrivée d'Obama, de plus en plus d'opérations d'espionnage cybernétique soupçonnées d'être d'origine chinoise sont répertoriées au sein des serveurs et réseaux américains. En plus d'effectuer de l'espionnage politique, opérations considérées normales et légitimes au sein du *jeu* que sont les relations internationales, ces cyberintrusions chinoises dilapident toutefois également la propriété intellectuelle d'entreprises américaines oeuvrant principalement dans le secteur des hautes technologies et de la défense.

Alors que les É.-U. sortent d'une crise économique aux fortes conséquences sur leur puissance militaire, ce que le général Alexander qualifiait à l'époque du « plus grand transfert de richesses de l'histoire de l'humanité » inquiète et semble prendre au dépourvu les É.-U. De plus, des recherches démontrent également que les forces armées chinoises pourrait lancer des cyberattaques surprises dès les premiers mouvements d'un conflit, attaques visant à aveugler et à rendre impotente une puissance militaire américaine dont l'efficacité dépend presque entièrement de l'utilisation des TIC et donc, conséquemment, du cyberespace. Pour Joel Brenner, cette situation n'est pas surprenante considérant que le cyberespace national américain est pour lui une véritable maison de verre[541] : malgré l'impression de sécurité qu'elle offre, sa transparence permet dans ce cas-ci l'espionnage et la surveillance, tandis qu'une seule roche, une seule cyberattaque, suffirait pour la briser en mille morceaux.

Devant une telle menace, la réponse américaine se fera en vertu du principe de l'*équilibre de la menace*. Les É.-U. n'ayant rien à prouver à personne sur la scène internationale, cette réplique se concentrera à contrecarrer et à défaire cette cybermenace planant depuis plusieurs années. Grâce à une NSA qui saura devenir, de manière autonome, le centre cyber par excellence du gouvernement américain et à quelques personnes dévouées et bien placées dans l'appareil bureaucratique, le USCYBERCOM verra le jour et permettra d'inverser le fardeau de la menace et de la faire peser sur la Chine. Ce faisant, cette

[541] Joel Brenner. *America the Vulnerable*, *op.cit.*

dernière devra dorénavant réévaluer les chances de succès de ses cyberopérations d'espionnage et de potentielles attaques militaires, mais devra aussi composer avec l'irritant psychologique qu'est la pénétration étendue et importante de la NSA dans ses propres réseaux. Ainsi, d'une menace chinoise envahissante, dilapidant la richesse économique des É.-U. et ayant longuement réfléchi aux possibilités de lancer des cyberattaques surprises dans les phases initiales d'un conflit, la Chine devient celle qui est pénétrée de toutes parts par la NSA. Elle met à son tour en place des mesures politiques afin de renforcer le contrôle étatique sur la cybersécurité du pays[542] et un commandement militaire responsable de l'espace et du cyberespace[543]. Dans ces initiatives, il est possible de déceler une réaction chinoise à ce qui était en soi une réaction des É.-U. Ce travail de recherche, très concentré sur la dynamique se déroulant dans le cyberespace entre les deux pays, et ce, dans une période donnée, n'a pas réellement pu se projeter dans un avenir pourtant proche.

Ce que nous pouvons voir, c'est une Chine émergente qui oriente son développement militaire sur les avantages asymétriques exploitant les vulnérabilités américaines, mais qui tente également d'atteindre une situation de parité stratégique avec les É.-U., notamment dans le domaine des munitions à guidage de précision[544]. Cette situation pourrait causer, à l'instar de la parité nucléaire durant la guerre froide, l'affaiblissement de la dynamique de dissuasion permettant d'assurer la sécurité des É.-U., mais aussi celle de ses alliés. En 2014, afin de préserver cet avantage stratégique et ses bienfaits, Chuck Hagel, alors secrétaire à la Défense, lançait la *troisième stratégie de contournement* (*third*

---

[542] Austin Ramzy. « What You Need to Know About China's Draft Cybersecurity Law ». *The New York Times*, 9 juillet 2015. En ligne, <sinosphere.blogs.nytimes.com/2015/07/09/what-you-need-to-know-about-chinas-draft-cybersecurity-law/>. Consulté le 27 avril 2016.

[543] The Economist. « Xi's new model army ». *The Economist*, 16 janvier 2016. En ligne, <www.economist.com/news/china/21688424-xi-jinping-reforms-chinas-armed-forcesto-his-own-advantage-xis-new-model-army>. Consulté le 28 avril 2016.

[544] Shawn Brimley. « Offset Strategies & Warfighting Regimes ». *War on the Rocks*, 15 octobre 2014. En ligne, <warontherocks.com/2014/10/offset-strategies-warfighting-regimes/>. Consulté le 15 février 2016.

offset)[545], impliquant « l'utilisation d'une technologie supérieure afin de contrer les avantages de l'adversaire, qu'ils soient quantitatifs, géographiques, ou une volonté à subir des pertes [...][546] ». Alors que l'on parle de plus en plus de l'utilisation militaire de nouvelles technologies avancées comme la robotisation, les systèmes autonomes, la miniaturisation, l'utilisation du *big data* ou de l'impression 3D, « le DoD réunira ces ensembles dans des constructions opérationnelles et organisationnelles novatrices afin d'assurer la liberté d'accès pour les forces américaines dans un environnement contesté par le A2/AD.[547] » Ce sont là des technologies utilisant intensément les capacités du cyberespace et nécessitant donc qu'on le protège davantage, au rythme où ces technologies révolutionnaires seront introduites sur le champ de bataille. Visiblement, ce qui se voulait être au départ un rééquilibrage interne américain visant une dynamique de cyberdissuasion semble se transformer en une course aux armements en bonne et due forme. Pour Jervis, si le concept de dissuasion « fournissait une compréhension du monde tel que vu par les décideurs et une explication de leurs actions spécifiques », celle de la course aux armements « fournit plutôt une explication sur la dynamique de leur interaction.[548] »

En conclusion, voici les mots de Robert S. McNamara, ayant déjà campé ce rôle de décideur, décrivant mieux que quiconque cette dynamique qui, à l'époque, imprégnait la problématique nucléaire:

> Quelles que soient leurs intentions – quelles que soient nos intentions, actions - ou même nos actions potentielles possibles – relativement à l'accumulation de forces nucléaires, qu'elles soient offensives ou défensives, elles vont nécessairement déclencher des réactions de l'autre côté. C'est précisément ce phénomène d'action-réaction qui alimente une course aux armements.[549]

---

[545] Robert Haddick. « Preserving U.S. Military Might: How to Make the Third Offset Strategy a Success ». *The Nation*, 7 décembre 2014. En ligne, <nationalinterest.org/feature/preserving-us-military-might-how-make-the-third-offset-11800>. Consulté le 26 avril 2016.

[546] Ashton B. Carter. « Keeping America's Military Edge ». *Foreign Affairs,* vol.80, no.1, p.99

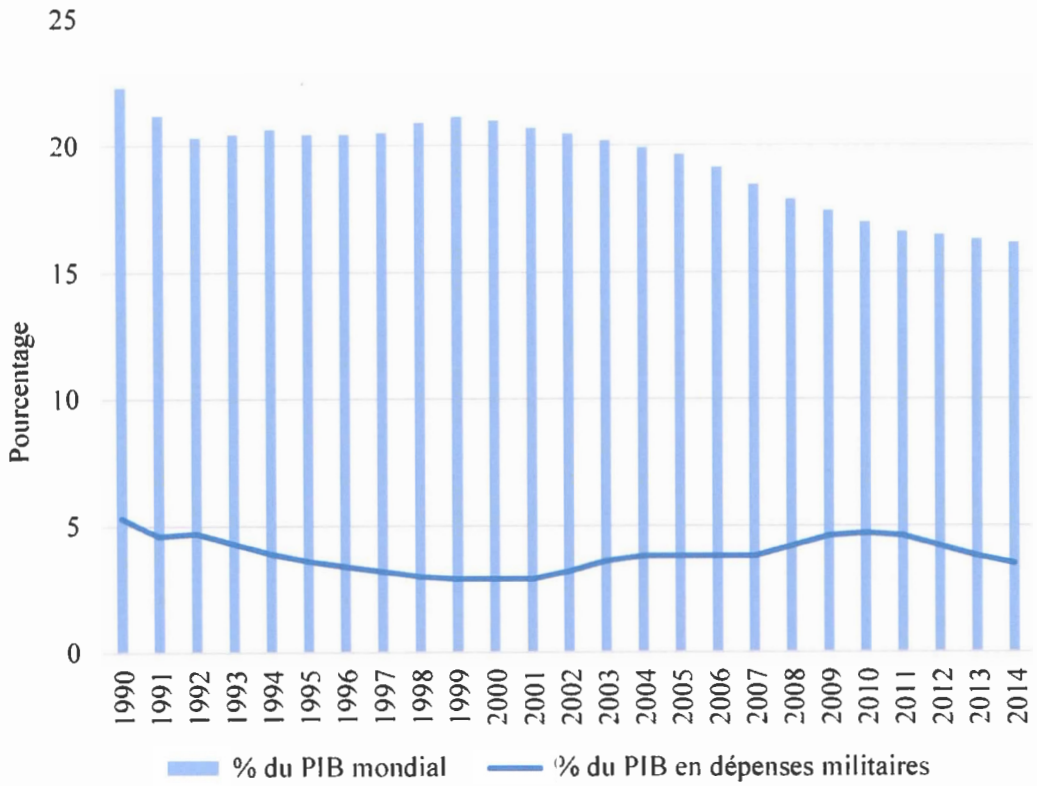
[547] États-Unis, Department of Defense. *Asia-Pacific : Maritime Security Strategy*. Washington D.C. : Department of Defense, 2015, p.22 35 p.

[548] Jervis, Deterrence, the Spiral Model and the Intentions of the Adversary, *op.cit.*, p.81

[549] États-Unis, Department of Defense. *Remarks by Secretary of Defense Robert McNamara, September 1967*. Washington D.C. : Department of Defense, 1967, p.28

ANNEXE A

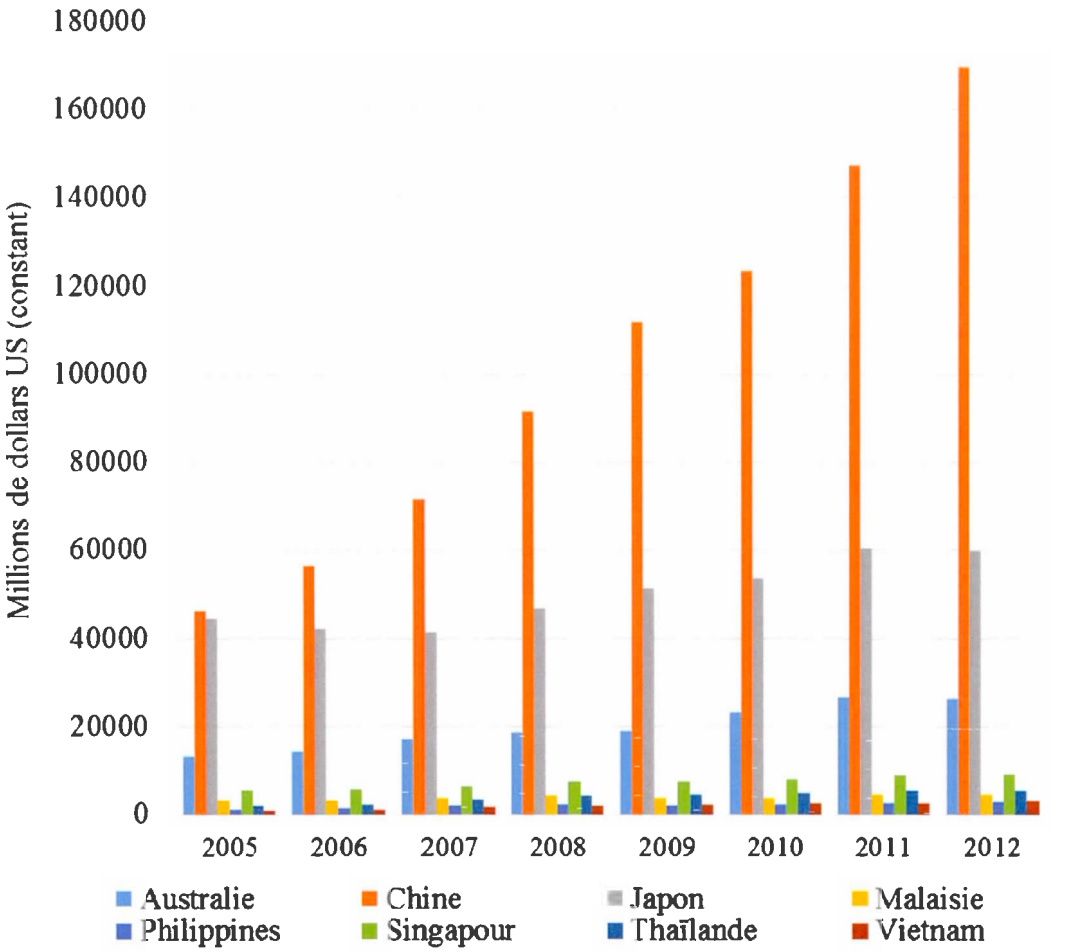
PROPORTION AMÉRICAINE DU PIB MONDIAL ET SES DÉPENSES MILITAIRES



Source : Quandl Economic and Financial Data/Stockholm International Peace Research Institute

ANNEXE B

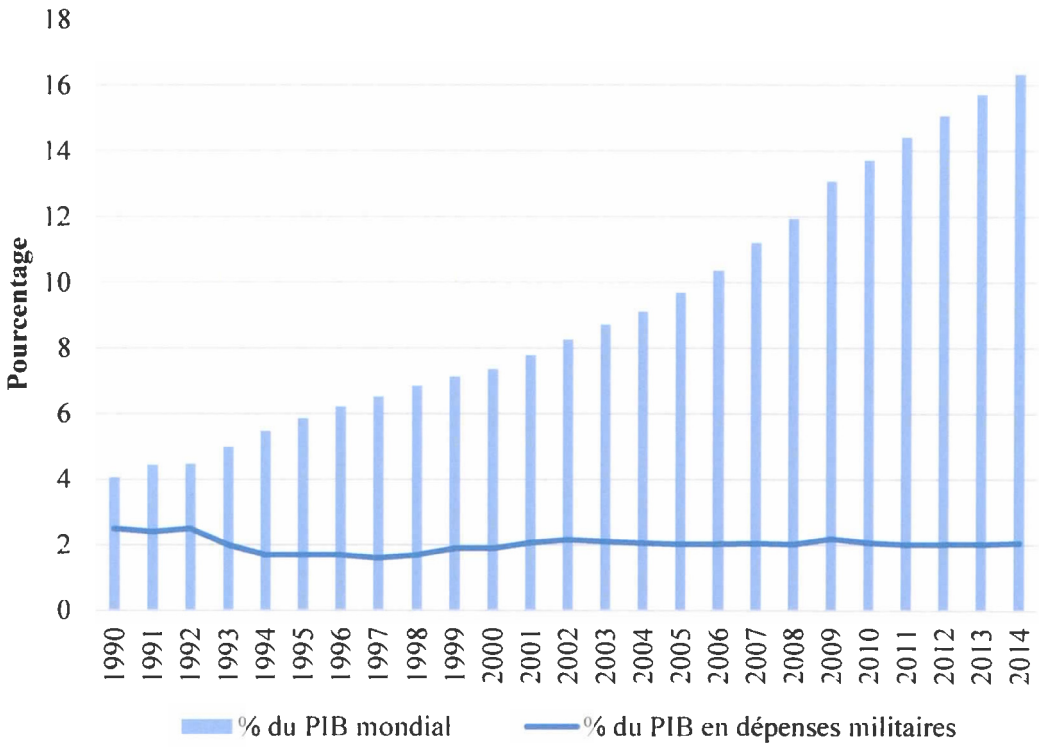
BUDGETS MILITAIRES DE QUELQUES PAYS DE LA RÉGION D'ASIE-PACIFIQUE ENTRE 2005 ET 2012.



Source : Stockholm International Peace Research Institute. *SIPRI Military Expenditure Database 2015*

ANNEXE C

PROPORTION CHINOISE DU PIB MONDIAL ET SES DÉPENSES MILITAIRES



Source : Quandl Economic and Financial Data/Stockholm International Peace Research Institute

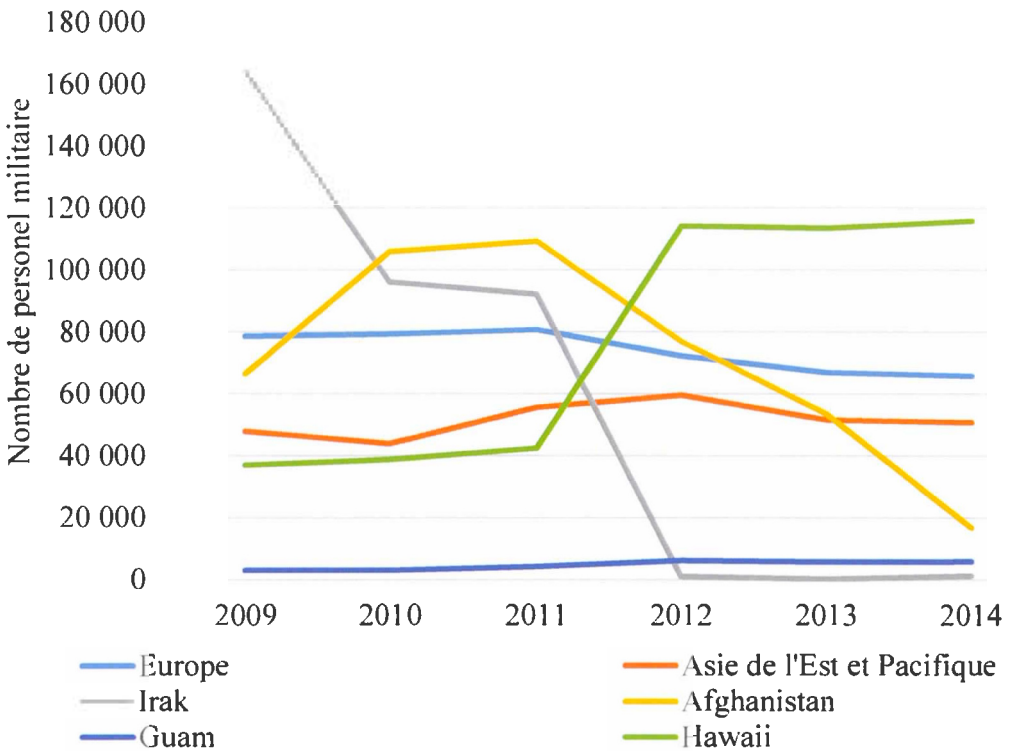
ANNEXE D

LES PRINCIPAUX POINTS DE LITIGES TERRITORIAUX ET OCÉANIQUES EN MER DE CHINE DU SUD

Source : Council on Foreign Relations, *CFR Backgrounders. South China Sea Tensions*. En ligne, <www.cfr.org/china/south-china-sea-tensions/p29790>. Consulté le 8 novembre 2015.

ANNEXE E

TRANSFERT DES FORCES ARMÉES AMÉRICAINES DÉPLOYÉES DANS QUELQUES THÉÂTRES RÉGIONAUX ET DANS LES BASES DE GUAM ET D'HAWAII ENTRE 2009 ET 2014



Source : États-Unis, Department of Defense. *Defense Manpower Data Center. DoD Personnel, Workforce Reports & Publications 2009 – 2014*. En ligne, <www.dmdc.osd.mil/appj/dwp/dwp_reports.jsp>. Consulté le 18 novembre 2015.

ANNEXE F

L'ÉTENDUE GÉOGRAPHIQUE DU CYBERESPIONNAGE CHINOIS EN SOL AMÉRICAIN

Source : Robert Windrem. « Exclusive: Secret NSA Map Shows China Cyber Attacks on U.S. Targets ». *NBC News*, 30 juillet 2015. En ligne, <www.nbcnews.com/news/us-news/exclusive-secret-nsa-map-shows-china-cyber-attacks-us-targets-n401211>. Consulté le 2 avril 2016.

ANNEXE G

LES DEUX CHAÎNES D'ÎLES

Source : États-Unis, Office of the Secretary of Defense. *Military and Security Developments Involving the People's Republic of China 2010*, Washington D.C.: Department of Defense, 2010, p.23.

ANNEXE H

LE « COLLIER DE PERLES » CHINOIS

Source : Philippe Raggi. « Le réveil de l'Asie au sein d'un monde multipolaire ». *Mécanoblog*, 23 mai 2010. En ligne, <mecanoblog.wordpress.com/2010/05/23/le-reveil-de-lasie-au-sein-dun-monde-multipolaire/>. Consulté le 15 février 2016.

BIBLIOGRAPHIE

« Excerpts From Pentagon's Plan: 'Prevent the Re-Emergence of a New Rival' », *The New York Times*, 8 mars 1992. En ligne, <www.nytimes.com/1992/03/08/world/excerpts-from-pentagon-s-plan-prevent-the-re-emergence-of-a-new-rival.html?pagewanted=all>. Consulté le 3 octobre 2015.

« Significant Cyberattack Incidents : Moonlight Maze, 1998-1999 ». *RealClearPolitics.com*, 26 février 2013. En ligne, <www.realclearpolitics.com/lists/cyber_attacks/moonlight_maze.html>. Consulté le 14 décembre 2015.

Adams, James. « Testimony of James Adams, Chief Executive Officer Infrastructure Defense, Inc. ». Audition devant le *Committee on Governmental Affairs* du 106e Congrès du Sénat américain, 2 mars 2000. En ligne, <fas.org/irp/congress/2000_hr/030200_adams.htm>. Consulté le 14 décembre 2015.

Agence France-Presse. « Experts: Drone market to hit $10 billion by 2024 ». *DefenseNews*, 3 octobre 2015. En ligne, <www.defensenews.com/story/defense/air-space/2015/10/03/experts-drone-market-hit-10-billion-2024/73282590/>. Consulté le 19 janvier 2016.

Aid, Matthew M. « Inside the NSA's Ultra-Secret China Hacking Group ». *Foreign Policy*, 10 juin 2013. En ligne, <foreignpolicy.com/2013/06/10/inside-the-nsas-ultra-secret-china-hacking-group/> Consulté le 17 mars 2016.

Aid, Matthew M. « Prometheus Embattled : A Post-9/11 Report Card on the National Security Agency », pp.41 – 73. Dans Loch K. Johnson (ed.). *Strategic Intelligence vol.2 - The Intelligence Cycle : The Flow of Secret Information from Overseas to the Highest Councils of Gouvernment*. Westport (CT) : Praeger Security International, 2007.

Aid, Matthew M. *The Secret Sentry : The Untold History of the National Security Agency*. New York : Bloomsbury Press, 2009, 432 p.

Alexander, Gen. Keith B. « Building a New Command in Cyberspace », *Strategic Studies Quarterly*, vol.5, no.2, 2011, pp.3 – 12.

Alexander, Gen. Keith B. « Warfighting in Cyberspace ». *Joint Forces Quarterly*, no.47, 2007, pp. 58 – 61.

Anderlini, Jamil et al. « Industrial espionage: Data out of the door », *Financial Times*, 1er février 2011. En ligne, <www.ft.com/cms/s/0/ba6c82c0-2e44-11e0-8733-00144feabdc0.html>. Consulté le 2 janvier 2016.

Andrews, Wilson et Todd Lindeman. « The Black Budget ». *The Washington Post*, 29 août 2013. En ligne, <www.washingtonpost.com/wp-srv/special/national/black-budget/>. Consulté le 2 février 2016.

Appelbaum, Jacob et al. « The Digital Arms Race: NSA Preps America for Future Battle ». *The Spiegel Online International*, 17 janvier 2015. En ligne, <www.spiegel.de/international/world/new-snowden-docs-indicate-scope-of-nsa-preparations-for-cyber-battle-a-1013409.html>. Consulté le 2 avril 2016.

Appelbaum, Jacob, Judith Horchert et Christian Stöcker. « Shopping for Spy Gear: Catalog Advertises NSA Toolbox ». *Der Spiegel*, 29 décembre 2013. En ligne, <www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html> Consulté le 26 avril 2016.

Arpagian, Nicolas. « Les entreprises: complices et victimes de la cyberguerre », *Revue internationale et stratégique*, vol.3, no.87, 2013, pp.65 – 72.

Art, Robert J. « Geopolitics Updated : The Strategy of Selective Engagement », *International Security*, vol.23, no.3, 1998, pp.79 – 113.

Art, Robert J. « Selective Engagement After Bush ». Dans Michèle Flournoy et Shawn Brimley (eds.). *Finding our Way : Debating American Grand Strategy*, Washington D.C : Center for a New American Century, Solarium Strategy Series, 2008, pp.23 – 41.

Ball, Desmond. « China's Cyber Warfare Capabilities », *Security Challenges*, vol.7, no.2, 2011, pp.81 – 103.

Bamford, James. *The Shadow Factory : The Ultra-Secret NSA from 9/11 to the Eavesdropping on America*. New York : Doubleday, 2008, 395 p.

Barrett Jr., Barrington. « Information Warfare: China's Response to U.S. Technological Advantages », *International Journal of Intelligence and Counterintelligence*, vol.18, no.4, 2005, pp.682 – 706.

BBC. « Taiwan Flashpoint – US Role », *BBC News*, s.d. En ligne, <news.bbc.co.uk/2/shared/spl/hi/asia_pac/04/taiwan_flashpoint/html/us_role.stm>. Consulté le 10 février 2016.

Beitelman, David A. « America's Pacific Pivot », *International Journal*, v.67, no.4, 2012, pp.1073 – 1094.

Betz, David. « Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed », *Journal of Strategic Studies*, vol.35, no.5, 2012, pp.689 – 711.

Boehler, Patrick et Gerry Doyle. « Use by Iraqi Military May Be a Boon for China-Made Drones ». *The New York Times*, 17 décembre 2015. En ligne, <www.nytimes.com/2015/12/18/business/international/china-drone-export-iraq.html>. Consulté le 15 janvier 2016.

Borger, Julian. « Pentagon kept the lid on cyberwar in Kosovo ». *The Guardian*, 9 novembre 1999. En ligne, <www.theguardian.com/world/1999/nov/09/balkans>. Consulté le 2 avril 2016.

Bosco, David. « Course Corrections : The Obama Administration at the United Nations », *The Hague Journal of Diplomacy*, vol.6, 2011, pp.335 – 349.

Brenner. Joel. *American the Vulnerable : Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. New York : Penguin Press, 2011, 320 p.

Brickey, Jon, Jacob Cox, John Nelson et Gregory Conti. « The Case for Cyber », *Small Wars Journal*, 2012. En ligne, <smallwarsjournal.com/jrnl/art/the-case-for-cyber>. Consulté le 25 novembre 2015.

Brimley, Shawn. « Offset Strategies & Warfighting Regimes ». *War on the Rocks*, 15 octobre 2014. En ligne, <warontherocks.com/2014/10/offset-strategies-warfighting-regimes/>. Consulté le 15 février 2016.

Brito, Jerry et Tate Watkins. 2011. « Loving the Cyber Bomb: The Dangers of Threat Inflation in Cybersecurity Policy », *Harvard National Security Journal*, vol.3, no.1, 2011, pp.39 – 84.

Brooks, Stephen G. « Dueling Realism ». *International Organization*, vol.51, no.3, 1997, pp.445 – 477.

Brooks, Stephen G. et William C. Wohlforth. « American Primacy in Perspective », *Foreign Affairs*, vol.81, no.4, 2002, pp.20 – 33.

Brooks, Stephen G., G. John Ikenberry et William C. Wohlforth, « Don't Come Home, America : The Case Against Retrenchment », *International Security*, vol.37, no.3, 2012, pp.7 – 51.

Burton, Charles. « China's Post-Mao Transition: The Role of the Party and Ideology in the *New Period* ». *Pacific Affairs*, vol.60, no.3, 1987, pp.431 – 446.

Buzan, Barry. *Peoples, States & Fear*, Colchester (UK): ECPR Press, 2007, 311 p.

Carr, Jeffrey. *Inside Cyber Warfare : Mapping the Cyber Underworld*. Sebastopol, CA : O'Reilly Media, 2012, 318 p.

Carter, Ashton B. « Keeping America's Military Edge ». *Foreign Affairs,* vol.80, no.1, pp.90 – 105.

Carter, Ashton B., William James Perry et John D. Steinbrunner. *A New Concept of Cooperative Security*. Washington D.C. : Brookings Institution, 1992, 65 p.

Central Intelligence Agency. « Economy », *The World Factbook*, 5 janvier 2016. En ligne, <www.cia.gov/library/publications/the-world-factbook/geos/us.html>. Consulté le 15 janvier 2016

Chang, Amy. *Warring States : China's Cybersecurity Strategy*. Washington D.C. : Center for a New American Century, 2014, 38 p.

Chertoff, Michael, William Lynn et Mike McConnell. « China's Cyber Thievery Is National Policy—And Must Be Challenged », *The Wall Street Journal*, 27 janvier 2012. En ligne, <www.wsj.com/articles/SB10001424052970203718504577178832338032176>. Consulté le 4 janvier 2016.

Chilton, Kevin et Greg Weaver, 'Waging Deterrence in the Twenty-First Century', *Strategic Studies Quarterly*, vol.1, no.3, 2009, pp.31 – 42

Cisco. « The Internet of Things ». *Cisco Visualisation*. s.d. En ligne, <share.cisco.com/internet-of-things.html>. Consulté le 7 janvier 2016.

Clarke, Richard A. et Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It*, New York: Harper Collins, 2010, 290 p.

Clérot, Fabienne et Victoire Mayor. « Jeu de go dans le cyberespace », *Revue internationale et stratégique*, vol.87, no.3, 2012, pp.111 – 119.

Clinton, Hillary. « America's Pacific Century », *Foreign Policy*, no.189, 2011, pp.56 – 63.

CNN. « Ron Paul : I'm no isolationist ». *The Situation Room*, 15 décembre 2011. Vidéo en ligne, <www.youtube.com/watch?v=UNOMmUQYlC4>

Cohen, Ariel. « The Dragon Looks West: China and the Shanghai Cooperation Organization », *Heritage Lectures*, no.961, 2006, 8 p.

Cohen, Michael A. « The Non-Return of American Isolationism ». *The Atlantic*, 24 juillet 2011. En ligne, <www.theatlantic.com/international/archive/2011/07/the-non-return-of-american-isolationism/241927/>. Consulté le 28 septembre 2015.

Cohen, Michael A. « The World According to Ron Paul », *Foreign Policy*, 23 décembre 2011. En ligne, <foreignpolicy.com/2011/12/23/the-world-according-to-ron-paul/>. Consulté le 28 septembre 2015.

Coleman, David G. *U.S. Military Personnel 1954-2014*. En ligne, <historyinpieces.com/research/us-military-personnel-1954-2014>. Consulté le 12 novembre 2015.

Council on Foreign Relations. « Russian and Chinese Assertiveness Poses New Foreign Policy Challenges : A Conversation With Robert M. Gates », *CFR Event*, 21 mai 2014. En ligne, <www.cfr.org/defense-and-security/russian-chinese-assertiveness-poses-new-foreign-policy-challenges/p35645>. Consulté le 11 janvier 2016.

Courmont, Barthélémy. *La tentation de l'Orient : une nouvelle politique américaine en Asie-Pacifique*. Québec : Septentrion, 2010, 507 p.

Cozad, Mark. « China's Regional Power Projection Prospects for Future Missions in the South and East China Seas ». Dans Roy Kamphausen (ed.), David Lai et Andrew Scobell. *Beyond the Strait: PLA Missions Other Than Taiwan*. Carlisle, PA : Strategic Studies Institute, 2009, pp.287 – 335.

Crosston, Matthew D. « Virtual Patriots and a New American Cyber Strategy : Changing the Zero-Sum Game ». *Strategic Studies Quarterly*, vol.6, no.4, 2012, pp.100 – 118.

Crosston, Matthew D. « World Gone Cyber MAD – How "Mutually Assured Debilitation" Is the Best Hope for Cyber Deterrence ». *Strategic Studies Quarterly*, vol.5, no.1, 2011, pp.100 – 116.

David, Charles-Philippe. *Au sein de la Maison-Blanche : de Truman à Obama, la formulation (imprévisible) de la politique étrangère des États-Unis*. Québec : Presses de l'Université Laval, 3e édition, 2015, 1180 p.

David, Charles-Philippe. *La guerre et la paix – Approches et enjeux de la sécurité et de la stratégie*, Paris : Presses de Sciences Po, 3e édition, 2013, 554 p.

Deibert, Ronald J. *Black Code: Inside the Battle for Cyberspace*, Toronto: McClelland & Stewart, 2013, 312 p.

Deibert, Ronald, Arnav Manchanda, Rafal Rohozinski, Nart Villeneuve et Greg Walton. *Tracking Ghostnet : Investigating a Cyber Espionage Network*. 2009, 52 p. PDF en ligne, <www.f-secure.com/weblog/archives/ghostnet.pdf>. Consulté le 30 août 2015.

Demchak, Chris et Peter Dombrowski. 2011. « Rise of a Cybered Westphalian Age », *Strategic Studies Quarterly*, vol.5, no.1, pp.32 – 61.

Derene, Glenn. « The Coming Cyberwar: Inside the Pentagon's Plan to Fight Back » *Popular Mechanics*, 1er octobre 2009. En ligne. <www.popularmechanics.com/technology/military/4277463>. Page consultée le 11 décembre 2013

Desrosier, Marie-Ève et Justin Massie. « Le néolibéralisme et la synthèse néo-néo ». Dans Alex Macleod et Dan O'Meara (dir.). *Théorie des relations internationales : contestation et résistance*, Montréal : Athéna Éditions, 2007, pp.153 – 173.

Douhet, Giulio. *The Command of the Air*. Washington D.C. : Air Force History and Museums Program, 1998, 394 p.

Douzet, Frédérick et Justin Vaïsse. « Obama, le président du pivot », *Hérodote*, vol.149, no.2, 2013, pp.7 – 21.

Dueck, Colin. *The Obama Doctrine : American Grand Strategy Today*. Oxford (R.-U.); New York : Oxford University Press, 2015, 336 p.

Ehrhard, Thomas P. et Robert O. Work, *Range, Persistence, Stealth, and Networking: The Case for a Carrier-Based Unmanned Combat System.* Washington, D.C.: Center for Strategic and Budgetary Assessments (CSBA), 2008, 248 p.

Ehrlich, Richard S. « China flexes its muscles in U.S.-led military exercises », *The Washington Times.* 12 février 2014. En ligne, <www.washingtontimes.com/news/2014/feb/12/china-flexes-its-muscles-in-us-led-military-exerci/>. Consulté le 8 novembre 2015.

Elliott, Michael. « Viewpoint: How Libya Became a French and British War », *Time.com*, 19 mars 2011. En ligne, <content.time.com/time/world/article/0,8599,2060412,00.html>. Consulté le 20 septembre 2015

Erickson, Andrew S., Lyle J. Goldstein et William S. Murray. *Chinese Mine Warfare – A PLA Navy 'Assassin's Mace' Capability.* Newport (RI) : China Maritime Studies Institute, U.S. Naval War College, 2009, 93 p.

Eriksson, Johan et Giampiero Giacomello. « The Information Revolution, Security and International Relations: (IR)relevant Theory? », *International Political Science Review*, vol. 27, no.3, 2006, pp.221 – 244.

États-Unis, 24th Air Force Office of History. *History of HQ Twenty-Fourth Air Force and 624th Operations Center*, 2014. En ligne, <www.24af.af.mil/shared/media/document/AFD-140429-035.pdf>. Consulté le 4 avril 2016.

États-Unis, Air Force Space Command. « Schriever Wargame 2010 », *High Frontier : The Journal for Space and Cyberspace Professional*, vol.7, no.1, 2010, 54 p.

États-Unis, Air-Sea Battle Office. *Air-Sea Battle : Service Collaboration to Address Anti-Access & Area Denial*. Washington D.C. : Air-Sea Battle Office, 2013, 13 p.

États-Unis, Defense Science Board. *Task Force Report : The Role of Autonomy in DoD Systems*. Washington D.C. : Department of Defense, 115 p. PDF en ligne, <www.acq.osd.mil/dsb/reports/AutonomyReport.pdf>. Consulté le 8 janvier 2016.

États-Unis, Deparment of Defense. « Doctrine ». Dans *DoD Dictionary of Military Terms*, s.d. En ligne, <www.dtic.mil/doctrine/dod_dictionary/data/d/3840.html>. Consulté le 15 avril 2016.

États-Unis, Deparment of Defense. « Joint Doctrine ». Dans *DoD Dictionary of Military Terms*, s.d. En ligne, <www.dtic.mil/doctrine/dod_dictionary/data/j/5003.html >. Consulté le 15 avril 2016.

États-Unis, Department of Air Force. *Cornerstones of Information Warfare*. Washington D.C. : Department of Air Force, 1995. En ligne, <www.csse.monash.edu.au/courseware/cse468/2006/cornerstones-iw.html>. Consulté le 15 février 2016.

États-Unis, Department of Defense. « Department of Defense Dictionary of Military and Associated Terms ». Washington D.C. : Department of Defense, 2010 (mise à jour 2016), p.40. En ligne, <www.dtic.mil/doctrine/new_pubs/jp1_02.pdf>. Consulté le 29 mars 2016.

États-Unis, Department of Defense. *Asia-Pacific : Maritime Security Strategy*. Washington D.C. : Department of Defense, 2015, 35 p.

États-Unis, Department of Defense. *Defense Planning Guidance, FY 1994-1999*. Washington D.C. : Department of Defense, 1992. PDF en ligne, <www.archives.gov/declassification/iscap/pdf/2008-003-doc18.pdf>. Consulté le 3 octobre 2015.

États-Unis, Department of Defense. *Deputy Secretary of Defense Speech - Remarks at Stratcom Cyber Symposium*. Washington D.C. : Department of Defense, 26 mai 2010. En ligne, <archive.defense.gov/speeches/speech.aspx?speechid=1477>. Consulté le 25 avril 2016.

États-Unis, Department of Defense. *Deterrence Operations - Joint Operating Concept*. Washington D.C. : Department of Defense, 2006, 76 p.

États-Unis, Department of Defense. *Directive Number 5105.19*. Washington D.C. : Department of Defense, 2006, 18 p.

États-Unis, Department of Defense. *DoD Releases Report on Estimated Sequestration Impacts.* Washington, D.C. : Department of Defense, 2014. En ligne, <www.defense.gov/news/newsarticle.aspx?id=122065>. Consulté le 29 juillet 2015.

États-Unis, Department of Defense. *Joint Operational Access Concept*. Washington D.C. : Department of Defense, 2012, 64 p.

États-Unis, Department of Defense. *Quadrennial Defense Review 2010*. Washington D.C. : Department of Defense, 2010, 105 p.

États-Unis, Department of Defense. *Quadrennial Defense Review Report 2006*. Washington D.C. : Deparment of Defense, 2006, 92 p.

États-Unis, Department of Defense. *Remarks by Secretary of Defense Robert McNamara, September 1967*. Washington D.C. : Department of Defense, 1967.

États-Unis, Department of Defense. *Remarks by Secretary of Defense Robert McNamara, September 1967*. Washington D.C. : Department of Defense, 1967, p.28

États-Unis, Department of Defense. *Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security*. Washington D.C.: Department of Defense, 2012. En ligne, <www.defense.gov/transcripts/transcript.aspx?transcriptid=5136>. Consulté le 12 janvier 2016.

États-Unis, Department of Defense. *Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security*. Washington: The White House, 2012. En ligne, <www.defense.gov/transcripts/transcript.aspx?transcriptid=5136>. Consulté le 25 avril 2016.

États-Unis, Department of Defense. *Statement of General Keith B. Alexander, Commander of United States Cyber Command Before the House Committee on Armed Service*. Washington D.C. : The White House, 2010, p.4

États-Unis, Department of Defense. *Statement of General Keith B. Alexander, Commander of United States Cyber Command, Director of National Security Agency, Chief of Central Security Service, Before the Senate Committee on Appropriations "Cybersecurity : Preparing for and Responding to the Enduring Threat"*. Washington D.C. : Department of Defense, 2013, 15 p.

États-Unis, Department of Defense. *Strategy for Operating in Cyberspace*. Washington D.C. : The White House, 2011, 13 p.

États-Unis, Department of Defense. *The National Defense Strategy of the United States of America*. Washington D.C. : Department of Defense, 2005, 25 p.

États-Unis, Department of Homeland Security. *Executive Order 13231 of October 16, 2001 - Critical Infrastructure Protection in the Information Age*. Washington D.C. : Department of Homeland Security, 2001, 13 p. PDF en ligne, <www.dhs.gov/xlibrary/assets/executive-order-13231-dated-2001-10-16-initial.pdf>. Consulté le 22 février 2016.

États-Unis, Department of State. *Comments by Secretary Clinton in Hanoi, Vietnam.* En ligne,<iipdigital.usembassy.gov/st/english/texttrans/2010/07/20100723164658su0.4912989.html>. Consulté le 15 avril 2016.

États-Unis, Department of the Army. *Field Manual 3-13 : Information Operations: Doctrine, Tactics, Techniques, and Procedures*. Washington D.C. : Department of Defense, 2003, 311 p.

États-Unis, Economics and Statistics Administration et United States Patent and Trademark Office. *Intellectual Property and the U.S. Economy: Industries in Focus*. Washington D.C. : U.S. Department of Commerce, mars 2012, 62 p. PDF en ligne, <www.uspto.gov/sites/default/files/news/publications/IP_Report_March_2012.pdf>. Consulté le 12 janvier 2016.

États-Unis, Federal Bureau of Investigation. « Focus on Economic Espionage », s.d. En ligne, <www2.fbi.gov/hq/ci/economic.htm#intro>. Consulté le 25 janvier 2016.

États-Unis, Government Accountability Office. *Financial Audit : Bureau of the Fiscal Service's Fiscal Years 2014 and 2013 Schedules of Federal Debt.* Washington, DC : Government Accountability Office, 2014. PDF en ligne, <www.gao.gov/assets/670/666824.pdf>. Consulté le 25 juillet 2015.

États-Unis, Government Accountability Office. *Information Security - DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System.* Washington D.C. : Government Accountability Office, 56 p.

États-Unis, Joint Chief of Staff. *Joint Vision 2010.* Washington D.C. : Joint Chief of Staff, 1995, 34 p.

États-Unis, Joint Chief of Staff. *The National Military Strategy for Cyberspace Operations*. Washington D.C. : Joint Chief of Staff, 2006, 20 p.

États-Unis, Joint Chief of Staff. *The National Military Strategy of the United States of America*. Washington D.C. : Joint Chief of Staff, 2004, 30 p.

États-Unis, Office of the National Counterintelligence Executive. *Foreign Spies Stealing U.S. Economic Secrets in Cyberespace*. Washington D.C. : Office of the Director of National Intelligence, 2011, 11 p.

États-Unis, Office of the Secretary of Defense. *FY04 Report to Congress on PRC Military Power*. Washington D.C. : Department of Defense, 2004, 54 p. PDF en ligne, <www.globalsecurity.org/military/library/report/2004/d20040528prc.pdf>. Consulté le 10 février 2016.

États-Unis, Office of the Secretary of Defense. *Military and Security Developments Involving the People's Republic of China 2010*, Washington D.C.: Department of Defense, 2010, 74 p.

États-Unis, Office of the Secretary of Defense. *Military and Security Developments Involving the People's Republic of China 2011*, Washington D.C.: Department of Defense, 2011, 84 p.

États-Unis, Office of the Secretary of Defense. *Military Power of the People's Republic of China 2009*, Washington D.C.: Department of Defense, 2009, 66 p.

États-Unis, Office of the Secretary of Defense. *Quadrennial Defense Review Report 2010.* Washington D.C. : Department of Defense, 2010, 105 p.

États-Unis, U.S. Congress. « Economic Espionage Act of 1996 », *U.S. Code*, 1996, pp. 3488 – 3513. PDF en ligne, <www.gpo.gov/fdsys/pkg/PLAW-104publ294/pdf/PLAW-104publ294.pdf>. Consulté le 12 janvier 2016.

États-Unis, United States Cyber Command. «Beyond the Build - Delivering Outcomes through Cyberspace ». Washington D.C. : Department of Defense, 11 p.

États-Unis, United States International Trade Commission. *China: Effects of Intellectual Property Infringement and Indigenous Innovation Policies on the U.S. Economy.* Washington D.C. : United States International Trade Commission, 2011, 308 p. PDF en ligne, <www.usitc.gov/publications/332/pub4226.pdf>. Consulté le 8 janvier 2016.

États-Unis, United States Strategic Command Public Affairs. « U.S. Strategic Command to Conduct Exercise Global Lightning ». *U.S. Strategic Command*, 22 avril 2016. En ligne,<www.stratcom.mil/news/2016/608/US_Strategic_Command_to_Conduct_Exercise_Global_Lightning/>. Consulté le 15 avril 2016.

États-Unis, United States Strategic Command. *The Cyber Warfare Lexicon.* Washington D.C. : Department of Defense, 2009, 45 p. En ligne, <info.publicintelligence.net/USSTRATCOM-CyberWarfareLexicon.pdf>. Consulté le 30 mars 2016.

États-Unis, White House. *Critical Foundations – Protecting America's Infrastructures.* Washington D.C. : The White House, 1997, 102 p.

États-Unis, White House. *International Strategy for Cyberspace : Prosperity, Security and Openness in a Networked World.* Washington D.C. : The White House, 2011, 25 p

États-Unis, White House. *Presidential Decision Directive 63.* Washington D.C. : The White House, 1998. En ligne, <fas.org/irp/offdocs/pdd/pdd-63.htm>. Consulté le 22 février 2016.

États-Unis, White House. *Presidential Policy Directive 20.* Washington D.C.: The White House. 2012, 18 p. PDF en ligne, <fas.org/irp/offdocs/ppd/ppd-20.pdf>. Consulté le 15 mars 2015.

États-Unis, White House. *Remarks By President Obama to the Australian Parliament.* Washington D.C.: The White House, 2011. En ligne, <www.whitehouse.gov/the-press-office/2011/11/17/remarks-president-obama-australian-parliament>. Consulté le 27 juillet 2015.

États-Unis, White House. *Remarks by the President in Address to the Nation on the Way Forward in Afghanistan and Pakistan.* Washington D.C. : The White House, 2009. En ligne, <www.whitehouse.gov/the-press-office/remarks-president-address-nation-way-forward-afghanistan-and-pakistan>. Consulté le 15 octobre 2015.

États-Unis, White House. *Remarks by the President on Securing our Nation's Cyber Infrastructure*. Washington D.C. : The White House, 2009. En ligne, <www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure>. Consulté le 20 février 2016.

États-Unis, White House. *Remarks by the President on Securing our Nation's Cyber Infrastructure*. Washington D.C. : The White House, 2009. En ligne, <www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure>. Consulté le 15 janvier 2016.

États-Unis, White House. *Remarks by the President to the United Nations General Assembly*. 23 septembre 2009. En ligne, <www.whitehouse.gov/the-press-office/remarks-president-united-nations-general-assembly>. Consulté le 2 octobre 2015

États-Unis, White House. *The National Security Strategy of the United States of America.* Washington D.C. : White House, 2002. PDF en ligne, <nssarchive.us/NSSR/2002.pdf>, p.30. Consulté le 3 octobre 2015

États-Unis, White House. *The National Strategy to Secure Cyberspace*, Washington D.C. : The White House, 2003, 60 p.

États-Unis. Department of Defense. *DoD Releases Fiscal 2015 Budget Proposal and 2014 QDR*. En ligne, <www.defense.gov/releases/release.aspx?releaseid=16567>. Consulté le 15 mars 2015

États-Unis. Department of Defense. *Retirement Ceremony for General Keith Alexander*, 2014. En ligne, <archive.defense.gov/Speeches/Speech.aspx?SpeechID=1837>. Consulté le 25 mars 2015.

États-Unis. Department of Defense. *Summary of the DoD Fiscal 2012 Budget Proposal*. PDF en ligne, <www.defense.gov/pdf/SUMMARY_OF_THE_DOD_FISCAL_2012_BUDGET_PROPOSAL_(3).pdf>. Consulté le 15 mars 2015

Evans, Gareth. « Cooperative Security and Intrastrate Conflict », *Foreign Policy*, no.96, 1994, pp.3 – 20.

Facon, Isabelle. « L'Organisation de Coopération de Shanghai : ambitions et intérêts russes », *Le Courrier des pays de l'Est*, no.1055, 2006, pp.26 – 37.

Farrell, Maria. « Quietly, symbolically, US control of the internet was just ended ». *The Guardian*, 14 mars 2016. En ligne, <www.theguardian.com/technology/2016/mar/14/icann-internet-control-domain-names-iana>. Consulté le 16 mars 2016.

Ferran, Benjamin. « XKeyscore et Prism, anatomie de la machine à espionner américaine ». *LeFigaro.fr*, 2 août 2013. En ligne, <www.lefigaro.fr/secteur/high-tech/2013/08/02/32001-20130802ARTFIG00313-xkeyscore-et-prism-anatomie-de-la-machine-a-espionner-americaine.php>. Consulté le 4 avril 2016.

Flora, Liz. « Complete Transcript: Thomas Donilon at Asia Society New York ». *Asia Society*, 11 mars 2013. En ligne, <asiasociety.org/new-york/complete-transcript-thomas-donilon-asia-society-new-york>. Consulté le 10 janvier 2016.

Frabel, Taylor. « The Evolution of China's Military Strategy : Comparing the 1987 and 1999 Editions of Zhanlüexue ». Dans David Finkelstein et James Mulvenon (eds.), *China's Revolution in Doctrinal Affairs : Emerging Trends in the Operational Art of the Chinese People's Liberation Army*. Alexandria, VA : CNA Corporation, 2005, pp.79-99.

France, Ministère de la Défense. *Droit des conflits armés*, 16 novembre 2011. En ligne, <www.defense.gouv.fr/sga/le-sga-en-action/droit-et-defense/droit-des-conflits-armes/droit-des-conflits-armes>. Consulté le 2 février 2016.

Freedberg, Sydney J. « Top Official Admits F-35 Stealth Fighter Secrets Stolen ». *Breaking Defense*, 20 juin 2013. En ligne, <breakingdefense.com/2013/06/top-official-admits-f-35-stealth-fighter-secrets-stolen/>. Consulté le 9 janvier 2016.

Gartzke, Erik. « The Myth of Cyberwar : Bringing War in Cyberspace Back Down to Earth ». *International Security*, vol.38, no.2, 2013, pp.41 – 73.

Gates Robert M. *Duty : Memoirs of a Secretart at War*. New York : Alfred A. Knopf, 2014, 618 p.

Gates, Robert M. « A Balanced Strategy : Reprogramming the Pentagon for a New Age ». *Foreign Affairs*, vol.88, no.1, 2009, pp.28 – 40.

Gates, Robert M. « Helping Others Defend Themselves : The Future of U.S. Security Assistance », *Foreign Affairs*, vol.89, no.3, 2010, pp.2 – 6.

Gerth, Jeff et James Risen. « 1998 Report Told of Lag Breaches and China Threat », *The New York Times*, 2 mai 1999. En ligne, <www.nytimes.com/1999/05/02/world/1998-report-told-of-lab-breaches-and-china-threat.html?pagewanted=all&src=pm>. Consulté le 13 décembre 2015.

Gertz, Bill. « China's armed drones appear built from stolen data from US cyber intrusions ». *Asia Times*, 29 décembre 2015. En ligne, <atimes.com/2015/12/chinas-armed-drones-appear-built-from-stolen-data-from-us-cyber-intrusions/>. Consulté le 15 janvier 2016.

Glaser, Charles L. « Political Consequences of Military Strategy : Expanding and Refining the Spiral and Deterrence Models », *World Politics*, vol.44, no.4, 1992, pp.497 – 538.

Glaser, Charles L. et Chairn Kaufmann. « What Is the Offense-Defense Balance and How Can We Measure It? ». *International Security,* vol.22, no.4, 1998, pp.44 – 82.

Goldberg, Adam W. et Joshua P. Galper. « Where Huawei Went Wrong in America ». *The Wall Street Journal*, 3 mars 2011. En ligne, <www.wsj.com/articles/SB10001424052748703559604576175692598333556>. Consulté le 25 avril 2016.

Google. « A new approach to China ». *Google Official Blog*, 12 janvier 2010. En ligne, <googleblog.blogspot.ca/2010/01/new-approach-to-china.html>. Consulté le 15 décembre 2015.

Gorman, Siobhan, August Cole et Yochi Dreazen. « Computer Spies Breach Fighter-Jet Project ». *The Wall Street Journal*, 21 avril 2009. En ligne, <www.wsj.com/articles/SB124027491029837401>. Consulté le 10 janvier 2016.

Graham, Bradley. «Hackers Attack Via Chinese Web Sites ». *The Washington Post*, 25 août 2005. En ligne,0 <www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318.html>. Consulté le 15 décembre 2015.

Greenwald, Glenn. *No Place to Hide : Edward Snowden, the NSA, and the U.S. Surveillance State*. New York : Metropolitan Books/Henry Holt, 2014, 259 p.

Guitton, Amaelle et al. « WikiLeaks - Chirac, Sarkozy et Hollande : trois présidents sur écoute ». *Libération.fr*, 23 juin 2015. En ligne, <www.liberation.fr/planete/2015/06/23/chirac-sarkozy-et-hollande-trois-presidents-sur-ecoute_1335767>. Consulté le 4 avril.

Gutmann, Ethan. « Hacker Nation : China's Cyber Assault », *World Affairs*, vol.173, no.1, 2010, pp.70 – 79.

Hachigian, Nina. « China's Cyber-Strategy », *Foreign Affairs*, vol.80, no.2. 2001, pp.118 – 133.

Haddick, Robert. « Preserving U.S. Military Might: How to Make the Third Offset Strategy a Success ». *The Nation*, 7 décembre 2014. En ligne, <nationalinterest.org/feature/preserving-us-military-might-how-make-the-third-offset-11800>. Consulté le 26 avril 2016.

Hannas, William C., James Mulvenon et Anna B. Puglisi. *Chinese Industrial Espionage : Technology Acquisition and Military Modernisation*. Londres; New York: Routledge, coll. *Asian Security Studies*, 2013, 296 p.

Hanne, Hugo. « Amérique, défendre le territoire », *Géoéconomie*, vol.66, no.3, 2013. pp.135 – 149.

Harries, Owen et Tom Switzer. « Leading from Behind : Third Time a Charm », *The American Interest*, vol.8, no.5, 2013, pp.7 – 15.

Harris, Shane. *@War : The Rise of the Military-Internet Complex*. New York : Houghton Mifflin Harcourt, 2014, 263 p.

Harris, Shane. « China's Cyber-Militia ». *National Journal*, 31 mai 2008. En ligne, <www.nationaljournal.com/magazine/china-s-cyber-militia-20080531>. Consulté le 15 février 2016

Harris, Shane. « The Cowboy of the NSA », *Foreign Policy,* 9 septembre 2013. En ligne, <www.foreignpolicy.com/articles/2013/09/08/the_cowboy_of_the_nsa_keith_alexander>. Consulté le 10 août 2014.

Harris, Shane. *The Watchers : The Rise of America's Surveillance State*. New York : Penguin Group, 2011, 424 p.

Hayden, Gen. Michael V. *Playing to the Edge : American Intelligence in the Age of Terror*, New York : Penguin Press, 2016, 464 p.

Hayton, Bill. *The South China Sea*. New Haven; Londres : Yale University Press, 2014, 320 p.

Herrera, Geoffrey L. « Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space ». Dans M. Cavelty, V. Mauer et S.F. Krishna-Hensel (eds.), *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace*, Aldershot; Burlington: Ashgate, 2007, pp.67 – 93.

Hjortdal, Magnus. « China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence », *Journal of Strategic Security*, vol.4, no.2, 2011, pp.1 – 24.

Hollis, David M. « USCYBERCOM : The Need for a Combatant Command versus a Subunified Command », Joint Force Quarterly, vol.58, no.3, 2010, pp.48 – 53.

Holm, Hannes, Waldo Rocha Flores et Göran Ericsson. 2013. « Cyber Security for a Smart Grid – What About Phishing? », *2013 4th IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe)*, Copenhague (Danemark), 6 au 9 octobre, 3 p.

Hopkins, Jamie Smith. « Sourcefire founder: Cisco deal is 'a good match' ». *The Baltimore Sun*, 28 juillet 2013. En ligne, <www.baltimoresun.com/business/bs-bz-sourcefire-martin-roesch-qa-20130728-story.html>

Huntington, Samuel. « The Lonely Superpower », *Foreign Affairs*, vol.78, no.2, 1999, pp.35 – 49.

Huntington, Samuel. « Why International Primacy Matters ». *International Security*, vol.17, no.4, 1993, pp.68 – 83.

Hvistendahl, Mara. « Hackers : The China Syndrome ». *Popular Science,* 23 avril 2009. En ligne, <www.popsci.com/scitech/article/2009-04/hackers-china-syndrome>. Consulté le 8 janvier 2016

Ikenberry, G. John, Michel Mastanduno et William C. Wohlforth. « Unipolarity, State Behavior, and Systemic Consequences ». *World Politics*, vol.61, no.1, 2009, pp.1 – 27.

Ikenberry, G. John. « An Agenda for Liberal International Renewal ». Dans Michèle Flournoy et Shawn Brimley (eds.). *Finding our Way : Debating American Grand Strategy*, Washington D.C : Center for a New American Century, Solarium Strategy Series, 2008, pp.43 – 59.

Ikenberry, G. John. « The Future of the Liberal World Order : Internationalism After America ». *Foreign Affairs*, vol.90, no.3, 2011, pp.56 – 68.

Ikenberry, G. John. « The Rise of China and the Future of the West : Can the Liberal System Survive? », *Foreign Affairs*, vol.87, no.1 (2008), pp.23 – 37.

Ikenberry, G. John. *Liberal Leviathan : The Origins, Crisis, and Transformation of the American World Order*. Princeton, New Jersey; Princeton University Press, 2011, 392 p.

Inkster, Nigel. « Chinese Intelligence in the Cyber Age », *Survival*, vol.55, no.1, 2013, pp.45 – 66.

International Institute for Strategic Studies. « Shangri-La Dialogue ». *About Shangri-La.* En ligne, <www.iiss.org/en/events/shangri-s-la-s-dialogue/about-shangri-la>. Consulté le 7 novembre 2015.

Jennifer Valentino-De Vries et Julia Angwin. « Defenses Against Hackers Are Like the 'Maginot Line,' NSA Chief Says ». *The Wall Street Journal*, 13 janvier 2012. En ligne, <blogs.wsj.com/digits/2012/01/13/u-s-business-defenses-against-hackers-are-like-the-maginot-line-nsa-chief-says/>. Consulté le 27 avril 2016.

Jervis, Robert. « Chapter Three : Deterrence, the Spiral Model and the Intentions of the Adversary ». Dans *Perception and Misperception in International Politics*. Princeton (N.J.) : Princeton University Press, 1976, 445 p.

Jervis, Robert. « Cooperation under the Security Dilemma ». *World Politics*, vol.30, no.2, 1978, pp.167 – 214.

Johnson, Loch K. *Secret Agencies : U.S. Intelligence in a Hostile World.* New Haven : Yale University Press, 1996, 262 p.

Jones, Terril Yue. « China has 'mountains of data' about U.S. cyber attacks: official ». *Reuters*, 5 juin 2013. En ligne, <www.reuters.com/article/us-china-usa-hacking-idUSBRE95404L20130605>. Consulté le 5 avril 2016.

Jordan, Amos A., William J. Taylor Jr.; Michael J. Meese et Suzanne C. Nielsen (eds.). *American National Security*. Baltimore, Maryland : John Hopkins University Press, 6e édition, 2009, 663 p.

Joye, Christopher. « Interview transcript: former head of the NSA and commander of the US cyber command, General Keith Alexander ». *The Australia Financial Review*, 8 mai 2014. En ligne, <www.afr.com/technology/web/security/interview-transcriptformer-head-of-the-nsa-and-commander-of-the-us-cyber-command-general-keith-alexander-20140507-itzhw>. Consulté le 15 avril 2016.

Kagan, Robert et William Kristol. « Burden of Power is Having to Wield It », *The Washington Post*, 19 mars 2000. En ligne, <carnegieendowment.org/2000/03/19/burden-of-power-is-having-to-wield-it/77e>. Consulté le 4 octobre 2015

Kagan, Robert. « America's Crisis of Legitimacy », *Foreign Affairs*, vol.83, no.2, 2004, pp.65 – 87.

Kagan, Robert. « Obama's Year One : Contra ». *World Affairs*, vol.172, no.3, 2010, pp.12 – 18.

Kagan, Robert. « The Benevolent Empire », *Foreign Policy*, no.111, 1998, pp.24 – 35.

Kan, Shirley A. *Taiwan: Major U.S. Arms Sales Since 1990*. Washington D.C. : Congressional Research Services, 2014, 59 p. PDF en ligne, <www.fas.org/sgp/crs/weapons/RL30957.pdf>. Consulté le 15 avril 2016.

Kang, David C. *China Rising : Peace, Power, and Order in East Asia*. New York : Columbia University Press. 2007, 274 p.

Kaplan, Fred. « 'WarGames' and Cybersecurity's Debt to a Hollywood Hack ». *The New York Times*, 19 février 2016. En ligne, <www.nytimes.com/2016/02/21/movies/wargames-and-cybersecuritys-debt-to-a-hollywood-hack.html>. Consulté le 21 février 2016.

Kaplan, Fred. *Dark Territory – The Secret History of Cyber War*. New York : Simon & Schuster, 2016, 352 p.

Kaplan, Robert D. « The Geography of Chinese Power : How Far Can Beijing Reach on Land and at Sea? », *Foreign Affairs*, vol.89, no.3, 2010, pp.22 – 41.

Kaplan, Robert D. *Asia's Cauldron : The South China Sea and the End of a Stable Pacific*. New York : Random House, 2014, 256 p.

Kaplan, Robert D. et Stephen S. Kaplan. « America Primed ». *The National Interest*, no.112, 2011, pp.42 – 54.

Kearn Jr., David W. « Air-Sea Battle, the Challenge of Access, and U.S. National Security Strategy », *American Foreign Policy Interest*, vol.36, no.1, 2014, pp.34 – 43.

Kearn Jr., David W. *Air-Sea Battle and China's Anti-Access and Area Denial Challenge. Orbis,* vol.58, no.1, 2013, pp.132 – 146

Kello, Lucas. « The Meaning of the Cyber Revolution : Perils to Theory and Statecraft ». *International Security*, vol. 38, no.2, 2013, pp.7 – 40.

Kennedy, Paul. « Grand Strategy in War and Peace : Toward a Broader Definition ». Dans Paul Kennedy, *Grand Strategies in War and Peace*, New Haven, London : Yale University Press, 1991, pp.1 – 7.

Kennedy, Paul. *Naissance et déclin des grandes puissances*. Paris : Éditions Payot, 2004, 991 p.

Keohane, Robert et Joseph S. Nye. *Power and Interdependance : World Politics in Transition*. Boston : Little, Brown, 1977, 273 p.

Kessler, Glenn. « Romney doubling down on debate mistatements », *The Washington Post*, 25 octobre 2012. En ligne, <www.washingtonpost.com/blogs/fact-checker/post/romney-doubling-down-on-debate-mistatements/2012/10/24/c1d34826-1e22-11e2-ba31-3083ca97c314_blog.html>. Consulté le 12 janvier 2016.

Klimburg, Alexander. « Mobilising Cyber Power », *Survival*, vol.53, no.1, 2011, pp.41 – 60.

Koren, Marina. « About Those Fingerprints Stolen in the OPM Hack ». *The Atlantic*, 23 septembre 2015. En ligne, <www.theatlantic.com/technology/archive/2015/09/opm-hack-fingerprints/406900/>. Consulté le 27 avril 2016.

Krauthammer, Charles. « The Unipolar Moment Revisited », *The National Interest*, no.70, 2003, pp.7 – 41.

Krauthammer, Charles. « The Unipolar Moment », *Foreign Affairs*, vol.70, no.1, 1990, pp.23 – 33.

Krekel, Bryan. *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network*. Washington D.C. : The US-China Economic and Security Review Commission, 2009, 88 p.

Krepinevich, Andrew F. « Strategy in a Time of Austerity », *Foreign Affairs*, vol.91, no.6, 2012, pp.58 – 69.

Krepinevich, Andrew F. *Why AirSea Battle?*. Washington D.C. : Center for Strategic and Budgetary Assessments, 2010, 40 p.

Kristol, William et Robert Kagan, « Toward a Neo-Reaganite Foreign Policy », *Foreign Affairs*, vol.75, no.4, 1996, pp.18 – 32.

Labonte, Marc et Andrew Hanna. *The Impact of Major Legislation on Budget Deficits : 2001 to 2009*. Washington, DC : Congressional Research Service, 2010, 32 p. PDF en ligne, <www.fas.org/sgp/crs/misc/R41134.pdf>. Consulté le 25 juillet 2015.

Lafrance, Adrienne. « The Truth About Bill Clinton's Emails ». *The Atlantic*, 12 mars 2015. En ligne, <www.theatlantic.com/technology/archive/2015/03/the-myth-about-bill-clintons-emails/387604/>. Consulté le 24 février 2015.

Landler, Mark. « Offering to Aid Talks, U.S. Challenges China on Disputed Islands », *The New York Times*, 23 juillet 2010. En ligne, <www.nytimes.com/2010/07/24/world/asia/24diplo.html>. Consulté le 15 juin 2015.

Landler, Mark. « How Hillary Clinton Became a Hawk ». *The New York Times*, 21 avril 2016. En ligne, <www.nytimes.com/2016/04/24/magazine/how-hillary-clinton-became-a-hawk.html?_r=0>. Consulté le 22 avril 2016.

Lanteigne, Marc. « China's Maritime Security and the "Malacca Dilemma" ». *Asian Security*, vol.4, no.2, 2008, pp.143 – 161.

Layne, Christopher. « From Preponderance to Offshore Balancing: America's Future Grand Strategy », *International Security*, vol.22, no.1, 1997, pp.86 – 124.

Lee, John. « Cyber Kleptomaniacs : Why China Steals Our Secrets », *World Affairs*, vol.176, no.3, 2013, pp.73 – 79.

Lewis, James A. « Computer Espionage, Titan Rain and China », *Center for Strategic and International Studies*, 14 décembre 2015. PDF en ligne, <csis.org/files/media/csis/pubs/051214_china_titan_rain.pdf>. Consulté le 15 décembre 2015

Liang, Qiao et Wang Xiangsui. *La Guerre hors limites*. Paris : Payot et Rivages, Coll. Rivages poche, 2006, 310 p.

Libicki, Martin C. « Cyberwar as a Confidence Game », *Strategic Studies Quarterly*, vol. 5, no 1, 2011, pp.132 – 146.

Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Santa Monica, CA : RAND, 2009, 214 p.

Liff, Adam P. « Cyberwar: A New 'Absolute Weapon'? ». *The Journal of Strategic Studies*, vol.35, no.3, 2012, pp.401 – 428.

Lindsay, Jon R. « Stuxnet and the Limits of Cyber Warfare », *Security Studies*, vol.22, no.3, 2013, pp.365 – 404.

Lizza, Ryan. « Leading From Behind », *The New Yorker,* 26 avril 2011. En ligne, <www.newyorker.com/news/news-desk/leading-from-behind>. Consulté le 20 septembre 2015.

Lizza, Ryan. « The Consequentialist », *The New Yorker,* 2 mai 2011. En ligne, <www.newyorker.com/magazine/2011/05/02/the-consequentialist>. Consulté le 20 septembre 2015.

Lohr, Steve. « National Security Experts Plan for Wars Whose Targets And Weapons Are All Digital ». *The New York Times,* 30 septembre 1996. En ligne, <www.nytimes.com/1996/09/30/business/national-security-experts-plan-for-wars-whose-targets-weapons-are-all-digital.html?pagewanted=all> Consulté le 3 avril 2016.

Lord, William T. « USAF Cyber Command : To Fly and Fight in Cyberspace ». *Strategic Studies Quarterly*, automne 2008, pp.5 – 17.

Lute, Jane Holl et Bruce McConnell. « Op-Ed : A Civil Perspective on Cybersecurity », *Wired*, 14 février 2011. En ligne, <www.wired.com/2011/02/dhs-op-ed/>. Consulté le 16 mars 2016.

Lynn III, William J. « Defending a New Domain: The Pentagon's Cyberstrategy », *Foreign Affairs*, vol.89, no.5, 2010, pp.97 – 108.

Macdonald, Paul K. et Joseph M. Parent. « Graceful Decline? The Surprising Success of Great Power Retrenchment », *International Security*, vol.35, no.4, 2011, pp.7 – 44.

Macleod, Alex. « Le néoréalisme ». Dans Alex Macleod et Dan O'Meara (dir.). *Théorie des relations internationales : contestation et résistance*, Montréal : Athéna Éditions, 2007, pp.87 – 112.

Majmudar, Nishad. « Fort Meade as Cyber Hub Turns Maryland Into a Startup Hot Spot ». *Bloomberg.com*, 30 janvier 2012. En ligne, <www.bloomberg.com/news/articles/2012-01-30/fort-meade-as-cyber-hub-turns-maryland-into-a-startup-hot-spot>. Consulté le 15 avril 2016.

Malfatto, Pierre-Louis. *Quand l'intelligence fait défaut : les services de renseignements américains à l'épreuve des attentats du 11 septembre 2001*. Paris : L'Harmattan, Coll. Raoul-Dandurand, 2009, 189 p.

Mandiant. *APT1 : Exposing One of China's Cyber Espionage Units*, 2013, 74 p. PDF en ligne, <intelreport.mandiant.com/Mandiant_APT1_Report.pdf>. Consulté le 25 novembre 2015.

Manjikian, Mary McEvoy. « From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik », *International Studies Quarterly*, vol.54, no.2, 2010, pp.381 – 401.

Manson, George Patterson. « Cyberwar : The United States and China Prepare For the Next Generation of Conflict », *Comparative Strategy*, vol.30, no.2, 2011, pp.121 – 133.

Markoff, John et David Barboza. « 2 China Schools Said to Be Tied to Online Attacks », *The New York Times*, 18 février 2010. En ligne, <www.nytimes.com/2010/02/19/technology/19china.html>. Consulté le 22 mars 2015.

Markoff, John, David E. Sanger et Thom Shanker. « In Digital Combat, U.S. Finds No Easy Deterrent », The New York Times, 25 janvier 2010. En ligne, <www.nytimes.com/2010/01/26/world/26cyber.html?pagewanted=all>. Consulté le 10 janvier 2016.

Markoff, John. « Cyberattack on Google Said to Hit Password System ». *The New York Times*, 19 avril 2010. En ligne, <www.nytimes.com/2010/04/20/technology/20google.html>. Consulté le 15 février 2016.

Marsh, Kevin. « Managing Relative Decline : A Neoclassical Realist Analysis of the 2012 US Defense Strategic Guidance », *Contemporary Security Policy*, vol.33, no.3, 2012, pp.487 – 511.

Massoud Amin et Anthony M. Giacomoni. 2012. « Smart Grid – Safe, Secure, Self-Healing : Challenges and Opportunities in Power System Security, Resiliency, and Privacy », *IEEE Power & Energy Magazine*, janvier/février 2012, p.33 – 40

Mazarr, Michael J. « Rivalry's New Face », *Survival*, vol. 54, no.4, 2012, pp.83 – 106.

McConnell, Mike. « Cyber Insecurities : The 21st Century Threatscape ». Dans K.M. Lord et Travis Sharp (eds.), *America's Cyber Future : Security and Prosperity in the Information Age – Volume II*, Washington D.C. : Center for A New American Society, 2011, pp.27 – 39.

McConnell, Mike. « Cyberwar is the New Atomic Age », *New Perspectives Quarterly*, vol.26, no.3, 2009, pp.72 – 77.

McDonough, David S. « Beyond Primacy : Hegemony and 'Security Addiction' in U.S. Grand Strategy », *Orbis*, vol.53, no.1, 2009, pp.6 – 22.

McGarry, Brendan. « Lawmaker: Chinese J-31, J-20 'Mirror' American F-35, F-22 ». *DefenseTech*, 8 janvier 2016. En ligne, <defensetech.org/2015/09/29/lawmaker-chinese-j-31-j-20-mirror-american-f-35-f-22/>. Consulté le 9 janvier 2016.

McGregor, James. « Time to rethink U.S.-China trade relations », *The Washington Post*, 19 mai 2010. En ligne, <www.washingtonpost.com/wp-dyn/content/article/2010/05/13/AR2010051303551.html>. Consulté le 3 janvier 2016.

Mearsheimer, John J. *The Tragedy of Great Power Politics*. New York : Norton, 2001, 555 p.

Mihm, Stephen. « China Didn't Invent Industrial Espionage ». *Bloomberg View*, 26 mai 2015. En ligne, <www.bloombergview.com/articles/2015-05-26/china-didn-t-invent-industrial-espionage>. Consulté le 15 janvier 2016.

Mondoux, André. *Histoire sociale des technologies numériques de 1945 à nos jours*. Montréal : Éditions Nota Bene, 2011, 220 p.

Monteiro, Nuno. « Unrest Assured: Why Unipolarity Is Not Peaceful », *International Security,* vol.36, no.3, 2012, pp.9 – 40.

Morningstar, James K. « Technologies, Doctrine, and Organization for RMA », *Joint Forces Quarterly*, no.15, 1997, pp.37 – 43.

Murdock, Clark et Kevin Kallmyer. « Applied Grand Strategy : Making Tough Choices in an Era of Limits and Constrait », *Orbis*, vol.55, no.4, 2011, pp.541 – 557.

Murray, Williamson, Richard Hart Sinnreich et James Lacey, *The Shaping of Grand Strategy : Policy, Diplomacy and War*, New York : Cambridge University Press, 2011, 294 p.

Nasheri, Hadieh. *Economic Espionage and Industrial Spying*. Cambridge (U.K.); New York : Cambridge University Press, 2005, 270 p.

Nathan, Andrew J. et Andrew Scobell. « How China Sees America : The Sum of Beijing's Fears », *Foreign Affairs,* vol.91, no.1, 2012, pp.32 – 47.

National Bureau of Asian Research. *The Report of the Commission on the Theft of American Intellectual Property*. 2013, 89 p. PDF *en ligne,* <www.ipcommission.org/report/IP_Commission_Report_052213.pdf>. Consulté le 2 janvier 2016

Nougayrède, Nathalie. « La guerre de Nicolas Sarkozy », *Le Monde.fr*, 23 septembre 2011. En ligne, <www.lemonde.fr/libye/article/2011/08/23/libye-la-guerre-de-nicolas-sarkozy_1562377_1496980.html>. Consulté le 20 septembre 2015.

NPR. « President Bush and 'the Google' », *National Public Radio*, 30 octobre 2006. En ligne, <www.npr.org/templates/story/story.php?storyId=6404911>. Consulté le 24 février 2016.

Nye, Joseph S. « The Future of American Power : Dominance and Decline in Perspective », *Foreign Affairs*, vol.89, no.6 (2010), pp.2 – 12.

Nye, Joseph S. « Hard and Soft Power in a Global Information Age ». Dans Mark Leonard (ed.). *Re-Ordering the World*. Londres : The Foreign Policy Centre, 2002, pp.2 – 10.

Nye, Joseph S. « The Decline of America's Soft Power ». *Foreign Affairs*, vol.83, no.3, 2004, pp.16 – 20.

Nye, Joseph S. et William A. Owens. « America's Information Edge », *Foreign Affairs,* vol.75, no.2, 1996, pp.20 – 36.

Obama, Barack. « Renewing American Leadership ». *Foreign Affairs*, vol.86, no.4, 2007, pp.2 – 16.

Onley, Dawn S. et Patience Wait. « Red Storm Rising: DoD's Efforts to Stave Off Nation-State Cyber Attacks Begin with China », *Government Computer News*, 17 août 2006, 4 p. En ligne, <gcn.com/Articles/2006/08/17/Red-storm-rising.aspx?Page=1>. Consulté le 12 décembre 2015.

Onyeji, Ijeoma, Morgan Bazilian et Chris Bronk. 2014. « Cyber Security and Critical Energy Infrastructure ». *The Electricity Journal*, vol. 27, no 2, pp.52 – 60.

Owens, Amiral William A. « The Emerging U.S. System-of-systems », *Strategic Forum*, no.63, 1996, 6 p.

Patrick, Stewart. « Irresponsible Stakeholders? The Difficulty of Integrating Rising Powers », *Foreign Affairs*, vol.89, no.6, 2010, pp.44 – 53.

PBS. « Interview : John Hamre ». *Frontline : Cyberwar!*, 24 avril 2003. En ligne, <www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/hamre.html>. Consulté le 1er avril 2016.

PBS. « The Warnings ». *Frontline : Cyberwar!*, 24 avril 2003. En ligne, <www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/>. Consulté le 1er avril 2016.

Pehrson, Christopher I. *String of pearls : meeting the challenge of China's rising power across the Asian littoral*. Carlisle, PA : Strategic Studies Institute, U.S. Army War College, 2006, 30 p.

Pengelly, Martin. « NSA targeted Chinese telecoms giant Huawei – report ». *The Guardian*, 22 mars 2014. En ligne, <www.theguardian.com/world/2014/mar/22/nsa-huawei-china-telecoms-times-spiegel>. Consulté le 4 avril 2016.

Perry, William J. « Desert Storm and Deterrence ». *Foreign Affairs*, vol.70, no.4, 1991, pp.66 – 82.

Pollack, Jonathan D. « Chinese Military Power : What Vexes the United States and Why? », *Orbis*, vol.51, no.4, 2007, pp.635 – 650.

Posen, Barry R. « Command of the Commons : The Military Foundation of U.S. Hegemony », *International Security*, vol.28, no.1, 2003, pp.5 – 46.

Posen, Barry R. « Pull Back : The Case for a Less Activist Foreign Policy ». *Foreign Affairs*, vol.92, no.1. 2013, pp.116 – 128.

Posen, Barry R. *A Grand Strategy of Restraint*. Dans Michèle Flournoy et Shawn Brimley (eds.). *Finding our Way : Debating American Grand Strategy*, Washington D.C : Center for a New American Century, Solarium Strategy Series, 2008, pp.83 – 102.

Posen, Barry R. et Andrew L. Ross. « Competing Visions for U.S. Grand Strategy ». *International Security,* vol.21, no.3, 1996, pp.5 – 53.

Posen, Barry R., *The Sources of Military Doctrine*, Ithaca; Londres : Cornell University Press, 1984, 283 p.

Raggi, Philippe. « Le réveil de l'Asie au sein d'un monde multipolaire ». *Mécanoblog*, 23 mai 2010. En ligne, <mecanoblog.wordpress.com/2010/05/23/le-reveil-de-lasie-au-sein-dun-monde-multipolaire/>. Consulté le 15 février 2016.

Rainie, Lee, Janna Anderson et Jennifer Connolly. « Cyber Attacks Likely to Increase ». *Pew Research Center*, 29 octobre 2014. En ligne, <www.pewinternet.org/2014/10/29/cyber-attacks-likely-to-increase/>. Consulté le 5 janvier 2016.

Ramzy, Austin. « What You Need to Know About China's Draft Cybersecurity Law ». *The New York Times*, 9 juillet 2015. En ligne, <sinosphere.blogs.nytimes.com/2015/07/09/what-you-need-to-know-about-chinas-draft-cybersecurity-law/>. Consulté le 27 avril 2016.

Rawlinson, Kevin. « NSA surveillance: Merkel's phone may have been monitored 'for over 10 years' », *The Guardian*, 26 octobre 2013. En ligne, <www.theguardian.com/world/2013/oct/26/nsa-surveillance-brazil-germany-un-resolution>. Consulté le 4 avril 2016.

Rawnsley, Adam. « Meet China's Killer Drones ». *Foreign Policy*, 14 janvier 2016. En ligne, <foreignpolicy.com/2016/01/14/meet-chinas-killer-drones/>. Consulté le 15 janvier 2016.

Razoux, Pierre. « Israël frappe la Syrie : un raid mystérieux », *Politique étrangère*, vol.73, n.1, 2008, pp.9 – 22.

Reuters. « China PLA officers call Internet key battleground ». *Reuters*, 3 juin 2011. En ligne, <www.reuters.com/article/us-china-internet-google-idUSTRE7520OV20110603>. Consulté le 15 mars 2016.

Rice, Condoleezza. « Campaign 2000 : Promoting the National Interest », *Foreign Affairs*, vol.79, no.1 (2000), pp.45 – 62.

Rid, Thomas et Ben Buchanan. « Attributing Cyber Attacks ». *Journal of Strategic Studies*, vol.38, no.1 – 2, 2015, pp.4 – 37.

Rid, Thomas. *Cyberwar Will Not Take Place*. Londres : Hurst & Company, 2013, 218 p.

Rogin, Josh. « NSA Chief : NSA Chief: Cybercrime constitutes the "greatest transfer of wealth in history" », *Foreign Policy*, 9 juillet 2012. En ligne, <foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/>. Consulté le 15 décembre 2015.

Samaan, Jean-Loup. « Beyond the Rift in Cyber Strategy: a Middle Ground for the US Military Posture in Cyberspace », *Strategic Insights*, vol.10, no.1, 2011, pp.4 – 14.

Samaan, Jean-Loup. « Une géographie américaine de la menace chinoise », *Hérodote*, no.140 (2011), pp.103 – 122.

Samaan, Jean-Loup. *La Menace chinoise : une invention du Pentagone?*, Paris : Vendémiaire, 2012, 167 p.

Sanger, David E. *Confront and Conceal : Obama's Secret Wars and Surprising Use of American Power*. New York : Broadway Paperbacks, 2012, 485 p.

Sanger, David E. et Nicole Perlroth. « N.S.A. Breached Chinese Servers Seen as Security Threat ». *The New York Times*, 22 mars 2014. En ligne, <www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html?hp>. Consulté le 6 avril 2016.

Sanger, David E. et Thom Shanker. « N.S.A. Devises Radio Pathway Into Computers ». *The New York Times*, 14 janvier 2014. En ligne, <www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html>. Consulté le 15 mars 2016.

Scahill, Jeremy et Glenn Greenwald. « The NSA's Secret Role in the U.S. Assassination Program ». *The Intercept*, 10 février 2014. En ligne, <theintercept.com/2014/02/10/the-nsas-secret-role/>. Consulté le 15 avril 2016

Schelling, Thomas. *Arms and Influence*. New Haven (N.J.); Londres : Yale University Press, 2008, 312 p.

Schmidt, Michael S. et David E. Sanger. « 5 in China Army Face U.S. Charges of Cyberattacks ». *The New York Times*. 19 mai 2014. En ligne, <www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html>. Consulté le 5 janvier 2016.

Scobell, Andrew. « Show of Force: Chinese Soldiers, Statesmen, and the 1995-1996 Taiwan Strait Crisis », *Political Science Quarterly*, vol.115, no.2, 2000, pp.227 – 246.

Segal, Adam. « The Code not Taken: China, the United States and the Future of Cyber Espionage », *Bulletin of the Atomic Scientist*, vol.69, no.5, 2013, pp.38 – 45.

Segal, Adam. « Chinese Computer Games : Keeping Sage in Cyberspace », *Foreign Affairs*, 1 mars 2012. En ligne, <www.foreignaffairs.com/articles/china/2012-03-01/chinese-computer-games>. Consulté le 10 janvier 2016.

Segal, Adam. Déclaration à la *House of the Representatives*, Committee on Foreign Affairs. *Communist Chinese Cyber-attacks, Cyber-Espionage and Theft of American Technology*. 15 avril 2011, 51 p. PDF en ligne, <fas.org/irp/congress/2011_hr/china-cyber.pdf>. Consulté le 8 janvier 2016.

Segal, Adam. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. Philadelphie : PublicAffairs, 2016, 300 p.

Shachtman, Noah. « Insiders Doubt 2008 Pentagon Hack Was Foreign Spy Attack (Updated) ». *Wired.com*, 25 août 2010. En ligne, <www.wired.com/2010/08/insiders-doubt-2008-pentagon-hack-was-foreign-spy-attack/>. Consulté le 10 avril 2016.

Shakarian, Paulo, Jane Shakarian et Andrew Ruef. *Introduction to Cyber-Warfare: A Multidisciplinary Approach*. Amsterdam : Morgan Kaufmann Publishers, 2013, 318 p.

Shorrock, Tim. *Spies for Hire : The Secret World of Intelligence Outsourcing*. New York : Simon & Schuster, 2009, 464 p.

Singer, P.W. et Allan Friedman. 2013. *Cybersecurity and Cyberwar : What Everyone Needs To Know*, New York : Oxford University Press, 2013, 306 p.

Sinnreich, Richard Hart. « Patterns of grand strategy ». Dans Williamson Murray, Richard Hart Sinnreich et James Lacey, *The Shaping of Grand Strategy : Policy, Diplomacy and War*, New York : Cambridge University Press, 2011, pp.254 – 270.

Skypek, Thomas M. « A Grand Strategy for Rand Paul ». *The National Interest*, 28 mars 2014. En ligne, <nationalinterest.org/commentary/grand-strategy-rand-paul-10147>. Consulté le 22 septembre 2015

Slocum, Mac. « Cyber warfare: don't inflate it, don't underestimate it ». *Radar*, 11 février 2010. En ligne, <radar.oreilly.com/2010/02/cyber-warfare-dont-inflate-it.html>. Consulté le 27 avril 2016.

Smith, Ben. « A victory for 'leading from behind'? ». *Politico.com,* 22 août 2011. En ligne, <www.politico.com/story/2011/08/a-victory-for-leading-from-behind-061849>. Consulté le 25 octobre 2015.

Sternstein, Aliya. « US Hiring Researchers to See if China's Military Robots Originiate from Hacked Designs ». *DefenseOne*, 15 janvier 2016. En ligne, <www.defenseone.com/technology/2016/01/us-thinks-china-may-have-stolen-military-robot-designs/125168/>. Consulté le 15 janvier 2016.

Szafranski, Richard et Martin C. Libicki. « " . . . Or Go Down in Flame?" : Toward an Airpower Manifesto for the Twenty-First Century ». *Air Power Journal*, vol.10, no.3, 1996, pp.65 – 77.

Szamosszegi, Andrew et Cole Kyle. *An Analysis of State-owned Enterprises and State Capitalism in China.* Washington D.C. : U.S.-China Economic and Security Review Commission. 2011, 116 p. PDF en ligne, <www.uscc.gov/sites/default/files/Research/10_26_11_CapitalTradeSOEStudy.pdf>. Consulté le 3 janvier 2015

Taliaferro, Jeffrey W. « Security Seeking under Anarchy : Defensive Realism Revisited », *International Security*, vol.25, no.3, 2001, pp.128 – 161.

Tellis, Ashley J. « U.S.-China Relations in a Realist World ». Dans David Shambaugh, *Tangled Titans : The United States and China*, Lanham (Maryland) : Rowman & Littlefield Publishers, 2013, pp.75 – 100.

Tellis, Ashley J. *Balancing without Containment : An American Strategy for Managing China.* Washington D.C. : Carnegie Endowment for International Peace, 2014, 105 p.

Tellis, Ashley. « Balancing without Containment: A U.S. Strategy for Confronting China's Rise », *The Washington Quarterly*, vol.36, no.4, 2013, pp.109 – 124.

Thayer, Bradley A. « In Defense of Primacy », *The National Interest*, no.86, 2006, pp.32 – 37.

The Economist. « Xi's new model army ». *The Economist*, 16 janvier 2016. En ligne, <www.economist.com/news/china/21688424-xi-jinping-reforms-chinas-armed-forcesto-his-own-advantage-xis-new-model-army>. Consulté le 28 avril 2016.

The Wall Street Journal. « China's Cyber-Theft Jet Fighter ». *The Wall Street Journal*, 12 novembre 2014. En ligne, <www.wsj.com/articles/chinas-cyber-theft-jet-fighter-1415838777>. Consulté le 20 décembre 2015.

Thompson, Loren. *Defense Secretary Declares War on Budget Control Act as Hollow Force Looms. Forbes.* 26 février 2014. En ligne, <www.forbes.com/sites/lorenthompson/2014/02/26/defense-secretary-declares-war-on-budget-control-act-as-hollow-force-looms/>. Consulté le 30 juillet 2015.

Thornburgh, Nathan. « The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them) », *Time*, vol.166, no.10, 5 septembre 2005. En ligne, <courses.cs.washington.edu/courses/csep590/05au/readings/titan.rain.htm>. Consulté le 12 décembre 2015.

Thornburgh, Nathan. « Inside the Chinese Hack Attack », *Time.com*, 25 août 2005. En ligne, <content.time.com/time/nation/article/0,8599,1098371,00.html>. Consulté le 12 décembre 2015.

Timberg, Craig et Ellen Nakashima. « Chinese hackers suspected in attack on The Post's computers », *The Washington Post*, 1 février 2013. En ligne, <www.washingtonpost.com/business/technology/chinese-hackers-suspected-in-attack-on-the-posts-computers/2013/02/01/d5a44fde-6cb1-11e2-bd36-c0fe61a205f6_story.html>. Consulté le 9 janvier 2016.

Tkacik Jr., John J. « Trojan Dragon: China's Cyber Threat ». *Backgrounder*, no.2106, 2008. En ligne, <www.heritage.org/research/reports/2008/02/trojan-dragon-chinas-cyber-threat>. Consulté le 15 novembre 2015.

Twomey, Christopher et Xu Hui. « Military Developments ». Dans Nina Hachigian (ed), *Debating China : The U.S. – China Relationship in Ten Conversations*. New York : Oxford University Press, 2014, 256 p.

Twomey, Christopher P. « The Military-Security Relationship », ». Dans David Shambaugh, *Tangled Titans : The United States and China*, Lanham (Maryland) : Rowman & Littlefield Publishers, 2013, pp.235 – 259.

U.S.-Canada Power System Outage Task Force. *Final Report on the August 14, 2003 Blackout in United States and Canada: Causes and Recommendations*. 2004, 228 p. En ligne, <energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf>. Consulté le 15 décembre 2015.

Vacca, W. Alexander. « Military Culture and Cyber Security », *Survival*, vol.53, no.6, 2012, pp.159 – 176.

Vaïsse, Justin. « Why Neoconservatism Still Matters », *Brookings Policy Paper*, no.20, 2010. PDF en ligne, <www.brookings.edu/~/media/research/files/papers/2010/4/05%20neoconservatism%20vaisse/05_neoconservatism_vaisse.pdf>. Consulté le 10 octobre 2015.

Van Evera, Stephen. « Offense, Defense, and the Causes of War ». *International Security,* vol.22, no.4, 1998, pp.5 – 43.

Van Sant, Shannon. « China's freelance hackers : For love of country (and proof that propaganda works). *CBS News*, 15 juillet 2013. En ligne, <www.cbsnews.com/news/chinas-freelance-hackers-for-love-of-country-and-proof-that-propaganda-works-57592999>. Consulté le 10 janvier 2016.

Van Tol, Jan *et al. AirSea Battle : A Point-of-Departure Operational Concept*. Washington D.C. : Center for Strategic and Budgetary Assessments, 2010, 123 p.

Walker, Paul. « Organizing for Cyberspace : Operations: Selected Issues ». *International Law Studies*, vol.89, no,341, 2013, p.342

Walt, Stephen M. « Alliance Formation and the Balance of World Power », *International Security*, vol.9, no.4, 1985, pp.3 – 43.

Walt, Stephen M. « Balancing Act (Asian Version) », *Foreign Policy*, 3 mai 2010. En ligne, <foreignpolicy.com/2010/05/03/balancing-act-asian-version/> Consulté le 15 avril 2015

Walt, Stephen M., « The End of American Era », *The National Interest*, n.116, 2011, pp.6 – 16.

Walt. Stephen M. « Taming American Power », *Foreign Affairs,* vol.84, no.5, 2005, pp.105 – 120.

Waltz, Kenneth. « Structural Realism after the Cold War », *International Security*, vol.25, no.1, 2000, pp.5 – 41.

Waltz, Kenneth. *Theory of International Politics*. Reading, Mass : Addison-Wesley, 1979, 251 p.

Warner, Michael et Michael Good. « Notes on Deterrence in Cyberspace ». Dans *Georgetown Journal of International Affairs – International Engagement on Cyber III : State Building on a New Frontier*. Washington D.C. : Edmund A. Walsh School of Foreign Service, 2013, pp.66 – 72.

Watson Institute of International & Public Affairs. « Economic Costs » dans *Costs of War*. 28 avril 2015. En ligne, <watson.brown.edu/costsofwar/costs/economic>. Consulté le 27 juillet 2015

West, Darrell M. *Technology and the Innovation Economy*. Washington D.C. : Brookings Institution Press, 2011, 11 p. PDF en ligne, <www.brookings.edu/~/media/research/files/papers/2011/10/19-technology-innovation-west/1019_technology_innovation_west.pdf>. Consulté le 9 janvier 2016

Windrem, Robert. « Exclusive: Secret NSA Map Shows China Cyber Attacks on U.S. Targets ». *NBC News*, 30 juillet 2015. En ligne, <www.nbcnews.com/news/us-news/exclusive-secret-nsa-map-shows-china-cyber-attacks-us-targets-n401211>. Consulté le 2 avril 2016.

Wohlforth, William C. « The Stability of Unipolar World ». *International Security*, vol.24, no.1, 1999, pp.5 – 41.

Yoshihara, Toshi et James R. Holmes. *Red Star over the Pacific : China's Rise and the Challenge to U.S. Maritime Strategy*. Annapolis, MD : Naval Institute Press, 2010, 292 p.

Zedong, Mao. *De la guerre prolongée*. PDF en ligne, <maozedong.fr/documents/guerreprolongee.pdf>, 163 p. Consulté le 5 février 2016.

Zetter, Kim. « Google Hack Attack Was Ultra Sophisticated, New Details Show », *Wired*, 14 janvier 1010. En ligne, <www.wired.com/2010/01/operation-aurora/>. Consulté le 20 décembre 2015.

Zetter, Kim. « US and China Reach Historic Agreement on Economic Espionage ». *Wired*, 25 septembre 2015. En ligne, <www.wired.com/2015/09/us-china-reach-historic-agreement-economic-espionage/>. Consulté le 25 avril 2016.