UNIVERSITÉ DU QUÉBEC À MONTRÉAL

COMMUNICATION, GOUVERNANCE ET CYBERSÉCURITÉ: CONSTRUCTION DU DISCOURS DES ADMINISTRATIONS OBAMA ET XI ENTOURANT LA CYBERATTAQUE CONTRE L'OFFICE OF PERSONNEL MANAGEMENT DES ÉTATS-UNIS

MÉMOIRE

PRÉSENTÉ
COMME EXIGENCE PARTIELLE
DE LA MAÎTRISE EN COMMUNICATION

PAR
KARINE PONTBRIAND

JUIN 2017

« *There is perhaps no relationship as significant to the future of world politics as that between the U.S. and China. And in their relationship, there is no issue that has risen so quickly and generated so much friction as cybersecurity.* »
Lieberthal et Singer, 2012, *Cybersecurity and U.S.-China Relations.*

« [...] l'étude du fonctionnement du discours oblige à assumer le fait que le discours n'est jamais neutre, qu'il est toujours porté par des intérêts. »
Maingueneau, 2012, Que cherchent les analystes du discours ?

REMERCIEMENTS

L'écriture de ce mémoire s'est avérée un travail de longue haleine, qui n'aurait pas été possible sans l'important soutien de plusieurs de mes proches. Je tiens à les remercier chaleureusement.

Tout d'abord, je dois souligner le grand apport de mon maître à penser, le professeur Claude-Yves Charron, qui en véritable *sensei* a su me transmettre avec patience et détermination sa passion pour les enjeux politiques et diplomatiques du cyberespace. Son aide si précieuse et sa présence indéfectible ont non seulement permis la rédaction efficace de ce mémoire, mais m'ont également lancée sur une voie professionnelle parsemée de belles rencontres et de rêves nouveaux. Je récolte déjà les fruits de cette belle collaboration. Merci pour tout.

J'aimerais également remercier mes chères collègues de la maîtrise en communication internationale et interculturelle, qui se reconnaîtront, pour nos discussions enlevantes lors de nombreux soupers arrosés de *vino*, permettant comme le veut la métaphore de « laisser fermenter » la réflexion. Le partage de nos inquiétudes mutuelles m'a constamment rappelé que le chemin de la maîtrise ne peut être parcouru sans difficultés et que toutes, nous avons partagé les aléas de cette épreuve. Merci les belles filles.

Merci par ailleurs à mes parents, qui m'ont insufflé cette curiosité intellectuelle et ce désir de réalisation de soi. Je n'aurais évidemment pas réussi sans votre constant support. Et finalement, merci à mon relecteur personnel, mon coéquipier favori dans le travail comme dans la vie, sans qui ce mémoire n'aurait pas atteint le niveau actuel de précision. Merci mon amour.

TABLE DES MATIÈRES

LISTE DES ABRÉVIATIONS

ADPIC	Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce
AGNU	Assemblée générale des Nations Unies
APL	Armée populaire de libération
APT	Attaques sophistiquées persistantes
CMTI	Conférence mondiale des télécommunications internationales
FBI	Federal Bureau of Investigation
MIT	Massachussets Institute of Technology
NCCIC	National Cybersecurity and Communications Integration Center
NSA	National Security Agency
OMC	Organisation mondiale du commerce
OPM	Office of Personnel Management
PCC	Parti communiste chinois
TIC	Technologies de l'information et de la communication
UIT	Union internationale des télécommunications

RÉSUMÉ

En 2015, l'Office of Personnel Management (OPM) des États-Unis, une agence fédérale, a été victime de l'une des pires cyberattaques jamais perpétrées contre une institution gouvernementale américaine. Les autorités ont dévoilé que les données confidentielles de 21,5 millions d'Américains avaient été dérobées. Tous les yeux se sont tournés vers le gouvernement chinois, bien que celui-ci ait nié son implication. C'est dans ce contexte que le président chinois Xi a rencontré le président Obama, en septembre 2015, lors d'une réunion au Sommet aux États-Unis. Les deux dirigeants ont alors convenu de coopérer en matière de cybersécurité, sans aborder publiquement la question de la cyberattaque contre l'OPM.

Ce mémoire s'intéresse aux différentes perspectives entourant la cyberattaque contre 21,5 millions de dossiers confidentiels. Il cherche également à démontrer quelles étaient les logiques d'intérêt en présence lors de la rencontre au Sommet des présidents Xi et Obama ayant eu lieu quelques mois après l'événement.

Nous pensons que le discours de chaque gouvernement a été construit autour de l'articulation d'un message clé en termes de coopération bilatérale et de respect des normes internationales du commerce, omettant volontairement la question de la cyberattaque contre l'Office of Personnel Management. L'objectif du gouvernement américain était de convaincre la Chine de cesser ses opérations de cyberespionnage économique contre les entreprises américaines, tandis que celui de la Chine était de poursuivre sa collaboration avec les États-Unis en matière de technologie et d'innovation et d'éviter que des sanctions économiques lui soient imposées.

Sur la scène mondiale, la Chine et les États-Unis sont les plus importantes puissances du domaine du cyberespace. Les enjeux entourant l'évolution, la gouvernance et la sécurité de ce domaine émergent sont donc particulièrement sensibles au sein de leurs relations bilatérales et la cyberattaque contre l'Office of Personnel Management en est, à ce jour, l'une des principales démonstrations. Quant au discours politique entourant cet événement sans précédent, il offre un corpus riche pour une analyse approfondie du processus de construction et d'articulation d'un message clé et ce, à partir de deux perspectives idéologiques et culturelles. Nous croyons donc à l'apport de ce mémoire pour la recherche internationale en matière de cybersécurité.

MOTS CLÉS: cyberattaque, cybersécurité, analyse discursive, Chine, États-Unis

INTRODUCTION

Au tournant du 21e siècle, Internet est devenu omniprésent dans la vie de la majorité de la population mondiale, qui l'utilise dans la plupart de ses activités quotidiennes. Durant la première décennie du siècle seulement, le nombre de gens connectés à Internet est passé de 350 millions à 2 milliards (Schmidt et Cohen, 2014). Aujourd'hui, ce sont 3 milliards d'individus qui sont connectés à Internet (Eisenach *et al.*, 2016), et ce chiffre continue de s'agrandir.

Malgré la quantité de possibilités promulguées par l'évolution du cyberespace, cette révolution technologique entraîne également de nouveaux risques en matière de sécurité et de nouveaux espaces de confrontation interétatiques. Les données personnelles et confidentielles des individus, des organisations, des entreprises et des gouvernements, de même que l'ensemble des infrastructures qui reposent sur un système informatique, peuvent être corrompues par les cybermenaces grandissantes. Les activités malveillantes dans le cyberespace continuent en effet de se répandre globalement et devraient représenter pour les entreprises un coût général de 2000 milliards $US d'ici 2019 (Eisenach *et al.*, 2016).

C'est à cette problématique que nous nous intéressons, c'est-à-dire aux risques générés par le développement du cyberespace qui en font désormais un enjeu sécuritaire, et à la place prépondérante qu'il occupe au sein des relations internationales. Sur la scène mondiale, la Chine et les États-Unis sont les deux plus importantes puissances du domaine du cyberespace, à la fois en regard de leur expertise, de leurs capacités militaires et de leur nombre d'utilisateurs. Toutefois,

alors que les relations économiques de ces deux États sont très imbriquées, en termes de cyberespace elles sont davantage conflictuelles.

En juin 2015, le gouvernement des États-Unis a dévoilé publiquement que l'une de ses agences fédérales, l'Office of Personnel Management (OPM), avait été victime d'une intrusion dans ses systèmes informatiques. Un mois plus tard, le gouvernement a fait savoir que les responsables de la cyberattaque avaient mis la main sur les dossiers confidentiels de 21,5 millions d'employés du gouvernement fédéral. Dans les médias américains, cette cyberattaque a été considérée comme l'une des pires de l'histoire en matière de sécurité nationale. Bien qu'aucune accusation officielle n'ait été formulée, certaines sources anonymes ont pointé du doigt le gouvernement chinois, qui s'est empressé de dénoncer ces accusations jugées « non scientifiques » et « irresponsables ».

C'est dans ce contexte que quelques mois plus tard, le président chinois Xi Jinping a rendu visite au président Barack Obama dans le cadre d'une rencontre au Sommet, en septembre 2015. Lors de cette rencontre, l'enjeu de la cybersécurité a été propulsé à l'avant-plan. Les deux présidents ont finalement signé un *cyber agreement* au sein duquel ils ont convenu de cesser toute forme de vol de propriété intellectuelle et de secrets commerciaux. La question de la cyberattaque contre l'OPM n'a pas, quant à elle, été adressée dans le discours public des deux présidents.

C'est donc à cette cyberattaque contre 21,5 millions d'Américains, l'une des plus importantes de l'histoire du gouvernement américain, et à la rencontre au Sommet ayant suivi que ce mémoire s'intéresse. L'objectif principal est de comprendre comment s'est articulé le processus de construction du discours politique des administrations Obama et Xi entourant la cyberattaque et le Sommet de septembre 2015.

Pour ce faire, ce mémoire sera composé de quatre chapitres. Dans le premier, nous préciserons la problématique d'ensemble de cette recherche. Nous commencerons par présenter les relations sino-américaines sous Obama et Xi et comment elles ont évolué en matière de cybersécurité. Nous présenterons par ailleurs le contexte international entourant la gouvernance du cyberespace et offrirons des définitions des concepts situés au cœur de notre recherche. Nous terminerons le premier chapitre en posant nos questions de recherche et les principaux objectifs de ce mémoire.

Dans le deuxième chapitre, nous présenterons notre cadre de référence théorique constitué de quatre auteurs clés. Tout d'abord, nous partons de l'hypothèse de Berger et Luckmann (1966) sur la construction sociale de la réalité. Les deux auteurs affirment en effet que ce sont les acteurs sociaux qui construisent la réalité et le savoir, en fonction d'un certain contexte social. Ensuite, nous adoptons la posture de l'interactionnisme symbolique d'Erving Goffman et sa métaphore théâtrale sur la présentation de soi dans la vie quotidienne. Goffman (1956) affirme que les individus cherchent toujours la poursuite de leurs intérêts et que leur façon d'interagir avec autrui en découle. Dans le théâtre des interactions sociales, ce qui se déroule sur scène, devant le public, et ce qui se déroule en coulisse, diffèrent nécessairement. Par ailleurs, nous retenons la théorie de la représentation du cyberespace, abordée par Alix Desforges (2014), qui croit que le cyberespace constitue un ensemble de représentations utilisé par les gouvernements en fonction de leur logique d'intérêt. Elle affirme que le terme n'est pas neutre, mais que le sens l'entourant est construit par les acteurs politiques. Finalement, nous mobilisons la posture de Myriam Dunn Cavelty (2012, 2013), qui stipule que le lien entre « cyberespace » et « sécurité nationale » est le fruit d'un processus politique de construction sociale.

Quant au troisième chapitre, il servira à présenter notre méthodologie en termes d'analyse de discours. Nous pensons en effet que l'analyse de discours pourra nous permettre d'accéder aux différents éléments à même de répondre à nos questions de

recherche. Nous commencerons par définir le discours pour éviter toute confusion terminologique et élaborerons sur l'analyse discursive comme méthode de recherche. Nous présenterons également notre grille d'analyse et les 15 documents qui composeront notre échantillon.

Finalement, le dernier chapitre de ce mémoire sera dédié à l'analyse et à la présentation des résultats. Nous y relèverons les éléments clés des discours des administrations Obama et Xi et répondrons aux questions de recherche afin de tirer nos conclusions. Nous serons ainsi en mesure de valider notre hypothèse de recherche.

CHAPITRE I

PROBLÉMATIQUE D'ENSEMBLE

Dans cette première partie, nous tenterons de contextualiser notre objet de recherche en offrant un panorama élargi des relations entre la Chine[1] et les États-Unis pendant la présidence de Barack Obama et celle de Xi Jinping. Nous souhaitons ainsi dresser un court bilan de la relation entre les deux hommes et leur gouvernement et effectuer un tour d'horizon des principaux enjeux de cette dynamique bilatérale. Par la suite, nous entrerons plus en détail sur leurs relations en matière de cyberespace et de cybersécurité. Nous tenterons par ailleurs de rappeler l'évolution du contexte international élargi en matière de cybersécurité. Afin de préciser la terminologie relative à notre objet d'étude, nous nous efforcerons également de définir les concepts clés de notre analyse, soit les termes « cyberespace », « cyberattaque », « cybersécurité », « cyberespionnage » et « cybersouveraineté ». Le lecteur pourra ainsi utiliser ce cadre de référence terminologique afin de cerner l'objet d'étude. Puis, nous relaterons les détails de la cyberattaque contre l'Office of Personnel Management afin de comprendre son ampleur pour la sécurité nationale américaine et poursuivrons avec la rencontre au Sommet de septembre 2015. Finalement, nous poserons notre question centrale de recherche et notre hypothèse d'ensemble, ainsi que la pertinence de ce mémoire pour le domaine d'étude de la communication internationale.

---

[1] Afin de simplifier la forme du texte, nous utilisons le nom «Chine» au lieu du nom complet «République populaire de Chine».

1.1. Relations sino-américaines sous Obama et Xi

Depuis la création de la République populaire de Chine en 1949, les relations entre la Chine et les États-Unis ont été généralement conflictuelles, caractérisées par des périodes de confrontation et de méfiance mutuelles (Harold *et al.*, 2016). Cependant, à son arrivée au pouvoir en janvier 2009, l'administration Obama a rapidement déclaré la nécessité d'un changement de cap et d'un « retour en Asie », la croissance économique rapide et dynamique de l'Asie ainsi que son poids stratégique ayant augmenté son importance pour les intérêts américains (Saunders, 2013). Le terme « pivot vers l'Asie » était alors employé par l'administration Obama pour signifier un changement de direction dans la politique étrangère américaine, à l'époque davantage orientée vers le Moyen-Orient, pour se tourner vers la région asiatique. Les autorités américaines affirmaient ainsi vouloir renforcer leurs relations avec l'Asie, dont la Chine était le principal partenaire visé.

Pour ce faire, de nouveaux espaces de coopération avec la Chine ont été mis de l'avant dans les rencontres entre les leaders américains et chinois. L'objectif était notamment de gagner la confiance et le respect des autorités chinoises:

> [...] *highlighting areas of cooperation and praising positive Chinese contributions, encouraging a greater Chinese role in global governance, seeking continuity in military-to-military relations to help avoid crises and increase cooperation* [...] (Saunders, 2013).

Par contre, ces motivations américaines étaient plutôt mal perçues au départ par les leaders chinois, qui y voyaient une tentative américaine de renforcer le contrôle des États-Unis sur l'ordre international. Toutefois, à l'arrivée de Xi Jinping en tant que secrétaire général et président de la commission militaire centrale du Parti communiste chinois (PCC) en novembre 2012, puis comme président de la

République populaire de Chine en mars 2013, une ouverture à la coopération sino-américaine s'est graduellement installée. En effet, Xi Jinping a fait valoir cette volonté d'instaurer un climat positif et coopératif avant même son ascension à la tête du PCC. Lors de son voyage aux États-Unis en 2012, alors que Xi Jinping était vice-président de la Chine, il a appelé à un « nouveau type de relations entre deux pays majeurs du 21^{e} siècle », considérant ainsi qu'un conflit n'était pas inévitable entre la Chine et les États-Unis et qu'il fallait suivre la voie de la coopération (Lampton, 2013).

Par la suite, le président Xi a réitéré son optimisme quant à la construction d'une telle relation lors d'une rencontre avec le président Obama en Californie en juin 2013[2]. Il a alors affirmé qu'il existait d'énormes espaces pour davantage de coopération entre la Chine et les États-Unis: « *Xi also stressed that the way to construct such a new great power relationship is to strengthen dialogue, enhance mutual trust, develop cooperation, and manage differences* » (Wu, 2014, p.66).

La Chine est ainsi devenue dans les dernières années l'un des principaux partenaires économiques des États-Unis. Selon le département d'État américain, les échanges entre la Chine et les États-Unis ont passé de 33 milliards $US en 1992, à 659 milliards $US en 2013. La Chine est aujourd'hui le 3e marché d'exportation américain, tandis que les États-Unis sont le premier marché des exportations chinoises (U.S. Department of State, 6 décembre 2016). Les deux États ont donc développé une relation complexe d'interdépendance.

Toutefois, si tout semblait indiquer la volonté réciproque des États-Unis et de la Chine de renforcer leurs relations bilatérales et d'y inscrire davantage de coopération,

---

[2] Cette première rencontre au Sommet entre les deux présidents sera abordée plus en détail un peu plus loin.

quelle place les enjeux de sécurité occupaient-ils au sein de ce « nouveau type de relations »?

Selon Duchâtel (2013), « un dilemme de sécurité sino-américain est identifié depuis des années », c'est-à-dire « comment éviter une guerre entre une puissance de statu quo déclinante et une puissance émergente et révisionniste » (p.174). Si, tel que mentionné plus haut, un conflit n'est toutefois pas considéré comme inévitable et une volonté de coopération se fait sentir de la part des deux administrations, il demeure que certains enjeux sécuritaires viennent en effet ternir ce « nouveau type de relations entre grandes puissances ». La question de la Corée du Nord, celle des droits humains, les disputes territoriales de la Chine et surtout celle concernant Taïwan, la rivalité militaire entre les deux pays et finalement, la cybersécurité font partie des enjeux sécuritaires sur lesquels les États-Unis et la Chine possèdent des différends. Afin de maintenir leurs échanges économiques et leurs bonnes relations, la Chine et les États-Unis doivent ainsi réussir à trouver un terrain d'entente pour chacun de ces enjeux. Selon Wu (2014), la réussite de la création d'un nouveau modèle de relations entre les deux puissants États repose sur la gestion efficace de leurs différends quant à ces enjeux clés.

Parmi ces enjeux, la question de la cybersécurité est certainement l'un des plus importants: « *Indeed, of all the areas where the relationship between the two sides is troubled, cyberspace has been one of the most contentious* » (Harold *et al.*, 2016, preface). En effet, à peine après avoir entamé des négociations formelles en 2013 afin de résoudre leurs différences en regard du cyberespace, les deux États y ont mis fin en 2014 en réponse aux accusations américaines de cyberespionnage envers des militaires chinois. C'est justement à la question plus précise du cyberespace que la prochaine section s'attardera en profondeur.

1.1.1. Relations en matière de cybersécurité

Sur le plan de la cybersécurité, la Chine et les États-Unis ont depuis de nombreuses années des relations tumultueuses. Les tensions sont vives entre les deux États, et pourtant ils jouent un rôle de plus en plus significatif sur la scène internationale en regard du cyberespace. Comme l'affirment Lieberthal et Singer (2012): « *There is perhaps no relationship as significant to the future of world politics as that between the U.S. and China. And in their relationship, there is no issue that has risen so quickly and generated so much friction as cybersecurity* » (p. vi). C'est que la Chine et les États-Unis sont les deux plus importantes puissances en matière de cyberespace, tout en étant de grands partenaires économiques. Malgré le fait que les enjeux entourant le cyberespace soient récents dans l'histoire des relations sino-américaines, il semble qu'ils soient devenus un défi pour leur relation aussi important que le sont traditionnellement les échanges économiques, les droits humains et les disputes territoriales régionales (Lieberthal et Singer, 2012).

La Chine et les États-Unis possèdent en effet des visions très différentes sur le développement du cyberespace. « *The two countries also have different perspectives on the roles played by norms and the legitimacy of state actions used to enforce such norms* » (Harold *et al.*, 2016, *Summary*). Ces différences expliquent pourquoi les relations sino-américaines en regard du cyberespace tendent à être conflictuelles et pourquoi la cybersécurité peut être considérée comme un risque important pour leurs relations.

À partir de juin 2012 et jusqu'à juin 2013, trois événements majeurs ont aggravé les relations sino-américaines en matière de cybersécurité: la découverte du virus

Stuxnet, les activités de cyberespionnage[3] chinoises et les révélations Snowden. Cette période est considérée par l'expert en géopolitique du cyberespace Adam Segal comme « l'An Zéro » dans la bataille du cyberespace. La tension entre la Chine et les États-Unis a ainsi atteint son paroxysme pendant cette année charnière.

Nous commencerons donc en abordant l'historique des relations sino-américaines en matière de cybersécurité précédant la cyberattaque contre l'Office of Personnel Management des États-Unis. Pour ce faire, nous tracerons l'évolution de l'enjeu de la cybersécurité selon chacune des perspectives, celles du gouvernement Obama et du gouvernement Xi, en développant sur chacun des trois événements majeurs de l'An Zéro. Cette mise en contexte essentielle permettra ainsi d'offrir au lecteur un éclairage sur la vision respective que la Chine et les États-Unis ont de cet enjeu et de leur relation bilatérale l'entourant.

1.1.2. La perspective du gouvernement américain

Dès son arrivée au pouvoir en 2009, le président Barack Obama a mis la cybersécurité au cœur de ses priorités. Lors d'une déclaration prononcée le 29 mai 2009 sur l'importance de sécuriser les cyberinfrastructures de la nation[4], il a ainsi affirmé:

> *This world -- cyberspace -- is a world that we depend on every single day. It's our hardware and our software, our desktops and laptops and cell phones and Blackberries that have become woven into every aspect of our lives. It's the broadband networks beneath us and the wireless signals around us, the local networks in our schools and hospitals and businesses,*

---

[3] Le terme cyberespionnage sera défini en détail à la section 1.3.5.

[4] Cette déclaration fait justement partie de l'échantillonnage à l'analyse dans ce mémoire.

> *and the massive grids that power our nation. It's the classified military and intelligence networks that keep us safe, and the World Wide Web that has made us more interconnected than at any time in human history* (Obama, 29 mai 2009).

En 2011, les États-Unis ont par la suite dévoilé leur toute première Stratégie internationale du cyberespace (*International Strategy for Cyberspace*), au sein de laquelle ils ont énoncé leurs principes d'action et leurs priorités en matière de cyberespace, soit la liberté d'expression, le respect de la vie privée et la libre circulation de l'information. Ce document affirme également que les États-Unis ont pour intérêt national un Internet ouvert, interopérable[5], sécuritaire et fiable qui permet le commerce international, le développement économique et l'innovation, qui renforce la sécurité internationale et qui fait la promotion de la liberté d'expression (The White House, 2011). Par ailleurs, leur stratégie internationale fait état des principaux défis en termes de cybermenaces envers non seulement la sécurité nationale, mais également envers la paix et la sécurité mondiale. Ils situent ainsi la coopération internationale comme principe premier de l'atteinte de leurs objectifs. Pour ce faire, ils affirment que l'État de droit (*Rule of Law*) doit être appliqué au cyberespace et que des normes comportementales doivent guider les actions des États.

C'est alors qu'un premier événement majeur survient sur la scène internationale. Selon Segal (2016), l'An Zéro a débuté avec la découverte du virus Stuxnet, un « logiciel malicieux » créé par les États-Unis en collaboration avec Israël, qui a réussi à s'attaquer aux infrastructures du programme nucléaire iranien. En infectant les systèmes de contrôle de l'installation iranienne située à Natanz, le virus a détruit

---

[5] L'interopérabilité est la capacité que possède un système ou un produit à fonctionner avec d'autres produits ou systèmes existants ou futurs, sans restriction d'accès ou de mise en œuvre (Larousse, 2017b).

environ un cinquième des centrifugeuses d'uranium, ayant pour effet de retarder le programme d'enrichissement nucléaire iranien d'au moins deux ans (Eisenach *et al.*, 2016). Cette cyberattaque était notable sur deux plans: non seulement le virus démontrait une grande ingéniosité et un niveau élevé de sophistication, mais il avait aussi réussi à pénétrer des ordinateurs non connectés à Internet. En effet, contrairement aux autres virus de l'époque, celui-ci ne visait pas l'infection du plus grand nombre d'ordinateurs possible, mais une cible bien précise et ne pouvait donc pas infecter plus de trois ordinateurs. Il était également muni d'un mécanisme d'autodestruction, signifiant que les créateurs du virus ne souhaitaient pas qu'il se propage indéfiniment (Singer et Friedman, 2014). Finalement, il a été démontré par la suite que le virus avait été transporté par les ordinateurs et les clés de mémoire (disques amovibles) personnels des scientifiques travaillant à la centrale (Singer et Friedman, 2014). Le virus Stuxnet a ainsi opéré un point tournant en matière de cyberattaque, démontrant la capacité d'un État à s'en prendre à des cibles physiques et à les endommager, ainsi que la volonté américaine de développer des capacités offensives en lien avec le cyberespace. Cet événement a permis de constater que malgré son appel à la coopération internationale et à l'établissement de normes guidant les comportements dans le cyberespace, le gouvernement américain s'est affairé à développer ses cybercapacités offensives.

Toutefois, pendant cette même période, les États-Unis étaient également victimes de cyberattaques de leur côté, provenant principalement de la Chine. Des hackers[6] chinois conduisaient en effet une campagne massive de cybervols contre les firmes technologiques américaines. En juillet 2012, le général Keith Alexander, directeur de la National Security Agency (NSA), a qualifié le cyberespionnage chinois contre les

[6] Le dictionnaire en ligne Larousse définit le terme « hacker » comme une personne qui, par jeu, goût du défi ou souci de notoriété, cherche à contourner les protections d'un logiciel, à s'introduire frauduleusement dans un système ou un réseau informatique (Larousse, 2015).

compagnies américaines de « plus grand transfert de richesse de l'histoire »[7] et estimé que les compagnies américaines avaient perdu 250 milliards $ en information volée et un autre 114 milliards $ en dépenses reliées (Segal, 2016, p.7). Les États-Unis reprochaient ainsi à la Chine de conduire des cyberattaques visant des cibles économiques.

En 2013, le rapport de l'entreprise de cybersécurité Mandiant a dévoilé l'étendue des cyberattaques chinoises en sol américain. « Le rapport de la société Mandiant a dénoncé des attaques sophistiquées persistantes (APT[8]) ciblant 141 entreprises dans le monde dont 115 aux États-Unis, qui auraient permis de dérober des centaines de téraoctets d'information, depuis au moins 2006 » (Douzet, 2013, p.44). De plus, ce rapport a conclu que le Parti communiste chinois avait chargé l'Armée populaire de libération (APL) de commettre un cyberespionnage systématique ainsi que des vols de données contre différentes organisations dans le monde, en citant les activités de l'Unité 61398 de l'armée chinoise (Mandiant, 2013). Ce rapport confirmait ainsi l'implication de la Chine dans de nombreuses cyberattaques envers les États-Unis et venait renforcer la perception américaine d'une importante cybermenace chinoise.

Dans son rapport annuel au congrès en 2013, le bureau du secrétaire américain à la défense a ainsi accusé le gouvernement chinois d'employer une stratégie visant le cyberespace pour la poursuite de ses objectifs stratégiques et pour le vol de propriété intellectuelle. « *These exploits, the report contends, can be used to benefit China's defence industry, high technology industries and the broader interests of Chinese policy makers* » (Shull, 2014, p.4).

---

[7] Traduction libre: *greatest transfer of wealth in history.*

[8] L'acronyme APT renvoie à la formulation anglophone « *Advanced Persistent Threats* ». Selon Singer et Friedman (2014), les APT sont le fruit d'une équipe fort bien organisée et combinent information, complexité et patience, visant toujours au départ une cible précise (p.56).

Finalement, il va sans dire que le cyberespace est un espace de développement économique important aux États-Unis. Les compagnies américaines dominent en effet l'économie mondiale d'Internet, alors que les États-Unis « représentaient 25% des revenus globaux de télécommunications en 2015 », ainsi que « près de 25% de l'économie du web des pays du G20 [9]» (Segal et Tang, 2016, p.46).

En résumé, selon le rapport cité précédemment, le principal enjeu dominant la perspective du gouvernement américain se rapporte au cyberespionnage économique chinois. Les États-Unis reprochent à la Chine de multiplier ses intrusions dans les réseaux des entreprises privées américaines afin d'effectuer des vols de propriété intellectuelle, de secrets commerciaux et d'informations confidentielles. La représentation de la cybermenace chinoise a ainsi occupé une place graduellement prépondérante au sein du discours stratégique américain (Douzet, 2013). Bien que les États-Unis reconnaissent qu'Internet soit un puissant outil de développement économique et de prospérité, duquel ils bénéficient grandement, ils y voient aussi un espace aux nombreuses vulnérabilités, générateur de multiples menaces, dont la plus inquiétante provient de la Chine.

1.1.3. La perspective du gouvernement chinois

En 2010, la Chine a dévoilé son premier livre blanc sur Internet, *The Internet in China*, faisant état de la situation d'Internet en Chine et de la vision du gouvernement en ce qui concerne le cyberespace. Le document stipule:

---

[9] Traduction libre: *U.S. technology companies dominate the global Internet economy, with the United States accounting for 25% of global telecom revenue in 2015 and capturing close to 25% of the G-20's Internet economy.*

> *The Chinese government fully understands the Internet's irreplaceable role in accelerating the development of the national economy, pushing forward scientific and technological advancement, and expediting the informational transformation of social services, and places emphasis on and actively supports Internet development and application* (PRC, 8 juin 2010).

Ce même document mentionne également que la Chine s'oppose à toute forme de cyberattaque et que la Chine est l'un des pays souffrant le plus des cyberattaques (PRC, 8 juin 2010).

Par ailleurs, la Chine a constamment nié les accusations américaines de cyberespionnage, affirmant qu'elle était aussi victime de cyberespionnage, que les accusations étaient non fondées et que les États-Unis ne disposaient pas de preuves suffisantes. « *It is unprofessional and groundless to accuse the Chinese military of launching cyber attacks without any conclusive evidence* » (Ministre chinois de la défense, 2013, cité dans Mandiant, 2013).

Puis, en juin 2013, la situation s'est aggravée lors de la diffusion des révélations de l'ancien consultant de la NSA Edward Snowden (Segal, 2016). Le journal anglais *The Guardian* avait alors publié une série d'articles démontrant les activités de surveillance et d'espionnage de la NSA à la fois sur les citoyens américains et sur des pays adversaires ou même alliés[10]. Ces révélations ont eu un impact majeur sur les relations internationales et la géopolitique du cyberespace. La Chine, de même que la

[10] Les révélations d'Edward Snowden ont notamment démontré qu'en utilisant un programme nommé PRISM, la NSA était en mesure d'avoir accès aux données entreposées chez la plupart des géants technologiques américains tels que Google, Apple, Facebook et Microsoft. Cet accès lui permettait ainsi de recueillir et d'analyser les courriels, textos, conversations, appels téléphoniques, publications Facebook, tweets et autres documents des individus à la grandeur de la planète entière (Segal, 2016).

Russie et d'autres pays, a utilisé les programmes de surveillance américains dans son argumentaire visant le contrôle d'Internet par les États-Unis[11] (Segal, 2016).

Selon la Chine, les révélations de Snowden ont par ailleurs suggéré que la NSA avait conduit plusieurs cyberattaques contre des cibles chinoises (Wu, 2014). La Chine a alors affirmé que ses systèmes informatiques étaient même davantage victimes d'attaques que les systèmes américains. Plusieurs auteurs et agents officiels chinois ont par ailleurs soutenu que la grande majorité des cyberattaques subies par la Chine étaient d'origine américaine, stipulant qu'elle avait été la cible d'au moins 34 000 attaques américaines (Lieberthal et Singer, 2012). Les critiques du président Obama concernant le cyberespionnage économique chinois ont donc été amoindries par ces révélations.

En 2014, lors de la première rencontre du *Central Network Security and Informatization Leading Group* de Chine, le président Xi a affirmé que « la sécurité des réseaux et de l'information est un enjeu stratégique majeur relié à la sécurité nationale » et qu'il ne pouvait y avoir de « sécurité nationale sans cybersécurité » (Segal et Tang, 2016, p.53). Selon Segal et Tang, il s'agissait de la première fois que la Chine situait la cybersécurité au plus haut niveau de ses priorités. Parmi les principales menaces à la sécurité nationale, la Chine reconnaissait alors les cyberattaques financées par les États-nations, les activités illégales en ligne visant notamment la stabilité du régime, le cyberterrorisme et la cyberguerre.

Le 1er juillet 2015, la Chine a adopté sa Loi nationale de sécurité (*National Security Law of the People's Republic of China*). Quelques jours plus tard, soit le 6 juillet 2015, elle a dévoilé la première version de sa Loi sur la cybersécurité (*Cybersecurity Law of the People's Republic of China*), clarifiant ainsi pour la première fois

[11] La question de la gouvernance d'Internet sera abordée à la section 1.2 sur le contexte international du cyberespace.

l'importance de la cybersécurité dans un document juridique (Segal et Tang, 2016). Cette loi a qualifié les menaces du cyberespace de risque imminent et sévère pour la sécurité nationale:

> Article 1: *This Law is formulated so as to ensure cybersecurity, to preserve cyberspace sovereignty, national security and societal public interest, to protect the lawful rights and interests of citizens, legal persons and other organizations, and to promote the healthy development of economic and social informatization* (China Law Translate, 6 juillet 2015).

Quant à sa position sur le développement et la gouvernance d'Internet, la Chine poursuit un agenda clair de promotion des concepts de cybersouveraineté [12] (contrôle des systèmes et du contenu en territoire chinois) et de sécurité de l'information. Elle argumente en effet que les compagnies informatiques étrangères souhaitant entrer en sol chinois doivent se soumettre aux lois et aux réglementations de la Chine, afin de protéger ses réseaux. Or, bien que les compagnies chinoises ne tentent de rattraper le niveau avancé de l'innovation technologique étrangère dans le domaine des technologies de l'information et de la communication (TIC), elles continuent d'être supplantées. Les fonctionnaires chinois sont donc conscients que pour un certain temps encore, la Chine dépend pour son développement économique et technologique des systèmes informatiques provenant de l'étranger (Inkster, 2016). La Chine doit ainsi trouver un équilibre entre la cybersouveraineté effective et l'impératif d'avoir accès aux technologies avancées provenant de l'étranger, nécessaires à la réussite de ses objectifs économiques et sociaux (Inkster, 2016).

Ainsi, la perspective chinoise quant à la position américaine en matière de cyberespace est plutôt hostile. La Chine considère que les États-Unis, en se portant à la défense de la liberté d'Internet et des droits humains en ligne, visent directement la Chine (Segal et Tang, 2016). Elle argumente également qu'elle est fait partie des

[12] Le concept de cybersouveraineté sera défini en détail à la section 1.3.4.

principales victimes de cyberattaques. Elle tente donc de son côté d'accroître ses propres cybercapacités (militaires ou autres) afin de s'éloigner de sa dépendance vis-à-vis des entreprises américaines et d'assurer la protection de ses réseaux informatiques et de sa sécurité nationale. En terminant, elle se défend de conduire toute forme de cyberattaque et nie toute accusation de cyberespionnage, qu'il soit économique ou politique.

1.1.4. Une première rencontre au Sommet Obama-Xi

Deux jours après le premier rapport Snowden publié par *The Guardian*, les présidents américain Barack Obama et chinois Xi Jinping se sont rencontrés à Sunnylands, en Californie, du 7 au 8 juin 2013 pour un court Sommet dans le but de construire une relation interpersonnelle et de diminuer leur manque de confiance réciproque (Segal, 2016). Le président Obama a alors affirmé avoir eu une conversation directe avec le président Xi concernant la cybersécurité :

> *Despite all the efforts at diplomatic bonhomie, President Obama told Charlie Rose that they had had "a very blunt conversation about cybersecurity" and that he had warned President Xi that hacking could "adversely affect the Fundamentals of the US-China relationship"* (Segal, 2016, p.8).

De même, le président Xi a affirmé, lors de la conférence de presse tenue le 7 juin 2013 en compagnie du président Obama, que la Chine et les États-Unis partageaient des préoccupations communes en matière de cybersécurité:

> Nous sommes parvenus à établir un groupe de travail sur Internet dans le cadre du Dialogue sino-américain concernant la sécurité stratégique pour accélérer les recherches sur ce problème. Nous devons de part et d'autre

> éliminer les soupçons et entreprendre des coopérations pour que la cybersécurité devienne le nouveau point d'attrait de la coopération sino-américaine (Xi, 7 juin 2013).

Les États-Unis et la Chine ont ainsi créé un dialogue bilatéral formel à propos du cyberespace en 2013 et instauré un groupe de travail sur la cybersécurité. Le *US-China Cybersecurity Working Group*, dont la création a été annoncée en avril 2013 par le secrétaire d'État américain John Kerry lors d'une rencontre avec le ministre des Affaires étrangères chinois Wang Yi, à Beijing. Ce groupe de travail avait pour objectif « d'accélérer les actions pour prévenir les cyberattaques »[13] (Reuters, 13 avril 2013).

Toutefois, la Chine y a mis un terme à peine un an plus tard, en 2014, alors que les États-Unis ont accusé cinq officiers chinois de l'Armée populaire de libération (APL) d'avoir conduit du cyberespionnage contre des entreprises américaines (Harold *et al.*, 2016 ; Shull, 2014). Les conclusions du rapport Mandiant de 2013 étaient sans doute à l'origine de ces accusations, alors que les officiers accusés par le département de la Justice américain étaient des membres de l'Unité 61398, dévoilée par le rapport (NY Times, 19 mai 2014).

Les cinq individus ont été reconnus coupables par la justice américaine de 31 chefs d'accusation, incluant piratage informatique, espionnage économique, conspiration pour commettre fraude et abus, vol de secrets commerciaux et vol d'identité (Shull, 2014). Ces accusations constituaient une action davantage symbolique, puisqu'il n'existait aucune chance que la Chine ne livre cinq membres de son armée aux États-Unis. Le procureur général des États-Unis Eric Holder a tout de même affirmé que les cyberattaques n'avaient été conduites pour aucune autre raison que pour avantager les

---

[13] Traduction libre: *speed up action to prevent hacking attacks.*

compagnies chinoises et les autres intérêts de la Chine, aux dépens des entreprises américaines (BBC News, 19 mai 2014).

Comme de fait, la Chine a rejeté les accusations contre les cinq militaires, demandant qu'elles soient retirées et affirmant qu'elles violaient les normes de base gouvernant les relations internationales et qu'elles mettaient à risque la coopération sino-américaine (Shull, 2014).

C'est donc dans ce contexte tendu de méfiance et d'attaques réciproques que les relations sino-américaines en matière de cybersécurité ont évolué à partir de juin 2012 jusqu'à la cyberattaque contre l'Office of Personnel Management de 2015. Beijing et Washington possèdent des différences significatives dans leur vision de l'ouverture d'Internet, des cyberattaques et des normes d'action dans le cyberespace et de la gouvernance d'Internet (Segal et Tang, 2016). Le résultat est que chacun perçoit l'autre comme un important, sinon le principal, compétiteur dans la poursuite de ses intérêts dans le cyberespace.

1.2. Contexte international entourant la cybersécurité

Jusqu'à présent, les débats internationaux persistent en matière de gouvernance du cyberespace. Les États n'ont pas de vision commune de la façon de faire et bien que plusieurs tentatives aient eu lieu afin de déterminer une organisation qui serait en charge d'établir les règles en matière de cyberespace, aucune ne s'est concrétisée.

Selon Roxana Radu (2014), outre lors de rencontres bilatérales, les principales discussions internationales en matière de cyberespace se sont déroulées au sein des organes des Nations Unies. Bien que plusieurs organes de l'ONU se soient attardés à

la question de la protection du cyberespace[14], les plus importantes discussions en matière de sécurité ont eu lieu à l'Assemblée générale des Nations Unies (AGNU) qui regroupe l'ensemble des 193 membres. Selon Radu, l'une des premières fois où l'AGNU a abordé la question de la sécurité du cyberespace fut en 1998, alors que les membres y avaient discuté d'une résolution sur le développement du champ de l'information et des télécommunications dans le contexte de la sécurité internationale. L'AGNU avait alors tracé un lien direct entre les technologies de l'information et la sécurité.

Or, comme l'expliquent Singer et Friedman (2014), plusieurs États (dont la Chine), ont par la suite manifesté leur désir de voir accorder à l'Union internationale des télécommunications (UIT) le rôle d'organisation internationale responsable du cyberespace. Lors de la Conférence mondiale des télécommunications internationales (CMTI), ayant eu lieu à Dubai, en 2012, l'idée a été mise de l'avant par ces États: « *At the meeting, nations like Russia, China, Sudan, and others pushed for the Internet to be included in the ITU's responsibilities, giving countries the right to manage how the Internet was structured* » (Singer et Friedman, 2014, p.183). Cependant, les États-Unis et d'autres États occidentaux n'approuvaient pas l'idée que la gouvernance d'Internet repose entièrement entre les mains des États, ce qui défiait le modèle multipartite (*multi-stakeholder*) préconisé, craignant que des États puissent ainsi contrôler l'accès à l'Internet même en dehors de leurs frontières et étendre leur surveillance sur le web (Signer et Friedman, 2014 ; Segal, 2016). La conférence de Dubai a ainsi rappelé à la communauté internationale sa division et l'existence de différentes conceptions en matière de gouvernance du cyberespace.

[14] La protection du cyberespace a été adressée à différents organes de l'ONU, dont le UN Institute for Disarmament Research (UNIDIR), le UN Global Alliance for ICT and Development (UN-GAID), l'Internet Governance Forum et l'Union internationale des télécommunications (UIT) (Radu, 2014).

Par ailleurs, en matière de droit international, il n'existe à ce jour encore aucune convention ou traité internationaux dictant les normes de conduites dans le domaine du cyberespace. Certains États argumentent qu'une convention abordant les comportements admissibles en regard du cyberespace, telle une « cyber Convention de Genève[15] », serait requise (Singer et Friedman, 2014), mais ils ne s'entendent pas sur les éléments qu'une telle convention devrait aborder. En effet, les puissants États du cyberespace ont chacun des intérêts bien différents et ne voient pas la signature d'un tel traité international de la même façon.

Ainsi, en l'absence d'une convention adressant directement le cyberespace, certains affirment que plusieurs normes actuelles peuvent être appliquées au cyberespace. Notamment, le réflexe général est de se tourner vers la Charte des Nations Unies (1945), particulièrement vers son article 2(4), pour l'interprétation des comportements inappropriés dans le domaine du cyberespace. L'article prévoit que :

> Les Membres de l'Organisation s'abstiennent, dans leurs relations internationales, de recourir à la menace ou à l'emploi de la force, soit contre l'intégrité territoriale ou l'indépendance politique de tout Etat, soit de toute autre manière incompatible avec les buts des Nations Unies (Charte des Nations Unies, 1945, article 2(4)).

Par contre, en ce qui concerne le cyberespace, les États ne s'entendent pas sur ce qui peut être défini comme « l'emploi de la force ». De même, plusieurs affirment que le cyberespace ne possède pas de frontières claires, et donc qu'il est impossible de déterminer ce qui est considéré comme « l'intégrité territoriale » d'un État dans le domaine du cyberespace. Il faut minimalement qu'une cyberattaque soit suffisamment grave et qu'elle cause des dommages physiques importants pour être assimilée à un « recours à la force », ce qui ne semble pas avoir été le cas jusqu'à aujourd'hui. Ainsi, la

---

[15] Les Conventions de Genève sont des traités internationaux qui dictent les règles de conduite des conflits armés.

grande majorité des cyberattaques ne peuvent être adressées par l'article 2(4) de la charte, et tombent alors dans un flou juridique international.

1.3. Définition des termes clés

Afin de situer le lecteur, il importe, pour la suite de l'analyse, de préciser quelques-uns des concepts clés qui seront abordés dans ce mémoire. Nous offrirons donc dans cette section une définition sommaire des termes « cyberespace », « cyberattaque », « cybersécurité », « cybersouveraineté » et « cyberespionnage ». Ces concepts se retrouvent en effet au cœur de notre analyse et c'est pourquoi nous pensons qu'il est nécessaire que nous en précisions notre interprétation, issue de notre revue de littérature.

1.3.1. Cyberespace

C'est le professeur Norbert Wiener du Massachussets Institute of Technology (MIT) qui a créé le terme « cybernétique », qu'il a défini en 1948[16] comme le champ entier de la théorie de la commande et de la communication. Suivant l'évolution des technologies de l'information et de la communication (TIC) ayant eu lieu à compter de la fin du 20e siècle, le préfixe « cyber » a été graduellement utilisé dans la construction d'une panoplie de termes relatifs à la société de l'information (Arpagian, 2015).

C'est le cas du « cyberespace », défini par Thomas L. Friedman (2007) comme un

[16] Wiener, N. (1948). *Cybernetics*, Paris, Hermann.

espace d'information où les ordinateurs sont reliés ensemble et forment des réseaux. Selon Friedman, le terme cyberespace peut également être employé comme un synonyme du mot « Internet ». Quant à lui, Westcott (2008) définit Internet comme un moyen de communication qui permet la publication, l'échange et l'emmagasinage de l'information. En jumelant ces deux perspectives, on obtient que le cyberespace puisse être à la fois perçu comme un nouveau monde virtuel et comme un nouveau moyen de communication.

1.3.2. Cyberattaque

En ce qui concerne le terme cyberattaque, dans son interprétation la plus réduite, il peut être simplement considéré comme « l'association de « cyberespace » et d'« attaque » (Ventre, 2011, p.51). Dans son ouvrage Cyberattaque et Cyberdéfense (2011), l'auteur Daniel Ventre dresse en effet un éventail de définitions possibles du terme cyberattaque, qu'il est finalement possible de réduire à une simple définition : une agression menée à la fois dans le cyberespace et contre le cyberespace. Dans cette optique, une cyberattaque peut faire référence à un large spectre d'actions. Selon Moens *et al.* (2015), il s'agit tout autant de l'accès non autorisé à de l'information privilégiée, de la perturbation ou l'arrêt des systèmes technologiques, de même que de la destruction ou les dommages physiques pouvant être administrés aux infrastructures. Par ailleurs, en raison de la dimension transfrontalière du cyberespace, il n'existe pas de limite géographique aux cyberattaques, qui peuvent être lancées de n'importe quel endroit et qui possèdent un potentiel d'infliger de grands dommages aux pays visés (Gendron et Rudner, 2012).

Précisons également que l'attribution d'une cyberattaque ou l'origine d'une intrusion est particulièrement difficile à déterminer. Selon Schmidt et Cohen (2014), il est à

l'heure actuelle presque impossible de retracer l'auteur d'une cyberattaque et donc de prouver avec certitude son identité. Les cyberattaques deviennent ainsi doublement intéressantes pour les États, qui d'un côté peuvent obtenir de l'information cruciale grâce à un vol de données confidentielles, et de l'autre n'ont pas besoin de craindre de représailles puisque leur culpabilité ne peut être établie. Schmidt et Cohen (2014) affirment ainsi que la cyberattaque est en quelque sorte devenue la meilleure arme des États : puissante, sur mesure et anonyme. « *States will do things to each other online that would be too provocative to do off-line* » (Schmidt et Cohen, 2014).

1.3.3. Cybersécurité

En ce qui concerne la cybersécurité, elle peut se définir simplement comme la façon de se prémunir contre ces différentes cybermenaces. Selon Bauer et Dutton (2014), la cybersécurité concerne l'ensemble des technologies, processus et politiques qui aident à prévenir ou à réduire l'impact négatif d'événements survenant dans le cyberespace, résultant d'actions délibérées de la part d'un acteur malveillant. À cette définition, Arpagian (2015) ajoute l'ensemble des usages à la fois défensifs et offensifs des systèmes d'information.

Pour les coauteurs de *Cybersecurity and Cyberwar* (2014), Singer et Friedman, la notion de sécurité doit nécessairement être associée à la présence d'un adversaire. Selon eux, un cyberproblème ne devient un problème de cybersécurité que lorsqu'un adversaire essaie d'obtenir quelque chose, « [...] *whether to obtain private information, undermine the system, or prevent its legitimate use* » (Signer et Friedman, 2014, p.34).

1.3.4. Cybersouveraineté

Le terme cybersouveraineté est principalement employé par les gouvernements qui désirent exercer un contrôle du cyberespace à l'intérieur de leurs frontières étatiques. Il est donc mis de l'avant par ces gouvernements comme un principe de gouvernance du cyberespace. Il peut être défini comme « le droit de chaque État d'appliquer ses propres idées et lois sur son cyberespace » (The Diplomat, 18 mai 2016). Le terme est directement issu de la jonction entre « cyberespace » et « souveraineté ». Le dernier renvoie au principe de souveraineté des États, reconnu en droit international comme l'indépendance en regard d'une portion du globe, c'est-à-dire le droit d'exercer sur ce territoire les fonctions d'un État, à l'exclusion de tout autre État [17] (Maftei, 2015).

Le terme a d'abord vu le jour en référence à plusieurs gouvernements du Moyen-Orient, qui censuraient le contenu disponible sur Internet considéré religieusement immoral ou socialement inacceptable (The Diplomat, 18 mai 2016). Or, en 2015, la Chine en a officiellement fait son cheval de bataille pour la gouvernance du cyberespace. Le directeur de l'administration du cyberespace de Chine, Lu Wei, a en effet publié un éditorial sur la question ayant pour titre « *Cyber Sovereignty Must Rule Global Internet* ». Dans ce texte, il affirme que les États-Unis et la Chine ne s'entendent pas sur plusieurs points en regard du cyberespace, notamment quant à la gouvernance du cyberespace:

> [...] *the U.S. advocates "multi-stakeholders" while China believes in "multilateral." "Multi-stakeholder" refers to all Internet participants on an equal footing making the rules and is considered more "people-centered" while "multilateral" refers to the state making the rules based*

[17] Traduction libre: *Sovereignty in the relations between States signifies independence; Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State.*

> *on the idea of the sovereignty of the nation-state representing its citizens* (Lu, 2015).

Selon un rapport sur la coopération en matière de cybersécurité entre les États-Unis et la Chine produit par un groupe de chercheurs de l'Université Columbia, les Chinois sont donc « tout autant concernés par la souveraineté dans l'arène virtuelle qu'ils le sont dans les arènes physiques. Ils voient le cyberespace comme une collection de différentes juridictions au lieu d'un espace commun et global devant être utilisé et contrôlé conjointement »[18] (Adelson *et al.*, 2014, p.10).

Par ailleurs, l'approche de la Chine (comme celles d'autres États autoritaires) en matière de cybersouveraineté vise à ce qu'elle puisse contrôler ses politiques internes du cyberespace, particulièrement en ce qui concerne le contenu qui y circule afin de censurer les discours dissidents. « *Their focus on information security is based on the Soviet-era concept of information warfare, in which a state secures its information space to ensure that its narrative goes unchallenged* » (Inkster, 2016, p.10).

Outre la Chine, la Russie semble aussi resserrer son contrôle du cyberespace en son territoire et se porterait donc en faveur de la promotion de la notion de cybersouveraineté (The Diplomat, 18 mai 2016). Le terme n'est donc pas employé par tous les États, mais plutôt par ceux qui souhaitent d'une façon ou d'une autre diminuer l'influence des États-Unis sur le cyberespace et conserver une main mise sur leur territoire et leurs citoyens, même en ce qui a trait à leurs activités numériques.

---

[18] Traduction libre : *The Chinese are just as concerned about sovereignty in virtual arenas as they are in physical ones. Cyberspace is seen as a collection of jurisdictions, rather than a common, global space to be jointly used and controlled.*

1.3.5. Cyberespionnage

Le cyberespionnage est en fait un nouveau moyen pour les États d'acquérir de l'information stratégique. Selon Bauer et Dutton (2014), le cyberespionnage se définit comme de l'espionnage gouvernemental ou industriel par l'accès illégal à des courriels ou à des systèmes informatiques. Ils ajoutent que les opérations de cyberespionnage peuvent ne jamais être détectées, puisqu'elles ne causent pas de dommages observables sur les systèmes. Pour Singer et Friedman (2014), « *cyber espionage is the use and targeting of computers to obtain a secret of some sort* » (p.93). Leur définition renvoie en fait aux traditionnelles formes d'espionnage visant des agences gouvernementales, à la différence des outils utilisés qui relèvent du numérique. Or, les deux auteurs établissent également que l'arrivée du numérique a propagé une nouvelle forme d'espionnage, économique cette fois, utilisée par des États pour se procurer un avantage comparatif: « *Examples range from the theft of several Western governments' preparatory documents for an edge in international negociations, to a spate of attacks targeting the F-35 fighter jet's design and manufacturing process* » (p.93). Selon eux, l'économie d'aujourd'hui est fortement dirigée par l'innovation, et le cyberespionnage offre un beau raccourci en matière de recherche et développement.

Cette différence entre le cyberespionnage de nature politique et miliaire (visant des secrets étatiques et de sécurité nationale) et celui de nature économique (vol de propriété intellectuelle, de secrets commerciaux, etc.) est particulièrement source de tension entre les États-Unis et la Chine. Alors que la Chine est principalement accusée de conduire des opérations de cyberespionnage économique, les États-Unis sont eux blâmés pour leurs opérations de nature politiques, notamment depuis les révélations d'Edward Snowden.

Pour cette raison, les États-Unis s'efforcent de distinguer ces deux formes de cyberespionnage. Il n'existe en effet aucune loi internationale interdisant l'espionnage politique et interétatique, qui est donc considéré légal sur le plan du droit international. Au contraire, les Américains considèrent que le cyberespionnage économique et industriel est intolérable et illégal, parce qu'il contrevient aux règles du jeu commercial. Les États-Unis reprochent ainsi à la Chine de ne pas respecter son engagement à titre de membre de l'Organisation mondiale du commerce (OMC), notamment en ce qui concerne l'Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce (ADPIC) (Inkster, 2016). Selon l'article 41 (1) de cet accord, les gouvernements sont obligés de protéger la propriété intellectuelle:

> Les Membres feront en sorte que leur législation comporte des procédures destinées à faire respecter les droits de propriété intellectuelle [...] de manière à permettre une action efficace contre tout acte qui porterait atteinte aux droits de propriété intellectuelle couverts par le présent accord [...] (ADPIC, Article 41 (1)).

La Chine rejette cette distinction entre les deux formes de cyberespionnage, qu'elle considère comme une tentative de définir unilatéralement les règles en ce qui a trait au cyberespace (Segal et Tang, 2016). L'intellectuel chinois Wu Xinbo, directeur du *Center for American Studies* à l'Université Fudan, affirme ainsi que les États-Unis adoptent une vision de « deux poids, deux mesures » sur la cybersécurité: « *It accuses other countries, especially China, of industrial espionage or other cyber attacks while the U.S. monitors other countries' senior officials or political figures almost constantly* » (China News Service, 21 septembre 2015). Par ailleurs, la Chine argumente que dans son cas, le développement économique est un enjeu de sécurité nationale et que dans cette optique, le cyberespionnage industriel peut être considéré quasi légitime (Inkster, 2016).

Autrement dit, la question du cyberespionnage est l'une des plus épineuses dans le débat entre les États-Unis et la Chine sur les normes du cyberespace. Chacun des gouvernements a sa propre vision et tente de légitimer ses propres actions, tout en s'efforçant de blâmer l'autre pour les siennes.

À la lumière de ces éclaircissements, nous constatons que le domaine du cyber et la terminologie qui lui est associée demeurent difficiles à définir avec exactitude. Or, ce manque de contours clairs entourant notamment les termes cyberattaque, cybersécurité et cyberespionnage permet ainsi leur emploi dans toutes sortes de contextes, chaque fois avec une connotation différente. Ce problème est important (et nous devons le considérer pour notre recherche), puisqu'il laisse place à de multiples interprétations possibles changeant en fonction des différentes perspectives en présence, et en fonction des intérêts poursuivis par chacun des acteurs.

1.4. La cyberattaque contre l'OPM : rappel des faits

Cette section sera dédiée à la mise en place de notre étude de cas, soit la cyberattaque contre l'Office of Personnel Management des États-Unis (OPM). Nous indiquerons les principaux événements entourant la cyberattaque, son dévoilement, ainsi que les rapports sino-américains en regard de cet événement. Le lecteur pourra ainsi comprendre quel est notre objet de recherche et retracer l'historique global de cette cyberattaque majeure.

En juin 2015, le gouvernement américain a révélé avoir été victime d'une cyberattaque concernant les données personnelles d'environ 4,2 millions d'employés de la fonction publique fédérale américaine. Les systèmes informatiques de l'Office

of Personnel Management (OPM) du gouvernement américain ont été infiltrés par des hackers. L'OPM est une agence gouvernementale œuvrant dans différents domaines ayant trait aux employés du gouvernement fédéral des États-Unis. Notamment, l'OPM détermine les mesures d'embauche pour les employés fédéraux, conduit des enquêtes de sécurité (*background investigations*) pour les futurs employés et accorde des cotes de sécurité, gère les pensions des employés retraités, administre les programmes d'assurance médicale et autres pour les employés et les retraités, etc. (OPM, About, s.d.). Autrement dit, l'OPM est l'agence gouvernementale américaine qui gère l'ensemble des informations personnelles et confidentielles de tous les anciens, présents et futurs employés fédéraux américains. En s'infiltrant dans ces systèmes, les hackers ont ainsi mis la main sur les données confidentielles de présents et d'anciens employés fédéraux, soit l'information concernant notamment le nom complet, la date de naissance, l'adresse de résidence, etc.

Cette cyberattaque a été détectée en avril 2015 alors que l'OPM effectuait justement l'implantation de meilleures défenses dans ses systèmes informatiques (WH, 9 juin 2015). Dévoilée au début du mois de juin, la cyberattaque a alors été présentée dans les médias comme l'une des pires intrusions dans les données des employés fédéraux (NY Times, 4 juin 2015). Sans accusation officielle, mais en raison de sources gouvernementales anonymes dans les médias, tous les yeux se sont alors tournés vers la Chine, soupçonnée d'être à l'origine de l'attaque. Les officiels de l'ambassade de Chine à Washington se sont empressés de nier un quelconque lien entre la Chine et l'attaque, affirmant que ces accusations étaient irresponsables et non scientifiques (The Guardian, 5 juin 2015). Les propos du porte-parole de l'ambassade de Chine à Washington, Zhu Haiquan, ont également été rapportés dans certains médias chinois.

> *Cyber attacks conducted across countries are hard to track and therefore the source of attacks is difficult to identify. Jumping to conclusions and making hypothetical accusation is not responsible and counterproductive* (Xinhuanet, 4 juin 2015).

Or, un mois plus tard, en juillet 2015, l'OPM a affirmé avoir été victime d'une seconde cyberattaque, cette fois visant les données de 21,5 millions d'Américains (OPM, 9 juillet 2015). Bien pire que la première attaque, la seconde ciblait les enquêtes de sécurité d'anciens, de présents et de futurs employés fédéraux, dévoilant ainsi des données particulièrement confidentielles, telles que le numéro d'assurance sociale, ou encore permettant d'identifier des agents travaillant à l'étranger sous couverture. Dans son communiqué du 9 juillet 2015, l'instance gouvernementale a ainsi affirmé que quiconque ayant postulé pour une enquête de sécurité depuis 2000 pouvait avoir été touché, de même que ses proches.

> *This includes 19.7 million individuals that applied for a background investigation, and 1.8 million non-applicants, predominantly spouses or co-habitants of applicants. [...] some records also include findings from interviews conducted by background investigators and approximately 1.1 million include fingerprints* [19] *. [...] If an individual underwent a background investigation through OPM in 2000 or afterwards (which occurs through the submission of forms SF 86, SF 85, or SF 85P for a new investigation or periodic reinvestigation), it is highly likely that the individual is impacted by this cyber breach* (OPM, 9 juillet 2015).

Sans situer l'origine de cette seconde cyberattaque, l'OPM a tout de même mentionné qu'elle était liée à la première révélée en juin (NY Times, 9 juillet 2015)[20].

Le jour même, lors d'une conférence électronique visant à préciser les actions entreprises par l'OPM en réponse aux cyberattaques, la directrice de l'OPM, Katherine Archuleta, a affirmé qu'elle ne comptait pas démissionner malgré

---

[19] Dans un document de l'OPM précisant les détails de la cyberattaque, il est plutôt révélé que ce sont 5,6 millions d'empreintes digitales qui ont été touchées. Les noms d'utilisateurs et les mots de passe utilisés par les candidats pour remplir les formulaires d'enquête de sécurité ont également été volés (OPM, Cybersecurity Resource Center, s.d.).

[20] Les deux cyberattaques étant considérée reliées, nous y faisons référence dans ce mémoire en tant qu'une seule cyberattaque.

l'insistance de certains membres du congrès : « *We are working very hard, not only at OPM, but across government, to ensure the cybersecurity of all our systems, and I will continue to do so* » (NY Times, 9 juillet 2015). Mme Archuleta a par ailleurs annoncé que de nouvelles mesures de sécurité seraient mises en place à l'agence et qu'aucune utilisation ni dévoilement supplémentaire de l'information provenant de l'OPM ne semblait avoir eu lieu. Le lendemain, elle a toutefois remis au président sa démission, affirmant qu'une nouvelle direction était nécessaire afin de « surmonter les présents défis »[21] (NY Times, 10 juillet 2015).

Ces deux cyberattaques jumelées contre le gouvernement américain ont été considérées par les officiels et les médias américains comme l'une des pires intrusions dans les systèmes informatiques du gouvernement américain et l'une des plus graves en matière de sécurité nationale. Le directeur du FBI James B. Comey a par ailleurs déclaré aux médias :

> *It is a very big deal from a national security perspective and from a counterintelligence perspective. [...] It is a treasure trove of information about everybody who has worked for, tried to work for, or works for the United States government* (Washington Post, 9 juillet 2015)

Ces deux cyberattaques ont également démontré la vulnérabilité des systèmes informatiques du gouvernement américain (NY Times, 9 juillet 2015 ; Washington Post, 9 juillet 2015).

Dans les médias chinois, les accusations selon lesquelles la Chine pouvait être en cause ont été décriées, qualifiées de « sans fondement » et dépeintes comme démontrant un « biais stéréotypé » contre la Chine.

---

[21] Traduction libre de : *move beyond the current challenges.*

> *It kind of becomes a regular stunt now, to blame China: it is easy, for no concrete evidence is needed to throw speculations over a country the United States sees as a challenger. Additionally, it seems "politically right" to demonize China at the moment* (Xinhuanet, 11 juin 2015).

Le 12 août 2015, le média chinois *Xinhuanet* a rapporté les nouveaux propos du porte-parole de l'ambassade chinoise à Washington Zhu Haiquan affirmant que « les accusations sans fondement et la diplomatie du microphone ne permettent de régler aucun problème »[22] (Xinhuanet, 12 août 2015). Le gouvernement chinois a en effet nié toute implication dans les cyberattaques contre l'OPM.

L'administration Obama s'est quant à elle abstenue d'accuser publiquement le gouvernement chinois, notamment afin d'éviter de divulguer les preuves récoltées dans le cadre de l'enquête (Washington Post, 21 juillet 2015).

S'inscrivant dans un contexte plus global entourant la gouvernance du cyberespace, la cyberattaque contre l'OPM a ainsi démontré les sérieux risques pour la sécurité nationale associés au cyberespace. La réussite de cette cyberattaque de même que son étendue ont atteint des proportions dépassant tout ce que les États-Unis avaient subi auparavant, et ses conséquences demeurent imprévisibles.

1.5. Rencontre au Sommet de septembre 2015

C'est dans ce contexte que quelques mois plus tard, en septembre 2015, le président chinois Xi Jinping s'est rendu aux États-Unis pour une rencontre au Sommet avec le

---

[22] Traduction libre: *Groundless accusations and microphone diplomacy are not solving any problems.*

président américain Barack Obama. Lors de cette rencontre, les deux présidents ont conclu une première entente historique en ce qui concerne le domaine du cyber[23].

Tout d'abord, les deux présidents ont convenu que leur gouvernement respectif ne soutiendrait pas le vol de propriété intellectuelle ou de secrets industriels.

> [...] *neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors* (WH, 2015b).

Les deux présidents se sont également entendus sur la nécessité d'identifier des normes de conduite dans le cyberespace et d'établir deux groupes de travail et une ligne de communication entre les deux côtés (Segal et Tang, 2016). De plus, ils ont convenu de coopérer sur le plan de la cybersécurité, d'offrir rapidement une réponse à une requête d'assistance, et d'enquêter sur les activités malveillantes provenant de leur territoire.

> *China and the United States agree that timely responses should be provided to requests for information and assistance concerning malicious cyber activities. Further, both sides agree to cooperate, in a manner consistent with their respective national laws and relevant international obligations, with requests to investigate cybercrimes, collect electronic evidence, and mitigate malicious cyber activity emanating from their territory* (MFAPRC, 26 septembre 2015).

En conférence de presse, le président Barack Obama a affirmé l'importance des enjeux du cyberespace, leur nature globale, et l'importance de travailler conjointement avec la Chine et l'ensemble de la communauté internationale pour sécuriser l'environnement du web (WH, 2015a). De son côté, le président chinois Xi Jinping a affirmé que la Chine et les États-Unis, en raison de leurs places

[23] Le terme généralement employé dans la littérature anglophone est celui de « *cyber agreement* ».

prépondérantes en matière de cyberespace, devaient coopérer et éviter de politiser cet enjeu (WH, 2015a).

La rencontre au Sommet de septembre 2015 peut ainsi être considérée comme le coup d'envoi d'un nouveau dialogue entre la Chine et les États-Unis en matière de cyberespace et de cybersécurité. Les effets à long terme de cette rencontre et de cette première entente entre les deux États sont toutefois difficiles à évaluer, et pour ce faire davantage de recul temporel sera nécessaire. Quant à la cyberattaque contre l'OPM, mentionnons que cette question n'a pas été abordée dans les discours publics des deux présidents lors de leur rencontre à Washington.

1.6. Question centrale et hypothèse d'ensemble

Tel que présenté dans cette partie sur la problématique d'ensemble, ce mémoire s'intéresse aux différentes perspectives en matière de cybersécurité, relativement à la cyberattaque contre l'OPM. Il s'intéresse également aux logiques d'argumentation présentes dans le discours politique des gouvernements chinois et américain entourant cette cyberattaque et la rencontre au Sommet des deux présidents en septembre 2015.

Nous posons ainsi la question centrale de recherche suivante : comment s'articule le processus de construction du discours des administrations Obama et Xi entourant la cyberattaque sur 21,5 millions d'enquêtes de sécurité et lors de la rencontre au Sommet de septembre 2015 ?

Nous postulons que le discours de chaque gouvernement a été produit en fonction d'un processus d'articulation d'un message clé en termes de coopération bilatérale, dont le but ultime était de servir des intérêts nationaux précis.

1.6.1. Questions sectorielles et objectifs de recherche

Quatre questions sectorielles appuient notre démarche. Elles permettent de cadrer notre analyse et ainsi, de répondre aux objectifs de ce mémoire. C'est également à partir de ces questions sectorielles et de leurs sous-questions que nous élaborerons notre grille d'analyse. Voici les questions sectorielles:

1. Quelle est la position politique défendue par les présidents Obama et Xi en matière de cybersécurité?

2. Quels messages clés (ou vérités) les discours des deux administrations tentent-ils de véhiculer?

3. Quel est le processus de construction du message employé par les deux administrations ?

4. Quels sont les intérêts nationaux poursuivis par chaque gouvernement ?

Notre recherche vise à soulever les intérêts dissimulés derrière le discours des administrations Obama et Xi entourant la cyberattaque contre l'OPM et leur rencontre au Sommet de septembre 2015, ainsi que la façon dont ils ont construit une certaine représentation de la cybersécurité et de leur coopération bilatérale.

Pour chacune des questions sectorielles, nous avons isolé un objectif de recherche précis. Il s'agit tout d'abord d'identifier la vision générale de chaque président relativement à la cybersécurité. Ensuite, nous cherchons à déterminer la posture de

chaque gouvernement quant à la cyberattaque contre l'Office of Personnel Management et à la rencontre au Sommet, ainsi qu'à comprendre comment les stratégies discursives employées par les deux gouvernements visaient à construire une certaine réalité. Finalement, nous souhaitons déterminer quelles sont les logiques d'intérêt en présence et en quoi la formulation du discours en permet efficacement la poursuite.

1.6.2. Pertinence communicationnelle

À notre avis, ce mémoire est particulièrement intéressant puisqu'il permet d'offrir une perspective communicationnelle à un nouvel enjeu de sécurité, davantage abordé par le champ de la science politique et des relations internationales. Jamais une cyberattaque de l'envergure de celle de l'OPM n'avait été réalisée et à ce jour, très peu de recherches scientifiques s'y sont intéressées. Notre mémoire vise à analyser à la fois le discours politique américain et le discours politique chinois et à démontrer comment ils visent la poursuite d'intérêts nationaux.

Le discours politique constitue une partie intégrante de la communication internationale, particulièrement lors d'une rencontre au sommet entre deux États et surtout, en lien avec la gestion d'une crise majeure comme celle de la cyberattaque contre l'OPM. Notre mémoire s'avère donc pertinent en ce qu'il vise à démontrer les rouages du pouvoir politique dissimulés derrière ce discours, et en fonction de deux différentes perspectives idéologiques et culturelles.

CHAPITRE II

DÉLIMITATION DU CADRE THÉORIQUE

Dans cette deuxième partie, nous décrirons les théories qui nous serviront de cadre de référence théorique en appui à notre analyse. Ce mémoire s'inscrit au sein du paradigme constructiviste, puisque nous nous intéressons à la construction du discours politique et aux différentes perspectives en présence entourant la cybersécurité et la cyberattaque contre l'OPM. Afin d'ancrer notre mémoire au sein de ce paradigme, nous délimitons notre cadre de référence théorique autour de trois concepts. Tout d'abord, nous nous intéressons à la construction sociale de la réalité, telle que présentée par Berger et Luckmann. Ensuite, nous mobilisons l'approche théâtrale de l'interactionnisme symbolique de Goffman. Puis, nous nous intéressons à la construction du lien entre cyberespace et sécurité. Nous mobilisons pour ce faire l'apport théorique d'Alix Desforges (2014) et son travail sur les représentations du cyberespace en tant qu'outil géopolitique, ainsi que la théorie de Myriam Dunn Cavelty (2013) qui argumente que le lien entre cyberespace et sécurité a été construit par un processus politique. Nous terminerons ce chapitre par la présentation de notre posture épistémologique.

2.1. La construction sociale de la réalité

S'intéressant à la sociologie du savoir, Berger et Luckmann ont mis la table à une théorie dominante du paradigme constructiviste dans leur ouvrage *The Social Construction of Reality* (1966). Leur théorie s'articule autour de la prémisse selon laquelle la réalité et le savoir sont socialement construits. Par réalité, ils entendent «

la qualité des phénomènes que nous reconnaissons comme ayant un être indépendant de notre propre volonté (nous ne pouvons pas «les désirer») » (p.13). Quant au savoir, ils le définissent comme « la certitude que les phénomènes sont réels et qu'ils possèdent des caractéristiques spécifiques » (p.13)[24]. Ainsi, ils argumentent que réalité et savoir dépendent de leur relativité sociale. Une réalité pour un individu ou une société pourrait ne pas exister, ou alors dans une conception différente, que pour un autre individu ou un autre groupe.

> *Sociological interest in questions of "reality" and "knowledge" is thus initially justified by the fact of their social relativity. What is "real" to a Tibetan monk may not be "real" to an American businessman. The "knowledge" of the criminal differs from the "knowledge" of the criminologist. It follows that specific agglomerations of "reality" and "knowledge" pertain to specific social context* [...] (Berger et Luckmann, 1966, p.15).

Selon cette hypothèse, le contexte social définit ce qui est réel et ce que l'on sait. Ce sont des acteurs sociaux qui construisent les réalités, en fonction d'un certain contexte. Il n'y a donc pas de réalité objective, mais plutôt une objectivation d'un processus subjectif par lequel les individus construisent le monde dans leur vie quotidienne (Berger et Luckmann, 1966). Pour comprendre le monde, il faut donc analyser le processus de construction des réalités employé par les acteurs sociaux.

Par ailleurs, les pratiques discursives sont partie intégrante de ce processus de construction, puisqu'elles permettent l'élaboration de significations collectives (O'Meara, 2010). Il s'agit donc, en analysant le discours des acteurs, de déterminer quelles sont les constructions qu'ils emploient au service de leur intérêt et comment ils construisent des significations collectives à partir de ces énoncés.

---

[24] Traduction libre: « [...] *to define 'reality' as a quality appertaining to phenomena that we recognize as having a being independent of our own volition (we cannot 'wish them away'), and to define 'knowledge' as the certainty that phenomena are real and that they possess specific characteristics* ».

Nous argumentons ainsi que la connaissance se transforme, car elle est socialement construite. Elle aussi évolue avec le temps et l'espace. Ce qui nous permet d'interpréter le monde, ce sont les symboles et les conventions construits et institutionnalisés par la société.

2.2. Goffman et la théorie de la mise en scène

L'apport du sociologue Erving Goffman pour le domaine de la communication est d'une grande importance. Il s'inscrit dans le courant de l'interactionnisme symbolique, qui argumente que le sens conféré aux choses par un individu dépend nécessairement de son interprétation et que cette interprétation découle des interactions qu'il a avec autrui. C'est donc l'interaction qui détermine le sens que les individus attribuent au monde. Or, ce sens peut être modifié à chaque nouvelle interaction, en fonction des circonstances en présence. Dans le cas de Goffman, c'est notamment son étude des interactions sociales, présentée sous la forme d'une métaphore théâtrale, qui lui vaut aujourd'hui une grande notoriété et qui nous interpelle plus précisément.

Introduite dans *The Presentation of Self in Everyday Life (1956)*, cette théorie associe les individus en contexte d'interaction à des acteurs lors d'une performance ou d'une représentation. Goffman analyse ainsi l'interaction entre individus comme une pièce de théâtre. Chaque individu joue un rôle différent en fonction de la nature de l'interaction, c'est-à-dire en fonction du contexte interpersonnel dans lequel il se trouve. La « performance » de l'individu sera modifiée selon les relations de groupe, l'impact de l'environnement, les mouvements et le sens de l'interaction.

> *I shall consider the way in which the individual in ordinary work situations presents himself and his activity to others, the ways in which he*

> *guides and controls the impression they form of him, and the kinds of things he may and may not do while sustaining his performance before them* (Goffman, 1956, preface).

Il s'agit d'une analyse dramaturgique de l'interaction, décrivant la nature sociologique et psychologique de l'individu lors d'interactions avec autrui, en face à face. L'interaction est ainsi perçue comme une performance, construite par l'environnement et l'audience, dont le but est de donner aux autres des impressions en lien avec les objectifs de l'acteur. L'acteur change de rôle en fonction de l'espace de jeu, influencé par les autres acteurs en présence ainsi que par le public, mais également par ses propres intérêts.

> *Thus, when an individual appears in the presence of others, there will usually be some reason for him to mobilize his activity so that it will convey an impression to others which it is in his interests to convey* (Goffman, 1956, p.3).

Autrement dit, les individus cherchent à poursuivre certains objectifs lors de leurs interactions. Leur façon d'interagir avec les autres et le public découlera nécessairement de ces intérêts. Par ailleurs, si les interactions sociales sont comparées à une scène, où il y a des acteurs et un public, cette scène comporte nécessairement des coulisses. Alors que la scène correspond au lieu où se déroule l'interaction et que les individus font office d'acteurs, les coulisses ramènent quant à elles à l'espace privé, ou encore à « l'arrière-scène », où l'impression livrée lors de la représentation peut être démentie. C'est notamment cette opposition entre « avant-scène » et « arrière-scène » qui nous intéresse dans le cadre de cette recherche sur le discours politique et les rencontres diplomatiques.

L'information présentée au public dans le discours du gouvernement relève de l'avant-scène et doit nécessairement servir les intérêts du dit gouvernement. À l'inverse, l'information concernant tout ce qui se déroule dans les « coulisses du pouvoir » n'est

pas accessible au public. C'est pourquoi nous supposons que la construction du discours politique orientée vers le public, à l'avant-scène, comporte une omission volontaire d'information.

Finalement, l'approche de Goffman se base sur l'étude du comportement des individus en public. Il observe les faits et gestes des individus, dans différentes situations du quotidien, pour en tirer des règles communes, généralisées. Le regroupement de ces différentes règles représente ce qu'il appelle l'ordre de l'interaction. L'objectif de Goffman est ainsi de déterminer les principales normes qui régissent les interactions de la vie quotidienne et d'en dégager les principes généraux qui forment l'ordre de l'interaction.

Goffman reconnaît toutefois que l'ordre de l'interaction se différencie d'une société à l'autre. Selon lui, chaque société se construit des normes sociales précises qui régissent l'ordre social. « *This constitutes one way in which a performance is, in a sense, socialised, moulded and modified to fit into the understanding and expectations of the society in which it is presented* » (Goffman, 1956, p. 22). Ainsi, la réalité observable (l'interaction) change en fonction de l'ordre social.

L'apport de Goffman sur l'étude des interactions pour notre mémoire est donc double. Premièrement, nous retenons que les individus modifient leur comportement en fonction de chaque « performance » (des autres acteurs en présence, de la scène, du public). Les individus agissent ainsi afin de répondre à leurs propres objectifs et pour ce faire, doivent s'assurer que le public et les autres acteurs perçoivent uniquement ce qu'ils souhaitent rendre perceptible. Ce qui ne doit pas être démontré publiquement se déroule à l'inverse en coulisse, à l'arrière-scène.

Deuxièmement, nous retenons qu'il existe des normes et pratiques sociales, constituant l'ordre de l'interaction, qui dictent les façons appropriées d'interagir en

fonction de différentes situations. Or, l'ordre de l'interaction n'est pas universel, en ce qu'il est différent d'une société à l'autre, d'une communauté à l'autre ou plus simplement, d'un groupe d'individus à l'autre. Il s'agit d'une considération importante pour notre mémoire, qui s'intéresse justement à deux perspectives culturelles possédant chacune des normes qui leur sont propres. Or, dans le cadre de leurs relations bilatérales, ces deux perspectives se doivent d'entrer en interaction, malgré leurs différences et c'est notamment ce qui rend intéressante l'étude d'une rencontre diplomatique.

2.3. Les représentations du cyberespace

Selon Stuart Hall (1997), la production de sens n'est pas innée, elle ne provient pas des choses en soi, mais elle est produite, construite. « *It is the result of a signifying practice – a practice that produces meaning, that makes things mean* » (Hall, 1997, p.10). C'est ce qu'il réfère à la théorie constructiviste de la représentation. Selon lui, la représentation est le processus qui nous permet de dire quelque chose d'intelligible, de présenter le monde aux autres avec sens, par l'utilisation du langage. Dans *The Work of Representation* (1997), Hall explique qu'il existe deux systèmes de représentation et qu'il faut les deux pour comprendre le sens de quelque chose. Le premier est celui qui nous permet d'offrir du sens au monde, en construisant des correspondances entre les choses et notre carte conceptuelle, c'est-à-dire notre compréhension de ce qu'elles sont. Le deuxième système de représentations dépend cette fois de la construction de correspondances entre notre carte conceptuelle et une série de signes organisés en un langage qui nous permet de représenter ces concepts.

Selon Hall, l'approche constructiviste de la représentation reconnaît le caractère public et social du langage. Les choses ne signifient rien en elles-mêmes. « *Things*

don't mean: we construct meaning, using representational systems – concepts and signs » (Hall, 1997, p.11). Ce sont donc les acteurs sociaux qui utilisent un système de représentations pour construire du sens, pour rendre le monde compréhensible et pour communiquer à propos de ce monde entre eux.

Ce qui nous amène à nous intéresser plus particulièrement à la théorie d'Alix Desforges (2014) sur les représentations du cyberespace, qui nous préoccupe directement, et la construction du sens entourant ce terme. Selon elle, le terme cyberespace n'est pas neutre. Il constitue « un système complexe de représentations qui s'enchevêtrent, s'agrègent et s'opposent » (Desforges, 2014, p.68) et qui est utilisé dans le cadre de stratégies politiques, économiques et/ou militaires. Par exemple, elle explique que dans le discours américain relatif à la gouvernance d'Internet, le cyberespace a largement été dépeint comme un espace de liberté, comme un facteur de progrès économiques et sociaux et même comme un symbole de la démocratie.

> La représentation d'un cyberespace comme espace de liberté a été [...] un outil puissant de la stratégie américaine pour mettre un frein aux velléités russes et chinoises de contrôle sur le réseau mais aussi pour conserver leur position dominante dans la gouvernance de l'Internet alors que celle-ci est de plus en plus critiquée (Desforges, 2014, p.73).

Desforges analyse donc les différentes représentations du cyberespace afin de mesurer leur mobilisation dans le cadre de rivalités étatiques relatives, entre autres, à la gouvernance du cyberespace.

Par ailleurs, elle stipule que le cyberespace représente pour les dirigeants des États un véritable défi, car il vient remettre en question l'exercice de leur pouvoir et leur autorité. Les États ont donc fait du cyberespace un enjeu de sécurité, en identifiant la cyberattaque comme relevant d'une question de sécurité nationale, afin de remédier à

leur perte de pouvoir. « De nombreux États ont placé les questions de cybersécurité et de cyberdéfense au premier plan de leur programme politique en les liant aux questions de sécurité nationale » (Desforges, 2014, p.77). La construction de cette menace leur a ainsi permis d'intensifier le sentiment d'insécurité de la population et, à plus forte raison, de justifier leur pouvoir en se plaçant comme protecteurs contre la menace issue d'Internet. Le cyberespace est devenu l'un des éléments essentiels de la sécurité du territoire, de l'indépendance nationale, du maintien de l'ordre et même, de l'identité culturelle. Selon Desforges, ce qui importe n'est pas de questionner la présence réelle d'une menace ou non, c'est plutôt la façon dont les États ont représenté le cyberespace comme un enjeu de sécurité nationale, dans la poursuite de leur logique d'intérêts.

2.4. Militarisation du cyberespace et représentations des cybermenaces

La chercheuse Myriam Dunn Cavelty s'intéresse elle aussi à la place de la cybersécurité en tant qu'enjeu de sécurité nationale, qu'elle considère comme l'un des plus importants de l'époque actuelle. Elle s'intéresse ainsi au fait que déjà depuis les débuts de l'émergence du cyberespace, un lien a été tracé avec la notion de sécurité nationale: « *From the very beginning of the cyber threat story in the 1980s, there was a national security connotation to it* » (Dunn Cavelty, 2012). Or, elle argumente que le lien entre cyberespace et sécurité nationale n'a rien de naturel (Dunn Cavelty, 2012, 2013). Selon elle, bien que ce lien soit souvent présenté comme une vérité incontestée, il a plutôt été forgé, argumenté et accepté par un processus politique, en fonction des différents cadrages utilisés.

Sa théorie veut que l'établissement des cybermenaces en tant que débat de sécurité

nationale, particulièrement parmi les États occidentaux, provienne de l'interrelation entre deux facteurs: la perception que les sociétés sont de plus en plus exposées à des vulnérabilités potentiellement catastrophiques, et la perception que des acteurs malintentionnés souhaitent exploiter ces vulnérabilités (Dunn Cavelty, 2012). Ce sentiment de vulnérabilité aurait donc entraîné un sentiment d'urgence, ayant à son tour conduit à la militarisation[25] du débat entourant la cybersécurité.

Ainsi, elle suppose que cette vision supporte à tort que les États puissent contrôler le cyberespace et qu'elle crée une atmosphère d'insécurité et de tension dans le système international, basé sur des mauvaises perceptions de la nature et du niveau des cyberrisques (Dunn Cavelty, 2012). Or, elle affirme que les mesures militaires ne peuvent pas jouer un grand rôle en matière de cybersécurité, en raison de la nature de l'environnement de l'information ainsi que de la nature de la menace.

Par ailleurs, elle affirme que la construction du lien entre cyberespace et sécurité est en réalité une pratique discursive en soi. Pour ce faire, elle part de la prémisse que les acteurs utilisent le discours afin de s'affirmer ainsi que leur mode d'argumentation dans le but d'établir un modèle dominant de discours.

> *I argue that only a broad understanding of cyber-security as discursive practice by a multitude of actors inside and outside of government reveals the variety of choices available to political actors at all times and enables us to show what the consequences of such choices are* (Dunn Cavelty, 2013, p.106).

Selon elle, la cybersécurité peut donc être comprise comme une combinaison de pratiques discursives, linguistiques ou non, provenant de différentes communautés d'acteurs. Ces communautés ont toutes pour sujet commun les ordinateurs et les

[25] Par militarisation, nous entendons la définition de Deibert (2003), selon laquelle la militarisation du cyberespace consiste en l'expansion et l'adoption de capacités militaires en regard des technologies de l'information.

réseaux d'ordinateurs, mais elles diffèrent « dans leur focalisation sur le type d'enjeu de niveau élevé qu'ils observent comme étant « connectés à » ou « influencés par » la sécurité des ordinateurs et des réseaux »[26]. La principale différence entre ces communautés est donc l'objet de référence auquel elles portent une attention particulière. Chaque groupe particulier d'acteurs va donc construire et opérer un discours autour des menaces spécifiques associées à leur objet de référence. Dunn Cavelty (2013) postule ainsi qu'il est possible d'observer un lien direct entre les représentations de la menace reliées aux différentes conceptions du cyberespace et l'établissement de pratiques générales ou de ripostes en matière de cybersécurité.

2.5. Relation entre culture, communication et discours

Selon Edward T. Hall (1959), « *culture is communication, and communication is culture* » (p.191). Notamment dans le cadre de la présente recherche en communication internationale et interculturelle, la culture occupe une place importante. Nous pensons donc qu'il importe de mentionner le caractère essentiel de la prise en compte de la culture, et des différences culturelles, au sein de notre recherche. Nous nous intéressons en effet à deux perspectives culturelles différentes (chinoise et américaine) et nous pensons qu'il est nécessaire de le considérer lors de notre analyse.

En continuité avec Berger et Luckmann (1966), nous retenons que les individus créent la culture, en construisant la réalité et le sens. La culture est donc socialement construite. Elle consiste en une variété de concepts (valeurs, croyances, normes, etc.),

---

[26] Traduction libre: « [...] *in their focus on the type of issues on a higher level, which they regard as being connected to or influenced by the security of computers and computer networks* » (p.108).

de comportements, d'artefacts et de systèmes (tels que le système communicationnel) (Baldwin *et al.*, 2014). Par ailleurs, la culture est directement reliée à la communication.

> [...] *if culture is the human-made part of our environment, then we would hot have any culture if people did not communicate to create it. Thus, culture is created (and changed) through communication* (Baldwin *et al.*, 2014, p.57).

C'est donc en communiquant que les individus créent la culture. Cette idée rejoint celle de Shi-Xu (2005), qui argumente que les notions de discours et de culture sont difficilement indissociables: « *I shall argue for a notion of discourse as culturally saturated forms of verbal communication, or, in other words, as a set of diversified and competing constructions of meaning associated with particular groups of people* » (p.1).

Selon Entman (1993), la culture est également considérée comme un ensemble (ou stock) de connaissances, présentes dans le discours et dans la pensée de la plupart des personnes appartenant à un groupe social. Lui aussi considère donc que la culture dicte en quelque sorte la construction du discours au sein d'un groupe précis, en ce qu'un communicateur doit nécessairement tenir compte du système de connaissances de la culture en présence afin que son discours soit correctement reçu et compris par le public.

Or, dans le cas des échanges interculturels, un degré de difficulté s'ajoute, puisque les interlocuteurs appartiennent à des contextes culturels différents. Selon Shi-Xu (2005), le discours peut être perçu comme un jeu de langages divergents et s'opposant (Shi-Xu, 2005). Cette vision identifie ainsi les échanges interculturels comme un jeu d'opposition entre différentes constructions symboliques, et comprend la culture comme une diversité de pratiques concurrentes de construction de sens appartenant à

des groupes particuliers d'individus. Le cas à l'étude au sein de cette recherche concerne donc, selon la vision de Shi-Xu, deux perspectives culturelles étant *de facto* en confrontation.

En définitive, une analyse de discours doit s'intéresser nécessairement à la culture au sein de laquelle le discours se construit, puisque la culture participe à la construction du sens dans les groupes d'individus. Ce type d'analyse ne peut donc s'effectuer sans la prise en compte du contexte culturel.

2.6. Posture épistémologique

Nous pensons que la dernière section de ce chapitre sur le cadre théorique doit servir à présenter notre posture épistémologique, puisqu'elle influence nécessairement la direction de l'analyse qui sera effectuée dans le cadre de cette recherche. Dans cette section, nous présenterons rapidement notre ontologie ainsi que notre posture épistémologique constructiviste, et ce en raison de notre vision du monde en tant que réalité évolutive. Nous allons donc tenter de justifier notre posture constructiviste et son lien avec une vision plus contextuelle de la réalité.

2.6.1. Ontologie

L'ontologie, qui signifie « théorie de l'être » dans sa définition la plus simple[27], correspond à la façon dont le chercheur perçoit la connaissance, à sa vision du monde et de la réalité. L'ontologie consiste à répondre aux questions suivantes: qu'est-ce qui existe? Qu'est-ce qui est vrai? Qu'est-ce que la réalité?

[27] Voir Larousse (2017a).

Selon notre vision du monde, la réalité évolue avec le temps et l'espace, et ce qu'on croyait être vrai ne l'est pas nécessairement, ou du moins ne l'est plus en fonction de l'époque qui change, des mentalités qui évoluent et de l'avancement de la science et des technologies. En référence à Berger et Luckmann (1966), notre propre vision se réfère à l'idée que la réalité (ce que l'on croit savoir) n'est pas fixe, mais qu'elle est contextuelle. Nous pensons que l'être humain perçoit les choses et croit qu'elles sont vraies, en raison de son propre cadre conceptuel dessiné par la société et l'époque au sein desquelles il évolue. Nous pensons ainsi que la vérité n'est pas neutre, mais qu'elle est plutôt déterminée par différents éléments contextuels (économie, politique, culture, etc.). Tout comme Foucault (1977), nous pensons que la vérité est un produit social et qu'elle dépend de chaque société.

Dans le cas de notre recherche, nous croyons que la vérité entourant les concepts de cyberespace et de cybersécurité est socialement construite et qu'on la perçoit d'une certaine façon en fonction du contexte dans lequel nous évoluons. Tel que démontré dans le premier chapitre, les perspectives chinoise et américaine relativement au développement et au contrôle d'Internet, à la sécurité nationale et aux risques issus du cyberespace diffèrent à plusieurs points de vue. La cybersécurité ne représente donc pas la même réalité d'une société à l'autre.

2.6.2. Épistémologie constructiviste

Par rapport à cette vision de la réalité comme interprétée en fonction d'un certain ordre social, et parce que nous croyons que toute vérité est subjective, nous nous ancrons davantage au sein d'une posture épistémologique constructiviste. Selon nous, la connaissance se transforme, car elle est socialement construite. Elle aussi évolue

avec le temps et l'espace. Ce qui nous permet d'interpréter le monde, ce sont les symboles et les conventions construits et institutionnalisés par notre société. Nous croyons que ce sont les acteurs sociaux qui utilisent un système de représentations pour construire du sens, et que ce sens est par la suite institutionnalisé au sein du savoir.

En lien avec notre mémoire, nous croyons que le discours politique entourant le concept de cybersécurité a contribué à construire des représentations, qui diffèrent d'ailleurs en fonction des gouvernements. La vérité en matière de cyberespace et de cybersécurité n'est donc pas immuable, mais plutôt subjective. Elle dépend de la façon dont le discours politique l'a dépeinte, et de l'intégration du discours par la société qui le reçoit. Finalement, nous nous demandons si le discours américain et chinois entourant la cyberattaque contre l'OPM visait à créer une nouvelle forme de représentation de la cybersécurité. Surtout, nous nous demandons en fonction de quelle logique d'intérêts.

Pour ce conclure ce chapitre, nous croyons que ce sont les acteurs sociaux qui utilisent un système de représentation pour construire du sens, et que ce sens est par la suite institutionnalisé au sein du savoir. Nous croyons que le discours politique, notamment lors d'une interaction entre chefs d'État, entourant le concept de cybersécurité a contribué à construire des représentations, qui diffèrent d'ailleurs en fonction de l'administration qui articule le discours et de la culture au sein de laquelle se construit le discours.

C'est pourquoi les différentes théories présentées – la construction sociale de la réalité, l'interactionnisme symbolique de Goffman, la théorie des représentations du cyberespace de Desforges et la construction de la cybersécurité de Dunn Cavelty – nous offrent un ancrage pertinent pour notre analyse. En effet, ce cadre de référence

théorique constitue les fondations de notre analyse et nous permettra de répondre à la question centrale de recherche posée dans ce mémoire, à savoir comment s'articule le processus de construction du discours des administrations Obama et Xi entourant la cyberattaque sur 21,5 millions d'enquêtes de sécurité et lors de la rencontre au Sommet de septembre 2015. Les bases de notre réflexion ayant été posées, le prochain chapitre servira à expliquer la méthodologie employée dans le cadre de ce mémoire afin de répondre adéquatement aux différentes questions qu'il pose.

CHAPITRE III

PRÉSENTATION DE LA MÉTHODOLOGIE

Ancré dans une posture constructiviste, notre recherche vise à démontrer comment, dans le cadre de leur rencontre en septembre 2015, les deux administrations ont articulé leur discours autour de la question de la cyberattaque sur 21,5 millions d'enquêtes de sécurité, et s'ils ont ainsi contribué à construire une nouvelle représentation de la cybersécurité. Nous souhaitons en réalité dégager les logiques d'intérêts dissimulées derrière le discours des gouvernements. Nous avons donc préconisé une approche qualitative en lien avec notre objectif, qui vise à mieux comprendre un phénomène. Dans cette partie du travail, nous allons exposer notre démarche, associée à l'analyse du discours, ainsi que notre méthode de collecte de données.

3.1. Pertinence de l'approche qualitative

Selon Pierre Mongeau (2008), professeur au Département de communication sociale et publique de l'Université du Québec à Montréal (UQAM), une approche de recherche qualitative vise à donner un sens à une situation encore relativement confuse ou encore à donner un nouveau sens à une situation mal comprise. Dans le cadre d'une approche de recherche qualitative, le chercheur va donc tenter de « dégager une interprétation qui permette de donner un sens aux données » (Mongeau, 2008, p.29). Cette interprétation, il l'offre à ses lecteurs qui décideront si elle se

rapporte adéquatement au contexte, c'est-à-dire si elle « fait sens » (p.30). Cette approche cadre donc très bien avec notre intérêt de recherche, puisque nous souhaitons comprendre davantage la situation analysée en fonction de son contexte, et en tirer de l'information nouvelle. Nous espérons ainsi qu'à la lumière de ce mémoire, les lecteurs auront une compréhension approfondie de notre objet de recherche et qu'ils sauront apprécier les conclusions que nous souhaitons tirer.

3.2. Le discours analysé

Nous croyons que la validité de notre recherche repose en grande partie sur la méthode d'analyse préconisée, soit l'analyse de discours. Nous pensons en effet que cette méthode permet de répondre adéquatement à notre question centrale ainsi qu'aux différents objectifs de recherche, et c'est pourquoi elle nous semblait fort appropriée. Il convient donc d'expliquer ce que nous entendons par « discours », de même que d'élaborer sur les opportunités d'analyse que nous offre cette méthode.

3.2.1. Qu'est-ce que le discours ?

Le discours peut prendre plusieurs formes et ne possède donc pas de définition simple. Selon Gee (2014), le terme discours est utilisé de différentes façons par plusieurs domaines académiques et il peut prendre différents sens, au sein même d'une discipline. Il peut être équivalent à la fois à la parole, au texte ou encore à l'interaction orale issue de la conversation (Maingueneau, 1997). Il peut également désigner « le système sous-jacent à un ensemble d'énoncés tenus à partir d'une certaine position sociale ou idéologique », tel que le « discours féministe » (Maingueneau, 1997, p.10). Parmi ces différentes définitions, nous nous rattachons

davantage à la dernière, qui suggère que le discours ne doit pas désigner simplement une allocution ou un énoncé, mais qu'il doit englober l'ensemble de ce qui a été dit relativement à un certain système de pensée. Dans le cas de notre recherche, il s'agit justement d'analyser le discours politique des deux administrations. Par discours politique, nous ne faisons pas référence à la simple prise de parole d'un politicien (bien que notre corpus comprend des déclarations, comme il sera présenté plus loin), mais plutôt à l'ensemble des prises de parole (orales ou écrites) publiques d'un gouvernement, qui témoignent nécessairement d'une certaine position idéologique.

Par ailleurs, selon Gee (2014), certains linguistes ont donné au discours le sens de « langage en utilisation ». Cette définition dépasse alors la simple formation du texte (grammaire, syntaxe, etc.) pour l'inscrire dans un contexte spécifique.

> *When we study language-in-use, we study language not just as abstract system ("grammar") but in terms of actual utterances or sentences in speech or writing in specific contexts of speaking and hearing or writing and reading* (Gee, 2014, p.19).

Il s'agit alors de s'intéresser à la relation entre le langage et le contexte, de façon à ce que le contexte permette de déterminer l'étendue totale du sens donné au texte. Le discours est donc le texte, mis en relation avec le contexte spécifique dans lequel il est développé. Cette définition a ce côté pratique qu'elle nous permet d'aborder le discours dans sa formation matérielle (un texte écrit ou une prise de parole orale), et de l'analyser contextuellement.

Ensuite, pour Macdonell (1986), le discours dépend avant tout du dialogue, qui en est la première condition. Il faut alors tenir compte à la fois de l'émetteur et du récepteur lorsqu'on étudie le discours, car c'est l'échange qui est une production sociale. Selon cette chercheuse, le discours ne dépend pas uniquement du contexte, mais d'un ensemble d'éléments sociaux qui diffèrent d'une société à l'autre. Un énoncé, les mots

utilisés et leur sens, dépendent ainsi de l'endroit où l'énoncé a été fait, de même que ce à quoi il s'opposait ou s'alignait. Le discours, puisqu'il peut varier d'un pays à l'autre, d'une région à l'autre, n'est donc pas homogène. « *Discourses differ with the kinds of institutions and social practices in which they take shape, and with the positions of those who speak and those whom they address* » (Macdonell, 1986, p.1). Selon cette définition, le discours est alors formé en fonction de l'institution où il est produit, de même que des positions (sociales ou idéologiques) de l'émetteur et du récepteur. Le discours est ainsi une production sociale complexe issue d'une interaction. Nous comprenons alors que sa définition doit tenir compte de l'ensemble de ces éléments: le choix des mots, le sens que l'auteur et le récepteur leur donnent, en fonction des pratiques de la société où il prend place.

Quant au discours défini selon Michel Foucault, il dépasse le langage ou son contexte. Selon le philosophe français, le discours n'est pas non plus l'ensemble des choses qu'on dit, ni la manière de les dire. Il ne s'agit pas simplement des énoncés. Le discours, c'est également ce qui n'est pas dit, mais qui se rapporte à un geste, à un comportement, etc. Le discours est ce qui détermine ce qui *peut* être dit, en fonction d'une époque. En 1971, dans *L'ordre du discours*, Foucault affirmait ainsi:

> Je suppose que dans toute société la production du discours est à la fois contrôlée, sélectionnée, organisée et redistribuée par un certain nombre de procédures qui ont pour rôle d'en conjurer les pouvoirs et les dangers, d'en maîtriser l'événement aléatoire, d'en esquiver la lourde, la redoutable matérialité (Foucault, 1971, pp.10-11).

Selon Foucault, plusieurs mécanismes sont donc à l'œuvre afin de contrôler le discours. En pratique, celui qui contrôle le discours contrôle la réalité: le discours peut ainsi être considéré comme une construction de la réalité sociale. L'un de ces mécanismes consiste en la détermination des conditions de mise en jeu du pouvoir, ainsi qu'en l'imposition aux individus détenant le pouvoir un certain nombre de

règles, dont le but ultime est de ne pas permettre à tous d'y avoir accès (Foucault, 1971, p. 38). Les différentes sociétés du discours ont donc pour fonction de produire et de conserver le discours, et de ne le distribuer que selon des règles strictes (Foucault, 1971, p.41). Ainsi, le discours renvoie à une production de sens déterminée par des contraintes, dont le but est justement de contraindre. Notons en terminant que malgré l'apport important de Foucault en ce qui concerne l'analyse discursive, le corpus beaucoup trop vaste que nécessiterait une méthodologie foucaldienne nous incite à mettre de côté une telle approche. Nous préférons retenir de Foucault sa conception du discours en tant que lieu où se construit la réalité sociale, contrôlé par des mécanismes de pouvoir au sein de chaque société. Nous retenons également de sa définition la présence de différents ordres du discours.

3.2.2. Le discours politique

Afin d'effectuer un ciblage par rapport aux différents ordres du discours, précisons que le discours qui nous intéresse est celui qui relève du domaine politique. Encore une fois, le « discours politique » pourrait se voir approprier différentes définitions, mais en fonction de notre recherche nous avons choisi de mobiliser la posture du psychosociologue Alexandre Dorna.

La théorie de Dorna (1995) part de la prémisse selon laquelle le discours politique est une prise de parole « extérieure », qui s'adresse donc à un public. De cette façon il rejoint la notion de « théâtre » présentée par Goffman. À cela, il ajoute que ce discours provient *de facto* d'une interaction entre le politicien et les citoyens. « Le discours politique produit un lien d'interaction entre les membres d'une société. Être dans la société, c'est participer à une interaction » (p.132). Tout comme l'approche

de Goffman, la posture de Dorna s'ancre dans l'étude des interactions, qu'il considère cette fois comme une condition *sine qua non* au discours politique.

> Le discours politique est une parole qui se « fabrique » plutôt par et dans le « dehors » que par et dans le « dedans » des acteurs politiques, au sein d'une dynamique complexe d'interactions, intelligible et cernable, à condition de se tenir à l'idée suivante : l'analyse du discours politique *in situ* se trouve doublement surdéterminée, en amont, par le poids des antécédents psycho-socio-culturels, qui agencent l'histoire et le vécu de la communauté humaine, en aval, par les perceptions d'avenir, les craintes et les projets collectifs, à l'aune d'un cadre concret d'existence (Dorna, 2007, p.593).

Selon Dorna, le discours politique vise également à organiser une réalité, c'est-à-dire le changement ou le maintien du statu quo de l'ordre existant. L'homme politique est donc « constructeur de réalités discursives » en fonction de la poursuite de ses objectifs (Dorna, 2007).

> L'homme politique se veut un constructeur de réalité (mécanisme de référentialisation) d'où une accumulation de faits et de causes par rapport auxquels le leader se positionne et qui lui servent de démonstration de la vérité de son raisonnement, la crédibilité étant assurée par l'ancrage du leader et de son parti (Dorna, 1995, p.134)

Pour ce faire, la fabrication du discours politique doit toutefois s'inscrire dans une histoire, un contexte et une problématique partagée par l'ensemble des interlocuteurs. Ainsi, le politicien et son auditoire doivent partager les mêmes références pour que le discours soit efficace et ces références sont inscrites dans un contexte précis, en fonction d'une « réalité co-construite et identifiable » par l'ensemble des interlocuteurs (Dorna, 1995). C'est l'organisation de cette réalité co-construite, de cet état des lieux, qui assure à son discours une résonance chez le public. Or, cette réalité se construit grâce aux différentes interactions du politicien avec le public.

En terminant, Dorna postule que le discours politique « repose sur la volonté absolue de convaincre » (1995, p.133). Le discours politique vise donc la persuasion, par le biais de l'utilisation de différentes représentations et figures de style. Afin de persuader et convaincre, le politique a besoin de produire du sens (Dorna, 2007). Il ajoute finalement que le discours politique s'inscrit dans un processus intentionnel qui procède par une « une logique du vraisemblable », et non du vrai. Notamment, l'utilisation de figures rhétorique permet de créer le sentiment d'évidence nécessaire à la portée du discours politique.

Maintenant, quel est le public visé? À quel auditoire le discours politique s'adresse-t-il lorsqu'il tente de convaincre? Selon Dorna (2007), il s'agit des « membres d'une communauté sociale organisée politiquement » (p.596). Dans cette optique, le discours politique s'adresse à la population et l'on comprend qu'il vise à orienter l'opinion publique, en faveur du politicien. Ce mémoire s'intéresse justement à la réception du discours politique par les populations de Chine et des États-Unis. Nous croyons ainsi que le discours analysé au sein de cette recherche s'adresse à la fois aux citoyens américains et chinois qu'il tente de convaincre. Ceci étant dit, il serait également possible de présumer que ce discours s'adresse à l'ensemble de la communauté internationale.

En résumé, ce que nous entendons par « discours », dans le cadre de cette recherche, se rapporte à l'amalgame efficace de ces différentes suggestions. Lorsque nous mentionnons le discours des administrations Obama et Xi, nous ne parlons pas du discours en termes d'énoncé ou d'allocution, nous faisons plutôt référence à *l'ensemble de ce qui a été dit par un gouvernement, dans un contexte précis et relativement à une situation spécifique.* Nous nous intéressons donc au sens produit par le discours, en fonction des pratiques sociales où il prend place, ainsi qu'à l'intention de l'émetteur. Nous considérons ainsi que le discours politique américain et le discours politique chinois proposent chacun leur version de la réalité sur la

cyberattaque contre l'OPM, dans le but de construire une nouvelle représentation de la cybersécurité et ultimement, d'influencer la perception du public.

3.2.2. L'analyse de discours comme méthode

En fonction de la définition du terme discours offerte précédemment, la méthode d'analyse de discours préconisée pour cette recherche ne se rapporte pas à l'étude unique de la syntaxe ou de la grammaire. Nous nous rattachons plutôt à celle présentée par Dominique Maingueneau (1997), selon laquelle « l'intérêt qui oriente l'analyse du discours, c'est en effet de n'appréhender ni l'organisation textuelle en elle-même, ni la situation de communication, mais de penser le dispositif d'énonciation qui lie une organisation textuelle et un lieu social déterminés » (p.13). Autrement dit, nous souhaitons analyser le processus de construction discursive employé par les acteurs à l'étude relativement à la problématique qui nous intéresse, soit à la cyberattaque contre l'OPM et au Sommet de septembre 2015, et plus largement au domaine du cyberespace et de la cybersécurité.

Toujours selon Maingueneau (2012), le discours est considéré par les chercheurs comme offrant des indices qui permettent au chercheur d'accéder à des « réalités » hors du langage. Le discours, c'est le lieu où se construit la réalité sociale. Il n'est jamais neutre, c'est-à-dire qu'il est toujours porté par des intérêts et ce sont ces intérêts auxquels le chercheur s'intéresse. Selon Mainguenau (2012), les « discursivistes » utilisant l'analyse de discours comme méthode qualitative considèrent « les approches en termes de discours comme des instruments qui permettent de traiter des corpus et de les interpréter » (p.5). Il ne s'agit donc pas d'étudier les composantes purement linguistiques du texte ou de l'énoncé, mais de déceler les logiques d'intérêts qu'il supporte. Dans cette posture, le chercheur vise avant tout à repérer un certain nombre d'indicateurs significatifs, pour accéder à des

représentations ou à des conjonctures socio-historiques. Et c'est d'autant plus le cas dans le cadre de l'analyse du discours politique. Selon Maingueneau (2012), « les chercheurs recherchent des intérêts cachés derrière les textes » (p.10).

Selon Burnham *et al.* (2004), le thème récurrent dans la littérature entourant l'analyse de discours est que le discours reproduit les présomptions quotidiennes de la société et que ces perceptions communes sont encouragées et renforcées par ceux ayant accès aux médias, c'est-à-dire les politiciens, les journalistes et les experts académiques.

> *Language and discourse therefore frame and constrain given courses of action, some of which are promoted as sensible, moral and commanding wide levels of support, while others are discouraged as stupid, immoral and illegitimate. [...] It is the function of discourse analysis to reveal the bases of these common assumptions and to show how they relate to different interests in society* (Burnham *et al.*, 2004, p.242).

Selon eux, l'analyse de discours est souvent perçue comme une approche visant à contribuer à l'émancipation humaine et s'inscrit alors dans une posture critique. Il est donc normal que les chercheurs en sciences sociales (plus précisément en science politique) s'intéressent à l'analyse de discours, puisque la politique peut être décrite comme étant la bataille pour la domination du langage politique. Cette idée n'est pas tout à fait partagée par Maingueneau, qui affirme que dans de nombreux travaux sur le discours politique, le chercheur, s'il recherche des intérêts cachés derrière les textes, n'adopte pas pour autant un point de vue critique sur le discours. Il reconnaît par contre que « l'étude du fonctionnement du discours oblige à assumer le fait que le discours n'est jamais neutre, qu'il est toujours porté par des intérêts » (p.12). Dans cette optique, le seul fait d'analyser un discours a en soi une force critique.

En somme, nous retenons que le langage et le discours sont politiquement construits et utilisés pour légitimer certaines actions (Burnham *et al.*, 2004). L'analyse de discours a donc pour but de démontrer à la fois le processus de construction du

discours et la logique d'intérêts qu'il sert. Nous croyons donc que cette méthode est tout à fait appropriée pour notre objectif de recherche, qui vise à soulever les intérêts dissimulés derrière le discours des administrations Obama et Xi entourant la cyberattaque contre l'OPM et leur rencontre au Sommet de septembre 2015, ainsi que la façon dont ils ont construit une certaine représentation de la cybersécurité.

3.3. Présentation des documents sélectionnés

Le corpus de cette recherche sera composé de 15 documents, qui ont été retenus en fonction de leur pertinence directe ou indirecte en lien avec la situation analysée. Les textes choisis sont issus de la période allant du début de la présidence d'Obama (janvier 2009) jusqu'à la fin de l'année pendant laquelle la rencontre au Sommet a eu lieu (décembre 2015).

Ces documents se rapportent à deux types de discours. Dans un premier temps, il s'agit de déclarations présidentielles portant sur la cybersécurité. Par déclarations[28], nous entendons des communications publiques prononcées verbalement par les présidents Obama et Xi et se rapportant directement à la sécurité du cyberespace, ou encore des extraits de communications plus générales qui mentionnent la cybersécurité. Bien que ces déclarations ne soient pas directement en lien avec le cas à l'étude (soit la cyberattaque contre l'OPM), leur analyse nous semble essentielle puisqu'elles permettent de contextualiser le discours en opération pendant la présidence Obama, en lien avec la protection du cyberespace. Ces déclarations ont

[28] Le dictionnaire Larousse définit déclaration comme une « action de déclarer, de porter à la connaissance du public ; acte, écrit, discours par lequel on fait publiquement une communication » (Larousse, 2017c).

également l'avantage d'être un reflet direct des deux logiques d'intérêt en présence, de même que de correspondre au discours politique dans son expression la plus concrète.

Dans un second temps, nous avons sélectionné les documents de renseignement des deux administrations (points de presse, conférences, communiqués, etc.) concernant directement la cyberattaque contre l'OPM et la rencontre au Sommet. Ces textes représentent un survol quasi exhaustif de ce qui a été dit par les présidents et les représentants de leur administration dans le contexte de la crise entourant la cyberattaque contre l'OPM, ainsi que dans le cadre de leur rencontre au Sommet de septembre 2015.

3.3.1. Discours américain

Afin d'analyser séparément les deux perspectives en présence (américaine et chinoise), les textes ont été répartis par catégorie d'analyse. Nous allons donc présenter ici les différents documents, en commençant d'abord par la perspective américaine. Le premier document analysé est la déclaration du président Obama sur l'importance de sécuriser les cyberinfrastructures de la nation, prononcée le 29 mai 2009. Lors de cette déclaration, le président nouvellement en poste a ainsi présenté aux Américains l'approche de son gouvernement pour sécuriser les cyberinfrastructures des États-Unis.

La seconde déclaration du président Obama étudiée a été prononcée en janvier 2015 au *National Cybersecurity and Communications Integration Center* (NCCIC). Sous la supervision du Département de la sécurité intérieure (*Department of Homeland Security*), le NCCIC est un centre de surveillance, de gestion et de réponse aux cyberincidents en fonction 24h par jour, 7 jours sur 7. Cette prise de parole publique

visait à revisiter ce qui avait été fait par son gouvernement pour renforcer la cybersécurité ainsi qu'à exprimer ce qu'il avait l'intention de faire à l'avenir pour défendre les systèmes de la nation.

La troisième déclaration a quant à elle été prononcée en février 2015 au *Cybersecurity and Consumer Protection Summit*, à Stanford. Ce sommet rassemblait des leaders du gouvernement fédéral américain, du secteur des affaires ou des autorités du maintien de l'ordre, ainsi que des étudiants et chercheurs de l'Université de Stanford. Ce sommet avait pour but d'aborder des questions touchant au partage d'information entre les secteur public et privé de même que de la mise en place de pratiques de cybersécurité, etc.

Quant aux documents informatifs produits par les représentants de l'administration américaine, il s'agit de deux points de presse de l'attaché de presse de la Maison-Blanche Josh Earnest touchant à la cyberattaque contre l'OPM (9 et 25 juin 2015), ainsi qu'un communiqué de la Maison-Blanche concernant la visite d'État du président Xi Jinping aux États-Unis, émis le 25 septembre 2015. Nous avons également retracé le contenu d'une conférence de presse téléphonique explicative précédant la visite du président Xi, s'étant tenue le 22 septembre 2015. Cette conférence et sa retranscription en ligne avaient pour objectif de présenter aux médias et au public le déroulement de la rencontre de même que les objectifs visés par le gouvernement américain. Finalement, le dernier document analysé du côté de la perspective américaine est la prise de parole du président Obama lors de la conférence de presse qu'il a tenu conjointement avec le président Xi à la Maison-Blanche en marge de leur rencontre au Sommet, le 25 septembre 2015.

3.3.2. Discours chinois

En ce qui concerne la perspective chinoise, trois déclarations présidentielles ont été choisies. La première a été prononcée le 16 novembre 2012 lors de la réunion élargie de la Commission militaire centrale par le Secrétaire général du Comité central du Parti communiste chinois nouvellement élu, Xi Jinping. Cette déclaration consistait en la première prise de parole du leader chinois concernant l'édification de la défense nationale et de l'armée, adressée notamment aux officiers de haut rang de l'armée chinoise.

La seconde déclaration du président chinois consiste en une prise de parole lors d'un dîner de bienvenue organisé par le Comité national sur les relations Chine-États-Unis (*National Committee on U.S.-China Relations*) le 22 septembre 2015, à Seattle, aux États-Unis. Il s'agit de l'unique déclaration publique du président Xi pendant sa visite officielle aux États-Unis, dans le cadre du Sommet 2015, en dehors de sa conférence de presse conjointe avec le président Obama.

La troisième déclaration du président Xi a quant à elle été prononcée quelques mois après sa rencontre au Sommet avec le président américain, soit en décembre 2015. Il s'agit du discours[29] d'ouverture de la 2e Conférence mondiale sur l'Internet (*World Internet Conference*), qui se tenait à Wuzhen, en Chine. Cette conférence rassemblait des représentants de gouvernements, d'organisations internationales, d'entreprises ainsi que d'organisations non gouvernementales provenant de partout dans le monde. L'objectif était d'échanger des idées notamment sur la gouvernance mondiale et le développement d'Internet ainsi que sur la cybersécurité.

---

[29] Le terme discours renvoie ici à une communication orale, prononcée en publique, lors d'une occasion solennelle (Larousse, 2017d). Dans ce contexte, nous l'employons également comme un synonyme du terme déclaration (Larousse, 2017c).

Finalement, nous avons sélectionné cinq documents informatifs produits par les représentants de l'administration chinoise relativement à la cyberattaque contre l'OPM, au Sommet et aux enjeux de cybersécurité. Il s'agit d'abord de deux conférences de presse régulières ainsi que d'un énoncé des porte-paroles du ministère des Affaires étrangères de la République populaire de Chine (Hong Lei et Hua Chunying) tenus les 5 juin, 10 juillet et 14 août 2015. Ensuite, nous avons retenu le communiqué du ministère des Affaires étrangères chinois émis le lendemain de la visite d'État du président Xi Jinping aux États-Unis, soit le 26 septembre 2015, et enfin, le dernier document est issu de la conférence de presse conjointe des deux présidents tenue à la Maison-Blanche, mais cette fois reprend les propos du président chinois.

En conclusion, nous pensons que ce corpus est représentatif, parce qu'il offre un traitement équitable des deux perspectives en présence.

3.4. Collecte de données et grille d'analyse

La méthode d'analyse et de collecte de données préconisée pour ce mémoire s'opère autour de l'utilisation d'une grille d'analyse, élaborée en fonction du cadre théorique et de l'approche méthodologique préconisés. Les données issues de la collecte seront par la suite analysées en fonction du contexte et de la problématique générale présentée.

Cette grille d'analyse a été construite à partir des questions sectorielles et de leurs sous-questions, et comporte ainsi quatre sections distinctes. La première section s'intéresse à la vision générale de chaque chef de gouvernement en matière de cybersécurité. La deuxième section se rapporte directement aux messages clés

transmis dans les discours des deux administrations et vise à déterminer la posture de chaque gouvernement quant à la cyberattaque contre l'Office of Personnel Management et à la rencontre au Sommet. La troisième section a pour objectif de comprendre les stratégies communicationnelles employées par les administrations et d'ainsi déterminer le processus de construction du message. Quant à la quatrième et dernière section, elle se rapporte aux logiques d'intérêt poursuivies par les gouvernements à l'étude. C'est donc en comptabilisant les données issues de cette analyse que nous pourrons répondre à notre question centrale de recherche. Voici cette grille:

Question centrale : Comment s'articule le processus de construction du discours des administrations Obama et Xi entourant la cyberattaque sur 21,5 millions d'enquêtes de sécurité et lors de la rencontre au Sommet de septembre 2015 ?

1) **Objectif:** Identifier la vision générale de chaque président relativement à la cybersécurité.

Question sectorielle: Quelle est la position politique défendue par les présidents Obama et Xi en matière de cybersécurité?

a) Quels sont les principaux thèmes abordés par les présidents?
b) Les deux présidents partagent-ils une vision commune en matière de cybersécurité?

2) **Objectif:** Déterminer la posture de chaque gouvernement quant à la cyberattaque contre l'Office of Personnel Management et à la rencontre au Sommet.

Question sectorielle: Quels messages clés (ou vérités) les discours des deux administrations tentent-ils de véhiculer?

a) Quelles sont les ressemblances et les différences entre les messages des deux administrations?
b) Comment la cyberattaque contre l'OPM et le Sommet sont-ils présentés?
c) Quels arguments viennent-ils en appui aux messages véhiculés?

3) **Objectif:** Comprendre comment les stratégies discursives employées par les deux gouvernements visent à construire une certaine réalité.

Question sectorielle: Quel est le processus de construction du message employé par les deux administrations ?

a) Quelles sont les principales expressions (mots clés) utilisées?
b) Comment les termes « cyberespace » et « cybersécurité » sont-ils employés?
c) Y aurait-il des « non-dits », ou encore des omissions, dans les discours officiels?

4) **Objectif:** Déterminer quelles sont les logiques d'intérêt en présence et en quoi la formulation du discours en permet efficacement la poursuite.

Question sectorielle: Quels sont les intérêts nationaux poursuivis par chaque gouvernement ?

a) Quelles positions les deux administrations tentent-elles de faire valoir?
b) Les intérêts sont-ils clairement perceptibles dans les discours?
c) En quoi le discours officiel entourant la cybersécurité contribue-t-il à la poursuite de ces intérêts?
d) Quels bénéfices les deux administrations tirent-elles ? L'une des deux en ressort-elle gagnante et si oui, en quoi est-elle avantagée?

3.5. Limites de la recherche

En terminant, mentionnons que notre recherche comporte certaines limites. En effet, elle s'intéresse à un important enjeu en matière de relations diplomatiques, de gouvernance mondiale et de sécurité nationale, et ce type de sujet est difficile à traiter dans le cadre d'une recherche académique.

Tout d'abord, la première limite à ce mémoire consiste en la difficulté d'accès à l'information, autant du côté américain que du côté chinois. En ce qui concerne la cyberattaque contre l'OPM, le gouvernement américain a en effet avantage à ne pas

s'étendre sur les dommages concrets que l'organisation a subis et sur les données, extrêmement confidentielles, qui lui ont été dérobées. L'information que nous possédons entourant cette attaque provient ainsi principalement de sources secondaires, soit des médias et des experts du monde académique. Il est impossible au chercheur d'avoir accès à l'information gouvernementale secrète, pour laquelle même les fonctionnaires fédéraux doivent d'abord passer une enquête de sécurité et être accrédités, ce qui n'est évidemment pas notre cas. Du côté du gouvernement chinois, l'accès à l'information est d'autant plus difficile que très peu de documents sont rendus publics, et encore moins accessibles aux étrangers. Notamment en matière de cybersécurité, contrairement aux États-Unis qui rendent publics leurs divers documents de stratégie nationale, la Chine se montre plus réservée en ce qu'elle se permet de dévoiler. Quant aux documents accessibles, s'il y en a, ils ne sont disponibles qu'en langue chinoise[30].

Ce qui nous amène à mentionner la deuxième limite de cette recherche, à savoir que nous ne possédons que des connaissances de base en chinois. C'est une limite à plusieurs niveaux, d'abord parce qu'elle nuit une fois de plus à l'accès à l'information en réduisant le champ des documents accessibles pour l'analyse. Ensuite, ne pas être suffisamment à l'aise avec le chinois nous empêche de saisir toutes les subtilités des propos originaux qui ne sont pas reproduites avec la traduction. Finalement, nous pensons que la maîtrise de la langue ouvre sur une connaissance plus approfondie de la culture en présence[31]. Or, le contexte culturel étant fort important pour ce type d'analyse communicationnelle, tel que mentionné précédemment, ne pas en avoir une compréhension parfaite ne peut que nuire à la perception et l'interprétation du discours. Par contre, nous pensons que l'essentiel du message de la perspective

---

[30] Il existe différentes langues parlées en Chine, dont les plus répandues sont le mandarin et le cantonais. Or, nous avons choisi par simplicité de les regrouper sous le terme de « chinois ».

[31] Lors d'une rencontre en privé avec la vice-consul de Chine à Montréal, elle a affirmé en français: « Pour connaître la Chine, il faut parler chinois ».

chinoise est tout de même suffisamment perceptible et c'est pourquoi nous pensons que l'analyse offrira des résultats pertinents.

En terminant, la troisième principale limite à cette recherche concerne son objet d'étude, à savoir que ce mémoire ne s'attarde pas à la réception médiatique et populaire du discours des administrations chinoise et américaine et donc, qu'il ne permet pas d'en mesurer l'efficacité. Nous pensons toutefois qu'il est nécessaire de circonscrire notre objet d'étude et ouvrons ainsi la porte à une analyse subséquente, qui pourra par ailleurs être plus facilement conduite avec davantage de recul dans l'échelle du temps.

CHAPITRE IV

ANALYSE ET PRÉSENTATION DES RÉSULTATS

Dans ce quatrième chapitre de notre mémoire, nous présenterons les résultats issus de l'analyse des documents afin de répondre aux questions soulevées et ultimement, aux différents objectifs de cette recherche. Pour ce faire, nous avons choisi de diviser l'analyse en deux parties. Dans la première, nous présenterons l'analyse discursive des déclarations présidentielles relatives à la cybersécurité en général. En commençant de la sorte, nous pouvons d'abord déterminer le contexte plus global des visions présidentielles entourant la cybersécurité. Dans la seconde partie, nous nous attardons directement aux documents faisant référence (de façon directe ou indirecte) à la cyberattaque contre l'OPM et à la rencontre au Sommet de septembre 2015. Par la suite, nous présenterons les résultats de notre analyse, c'est-à-dire que nous répondrons à chacune des questions sectorielles posées dans ce mémoire. Finalement, nous répondrons à la question centrale et validerons notre hypothèse de recherche.

4.1. Analyse des déclarations présidentielles

La première partie de notre analyse se penche sur les déclarations présidentielles, c'est-à-dire qu'elles ont été prononcés par les présidents Obama et Xi, lors desquelles ils se sont attardés, ne serait-ce que l'espace de quelques mots, à la cybersécurité. Par cette analyse, nous espérons être en mesure d'identifier la vision politique de chaque président entourant cet enjeu. Une fois effectuée, cette analyse nous permettra de déterminer la posture politique de chaque président en regard de la cybersécurité et

ainsi de répondre à la première question sectorielle. Les documents choisis pour cette analyse sont, du côté américain, la Déclaration du président Obama sur l'importance de sécuriser les cyberinfrastructures de la nation (29 mai 2009), la Déclaration du Président Obama au *National Cybersecurity and Communications Integration Center* (13 janvier 2015) et la Déclaration du Président Obama au *Cybersecurity and Consumer Protection Summit*, à Stanford (13 février 2015). Du côté chinois, nous analyserons la déclaration du président Xi Jinping prononcée lors de la réunion élargie de la Commission militaire centrale (16 novembre 2012), la déclaration du président Xi lors d'un dîner de bienvenue organisé par le Comité national sur les relations Chine-États-Unis à Seattle (22 septembre 2015) ainsi que le discours[32] du président Xi lors de la cérémonie d'ouverture de la deuxième Conférence mondiale sur l'Internet (16 décembre 2015).

4.1.1. Perspective du président américain

À la lumière de l'analyse discursive portant sur les déclarations du président américain Barack Obama, nous avons été en mesure de définir six grands thèmes récurrents entourant la cybersécurité. La première thématique renvoie à l'importance du cyberespace pour la société américaine dans son ensemble. En effet, tel que présenté dans le premier chapitre, le président Obama a mentionné aux citoyens américains le caractère essentiel du cyberespace pour les États-Unis dès la première année de sa présidence, en 2009. Lors d'une déclaration à la Maison-Blanche, il a affirmé:

> [...] *none of this progress would be possible, and none of these 21st century challenges can be fully met, without America's digital*

[32] Discours est ici encore une fois utilisé comme un synonyme du terme déclaration (Larousse, 2017c).

> *infrastructure -- the backbone that underpins a prosperous economy and a strong military and an open and efficient government* (Obama, 29 mai 2009).

Le président américain réitère ainsi à plusieurs reprises dans ses déclarations que l'économie américaine et son commerce international dépendent désormais du cyberespace, qui procure aux Américains des opportunités extraordinaires et qui permet de créer des emplois (Obama, 13 janvier 2015 ; 13 février 2015).

Plus encore, il affirme que la compétitivité économique des États-Unis est directement reliée à leur capacité d'innover et de commercer en ligne:

> *As a nation, we do more business online than ever before -- trillions of dollars a year. And high-tech industries, like those across the Valley, support millions of American jobs. All this gives us an enormous competitive advantage in the global economy* (Obama, 13 février 2015).

Selon le président Obama, les États-Unis dépendent donc du cyberespace pour leur sécurité économique. Il affirme que le commerce électronique à lui seul représente annuellement plusieurs milliers de milliards de dollars US (Obama, 29 mai 2009 ; 13 février 2015).

Or, le second thème abordé dans chacune des déclarations du président fait référence aux nombreux risques et menaces que comporte également le cyberespace. Barack Obama affirme en effet qu'il s'agit de l'un des plus grands défis du 21^{e} siècle, à la fois en matière de sécurité économique, mais également en matière de sécurité nationale. « [...] *it's now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation* » (Obama, 29 mai 2009).

La cybermenace envers l'économie américaine est donc considérée comme l'une des priorités pour le gouvernement américain. Le président affirme directement que les

compagnies américaines sont la cible de différents pirates informatiques : « [...] *their trade secrets stolen, intellectual property ripped off* [...] *And these attacks are hurting American companies and costing American jobs. So this is also a threat to America's economic security* » (Obama, 13 février 2015). Pour cette raison, le président stipule que les différentes cybermenaces représentent le plus important défi pour la sécurité économique américaine et que de les combattre est une priorité pour son gouvernement (Obama, 13 février 2015).

En ce qui concerne les acteurs impliqués dans les principales cybermenaces, le président américain affirme que les cyberattaques peuvent provenir à la fois de gouvernements étrangers que de criminels (Obama, 13 janvier 2015). Lors de son discours au Sommet sur la cybersécurité de l'Université de Stanford, il va même jusqu'à faire directement référence aux menaces provenant de la Chine et de la Russie:

> *And it's one of the great paradoxes of our time that the very technologies that empower us to do great good can also be used to undermine us and inflict great harm. The same information technologies that help make our military the most advanced in the world are targeted by hackers from China and Russia who go after our defense contractors and systems that are built for our troops* (Obama, 13 février 2015).

Le président américain mentionne également la menace terroriste, de même que les risques en regard des infrastructures essentielles telles que les systèmes de finance, les réseaux électriques et les systèmes de santé, qui utilisent toutes Internet, ce qui en fait une question de sécurité publique (Obama, 29 mai 2009; 13 février 2015).

Tous ces risques sont considérés comme une menace en matière de sécurité nationale et doivent donc être adressés. Pour ce faire, le président Obama souhaite renforcer les défenses américaines: « *This status quo is no longer acceptable -- not when there's so much at stake. We can and we must do better* » (Obama, 29 mai 2009). Le président

croit que les États-Unis doivent tout faire pour demeurer à l'avant-plan en matière d'innovation et de cyberdéfense, puisque leurs adversaires sont de plus en plus sophistiqués et déterminés (Obama, 13 janvier 2015 ; 13 février 2015).

Le troisième thème récurrent dans le discours du président Obama est celui de la nécessité d'investir en innovation et en éducation. Le président américain croit en effet que la meilleure façon pour les États-Unis de poursuivre sur la voie du développement économique, social et sécuritaire, est d'encourager la relève et d'investir dans le domaine du numérique. En 2009, il annonce ainsi: « [...] *we will continue to invest in the cutting-edge research and development necessary for the innovation and discovery we need to meet the digital challenges of our time* » (Obama, 29 mai 2009). Selon le président américain, les États-Unis doivent réussir dans le monde numérique, continuer à innover et à créer des entreprises et des emplois afin d'étendre la connectivité à davantage d'individus (Obama, 13 février 2015).

De plus, il argumente également dans ses différentes déclarations que les jeunes doivent être formés en matière de littératie numérique, afin de créer une « *digital workforce* » pour le 21^{e} siècle : « [...] *social networking and e-mailing and texting and blogging -- we need them to pioneer the technologies that will allow us to work effectively through these new media and allow us to prosper in the future* » (Obama, 29 mai 2009). Pour ce faire, il souhaite accroître le nombre de communautés et d'individus connectés à Internet aux États-Unis et offrir un Internet moins cher, afin de donner à tous des opportunités d'innovation (Obama, 13 février 2015). Finalement, il souhaite également investir dans la formation des professionnels de la cybersécurité pour leur permettre de développer de nouveaux talents (Obama, 13 janvier 2015). Ils seraient ainsi en mesure de mieux protéger les réseaux informatiques des États-Unis.

Le quatrième thème présent dans le discours du président américain est celui de la gouvernance multipartite, c'est-à-dire de la collaboration en matière de cybersécurité. Le président Obama affirme en effet que le meilleur moyen de relever les défis du cyberespace est de favoriser la collaboration entre tous les acteurs clés provenant de différents secteurs (gouvernement fédéral, gouvernements locaux, secteur privé). Pour répondre adéquatement aux cyberattaques et aux incidents, les acteurs doivent partager de l'information et s'assurer d'une réponse coordonnée, sans pourtant que le gouvernement ne s'immisce dans les façons de faire de l'industrie :

> [...] *we will strengthen the public/private partnerships that are critical to this endeavor.* [...] *So let me be very clear: My administration will not dictate security standards for private companies. On the contrary, we will collaborate with industry to find technology solutions that ensure our security and promote prosperity* (Obama, 29 mai 2009).

Selon le président Obama, la protection du cyberespace relève d'une responsabilité partagée entre les secteurs public et privé, car aucun ne peut défendre seul la nation. Il affirme que le gouvernement et l'industrie doivent travailler main dans la main en tant que partenaires (Obama, 13 janvier 2015). Il s'agit selon lui de la seule façon de protéger adéquatement les États-Unis des cybermenaces:

> [...] *Just as we're all connected like never before, we have to work together like never before, both to seize opportunities but also meet the challenges of this Information Age* [...] *There's only one way to defend America from these cyber threats, and that is through government and industry working together, sharing appropriate information as true partners* (Obama, 13 février 2015).

Quant à la cinquième thématique, plus subtile mais tout aussi présente, il s'agit de l'importance de respecter la vie privée des citoyens, l'un des grands principes du gouvernement américain sous Obama. Selon lui, il s'agit d'une part de protéger les informations personnelles et confidentielles des individus contre des acteurs

malveillants (pirates informatiques, cybercriminels, etc.) et d'autre part, de promettre que le gouvernement respectera la vie privée et les droits civils des Américains (Obama, 13 janvier 2015 ; 13 février 2015). Au tout début de son premier mandat en tant que président des États-Unis, Barack Obama affirme ainsi que son gouvernement va préserver et protéger la vie personnelle des citoyens et des entreprises américaines. Le respect de la vie privée est une valeur américaine et le président s'engage dans ses différentes déclarations sur la cybersécurité à ce que son gouvernement la protège: « *Our pursuit of cybersecurity will not -- I repeat, will not include -- monitoring private sector networks or Internet traffic* » (Obama, 29 mai 2009).

Finalement, le sixième thème renvoie à l'importance pour les États-Unis de promouvoir leurs valeurs et leur leadership en matière de cyberespace. Le président Obama positionne en effet les États-Unis en tant que leader de l'économie numérique (13 février 2015). Il tient à rappeler que les États-Unis ont inventé Internet et qu'ils doivent ainsi s'assurer de diriger son évolution afin d'accroître le potentiel de prospérité:

> [...] *the United States -- the nation that invented the Internet, that launched an information revolution, that transformed the world -- will do what we did in the 20th century and lead once more in the 21st* (Obama, 29 mai 2009).

Il affirme également que le leadership américain doit permettre de favoriser les valeurs américaines au sein du développement du cyberespace: « [*cyberspace*] *will not just be about technology, it will be about the values that we've embedded in the architecture of this system* » (Obama, 13 février 2015).

4.1.2. Perspective du président chinois

En ce qui concerne le président chinois Xi Jinping, il emploie dans ses déclarations cinq grands thèmes récurrents en matière de cybersécurité. Le premier thème fait référence à l'importance pour la Chine de son développement économique et du lien qu'elle établit entre prospérité et innovation technologique. La Chine est ainsi sur la voie de la modernisation à plusieurs niveaux:

> *The key to China's development lies in reform. Our reform is aimed at modernizing the country's governance system, and governance capabilities so that the market can play a decisive role in the allocation of resources* (Xi, 22 septembre 2015)

Selon le Président Xi, le cyberespace occupe une place de premier plan au sein des objectifs de développement chinois. Il perçoit ainsi le cyberespace et l'ensemble des technologies de l'information et de la communication comme un facteur essentiel pour la croissance économique du pays: « *The Internet is now deeply integrated into China's economic and social development and the life of the Chinese people* » (Xi, 2015b). Ainsi, le cyberespace est considéré essentiel pour la prospérité de la Chine et le président Xi situe l'innovation technologique et l'utilisation globale d'Internet à la base de son plan de développement dans la quasi-totalité des secteurs.

> [...] *promote innovative development of cyber economy for common prosperity. The world economy is on a difficult and tortuous path to recovery. The Chinese economy is also under a certain downward pressure. Solution lies in an innovation driven development, which will open new horizons of development. China is now implementing the Internet Action Plan, advancing the building of digital China, developing the sharing economy and supporting Internet based innovation in all forms, with the view of improving the quality and efficiency of development* (Xi, 16 décembre 2015)

Le président Xi a également affirmé dans son discours de décembre 2015, lors de l'ouverture de la Conférence mondiale sur Internet, qu'il souhaitait intégrer le développement d'Internet au progrès économique et social de la Chine. Pour ce faire, il a pour objectif de s'assurer que 1,3 milliard de Chinois (soit l'entière population de Chine) auront accès à Internet et pourront en bénéficier (Xi, 16 décembre 2015). Par ailleurs, le président chinois reconnaît que le développement du cyberespace, s'il est essentiel à la prospérité économique de la Chine, est également essentiel pour l'ensemble de la communauté internationale, affirmant : « [...] *the Internet will only play a bigger role in the progress of human civilization* » (Xi, 16 décembre 2015).

Le deuxième thème présent dans les différentes déclarations du président chinois consiste en l'établissement du lien entre cyberespace et sécurité nationale. En effet, parce que le président reconnaît le caractère essentiel du cyberespace pour le développement et la prospérité, il reconnaît la nécessité d'en faire la protection. À ce sujet, il affirme: « *Security and development are like the two wings of a bird or the two wheels of a bicycle. Security ensures development and development is what security is aimed at* » (Xi, 16 décembre 2015).

Ainsi, la protection du cyberespace (ou cybersécurité) est définie comme un enjeu de premier plan en matière de sécurité nationale. C'est que le président croit en l'émergence de nouvelles menaces mondiales issues du cyberespace. Selon lui, la cybersurveillance, les cyberattaques et le cyberterrorisme sont devenus un fléau global et représentent un défi international (Xi, 16 décembre 2015). À ce titre, il affirme que la Chine est un grand défenseur de la cybersécurité, notamment parce qu'elle est elle-même victime de cyberattaques et d'intrusion informatique (Xi, 22 septembre 2015).

C'est pourquoi le Président Xi a reconnu, dès son entrée en poste à titre de secrétaire général et président de la Commission militaire centrale du Parti communiste chinois en 2012, l'importance de moderniser les forces armées chinoises et d'augmenter de manière générale les cybercapacités militaires:

> La souveraineté et la sécurité nationale doivent passer avant toute autre considération. Pour cela, l'armée doit insister sur l'importance primordiale de sa préparation au combat, augmenter de manière générale nos capacités en termes de dissuasion et de combat cybernétiques, et protéger les intérêts d'État en matière de souveraineté, de sécurité et de développement [...] Nous approfondirons la réforme militaire, afin de construire un système moderne de forces armées aux caractéristiques chinoises (Xi, 16 décembre 2012).

Par ailleurs, le président affirme qu'un cyberespace sécuritaire, stable et prospère revêt une grande importance pour l'ensemble des pays. Il dit souhaiter que le cyberespace ne devienne pas un « champ de bataille » permettant aux États de lutter les uns contre les autres, et encore moins un bassin pour le crime (Xi, 16 décembre 2015).

La troisième thématique renvoie à l'importance de la coopération internationale en matière de cybersécurité. En effet, le président chinois affirme qu'aucun pays ne peut se protéger seul et que la communauté internationale doit travailler main dans la main afin d'établir un cyberespace sécuritaire : « *Cyber security is a global challenge and no country can stay aloof or immune from it. Maintaining cyber security is the shared responsibility of the international community* » (Xi, 16 décembre 2015). Dans ses déclarations, le président chinois fait état de la coopération internationale en regard de la protection du cyberespace contre son utilisation pour les crimes, tels que le terrorisme, la pornographie, le trafic de drogue, etc. Il se positionne de façon claire pour l'établissement d'un dialogue international reposant sur le respect et la confiance mutuels (Xi, 22 septembre 2015; 16 décembre 2015).

> *The future of cyberspace should be in the hands of all countries. Countries should step up communication, broaden consensus and deepen cooperation to jointly build a community of shared future in cyberspace* (Xi, 16 décembre 2015).

Cette idée de responsabilité partagée renvoie ainsi à la quatrième thématique présente dans le discours du Président Xi, soit la nécessité du multilatéralisme comme forme de gouvernance mondiale d'Internet et de la promotion de normes internationales en regard du cyberespace. En effet, le président est clair quant à cette position: il défend tout pays (et indirectement les États-Unis) d'aspirer à être le seul arbitre sur la scène internationale et particulièrement en ce qui a trait à la gouvernance du cyberespace.

> *International cyberspace governance should feature a multilateral approach with multiparty participation. It should be based on consultation among all parties, leveraging the role and various players including governments, international organizations, Internet companies, technology companies, non-governmental institutions and individual citizens. There should be no unilateralism. Decisions should not be made with one party calling the shot or only a few parties discussing among themselves* (Xi, 16 décembre 2015).

Le président se fait ainsi le défenseur du droit international et milite pour la création de normes internationales quant à l'utilisation et le développement d'Internet. Il affirme que le cyberespace ne doit pas être au-dessus de l'État de droit (Rule of Law) et que les droits et obligations des parties concernées devraient être clairement définis (Xi, 16 décembre 2015).

Enfin, le cinquième thème fait référence à la cybersouveraineté de chaque État, et nommément à celle de la Chine, ainsi qu'au respect des différences entre les États et la non-ingérence dans les affaires internes. Le Président Xi mentionne à plusieurs reprises que le respect de la cybersouveraineté est directement lié au principe de

souveraineté inscrit dans la Charte des Nations Unies comme l'un des fondements des normes des relations internationales contemporaines (Xi, 16 décembre 2015). Il affirme que les pays ont le droit individuel de choisir leur propre modèle de développement et de régulation du cyberespace de même que le droit de participer, sur un pied d'égalité, dans la gouvernance internationale du cyberespace : « *No country should pursue cyber hegemony, interfere in other countries internal affairs and engaged in or support cyber activities that undermine other countries national security and maintenance of peace and security* » (Xi, 16 décembre 2015).

Par ailleurs, il ajoute qu'il est essentiel de respecter les différences entre les États: « [...] *we must manage our differences properly and effectively. As a Chinese saying goes, the sun and moon shine in different ways yet their brightness is just right for the day and night, respectively* » (Xi, 22 septembre 2015). Il va sans dire qu'une telle prise de position résonne comme une mise en garde.

4.2. Analyse des documents entourant la cyberattaque et le Sommet

La seconde partie de l'analyse sera dédiée aux documents produits par les deux administrations en regard de la cyberattaque contre l'OPM et de la rencontre au Sommet de septembre 2015. Nous avons une fois de plus divisé cette partie en deux sous-sections, c'est-à-dire que nous allons d'abord analyser les documents de l'administration américaine et qu'ensuite nous allons analyser ceux de l'administration chinoise. Cette façon de procéder nous permet ainsi d'analyser les deux perspectives séparément, avant de les comparer lors de la présentation des résultats. Cette section nous permettra de déterminer les stratégies discursives employées par chaque gouvernement. Elle nous permettra également de repérer les logiques d'intérêt en présence. Parmi l'ensemble des échantillons, un seul sera analysé deux fois: la

conférence de presse conjointe tenue par les présidents Obama et Xi, à la Maison-Blanche, lors du Sommet de septembre 2015.

4.2.1. Documents de l'administration américaine

En ce qui concerne la perspective de l'administration américaine, l'analyse porte sur cinq documents: les deux points de presse de l'attaché de presse de la Maison-Blanche Josh Earnest les 9 et 25 juin 2015, la conférence téléphonique avec les médias précédant la visite du président Xi le 22 septembre 2015, la conférence de presse conjointe des présidents Obama et Xi à la Maison-Blanche en marge de leur rencontre au Sommet [extraits du président américain] le 25 septembre 2015 et finalement, le communiqué de la Maison-Blanche concernant la visite d'État du président Xi Jinping aux États-Unis publié le 25 septembre 2015.

Le premier constat issu de l'analyse des documents de l'administration américaine est que dès le dévoilement de la cyberattaque, la Maison-Blanche ne souhaite pas tirer de conclusions hâtives quant à l'origine de l'attaque ni aux possibles représailles envisagées. Lors de ses deux conférences de presse, l'attaché de la Maison-Blanche Josh Earnest rappelle qu'une enquête du Federal Bureau of Investigation (FBI) est en cours et qu'elle vise à déterminer à la fois l'étendue de la cyberattaque, les individus qui sont derrière l'attaque ainsi que leurs motifs, et s'ils travaillaient dans un but criminel ou plutôt pour le compte d'un État (WH, 9 juin 2015). Aucun suspect n'est alors dévoilé, bien que l'attaché de presse reconnaisse qu'il s'agissait d'individus fort bien outillés et persistants. Le gouvernement se montre donc bien prudent en matière d'attribution et évite de se mouiller en pointant du doigt quelconque adversaire.

Toutefois, la Maison-Blanche laisse entendre que peu importent les individus derrière l'attaque, de possibles sanctions pourraient être imposées aux coupables. À ce titre, elle fait savoir qu'elle dispose d'outils lui permettant d'imposer des sanctions économiques à ceux qui sont responsables ou qui ont bénéficié d'une cyberattaque (WH, 9 juin 2015, 25 juin 2015). S'il n'est pas clair à ce moment que la Chine est la principale cible visée par ces avertissements, une menace de représailles lui est lancée par le président Obama lors de la conférence de presse du 25 septembre 2015. Le président a en effet laissé entendre à son homologue chinois que les États-Unis utiliseront tous les outils dont ils disposent pour s'en prendre aux cybercriminels, que ce soit rétrospectivement ou prospectivement. Il ajoute toutefois que ce ne sont pas outils généralement utilisés contre les gouvernements, mais plutôt contre les individus (WH, 2015a). Tout de même, on peut en déduire que le président américain laisse planer un avertissement envers le président Xi.

Un autre constat issu de l'analyse de la perspective américaine est l'importance pour les États-Unis de maintenir un climat de collaboration avec la Chine. L'administration Obama réitère à plusieurs reprises que son partenariat économique avec la Chine est l'un des piliers au centre des intérêts économiques américains (WH, 22 septembre 2015). Or, cette collaboration économique sino-américaine dépend en grande partie d'une amélioration dans le domaine du cyber, devenu un enjeu majeur de leur relation bilatérale. Ce différend entre les deux États, en particulier en matière de vol de secrets commerciaux et de propriété intellectuelle, est l'un des principaux enjeux mettant à risque leur coopération future et à ce titre, il devient une priorité américaine lors du Sommet de septembre 2015. Pendant la conférence téléphonique en préparation au Sommet, l'administration Obama affirme directement que « l'enjeu du cyber et particulièrement les inquiétudes qu'ils ont en regard des divers comportements

chinois dans le royaume du cyber seront un point de mire clé lors des discussions entre les deux présidents [33]» (WH, 22 septembre 2015).

L'objectif des États-Unis à cet égard est donc d'amener la Chine à respecter les règles du jeu du commerce international et de lui faire comprendre que c'est dans son intérêt propre. Ils affirment que la Chine ne peut plus être un « *free-rider* » du système international. Les Américains veulent donc mettre l'emphase sur l'importance de protéger la propriété intellectuelle afin de permettre aux entreprises d'opérer sans crainte de cybervols. C'est d'ailleurs leur principale réussite lors du Sommet: les États-Unis et la Chine ont en effet convenu, au cœur de leur entente de septembre 2015, de ne pas conduire ni soutenir le vol de secrets commerciaux et de propriété intellectuelle. En conférence de presse, le président Obama affirme ainsi:

> *I raised once again our very serious concerns about growing cyber-threats to American companies and American citizens. I indicated that it has to stop. The United States government does not engage in cyber economic espionage for commercial gain. And today, I can announce that our two countries have reached a common understanding on the way forward. We've agreed that neither the U.S. or the Chinese government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage* (Obama, 25 septembre 2015).

L'importance de régler la question du cyberespionnage économique envers les entreprises américaines était donc au cœur de la rencontre entre les deux présidents. Par ailleurs, les États-Unis ont été bien clairs sur la différence entre l'espionnage dit traditionnel, et l'espionnage économique. En effet, ils ont rappelé lors de la conférence téléphonique précédant le Sommet qu'il ne s'agissait pas d'un enjeu concernant l'espionnage traditionnel des États, mais plutôt d'un enjeu économique:

---

[33] Traduction libre : « *the issue of cyber and particularly of the concerns that we have with various Chinese behaviors in the cyber realm will be a key focus of the discussions* » .

> [...] *we're drawing a very clear distinction between the fact that, look, there are activities that all governments engage in as it relates to national security, but what we don't engage in as the United States is the theft of trade secrets. And that's something that gets at the integrity of the global economy, and that's why we've been so focused on this* (WH, 22 septembre 2015).

À notre avis, cette différenciation en matière d'espionnage vise à affirmer indirectement que les États-Unis considèrent la cyberattaque contre l'OPM comme un acte d'espionnage politique traditionnel.

C'est d'ailleurs pourquoi nous pensons, en matière d'omission d'information, qu'on ne retrouve aucune référence à la cyberattaque contre l'OPM dans les documents entourant le Sommet. En effet, si la question du cyber et son caractère prioritaire sont réitérés à plusieurs reprises, jamais l'administration Obama ne fait référence de manière explicite à cet événement. Nous pensons que la question de la cyberattaque contre l'OPM a été volontairement occultée, comme nous le préciserons dans la section sur les stratégies discursives.

En résumé, le principal objectif clairement énoncé dans le discours de l'administration Obama était de convaincre la Chine d'arrêter son cyberespionnage économique et industriel contre les entreprises américaines, ce qu'elle a réussi lors de la rencontre au Sommet entre les deux présidents. Le gouvernement américain s'abstient également d'attribuer au gouvernement chinois la cyberattaque contre l'OPM et n'y fait pas référence dans son discours entourant le Sommet.

4.2.2. Documents de l'administration chinoise

L'analyse de la perspective chinoise porte sur cinq documents: deux conférences de presse régulières des porte-paroles du ministère des Affaires étrangères de Chine les 5 juin et 10 juillet 2015, les remarques du porte-parole du ministère des Affaires étrangères de Chine, Hua Chunying, sur le battage médiatique américain sur les enjeux de cybersécurité concernant la Chine le 14 août 2015, la conférence de presse conjointe des présidents Obama et Xi à la Maison-Blanche [extraits du président chinois] du 25 septembre 2015 et en terminant, le communiqué du ministère des Affaires étrangères de Chine concernant les résultats de la visite d'État du président Xi Jinping aux États-Unis publié le 26 septembre 2015.

Tout d'abord, en ce qui concerne la cyberattaque contre l'OPM, l'administration Xi reproche aux médias américains de faire des accusations non fondées et non scientifiques. Elle affirme en effet que les cyberattaques sont conduites de façon anonyme, qu'elles traversent les frontières et qu'il est particulièrement difficile d'en retracer les auteurs (MFAPRC, 5 juin 2015, 14 août 2015). Elle souhaite que les accusations non fondées cessent, affirmant que ce n'est dans l'intérêt d'aucune partie : « *Groundless speculation, hyping up or accusation is not helpful to solve the problem nor conducive to any party's interests* » (MFAPRC, 14 aout). Par ailleurs, le gouvernement chinois réitère que la Chine est elle-même victime de cyberattaques: « *China has long suffered from massive cyber attacks from abroad and severe threats to national security and interests* » (MFAPRC, 14 aout 2015). La Chine se positionne donc comme un grand défenseur de la cybersécurité et affirme combattre toutes formes de cyberattaques. Dans cette optique, elle ne reconnaît d'aucune façon que la cyberattaque contre l'OPM puisse provenir de la Chine et refuse toute possibilité d'attribution.

Dans son discours entourant le cyberespace, le gouvernement Xi souhaite de plus établir une coopération internationale afin de construire un cyberespace paisible, sécuritaire et ouvert (MFAPRC, 5 juin 2015). À ce titre, le gouvernement Xi souhaite qu'un code de conduite du cyberespace soit créé et veut, pour ce faire, collaborer à travers un dialogue amélioré (MFAPRC, 14 août 2015). Dans son discours entourant la rencontre au Sommet avec le président américain, la Chine reconnaît pour l'une des premières fois l'importance de respecter les standards internationaux en matière de commerce ainsi que la participation du secteur privé dans le développement des technologies. La Chine accepte même de ne pas imposer inutilement de conditions sur la vente ou l'achat de produits du secteur des TIC. On peut ainsi lire dans le communiqué du ministère des Affaires étrangères au lendemain de la rencontre au Sommet:

> *Both countries commit that generally applicable measures to enhance information and communication technology cybersecurity in commercial sectors (ICT cybersecurity regulations) should be consistent with WTO agreements, be narrowly tailored, take into account international norms, be nondiscriminatory, and not impose nationality-based conditions or restrictions, on the purchase, sale, or use of ICT products by commercial enterprises unnecessarily* (MFAPRC, 26 septembre 2015).

Par rapport au précédent discours chinois, il s'agit d'un important revirement de situation quant à la régulation des entreprises en territoire chinois. En effet, la Chine qui affirmait vouloir imposer ses lois nationales sur les entreprises étrangères, tel que présenté dans la problématique, se ravise à ce titre par la suite.

Quant à sa relation avec les États-Unis en matière de cyberespace et de cybersécurité, l'administration Xi réaffirme l'importance d'une profonde collaboration bilatérale. Elle reconnaît que les deux États sont complémentaires économiquement et qu'il existe un grand potentiel pour approfondir leur coopération (WH, 2015a). La Chine affirme par ailleurs que la technologie est l'un des piliers de leur relation économique

et qu'il importe de créer des conditions nécessaires à l'expansion de ce commerce (MFAPRC, 26 septembre 2015). Pour ce faire, l'administration Xi reconnaît que la Chine et les États sont deux « pays majeurs du cyberespace » et souhaite renforcer le dialogue et la coopération entre les deux États en ce qui concerne le cyberespace. Le président Xi affirme ainsi lors de sa conférence de presse conjointe avec le président Obama à la Maison-Blanche:

> *Overall, the United States is the strongest country in terms of cyber strength. China is the world's biggest cyber country in terms of the number of Web users. We have more than 600 million of netizens. Our two sides should cooperate because cooperation will benefit both, and confrontation will lead to losses on both sides. We are entirely able to carry out government department and expert levels of dialogue and exchanges to strengthen our cooperation in many respects and turn the cybersecurity between the two countries into a new growth source, rather than a point of confrontation between the two sides* (WH, 2015a).

Il s'agit encore une fois d'un important pas en avant, puisque la Chine affirme qu'elle possède des intérêts en commun avec les États-Unis dans le domaine du cyber et qu'elle veut éviter toute confrontation (MFAPRC, 14 août 2015; WH, 2015a). Auparavant, il était plutôt évident que le domaine du cyber représentait un espace de discorde entre les deux États, ce à quoi l'administration Xi ne fait nullement référence dans son discours entourant la cyberattaque contre l'OPM et la rencontre au Sommet de septembre 2015. Contrairement aux États-Unis, qui affirment qu'il s'agit d'un enjeu important et sensible dans leur relation bilatérale, la Chine se contente d'affirmer que les deux États ont tout intérêt à collaborer.

Finalement, le gouvernement Xi s'engage à cesser toute forme de vol de propriété intellectuelle ou de secrets industriels : « *China strongly opposes and combats the theft of commercial secrets and other kinds of hacking attacks* » (WH, 2015a ; MFAPRC, 26 septembre 2015). Le gouvernement Xi ne fait toutefois pas référence aux nombreuses accusations américaines de cyberespionnage économique et ne

s'approprie aucune part de responsabilité. De même, jamais le président Xi ou son administration ne font référence à la cyberattaque contre l'OPM, mis à part pour nier les allégations de cyberattaque en général en affirmant qu'elles ne sont pas scientifiques.

Autrement dit, les principaux messages du gouvernement chinois renvoient d'abord à l'importance d'éviter les accusations réciproques de cyberattaques ou de cyberespionnage. Ensuite, le gouvernement affirme l'importance de la relation économique sino-américaine et particulièrement dans le domaine du cyber et souhaite ainsi renforcer sa coopération avec les États-Unis. Pour ce faire, la Chine s'engage finalement à respecter les normes internationales du commerce et à ne pas soutenir les activités de vol de propriété intellectuelle ou de secrets commerciaux ni toute autre forme de cyberattaque.

4.3. Présentation des résultats

La dernière partie du chapitre sur l'analyse porte sur les résultats, c'est-à-dire que nous allons ici répondre aux quatre questions sectorielles posées par ce mémoire et ultimement, à notre question centrale. Nous allons donc décortiquer nos résultats en prenant chacune des questions une par une, en y comparant les deux perspectives en présence, en fonction de notre cadre de référence théorique.

4.3.1. Vision des présidents en matière de cybersécurité: entre similitudes et différences

Tout d'abord, les deux présidents partagent une vision relativement semblable de la cybersécurité. Parmi les points de vue qu'ils ont en commun, tous deux affirment qu'il

existe un lien important entre cyberespace, innovation technologique et prospérité économique. Le président chinois croit que le cyberespace permettra de contribuer au développement économique de la Chine, tandis que le président Obama perçoit que le cyberespace offre d'immenses opportunités d'innovation et d'occasions d'affaires dont les États-Unis bénéficient déjà à grande échelle.

Tous deux reconnaissent par ailleurs les risques attribuables au cyberespace et à ses vulnérabilités et donc, l'importance de la cybersécurité. Ils construisent un lien entre les différentes menaces présentes dans le cyberespace et la question de la sécurité nationale. Le président Obama représente les cyberattaques principalement comme une menace pour la sécurité économique des États-Unis et, *a fortiori*, pour la sécurité nationale américaine. Le président chinois l'aborde d'une autre façon: il affirme que la Chine est elle aussi grandement victime de cyberattaques, mais sans ne jamais préciser de quel type d'attaques il est question exactement. Il ne veut surtout pas que le cyberespace devienne un « champ de bataille » et pour cela, il réitère l'importance de créer des normes de conduites du cyberespace.

Or, en matière de gouvernance, le gouvernement Obama mentionne à quelques reprises vouloir instaurer des normes internationales du cyberespace, mais affirme surtout que les États-Unis doivent demeurer des leaders et conserver leur avantage comparatif, menacé par un ensemble d'acteurs: criminels, terroristes, États-nations, etc.

En terminant, les deux présidents ne partagent pas la même vision quant à la gouvernance du cyberespace et aux parties impliquées dans son développement. Alors que le président Obama souhaite la mise en place d'un partenariat public-privé efficace et opte donc pour un modèle de gouvernance multipartite, le président Xi est plutôt d'avis que ces discussions doivent avoir lieu dans un forum multilatéral ou tous

les États ont leur mot à dire, bien qu'il laisse entendre qu'il comprend l'importance de l'implication du secteur privé dans le développement des technologies.

4.3.2. Messages clés dans les discours des deux administrations

Le principal message de l'administration Obama quant à la cyberattaque contre l'Office of Personnel Management et à la rencontre au Sommet est d'abord qu'aucun responsable n'a été identifié. Le gouvernement américain veut éviter de pointer du doigt son homologue chinois, mais laisse tout de même savoir clairement que de possibles sanctions économiques pourront être imposées. La cyberattaque est présentée comme une faille dans les systèmes de protection des réseaux informatiques du gouvernement et il importe donc que le gouvernement américain renforce ses défenses. La gravité de la cyberattaque n'est pas abordée dans le discours du gouvernement Obama, qui affirme plutôt qu'une enquête est en cours afin de déterminer l'étendue des dommages et que le gouvernement n'est pas le seul à subir des cyberattaques, mais qu'il s'agit d'un défi qui préoccupe également les entreprises. C'est pourquoi le gouvernement doit viser une meilleure coopération avec le secteur privé.

Par ailleurs, en ce qui concerne la rencontre au Sommet, l'administration Obama insiste sur le caractère important de la relation économique sino-américaine qu'elle souhaite maintenir sur la voie de la collaboration, mais que pour ce faire, les États-Unis et la Chine doivent régler certains de leurs différends, notamment la question du domaine numérique et du cyberespionnage économique. Le gouvernement laisse savoir à la Chine que son propre intérêt économique est menacé si les entreprises ne peuvent avoir confiance et opérer sans être inquiétées par des risques de cybervols. Les États-Unis laissent planer la menace économique, et ajoutent qu'ils espèrent que

la voie du dialogue et de la diplomatie sera préconisée afin qu'une confiance et qu'une compréhension mutuelles s'installent.

Quant au principal message de l'administration Xi entourant la cyberattaque contre l'OPM, il renvoie au fait que toute accusation envers la Chine est non fondée et irresponsable, rappelant la difficulté d'attribution des cyberattaques. Le gouvernement chinois met donc en garde les États-Unis et affirme que des accusations ne pourraient que nuire à la résolution et à la création d'un climat de coopération. Le gouvernement chinois rappelle par ailleurs que la Chine est elle-même victime de cyberattaques et que pour cette raison, elle est un grand défenseur de la cybersécurité.

En ce qui concerne le Sommet, le message clé du gouvernement est l'importance de renforcer la collaboration entre la Chine et les États-Unis dans le domaine du cyber et de la cybersécurité. Le gouvernement Xi rappelle que les États-Unis et la Chine, en tant que deux puissances du cyberespace, ont des intérêts communs à collaborer et que la confrontation ne pourrait que leur nuire mutuellement.

4.3.3. Construction du message : stratégies discursives décortiquées

Il s'agit ensuite de déterminer quelles étaient les stratégies discursives employées par les deux gouvernements et comment elles visaient à construire une certaine réalité entourant la cybersécurité. Commençons par le gouvernement américain. En premier lieu, le gouvernement Obama emploie le terme « intrusion » pour désigner la cyberattaque contre l'OPM et le terme « étendue » (*scope*) pour désigner les potentiels dommages. Jamais le porte-parole de la Maison-Blanche ou encore les autres membres de l'administration n'emploient le terme cyberattaque pour désigner ce qui s'est produit, sauf lorsqu'il est question des possibles sanctions pouvant être

imposées à des individus ayant commis des cyberattaques (WH, 25 juin 2015). Quant aux possibles coupables, les termes « individus » ou « entités » sont employés pour en faire mention, un mot vague qui empêche le gouvernement américain de se mouiller. Le champ lexical utilisé est donc plutôt flou et imprécis et contribue à construire une autre réalité entourant la cyberattaque contre l'OPM: il ne s'agit pas d'une cyberattaque, mais bien d'une simple intrusion.

En second lieu, pour aborder l'enjeu du cyberespace et la rencontre au Sommet, le mot clé « différences » est utilisé pour faire référence aux multiples enjeux en présence, dont celui du cyberespace. Le terme « cyberespace », lorsqu'il est employé par l'administration Obama, est presque systématiquement mis en relation avec le concept de gouvernance internationale et la mise en place de règles internationales du cyberespace (WH, 25 septembre 2015). Quant au terme « cybersécurité », il fait référence à une priorité pour le gouvernement américain, à un enjeu important et sérieux, à une question de sécurité nationale: « *Well, the President has confidence that every single member of his staff understands that cybersecurity needs to be a priority* » (WH, 9 juin 2015).

Or, en quoi est-ce un enjeu de sécurité nationale *exactement* ? On ne retrouve en effet dans le discours de l'administration Obama aucun détail précisant directement pourquoi la cybersécurité est considérée comme un enjeu de sécurité nationale. Le lien le plus direct établi par le gouvernement entre cybersécurité et sécurité nationale se retrouve dans la question de l'économie se voyant menacée par les cyberattaques telles que le vol de propriété intellectuelle et de secrets industriels. Nous pensons que par cette pratique discursive, l'administration Obama s'efforce de construire une réalité au sein de laquelle toute menace envers l'économie américaine est une menace envers la sécurité nationale des États-Unis. En partant de la posture théorique de Dunn Cavelty (2013) sur les représentations de la menace, il est possible d'observer que l'administration Obama a opéré un discours autour d'une menace

spécifique, celle du cyberespionnage économique, qu'elle a associée à un enjeu de sécurité nationale.

En troisième lieu, il importe de s'intéresser aux « non-dits », aux omissions présentes dans le discours officiel qui sont plutôt révélatrices. Il nous semble particulièrement éclairant de constater qu'il n'existe aucune mention directe à la cyberattaque contre l'OPM dans les documents de l'administration Obama, notamment entourant la rencontre au Sommet. Nous pensons qu'il s'agit d'une omission volontaire, visant à en réduire la portée. Il nous semble en effet que le gouvernement Obama aurait pu faire savoir plus directement son mécontentement à la Chine et la menacer sévèrement de représailles, comme ce fut le cas lors des accusations de cyberespionnage envers les militaires chinois. Or, ils ont plutôt opté pour une certaine discrétion, dont le but était de limiter la portée de la cyberattaque contre l'OPM et de dévier l'attention du public. Le gouvernement avait en effet intérêt à ce que cet événement gênant ne prenne pas davantage d'ampleur, car il s'agissait d'un véritable échec en matière de protection de l'information. Cela dit, nous nous permettons de croire que dans les coulisses du Sommet, la cyberattaque contre l'OPM a probablement fait partie des discussions entre les représentants de l'administration Obama et ceux de l'administration Xi.

En résumé, ces résultats nous permettent d'affirmer que l'administration Obama a construit son message en réduisant la portée de la cyberattaque contre l'OPM, considérée plutôt comme une simple intrusion et dont l'identification des responsables ne semble pas être une priorité. Rappelons que 21,5 millions de fonctionnaires américains ont été touchés par cette cyberattaque, considérée par les médias et certains experts comme l'une des pires en matière de sécurité nationale (Washington Post, 9 juillet 2015). Pourtant, on ne retrouve pas cette considération ni cette inquiétude dans le discours de l'administration Obama, qui évite de parler de cyberattaque ou même simplement d'aborder l'événement. Comme le suppose

l'interactionnisme symbolique de Goffman (1956), l'administration Obama s'est assurée dans ses « performances » de ne rendre perceptible que ce qui devait l'être, c'est-à-dire qu'une enquête est en cours et qu'il pourrait y avoir des sanctions. En coulisse, nous supposons que le discours a dû être tout autre et que la cyberattaque a probablement été considérée bien plus grave que le gouvernement ne l'a affirmé publiquement. Or, le gouvernement américain s'efforce plutôt de représenter la protection des secrets industriels et de la propriété intellectuelle des entreprises comme un enjeu nettement plus important en matière de sécurité nationale.

En ce qui concerne l'administration Xi, elle emploie directement le terme « cyberattaque » pour parler de l'événement entourant l'Office of Personnel Management. Elle est en effet beaucoup plus prompte à parler de cyberattaque, mais ajoute toutefois systématiquement qu'il est difficile d'identifier l'origine des cyberattaques. Les termes « irresponsable » et « sans fondement » sont articulés dans le discours de l'administration Xi autour de la cyberattaque contre l'OPM. Il semble clair que le message du gouvernement chinois est construit comme une mise en garde: toute accusation (jugée irresponsable) pourrait ultimement nuire aux relations sino-américaines.

Par ailleurs, en matière de relations entre la Chine et États-Unis, le gouvernement chinois ne manque pas de parler de « coopération », que ce soit lorsqu'il aborde le terme « cyberespace » ou encore le terme « cybersécurité ». Le terme « coopération », ou son dérivé l'adjectif « coopératif », est en effet utilisé au moins vingt fois dans le discours chinois entourant le domaine du cyber. Contrairement à l'administration américaine, qui identifie la cybersécurité comme une priorité, l'administration chinoise met plutôt l'emphase sur la coopération située au cœur de la politique étrangère chinoise dans chaque document analysé. Par exemple, le président Xi affirme lors de la conférence de presse conjointe à la Maison-Blanche: « *To work with the United States to build the new model of major-country relationship without*

conflict, without confrontation, with mutual respect and win-win cooperation is a priority in China's foreign policy » (WH, 2015a). Ce que le président chinois tente de construire par cette pratique discursive en termes de répétition du mot clé « coopération », c'est une réalité au sein de laquelle les États-Unis et la Chine sont des partenaires et qu'ils possèdent davantage d'intérêts en commun que d'espaces de confrontation.

En matière de « non-dit » ou d'omission d'information, le gouvernement chinois ne fait jamais référence à sa possible implication dans la cyberattaque contre l'OPM. Sans nier directement qu'il soit impliqué, la stratégie du gouvernement est plutôt de rappeler les difficultés liées à l'attribution des cyberattaques et les risques associés à de telles accusations pour la relation sino-américaine et leur entente. Autrement dit, le processus de construction du message employé par l'administration Xi serait de représenter le cyberespace comme un domaine de coopération entre les États-Unis et la Chine, et non comme un espace de confrontation. Le champ discursif utilisé autour de l'enjeu est en effet plutôt positif, rappelant les « intérêts en commun » qu'ont la Chine et les États-Unis dans le domaine du cyber. Le gouvernement s'efforce donc toujours de réitérer son désir de collaboration. Même lorsqu'il mentionne les risques associés aux accusations envers la Chine en matière de cyberattaques, il le fait en ramenant à l'avant-plan la question de la relation sino-américaine qui se doit d'être collaborative et positive. À l'avant-scène, le gouvernement chinois performe un discours visant à convaincre le gouvernement américain de sa bonne foi et de son désir de collaboration.

4.3.4. Quelles logiques d'intérêts en présence?

L'objectif de la quatrième et dernière question sectorielle est de déterminer quelles sont les logiques d'intérêt en présence et en quoi la formulation du discours en permet

efficacement la poursuite. À ce sujet, nous comprenons que le principal intérêt américain lors du Sommet de septembre 2015 était de convaincre le gouvernement chinois de cesser son cyberespionnage économique. En effet, à plusieurs reprises le gouvernement américain réitère que le cyberespionnage économique, qu'il considère illégal sur le plan du droit international en matière de commerce, nuit grandement aux entreprises américaines. Cet intérêt est clairement perceptible dans les documents de l'administration Obama entourant la rencontre au Sommet, ainsi que dans les déclarations du président Obama. Nous pensons qu'en articulant son message autour de l'enjeu du cyberespionnage économique, l'administration Obama tentait de convaincre un public double: les citoyens américains, auxquels il rappelle que les cybermenaces, particulièrement économiques, représentent « l'un des plus grands défis du 21^{e} siècle », ainsi que le gouvernement de la Chine, auquel il indique que s'il ne respecte pas les règles du commerce international, il perdra des opportunités commerciales importantes. Le gouvernement américain positionne donc cet enjeu à l'avant-plan de ses intérêts et en informe directement son auditoire.

Par ailleurs, nous comprenons qu'un second intérêt du gouvernement américain était de minimiser l'impact de la cyberattaque sur 21,5 millions d'Américains. Nous l'expliquons par deux raisons. Tout d'abord, le gouvernement américain souhaitait éviter d'être sévèrement critiqué pour son incapacité à protéger les données confidentielles de ses citoyens et pour ce faire, a détourné leur regard vers un enjeu qu'il affirme plus important, celui de la sécurité économique. Rappelons en effet que la protection de la vie privée faisait partie des principaux thèmes abordés par le président Obama dans ses déclarations sur la cybersécurité. Alors que le président avait promis que son gouvernement protégerait la vie privée des citoyens américains, il ne s'est pas avéré en mesure de protéger adéquatement les renseignements particulièrement confidentiels de 21,5 millions d'Américains. Ensuite, en rappelant la différence entre le cyberespionnage traditionnel et le cyberespionnage économique, le gouvernement américain laisse entendre qu'il considère l'attaque contre l'OPM

comme un acte d'espionnage politique et militaire, et donc légal sur le plan du droit international. Il ne peut toutefois l'admettre directement, car il devrait alors reconnaître ouvertement qu'aucune mesure de représailles ne peut être prise et l'ensemble de ses menaces de sanctions économiques envers la Chine tomberait.

En résumé, nous pensons que le gouvernement américain a bien joué ses cartes, offrant une belle performance théâtrale diplomatique, car il a réussi la poursuite de sa logique d'intérêt: il a obtenu de la Chine une promesse de cessation du vol de propriété intellectuelle, et la question de la cyberattaque contre l'OPM s'est presque effacée au profit du *cyber agreement* de septembre 2015.

Quant au principal intérêt du gouvernement chinois, il s'agissait de maintenir un climat de coopération commerciale avec les États-Unis, notamment dans le domaine des technologies et de l'innovation, donc du cyberespace. Cet objectif est clairement perceptible dans le discours de l'administration Xi, alors qu'elle affirme que la coopération avec les États-Unis est une priorité pour leur gouvernement. Pour ce faire, il était également dans l'intérêt de la Chine d'éviter de se voir imposer des sanctions économiques de la part des États-Unis et c'est pourquoi le gouvernement Xi a rappelé à de nombreuses reprises qu'il est « irresponsable » d'attribuer des cyberattaques et que des accusations seraient mal reçues.

Dans son discours officiel entourant la cybersécurité, le gouvernement Xi rappelle par ailleurs qu'elle est essentielle pour le développement économique de la Chine et insiste sur la nécessité d'établir un code de conduite du cyberespace. La Chine poursuivait donc également un double objectif: celui de diminuer l'influence américaine dans la gouvernance du cyberespace, notamment en militant pour un code de conduite et pour un modèle de gouvernance multilatérale, ainsi que de conserver ses relations économiques avec les entreprises américaines dans le domaine des technologies et de l'innovation. Pour ce faire, le gouvernement Xi se devait de

montrer sa bonne foi, et c'est pourquoi nous pensons qu'il a accepté de cesser ses activités de cyberespionnage économique. Nous pensons en terminant que les deux administrations sont ressorties gagnantes de leur rencontre au Sommet, car elles ont toutes deux respecté leurs principales lignes de communication en fonction de leur logique d'intérêt, et atteint leurs objectifs réciproques.

4.3.5. Question centrale et principales conclusions

Il semble donc clair qu'en ce qui concerne le discours de l'administration Obama, il a été construit autour de l'articulation d'un message clé portant sur l'aspect primordial de la cybersécurité pour l'économie américaine et ciblant pour principale menace le cyberespionnage chinois, ainsi que par un processus d'omission, évitant de mentionner la cyberattaque contre l'OPM présentée plutôt comme une simple intrusion. L'analyse du discours politique du gouvernement Obama nous a en effet permis de percevoir le double jeu de sa performance discursive: sous les projecteurs, le gouvernement américain a articulé ses messages clés autour de la cybermenace économique, omettant délibérément de mentionner l'enjeu de la cyberattaque sur 21,5 millions d'enquêtes de sécurité. Il est pertinent de mentionner que cette conclusion issue de notre analyse ne faisait pas partie de notre hypothèse de départ quant au discours américain. Elle constitue ainsi une découverte des plus intéressantes et démontre que notre hypothèse était incomplète.

En ce qui concerne l'administration Xi, son discours a été construit autour d'un objectif clairement établi en termes de coopération bilatérale (avec les États-Unis) et multilatérale (en matière de gouvernance du cyberespace). Sa stratégie discursive était donc tout d'abord d'utiliser la répétition: plus d'une vingtaine de fois le terme « coopération » a été employé, tandis que son message décrivant les accusations américaines relativement à la cyberattaque contre l'OPM de « non fondées » a lui

aussi été répété à plusieurs reprises (dans trois des cinq documents à l'étude). Le gouvernement chinois s'est ainsi efforcé de représenter le cyberespace comme un domaine de coopération entre les États-Unis et la Chine. Qui plus est, la Chine devait éviter de se voir imposer des sanctions économiques, notamment afin de continuer sa collaboration avec les États-Unis, et elle s'est donc assurée de faire savoir que les accusations de cyberattaques à son endroit étaient perçues négativement et jugées « irresponsables ». Cette conclusion vient finalement valider notre hypothèse selon laquelle le discours de l'administration chinoise a été articulé autour d'un message clé portant sur la poursuite et l'amélioration de la coopération bilatérale, en fonction de la logique d'intérêts de la Chine.

CONCLUSION

La Chine et les États-Unis sont parmi les plus importants joueurs dans le développement du cyberespace sur la scène internationale. À la fois en termes d'expertise et de capacités, les deux États dominent actuellement dans le domaine du cyber et sont considérées comme des cyber superpuissances. Ils sont également de grands partenaires économiques et leur prospérité réciproque dépend en grande partie de leur capacité à poursuivre sur la voie du commerce et de la coopération. Toutefois, le cyberespace représente un lieu de tension entre le géant américain et l'empire du Milieu. Un événement majeur survenu en 2015 a en effet menacé de devenir un important objet de litige entre les deux États, soit la cyberattaque contre l'Office of Personnel Management. Les données personnelles et extrêmement confidentielles de 21,5 millions de fonctionnaires américains ont été touchées par une intrusion dans les systèmes informatiques de cette agence fédérale américaine, représentant une vraie mine d'or d'information pour les responsables de l'attaque. C'est donc à cette étude de cas précise que ce mémoire s'est intéressé.

La cyberattaque contre l'OPM constituait un précédent: jamais une brèche dans des systèmes gouvernementaux n'avait fourni l'accès à une masse de données aussi vaste et critique. Pourtant, lors de la rencontre au Sommet entre le président américain Barack Obama et son homologue chinois le président Xi Jinping, ayant eu lieu à peine deux mois plus tard et pendant laquelle ils ont conclu un *cyber agreement*, l'enjeu de la cyberattaque contre l'OPM a été entièrement occulté dans le discours des deux administrations. Ce mémoire visait donc à déterminer le processus de construction du discours de chaque gouvernement entourant la cyberattaque et le Sommet, ainsi que les logiques d'intérêt à l'origine de leurs stratégies discursives.

Adoptant une posture constructiviste, nous avons sollicité pour ce faire les outils théoriques de quatre auteurs clés s'intéressant tout d'abord à la construction sociale de la réalité, de même qu'aux représentations du cyberespace et à la construction des cybermenaces, et finalement à la mise en scène des interactions sociales. Ce cadre de référence théorique nous a incité à adopter l'analyse de discours comme méthodologie, que nous avons présentée au troisième chapitre. Puis, une grille d'analyse a été élaborée autour de quatre questions sectorielles de recherche, et notre collecte de donnée s'est articulée autour de 15 documents qui ont été sélectionnés pour composer l'échantillonnage.

L'analyse des déclarations des présidents Xi et Obama nous a ainsi permis d'identifier la vision globale de chaque président entourant la cybersécurité en général. Alors que le président Obama considère la cybersécurité comme une priorité en matière de sécurité nationale, il articule son discours principalement autour de l'aspect économique et argumente que le cyberespace doit permettre aux entreprises américaines de prospérer. Le secteur privé est situé au centre de son discours sur le cyberespace, à la fois en matière de développement et d'innovation technologique ainsi qu'en matière de gouvernance. Le président américain adopte une posture multipartite et souhaite que le cyberespace soit un moteur de prospérité et un espace de leadership pour les États-Unis sur le plan du commerce international.

Le président Xi considère quant à lui que le cyberespace est un domaine de développement pour la Chine et souhaite augmenter les cybercapacités chinoises. Il argumente que la gouvernance du cyberespace doit reposer entre les mains des États et affirme que le principe de souveraineté étatique doit être respecté dans le domaine numérique. La cybersécurité est ainsi présentée dans son discours comme la protection du cyberespace chinois contre les cyberattaques, bien que la nature de ces dites attaques ne soit pas précisée dans son discours. Autrement dit, cet éclairage était

nécessaire pour comprendre par la suite les logiques d'intérêts des deux administrations en relation avec le cas d'étude précis de la cyberattaque contre l'OPM et de la rencontre au Sommet.

L'analyse des documents des deux administrations a permis de déterminer que le processus de construction du discours entourant notre étude de cas a été articulé autour de deux messages clés. Tout d'abord, du côté américain, il s'agissait de mettre à l'avant-plan la cybermenace chinoise envers les secrets industriels et la propriété intellectuelle, et d'éviter d'accorder de l'importance à la cyberattaque contre l'OPM, qui représente un véritable échec gouvernemental en matière de protection de la vie privée. Dans son discours, le gouvernement américain a représenté le cyberespionnage économique comme une menace plus importante sur le plan de la sécurité nationale.

Du côté chinois, il s'agissait plutôt d'insister sur l'amélioration de la coopération sino-américaine et d'amenuiser toute tension pouvant nuire à leurs échanges commerciaux. C'est pourquoi le gouvernement a accepté de ne pas soutenir le vol de propriété intellectuelle, afin de démontrer sa bonne foi, mais également afin de s'innocenter quant à la cyberattaque contre l'OPM. L'autre message clé du gouvernement chinois consistait en effet à rappeler que toute accusation de cyberattaque est considérée irresponsable et non fondée par la Chine. Nous pouvons interpréter ce message de la sorte: si le gouvernement américain souhaite convaincre la Chine de signer l'entente sur la protection de la propriété intellectuelle, il se doit en contrepartie de ne pas imposer de sanctions économiques envers la Chine ni d'accuser officiellement le gouvernement chinois de la cyberattaque contre l'OPM.

En résumé, notre analyse nous a permis de valider notre hypothèse de départ selon laquelle le discours a été construit autour d'un message clé en termes de coopération bilatérale, en fonction d'intérêts nationaux. Par contre, nous avons pu constater que

notre hypothèse était incomplète, puisqu'elle n'abordait pas le message clé du gouvernement américain qui lui s'articulait davantage autour de la question économique.

En guise de conclusion, nous pensons que ce mémoire, se penchant sur la pire cyberattaque subie par le gouvernement américain de même que sur la signature historique de la première entente bilatérale sino-américaine en matière de cyberespace, a permis de jeter un éclairage sur un enjeu international qui demeure peu abordé par la recherche académique.

Or, bien que notre recherche ait permis de tirer d'intéressantes conclusions pertinentes pour le champ de la communication internationale, elle comportait certaines limites. En matière d'accès à l'information, nous n'avons eu accès qu'aux documents publics compte tenu du caractère secret de l'information gouvernementale entourant la cybersécurité. De même, toute la portion de l'interaction entre les deux administrations se déroulant « en coulisse », pour reprendre la posture de Goffman, nous était donc inaccessible et notre analyse se trouvait ainsi limitée à une certaine interprétation. Par ailleurs, nous n'avons utilisé que des documents traduits en anglais ou en français, et notre incompréhension de la langue chinoise a ainsi réduit notre échantillonnage, de même qu'imposé le risque d'une altération du discours à l'étude.

Autres pistes de recherche

En terminant, par nécessité de circonscrire notre objet d'étude et en raison de limites dans l'échelle du temps, ce mémoire ne s'est pas intéressé à l'efficacité du *cyber agreement* de septembre 2015 sur le plan du cyberespionnage. Parmi les futures pistes de recherche, nous pensons qu'il serait pertinent d'observer les résultats concrets de l'entente entre la Chine et les États-Unis, à savoir si la Chine a bel et bien

respecté son engagement et depuis, ne soutient pas le cybervol de propriété intellectuelle et de secrets industriels.

Quant au débat entourant la gouvernance et le développement de normes internationales du cyberespace, il se poursuit globalement et son issue pourrait avoir un impact important, à la fois sur les relations sino-américaines et plus largement sur la géopolitique mondiale d'Internet. Particulièrement avec l'arrivée d'un nouveau président américain, nous nous demandons comment le débat évoluera au cours des prochaines années. L'ère Obama s'est en effet achevée après huit ans de présidence pendant laquelle l'enjeu des cyberattaques a évolué considérablement jusqu'à occuper aujourd'hui une place prépondérante dans les relations internationales. Cet enjeu désormais majeur a même éclaboussé l'élection présidentielle américaine de 2016 avec notamment la question de la cyberattaque contre la Convention nationale démocrate et les allégations de piratage informatique en provenance de la Russie. Dans cette optique, nous nous demandons comment le gouvernement de Donald Trump se positionnera globalement sur la cybersécurité et quel sera l'impact de sa présidence sur les dynamiques internationales de gouvernance du cyberespace.

ANNEXE A

LISTE DES DOCUMENTS À L'ÉTUDE

a) Discours américain

Déclarations présidentielles :

1. Déclaration du Président Obama sur l'importance de sécuriser les cyberinfrastructures de la nation (29 Mai 2009)

2. Déclaration du Président Obama au *National Cybersecurity and Communications Integration Center* (13 janvier 2015)

3. Déclaration du Président Obama au *Cybersecurity and Consumer Protection Summit* (13 février 2015)

Renseignements relativement à la cyberattaque et au Sommet:

4. Point de presse de l'attaché de presse de la Maison-Blanche Josh Earnest (9 juin 2015)

5. Point de presse de l'attaché de presse de la Maison-Blanche Josh Earnest (25 juin 2015)

6. Conférence téléphonique précédant la visite du président Xi (22 septembre 2015)

7. Conférence de presse conjointe des présidents Obama et Xi à la Maison-Blanche en marge de leur rencontre au Sommet [extraits du président américain] (25 septembre 2015)

8. Communiqué de la Maison-Blanche concernant la visite d'État du président Xi Jinping aux États-Unis (25 septembre 2015)

b) Discours chinois

Déclarations présidentielles :

9. Propos du Secrétaire général du Comité central du Parti communiste chinois Xi Jinping lors de la réunion élargie de la Commission militaire centrale (16 novembre 2012)

10. Discours du Président Xi lors d'un dîner de bienvenue organisé par le Comité national sur les relations Chine-États-Unis à Seattle (22 septembre 2015).

11. Discours du Président Xi lors de la cérémonie d'ouverture de la deuxième Conférence mondiale sur l'Internet (16 décembre 2015).

Renseignements relativement à la cyberattaque et au Sommet:

12. Conférence de presse régulière du porte-parole du ministère des Affaires étrangères de la République populaire de Chine, Hong Lei (5 juin 2015)

13. Conférence de presse régulière du porte-parole du ministère des Affaires étrangères de la République populaire de Chine, Hua Chunying (10 juillet 2015)

14. Remarques du porte-parole du ministère des Affaires étrangères de la République populaire de Chine, Hua Chunying, concernant le battage médiatique américain sur les enjeux de cybersécurité concernant la Chine (14 août 2015)

15. Conférence de presse conjointe des présidents Obama et Xi à la Maison-Blanche en marge de leur rencontre au Sommet [extraits du président chinois] (25 septembre 2015)

16. Communiqué du ministère des Affaires étrangères de la République populaire de Chine concernant les résultats de la visite d'État du président Xi Jinping aux États-Unis (26 septembre 2015)

ANNEXE B

ÉCHANTILLONS 1 À 15

Échantillon 1.

Remarks by US President Barack Obama on Securing the Nation's Cyber Infrastructire, 29 May 2009

THE PRESIDENT: Everybody, please be seated. We meet today at a transformational moment -- a moment in history when our interconnected world presents us, at once, with great promise but also great peril. Now, over the past four months my administration has taken decisive steps to seize the promise and confront these perils. We're working to recover from a global recession while laying a new foundation for lasting prosperity. We're strengthening our armed forces as they fight two wars, at the same time we're renewing American leadership to confront unconventional challenges, from nuclear proliferation to terrorism, from climate change to pandemic disease. And we're bringing to government -- and to this White House -- unprecedented transparency and accountability and new ways for Americans to participate in their democracy. But none of this progress would be possible, and none of these 21st century challenges can be fully met, without America's digital infrastructure -- the backbone that underpins a prosperous economy and a strong military and an open and efficient government. Without that foundation we can't get the job done. It's long been said that the revolutions in communications and information technology have given birth to a virtual world.

But make no mistake: This world -- cyberspace -- is a world that we depend on every single day. It's our hardware and our software, our desktops and laptops and cell phones and Blackberries that have become woven into every aspect of our lives. It's the broadband networks beneath us and the wireless signals around us, the local networks in our schools and hospitals and businesses, and the massive grids that power our nation. It's the classified military and intelligence networks that keep us safe, and the World Wide Web that has made us more interconnected than at any time in human history. So cyberspace is real. And so are the risks that come with it. It's the great irony of our Information Age -- the very technologies that empower us to create and to build also empower those who would disrupt and destroy. And this paradox -- seen and unseen -- is something that we experience every day. It's about the privacy and the economic security of American families. We rely on the Internet to pay our bills, to bank, to shop, to file our taxes. But we've had to learn a whole new vocabulary just to stay ahead of the cyber criminals who would do us harm --

spyware and malware and spoofing and phishing and botnets. Millions of Americans have been victimized, their privacy violated, their identities stolen, their lives upended, and their wallets emptied. According to one survey, in the past two years alone cyber crime has cost Americans more than $8 billion. I know how it feels to have privacy violated because it has happened to me and the people around me. It's no secret that my presidential campaign harnessed the Internet and technology to transform our politics. What isn't widely known is that during the general election hackers managed to penetrate our computer systems. To all of you who donated to our campaign, I want you to all rest assured, our fundraising website was untouched. So your confidential personal and financial information was protected. But between August and October, hackers gained access to emails and a range of campaign files, from policy position papers to travel plans. And we worked closely with the CIA -- with the FBI and the Secret Service and hired security consultants to restore the security of our systems. It was a powerful reminder: In this Information Age, one of your greatest strengths -- in our case, our ability to communicate to a wide range of supporters through the Internet -- could also be one of your greatest vulnerabilities.

This is a matter, as well, of America's economic competitiveness. The small businesswoman in St. Louis, the bond trader in the New York Stock Exchange, the workers at a global shipping company in Memphis, the young entrepreneur in Silicon Valley -- they all need the networks to make the next payroll, the next trade, the next delivery, the next great breakthrough. Ecommerce alone last year accounted for some $132 billion in retail sales. But every day we see waves of cyber thieves trolling for sensitive information -- the disgruntled employee on the inside, the lone hacker a thousand miles away, organized crime, the industrial spy and, increasingly, foreign intelligence services. In one brazen act last year, thieves used stolen credit card information to steal millions of dollars from 130 ATM machines in 49 cities around the world -- and they did it in just 30 minutes. A single employee of an American company was convicted of stealing intellectual property reportedly worth $400 million. It's been estimated that last year alone cyber criminals stole intellectual property from businesses worldwide worth up to $1 trillion.

In short, America's economic prosperity in the 21st century will depend on cybersecurity. And this is also a matter of public safety and national security. We count on computer networks to deliver our oil and gas, our power and our water. We rely on them for public transportation and air traffic control. Yet we know that cyber intruders have probed our electrical grid and that in other countries cyber attacks have plunged entire cities into darkness. Our technological advantage is a key to America's military dominance. But our defense and military networks are under constant attack. Al Qaeda and other terrorist groups have spoken of their desire to unleash a cyber attack on our country -- attacks that are harder to detect and harder to defend against. Indeed, in today's world, acts of terror could come not only from a few extremists in suicide vests but from a few key strokes on the computer -- a weapon of mass

disruption. In one of the most serious cyber incidents to date against our military networks, several thousand computers were infected last year by malicious software -- malware. And while no sensitive information was compromised, our troops and defense personnel had to give up those external memory devices -- thumb drives -- changing the way they used their computers every day. And last year we had a glimpse of the future face of war. As Russian tanks rolled into Georgia, cyber attacks crippled Georgian government websites. The terrorists that sowed so much death and destruction in Mumbai relied not only on guns and grenades but also on GPS and phones using voice-overthe-Internet. For all these reasons, it's now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation. It's also clear that we're not as prepared as we should be, as a government or as a country. In recent years, some progress has been made at the federal level. But just as we failed in the past to invest in our physical infrastructure -- our roads, our bridges and rails -- we've failed to invest in the security of our digital infrastructure. No single official oversees cybersecurity policy across the federal government, and no single agency has the responsibility or authority to match the scope and scale of the challenge. Indeed, when it comes to cybersecurity, federal agencies have overlapping missions and don't coordinate and communicate nearly as well as they should -- with each other or with the private sector. We saw this in the disorganized response to Conficker, the Internet "worm" that in recent months has infected millions of computers around the world.

This status quo is no longer acceptable -- not when there's so much at stake. We can and we must do better. And that's why shortly after taking office I directed my National Security Council and Homeland Security Council to conduct a top-to-bottom review of the federal government's efforts to defend our information and communications infrastructure and to recommend the best way to ensure that these networks are able to secure our networks as well as our prosperity. Our review was open and transparent. I want to acknowledge, Melissa Hathaway, who is here, who is the Acting Senior Director for Cyberspace on our National Security Council, who led the review team, as well as the Center for Strategic and International Studies bipartisan Commission on Cybersecurity, and all who were part of our 60-day review team. They listened to a wide variety of groups, many of which are represented here today and I want to thank for their input: industry and academia, civil liberties and private -- privacy advocates. We listened to every level and branch of government -- from local to state to federal, civilian, military, homeland as well as intelligence, Congress and international partners, as well. I consulted with my national security teams, my homeland security teams, and my economic advisors.

Today I'm releasing a report on our review, and can announce that my administration will pursue a new comprehensive approach to securing America's digital infrastructure. This new approach starts at the top, with this commitment from me: From now on, our digital infrastructure -- the networks and computers we depend on

every day -- will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a national security priority. We will ensure that these networks are secure, trustworthy and resilient. We will deter, prevent, detect, and defend against attacks and recover quickly from any disruptions or damage. To give these efforts the high-level focus and attention they deserve -- and as part of the new, single National Security Staff announced this week -- I'm creating a new office here at the White House that will be led by the Cybersecurity Coordinator. Because of the critical importance of this work, I will personally select this official. I'll depend on this official in all matters relating to cybersecurity, and this official will have my full support and regular access to me as we confront these challenges.

Today, I want to focus on the important responsibilities this office will fulfill: orchestrating and integrating all cybersecurity policies for the government; working closely with the Office of Management and Budget to ensure agency budgets reflect those priorities; and, in the event of major cyber incident or attack, coordinating our response. To ensure that federal cyber policies enhance our security and our prosperity, my Cybersecurity Coordinator will be a member of the National Security Staff as well as the staff of my National Economic Council. To ensure that policies keep faith with our fundamental values, this office will also include an official with a portfolio specifically dedicated to safeguarding the privacy and civil liberties of the American people. There's much work to be done, and the report we're releasing today outlines a range of actions that we will pursue in five key areas. First, working in partnership with the communities represented here today, we will develop a new comprehensive strategy to secure America's information and communications networks. To ensure a coordinated approach across government, my Cybersecurity Coordinator will work closely with my Chief Technology Officer, Aneesh Chopra, and my Chief Information Officer, Vivek Kundra.

To ensure accountability in federal agencies, cybersecurity will be designated as one of my key management priorities. Clear milestones and performances metrics will measure progress. And as we develop our strategy, we will be open and transparent, which is why you'll find today's report and a wealth of related information on our Web site, www.whitehouse.gov. Second, we will work with all the key players -- including state and local governments and the private sector -- to ensure an organized and unified response to future cyber incidents. Given the enormous damage that can be caused by even a single cyber attack, ad hoc responses will not do. Nor is it sufficient to simply strengthen our defenses after incidents or attacks occur. Just as we do for natural disasters, we have to have plans and resources in place beforehand -- sharing information, issuing warnings and ensuring a coordinated response. Third, we will strengthen the public/private partnerships that are critical to this endeavor. The vast majority of our critical information infrastructure in the United States is owned and operated by the private sector. So let me be very clear: My administration will not dictate security standards for private companies. On the contrary, we will

collaborate with industry to find technology solutions that ensure our security and promote prosperity. Fourth, we will continue to invest in the cutting-edge research and development necessary for the innovation and discovery we need to meet the digital challenges of our time. And that's why my administration is making major investments in our information infrastructure: laying broadband lines to every corner of America; building a smart electric grid to deliver energy more efficiently; pursuing a next generation of air traffic control systems; and moving to electronic health records, with privacy protections, to reduce costs and save lives.

And finally, we will begin a national campaign to promote cybersecurity awareness and digital literacy from our boardrooms to our classrooms, and to build a digital workforce for the 21st century. And that's why we're making a new commitment to education in math and science, and historic investments in science and research and development. Because it's not enough for our children and students to master today's technologies -- social networking and e-mailing and texting and blogging -- we need them to pioneer the technologies that will allow us to work effectively through these new media and allow us to prosper in the future. So these are the things we will do. Let me also be clear about what we will not do. Our pursuit of cybersecurity will not -- I repeat, will not include -- monitoring private sector networks or Internet traffic. We will preserve and protect the personal privacy and civil liberties that we cherish as Americans. Indeed, I remain firmly committed to net neutrality so we can keep the Internet as it should be -- open and free. The task I have described will not be easy. Some 1.5 billion people around the world are already online, and more are logging on every day. Groups and governments are sharpening their cyber capabilities. Protecting our prosperity and security in this globalized world is going to be a long, difficult struggle demanding patience and persistence over many years. But we need to remember: We're only at the beginning. The epochs of history are long -- the Agricultural Revolution; the Industrial Revolution. By comparison, our Information Age is still in its infancy. We're only at Web 2.0. Now our virtual world is going viral. And we've only just begun to explore the next generation of technologies that will transform our lives in ways we can't even begin to imagine.

So a new world awaits -- a world of greater security and greater potential prosperity -- if we reach for it, if we lead. So long as I'm President of the United States, we will do just that. And the United States -- the nation that invented the Internet, that launched an information revolution, that transformed the world -- will do what we did in the 20th century and lead once more in the 21st. Thank you very much, everybody. Thank you.

Échantillon 2.

President Obama delivers remarks at the National Cybersecurity and Communications Integration Center, January 13, 2015.

Barack Obama
Good afternoon, everybody. I want to thank Secretary Johnson, Deputy Secretary Mayorkas, and the dedicated public servants of the Department of Homeland Security for welcoming me here today. I've kind of taken over your work space. I apologize for that, but just pretend that I'm not here. (Laughter.) I want you to keep working. I did ask who dressed up for this event, and apparently, a few were brave enough to admit it.

But in advance of my State of the Union address next week, I've been rolling out my proposals for keeping our economy on track, keeping it growing, making sure we're creating jobs and opportunity for the American people. And that includes the extraordinary opportunities that exist in our digital economy.

Yesterday, I announced new proposals to better protect Americans from identity theft and to ensure our privacy, including making sure that our kids are safe from digital marketing and intrusions on their privacy based on what they're doing at school. Tomorrow in Iowa, I'll talk about how we can give more families and communities faster, cheaper access to the broadband that allows them to successfully compete in this global economy. And on Thursday, the Vice President will be in Norfolk to highlight the need to continue to invest in the education and skills for our cybersecurity professionals. But today I am here at DHS to highlight how we can work with the private sector to better protect American companies against cyber threats.

Shortly after I took office, I declared that cyber threats pose an enormous challenge for our country. It's one of the most serious economic and national security challenges we face as a nation. Foreign governments, criminals and hackers probe America's computer networks every single day. We saw that again with the attack at Sony, which actually destroyed data and computer hardware that is going to be very costly for that company to clean up. Just yesterday, we saw the hack of a military Twitter account and You Tube channel. No military operations were impacted. So far, it appears that no classified information was released. But the investigation is ongoing, and it's a reminder that cyber threats are an urgent and growing danger.

Moreover, much of our critical infrastructure -- our financial systems, power grids, pipelines, health care systems --run on networks connected to the Internet. So this is a

matter of public safety and of public health. And most of this infrastructure is owned and operated by the private sector. So neither government, nor the private sector can defend the nation alone. It's going to have to be a shared mission -- government and industry working hand in hand, as partners.

And that's why I've said that protecting our digital infrastructure is a national security priority and a national economic priority. Over the past six years, we've pursued a comprehensive strategy, boosting our defenses in government, sharing more information with the private sector to help them defend themselves, working with industry through what we call the Cybersecurity Framework not just to respond to threats and recover from attacks but to prevent and disrupt them in the first place.

And that's where these good folks come in. We are currently at the National Cybersecurity Communications Integration Center -- also known as NCCIC. I just got a tour and a briefing. I want to thank everybody here, not just from DHS but from across government and the private sector, because, again, this is a shared responsibility.

This center is one of the critical lines of America's cyber defenses. These men and women work around the clock, 24/7, monitoring threats, issuing warnings, sharing information with the private sector, and keeping Americans safe. So, as a nation, we owe them thanks, and as a nation, we are making progress. We're more prepared to defend against cyber attacks. But every day, our adversaries are getting more sophisticated and more determined, and more plentiful. So every day, we've got to keep upping our game at the same time. We've got to stay ahead of those who are trying to do us harm.

The problem is that government and the private sector are still not always working as closely together as we should. Sometimes it's still too hard for government to share threat information with companies. Sometimes it's still too hard for companies to share information about cyber threats with the government. There are legal issues involved and liability issues. Sometimes, companies are reluctant to reveal their vulnerabilities or admit publicly that they have been hacked. At the same time, the American people have a legitimate interest in making sure that government is not potentially abusing information that it's received from the private sector.

So all of us -- government and industry -- are going to have to keep doing better. The new legislation and proposals I put forward yesterday will help, especially for a strong, single national standard for notifying Americans when their information has been breached. Today, I want to announce some additional steps.

First, we're proposing new cybersecurity legislation to promote the greater information sharing we need between government and the private sector. This builds

and improves upon legislation that we've put forward in the past. It reflects years of extensive discussions with industry. It includes liability protections for companies that share information on cyber threats. It includes essential safeguards to ensure that government protects privacy and civil liberties even as we're doing our job of safeguarding America's critical information networks.

I raised this issue again and the need for this legislation with congressional leaders this morning, including Speaker Boehner and Leader McConnell, and we all agree that this is a threat that has to be addressed, and I am confident that we should be able to craft bipartisan legislation soon to put these systems in place. We're going to keep on working with Congress to get this done. And in the meantime, we're going to do everything we can with our existing authorities to make sure industry gets the information it needs to better defend itself.

Second, we're proposing to update the authorities that law enforcement uses to go after cyber criminals. We want to be able to better prosecute those who are involved in cyber attacks, those who are involved in the sale of cyber weapons like botnets and spyware. We want to ensure that we're able to prosecute insiders who steal corporate secrets or individuals' private information. And we want to expand the authority of courts to shut down botnets and other malware. The bottom line, we want cyber criminals to feel the full force of American justice, because they are doing as much damage, if not more, these days as folks who are involved in more conventional crime.

Finally, and since this is a challenge that we can only meet together, I'm announcing that next month we'll convene a White House summit on cybersecurity and consumer protection. It's a White House summit where we're not going to do it at the White House; we're going to go to Stanford University. And it's going to bring everybody together -- industry, tech companies, law enforcement, consumer and privacy advocates, law professors who are specialists in the field, as well as students -- to make sure that we work through these issues in a public, transparent fashion.

Because they're hard and they're complicated issues. But if we keep on working on them together, and focus on concrete and pragmatic steps that we can take to boost our cybersecurity and our privacy, I'm confident that both our privacy will be more secure and our information, our networks, public health, public safety will be more secure. We're going to keep on at this as a government, but we're also going to be working with the private sector to detect, prevent, defend, deter against attacks, and to recover quickly from any disruptions or damage. And as long as I'm President, protecting America's digital infrastructure is going to remain a top national security priority.

In closing, I want to say one of the areas I'll be working with Congress is to ensure that we don't let any disagreements keep us from fulfilling our most basic

responsibilities. Last week's attack in Paris was a painful reminder that we have no greater duty than the security of the American people. And our national security should never be subject to partisan political games. Congress needs to fully fund our Department of Homeland Security, without delay, so that the dedicated public servants working here can operate with the certainty and confidence they need to keep the American people safe. And that's true across the board in the Department of Homeland Security.

So, again, I want to thank Jeh and Deputy Secretary Mayorkas, and everybody here at NCCIC and DHS for the great job you are doing. You are helping to keep the nation safe and secure.

And with that, we're going to get out of here so you can get back to work. Who knows what's been happening while you've been paying attention to me? (Laughter.) All right? Thank you very much, everybody. (Applause.)

Échantillon 3.

Remarks by the President at the Cybersecurity and Consumer Protection Summit, Stanford University, California

THE PRESIDENT: Hello, Stanford! (Applause.) Thank you so much. Thank you. Thank you, everybody. Have a seat. Have a seat.

AUDIENCE MEMBER: Yes, we can!

THE PRESIDENT: Yes, we can! (Applause.)
First of all, let me thank President Hennessy for not just the introduction but for your outstanding leadership at one of the great universities of the world. (Applause.) I've got to admit, like, I kind of want to go here. (Laughter and applause.) I was trying to figure out why it is that a really nice place like this is wasted on young people -- (laughter) -- who don't fully appreciate what you got. It's really nice. And everybody here is so friendly and smart, and it's beautiful. And what's there not to like?

I want to thank you and everyone at Stanford for hosting this summit, especially Amy Zegart, George Triantis, and someone who served as a great advisor to me at the White House and as an outstanding ambassador to Russia before coming back to The Farm -- Mike McFaul. (Applause.)

It is great to be here at Leland Stanford Junior University. And I'm pleased to be joined by members of my team who bleed Cardinal red. We're infiltrated with Stanford people. We've got Senior Advisor Valerie Jarrett, National Security Advisor Susan Rice, Secretary of Commerce Penny Pritzker. (Applause.) And, let's face it, I like Stanford grads. I noticed Steve Chu was around here, who helped lead our Energy Department for a while. (Applause.) And he's now hanging out. I'm also pleased to be joined by other members of my Cabinet -- our Secretary of Homeland Security Jeh Johnson is here, and our Small Business Administrator, Maria Contreras-Sweet. And I want to acknowledge my tireless Homeland Security Advisor who helped, and continues to shape, our cybersecurity efforts -- Lisa Monaco. (Applause.) Thank you, Lisa.

So I'd always heard about this campus, and everybody is riding bikes, and people hopping into fountains -- (laughter) -- and the current holder of The Axe. (Applause.) This is the place that made "nerd" cool. (Laughter.) I was thinking about wearing some black-rimmed glasses, some tape in the middle, but I guess that's not what you do anymore. Ambassador McFaul told me if I came to Stanford, you'd "talk nerdy to me." (Laughter.)

But I'm not just here to enjoy myself. As we gather here today, America is seeing incredible progress that we can all be proud of. We just had the best year of job growth since the 1990s. (Applause.) Over the past 59 months, our businesses have created nearly 12 million new jobs, which is the longest streak of private sector job growth on record. And in a hopeful sign for middle-class families, wages are beginning to rise again.

And, meanwhile, we're doing more to prepare our young people for a competitive world. Our high school graduation rate has hit an all-time high. More Americans are finishing college than ever before. Here at Stanford and across the country, we've got the best universities, we've got the best scientists, the best researchers in the world. We've got the most dynamic economy in the world. And no place represents that better than this region. So make no mistake, more than any other nation on Earth, the United States is positioned to lead in the 21st century.

And so much of our economic competitiveness is tied to what brings me here today, and that is America's leadership in the digital economy. It's our ability -- almost unique across the planet -- our ability to innovate and to learn, and to discover, and to create, and build, and do business online, and stretch the boundaries of what's possible. That's what drives us. And so when we had to decide where to have this summit, the decision was easy, because so much of our Information Age began right here, at Stanford.

It was here where two students, Bill Hewlett and Dave Packard, met and then, in a garage not far from here, started a company that eventually built one of the first personal computers, weighing in at 40 pounds. (Laughter.) It was from here, in 1968, where a researcher, Douglas Englebart, astonished an audience with two computers, connected "online," and hypertext you could click on with something called a "mouse."

A year later, a computer here received the first message from another computer 350 miles away -- the beginnings of what would become the Internet. And, by the way, it's no secret that many of these innovations built on government-funded research is one of the reasons that if we want to maintain our economic leadership in the world, America has to keep investing in basic research in science and technology. It's absolutely critical. (Applause.)

So here at Stanford, pioneers developed the protocols and architecture of the Internet, DSL, the first webpage in America, innovations for cloud computing. Student projects here became Yahoo and Google. Those were pretty good student projects. (Laughter.) Your graduates have gone on to help create and build thousands of companies that have shaped our digital society -- from Cisco to Sun Microsystems, YouTube to Instagram, StubHub, Bonobos. According to one study, if all the companies traced back to Stanford graduates formed their own nation, you'd be one the largest economies in the world and have a pretty good football team as well. (Laughter and applause.)

And today, with your cutting-edge research programs and your new cyber initiatives, you're helping us navigate some of the most complicated cyber challenges that we face as a nation. And that's why we're here. I want to thank all of you who have joined us today -- members of Congress, representatives from the private sector, government, academia, privacy and consumer groups, and especially the students who are here. Just as we're all connected like never before, we have to work together like never before, both to seize opportunities but also meet the challenges of this Information Age.

And it's one of the great paradoxes of our time that the very technologies that empower us to do great good can also be used to undermine us and inflict great harm. The same information technologies that help make our military the most advanced in the world are targeted by hackers from China and Russia who go after our defense contractors and systems that are built for our troops. The same social media we use in government to advocate for democracy and human rights around the world can also be used by terrorists to spread hateful ideologies. So these cyber threats are a challenge to our national security.

Much of our critical infrastructure -- our financial systems, our power grid, health systems -- run on networks connected to the Internet, which is hugely empowering but also dangerous, and creates new points of vulnerability that we didn't have before. Foreign governments and criminals are probing these systems every single day. We only have to think of real-life examples -- an air traffic control system going down and disrupting flights, or blackouts that plunge cities into darkness -- to imagine what a set of systematic cyber attacks might do. So this is also a matter of public safety.

As a nation, we do more business online than ever before -- trillions of dollars a year. And high-tech industries, like those across the Valley, support millions of American jobs. All this gives us an enormous competitive advantage in the global economy. And for that very reason, American companies are being targeted, their trade secrets stolen, intellectual property ripped off. The North Korean cyber attack on Sony Pictures destroyed data and disabled thousands of computers, and exposed the personal information of Sony employees. And these attacks are hurting American companies and costing American jobs. So this is also a threat to America's economic security.

As consumers, we do more online than ever before. We manage our bank accounts. We shop. We pay our bills. We handle our medical records. And as a country, one of our greatest resources are the young people who are here today -- digitally fearless and unencumbered by convention, and uninterested in old debates. And they're remaking the world every day. But it also means that this problem of how we secure this digital world is only going to increase.

I want more Americans succeeding in our digital world. I want young people like you to unleash the next waves of innovation, and launch the next startups, and give Americans the tools to create new jobs and new businesses, and to expand connectivity in places that we currently can't imagine, to help open up new world and new experiences and empower individuals in ways that would seem unimaginable 10, 15, 20 years ago.

And that's why we're working to connect 99 percent of America's students to high-speed Internet -- because when it comes to educating our children, we can't afford any digital divides. It's why we're helping more communities get across to the next generation of broadband faster, with cheaper Internet, so that students and entrepreneurs and small businesses across America, not just in pockets of America, have the same opportunities to learn and compete as you do here in the Valley. It's why I've come out so strongly and publicly for net neutrality, for an open and free Internet -- (applause) -- because we have to preserve one of the greatest engines for creativity and innovation in human history.

So our connectivity brings extraordinary benefits to our daily lives, but it also brings risks. And when companies get hacked, Americans' personal information, including their financial information, gets stolen. Identity theft can ruin your credit rating and turn your life upside down. In recent breaches, more than 100 million Americans had their personal data compromised, including, in some cases, credit card information. We want our children to go online and explore the world, but we also want them to be safe and not have their privacy violated. So this is a direct threat to the economic security of American families, not just the economy overall, and to the wellbeing of our children, which means we've got to put in place mechanisms to protect them.

So shortly after I took office, before I had gray hair -- (laughter) -- I said that these cyber threats were one of the most serious economic national security challenges that we face as a nation, and I made confronting them a priority. And given the complexity of these threats, I believe we have to be guided by some basic principles. So let me share those with you today.

First, this has to be a shared mission. So much of our computer networks and critical infrastructure are in the private sector, which means government cannot do this alone. But the fact is that the private sector can't do it alone either, because it's government that often has the latest information on new threats. There's only one way to defend America from these cyber threats, and that is through government and industry working together, sharing appropriate information as true partners.

Second, we have to focus on our unique strengths. Government has many capabilities, but it's not appropriate or even possible for government to secure the computer networks of private businesses. Many of the companies who are here today are cutting-edge, but the private sector doesn't always have the capabilities needed during a cyber attack, the situational awareness, or the ability to warn other companies in real time, or the capacity to coordinate a response across companies and sectors. So we're going to have to be smart and efficient and focus on what each sector does best, and then do it together.

Third, we're going to have to constantly evolve. The first computer viruses hit personal computers in the early 1980s, and essentially, we've been in a cyber arms race ever since. We design new defenses, and then hackers and criminals design new ways to penetrate them. Whether it's phishing or botnets, spyware or malware, and now ransomware, these attacks are getting more and more sophisticated every day. So we've got to be just as fast and flexible and nimble in constantly evolving our defenses.

And fourth, and most importantly, in all our work we have to make sure we are protecting the privacy and civil liberty of the American people. And we grapple with these issues in government. We've pursued important reforms to make sure

we are respecting peoples' privacy as well as ensuring our national security. And the private sector wrestles with this as well. When consumers share their personal information with companies, they deserve to know that it's going to be protected. When government and industry share information about cyber threats, we've got to do so in a way that safeguards your personal information. When people go online, we shouldn't have to forfeit the basic privacy we're entitled to as Americans.

In recent years, we've worked to put these principles into practice. And as part of our comprehensive strategy, we've boosted our defenses in government, we're sharing more information with the private sector to help those companies defend themselves, we're working with industry to use what we call a Cybersecurity Framework to prevent, respond to, and recover from attacks when they happen.

And, by the way, I recently went to the National Cybersecurity Communications Integration Center, which is part of the Department of Homeland Security, where representatives from government and the private sector monitor cyber threats 24/7. And so defending against cyber threats, just like terrorism or other threats, is one more reason that we are calling on Congress, not to engage in politics -- this is not a Republican or Democratic issue -- but work to make sure that our security is safeguarded and that we fully fund the Department of Homeland Security, because it has great responsibilities in this area.

So we're making progress, and I've recently announced new actions to keep up this momentum. We've called for a single national standard so Americans know within 30 days if your information has been stolen. This month, we'll be proposing legislation that we call a Consumer Privacy Bill of Rights to give Americans some baseline protections, like the right to decide what personal data companies collect from you, and the right to know how companies are using that information. We've proposed the Student Digital Privacy Act, which is modeled on the landmark law here in California -- because today's amazing educational technologies should be used to teach our students and not collect data for marketing to students.

And we've also taken new steps to strengthen our cybersecurity -- proposing new legislation to promote greater information sharing between government and the private sector, including liability protections for companies that share information about cyber threats. Today, I'm once again calling on Congress to come together and get this done.

And this week, we announced the creation of our new Cyber Threat Intelligence Integration Center. Just like we do with terrorist threats, we're going to have a single entity that's analyzing and integrating and quickly sharing intelligence about cyber threats across government so we can act on all those threats even faster.

And today, we're taking an additional step -- which is why there's a desk here. You were wondering, I'm sure. (Laughter.) I'm signing a new executive order to promote even more information sharing about cyber threats, both within the private sector and between government and the private sector. And it will encourage more companies and industries to set up organizations -- hubs -- so you can share information with each other. It will call for a common set of standards, including protections for privacy and civil liberties, so that government can share threat information with these hubs more easily. And it can help make it easier for companies to get the classified cybersecurity threat information that they need to protect their companies.

I want to acknowledge, by the way, that the companies who are represented here are stepping up as well. The Cyber Threat Alliance, which includes companies like Palo Alto Networks and Symantec, are going to work with us to share more information under this new executive order. You've got companies from Apple to Intel, from Bank of America to PG&E, who are going to use the Cybersecurity Framework to strengthen their own defenses. As part of our BuySecure Initiative, Visa and MasterCard and American Express and others are going to make their transactions more secure. Nationstar is joining companies that are giving their companies [customers] another weapon to battle identity theft, and that's free access to their credit scores.

And more companies are moving to new, stronger technologies to authenticate user identities, like biometrics -- because it's just too easy for hackers to figure out usernames and passwords, like "password." (Laughter.) Or "12345 -- (laughter) -- 7." (Laughter.) Those are some of my previous passwords. (Laughter.) I've changed them since then. (Applause.)

So this summit is an example of what we need more of -- all of us working together to do what none of us can achieve alone. And it is difficult. Some of the challenges I've described today have defied solutions for years. And I want to say very clearly that, as somebody who is a former constitutional law teacher, and somebody who deeply values his privacy and his family's privacy -- although I chose the wrong job for that -- (laughter) -- but will be a private citizen again, and cares deeply about this -- I have to tell you that grappling with how government protects the American people from adverse events while, at the same time, making sure that government itself is not abusing its capabilities is hard.

The cyber world is sort of the wild, wild West. And to some degree, we're asked to be the sheriff. When something like Sony happens, people want to know what can government do about this. If information is being shared by terrorists in the cyber world and an attack happens, people want to know are there ways of stopping that from happening. By necessity, that means government has its own significant

capabilities in the cyber world. But then people, rightly, ask, well, what safeguards do we have against government intruding on our own privacy? And it's hard, and it constantly evolves because the technology so often outstrips whatever rules and structures and standards have been put in place, which means that government has to be constantly self-critical and we have to be able to have an open debate about it.

But we're all here today because we know that we're going to have to break through some of these barriers that are holding us back if we are going to continue to thrive in this remarkable new world. We all know what we need to do. We have to build stronger defenses and disrupt more attacks. We have to make cyberspace safer. We have to improve cooperation across the board. And, by the way, this is not just here in America, but internationally -- which also, by the way, makes things complicated because a lot of countries don't necessarily share our investment -- or our commitment to openness, and we have to try to navigate that.

But this should not be an ideological issue. And that's one thing I want to emphasize: This is not a Democratic issue, or a Republican issue. This is not a liberal or conservative issue. Everybody is online, and everybody is vulnerable. The business leaders here want their privacy and their children protected, just like the consumer and privacy advocates here want America to keep leading the world in technology and be safe from attacks. So I'm hopeful that through this forum and the work that we do subsequently, that we're able to generate ideas and best practices, and that the work of this summit can help guide our planning and execution for years to come.

After all, we are just getting started. Think about it. Tim Berners-Lee, from his lab in Switzerland, invented the World Wide Web in 1989, which was only 26 years ago. The great epochs in human history -- the Bronze Age, Iron Age, Agricultural Revolution, Industrial Revolution -- they spanned centuries. We're only 26 years into this Internet Age. We've only scratched the surface. And as I guess they say at Google, "The future is awesome." (Laughter.) We haven't even begun to imagine the discoveries and innovations that are going to be unleashed in the decades to come. But we know how we'll get there.

Reflecting on his work in the 1960s on ARPANET, the precursor of the Internet, the late Paul Baran said this: "The process of technological developments is like building a cathedral. Over the course of several hundred years, new people come along and each lays down a block on top of the old foundations, each saying, 'I built the cathedral.' And then comes along an historian who asks, 'Well, who built the cathedral?'" And Baran said, "If you're not careful, you can con yourself into believing that you did the most important part. But the reality is that each

contribution has to follow on to previous work. Everything is tied to everything else."

Everything is tied to everything else. The innovations that first appeared on this campus all those decades ago -- that first mouse, that first message -- helped lay a foundation. And in the decades since, on campuses like this, in companies like those that are represented here, new people have come along, each laying down a block, one on top of the other. And when future historians ask who built this Information Age, it won't be any one of us who did the most important part alone. The answer will be, "We all did, as Americans."

And I'm absolutely confident that if we keep at this, if we keep working together in a spirit of collaboration, like all those innovators before us, our work will endure, like a great cathedral, for centuries to come. And that cathedral will not just be about technology, it will be about the values that we've embedded in the architecture of this system. It will be about privacy, and it will be about community. And it will be about connection. What a magnificent cathedral that all of you have helped to build. We want to be a part of that, and we look forward to working with you in the future.

Thank you for your partnership. With that, I'm going to sign this executive order. Thank you. (Applause.)

Échantillon 4.

Press Briefing by Press Secretary Josh Earnest, 6/9/2015

Q: On the OPM hack. We learned that up to 4 million current and former government employees had -- their personal information was vulnerable to these hackers. Does that universe of people include Cabinet Secretaries?

MR. EARNEST: Jon, there is an ongoing investigation to this specific matter and that investigation includes the scope of this particular intrusion. So if there's more information that we have to share about who precisely was affected, that's information that would come from the FBI who is leading this investigation.

Q: Were the vulnerable personnel files -- did they include the Secret Service, FBI?

MR. EARNEST: Again, part of this investigation is to determine the precise scope of the intrusion and to get a better sense of exactly what information was put at risk and

what information was potentially exfiltrated. And so that's work that is ongoing right now.

Q: But we were told this was a universe of up to 4 million, so you must have known what the universe is. Does that universe of possible vulnerabilities include Cabinet Secretaries, people employed by the Secret Service, FBI and the like?

MR. EARNEST: Again, the scope of this particular intrusion is something that continues to be investigated by the FBI.

Q: So what did you mean when we were told it was 4 million -- up to 4 million?

MR. EARNEST: Well, that was a number that was based on our assessment at that time of precisely the number of records that were affected by this particular intrusion. But this is an ongoing investigation and --

Q: You must information as to -- I mean, that number didn't come out of the blue. I mean, it was 4 million who, 4 million what?

MR. EARNEST: We've described them as either former or current federal employees.

Q: And is there any suggestion that this information that was taken, or feared to have been taken, could be used to either blackmail individuals or to steal the identity of individuals that have sensitive security positions?

MR. EARNEST: Jon, again, the investigation doesn't just include the scope of this particular intrusion, but it also includes an effort to try to determine the motive of the individuals who may have been acting in this case. As a precautionary measure, those individuals that are determined to be at risk here will be offered by the Office of Personnel Management some identity theft protection and other advice about steps they can take --

Q: Okay. So then you're offering that to somebody. So is that being offered to Cabinet Secretaries, members of the Secret Service or FBI?

MR. EARNEST: It's being offered to individuals who may have potentially been affected in this case.

Q: And so does those individuals include --
MR. EARNEST: I'm not going to talk about the individuals who may have been affected.

Q: So you're not ruling out that the group of people that I just mentioned were included in this group?

MR. EARNEST: You should check with the FBI, and if they have more information to share with you they'll share it.

Q: How concerned are you about this? And what is the nature of the concern? Is the concern that people might be ripped off because their identities might be stolen? Or is there a greater concern -- security concern?

MR. EARNEST: I think the concern that the President has is that this highlights the clear vulnerabilities that exist in many elements of the federal government's computer architecture. And this administration, for years now, has been working diligently to try to upgrade our defenses and to put in place measures that would mitigate against those intrusions and respond to them when necessary. This is --

Q: So is the President upset of the gross failure here? I mean, supposedly, these people had access to personnel records for months without even being detected.

MR. EARNEST: The President is concerned about the vulnerabilities that were highlighted here. But the other thing the President indicated, in talking about this yesterday, is that the reason that this intrusion was detected is that OPM was actually in the process of implementing better defenses of their computer network when this particular intrusion was detected. So that's an indication that they're making progress. But there's clearly more important work that needs to be done not just at OPM, but at other government agencies.

But, again, this is not different than the kind of threat that we see in the private sector as well. And all of you represent news organizations, many of which have been subjected to intrusions like this, and your security professionals are doing the same thing that our security professionals are doing, which is making sure that we're rapidly adapting to the innovative and persistent adversary that's out there.

Q: Was China behind this?

MR. EARNEST: The specific individuals or entities who carried out this particular intrusion is something that's still being investigated by the FBI.

Q: Do you have reason to believe it was a foreign government or somebody working on behalf of a foreign government?

MR. EARNEST: What the FBI is doing is trying to determine who those individuals are and if they were acting on behalf of a criminal enterprise or a nation state. They're going to do their best to work to determine that.

As is consistent with the strategy that we've used in investigating previous cyber intrusions, I can't promise you that we'll be in a position at any point in the future to make a grand pronouncement about who may have been responsible for this particular intrusion, but it's something that we are working hard to try to determine. And if a response is necessary, then the President, because of steps that he announced a couple of months ago, has more tools at his disposal to respond to this particular incident -- and I'm referring to the executive order the President signed that authorized the Secretary of the Treasury to impose financial sanctions against those who are deemed to be responsible or benefit from a cyber-attack.
[...]

Julie.
Q: Thanks. Just getting back to the breach of federal employee data. I know you said, and they've said at OPM that the reason they discovered it was because they were installing additional safeguards. But I'm wondering whether the President thinks that there was a management failure here. I mean, this is, after all, an agency that handles sensitive personal information for the vast majority of federal government employees. They had been told by their IG that they had vulnerabilities. Even though they were addressing those, it wasn't happening in a quick enough way, obviously, to stop this from happening. So does he have confidence in the director over there and senior leadership that they have their hands around this issue?

MR. EARNEST: Well, the President has confidence that every single member of his staff understands that cybersecurity needs to be a priority. And, again, in talking about this yesterday, the President was pretty direct about the fact that we've got our work cut out for us when it comes to taking what, in some cases, are pretty old computer systems and making sure that they have modern, adaptable security measures in place to protect against cyber intrusions.
What's also clear is that our adversaries -- whether we're talking about criminal enterprises or federal governments, or entities acting on behalf of foreign governments -- that these adversaries are persistent and well-resourced, and we need to make sure on our side that we're vigilant and well-resourced to meet this threat. And it requires an approach that understands that this is a very adaptive environment, that particularly when we're talking about modern technology, we're talking about very complex mechanisms and the need to make sure that our defenses adapt as rapidly as our adversaries do.

Q: So does he feel that the OPM Director is up to that challenge?

MR. EARNEST: Well, the President certainly believes that the Director of the OPM is aware that this is a priority. And this is a message that's been delivered to -- the President convened this Cabinet meeting a couple of weeks ago -- two or three weeks ago, I guess it was now -- where this was an item on the agenda, the need to make sure that, institutionally, agencies across the administration understand that these kinds of threats are real and require the attention of the senior-level officials at each of these agencies.
[...]

Q: Just to follow up on what you were saying when we were all evacuated. You were talking about a Cabinet meeting where the President raised this several weeks ago -- or a couple of weeks ago.

MR. EARNEST: Yes, I was.

Q: I wanted to clarify, was that before or after he had been made aware, and you at the White House became aware of this breach of 4 million people's identifying information?

MR. EARNEST: I don't know of the precise sequence of those events. But I will tell you that it is not unusual for the President to spend time at a Cabinet meeting talking to the leaders of his government about the importance of cybersecurity. But I do know that as recently as the most recent Cabinet meeting which occurred two or three weeks ago, that this was an agenda item and the President made clear to members of his Cabinet how seriously he takes cybersecurity and how important it is for the leaders of those organizations to prioritize the effort to upgrade our cyber defenses, put in place software that can mitigate the threat from cyber intrusions, and also make sure that we have the tools that are necessary to adapt to the ever-evolving threat.

Q: And has he talked with the OPM Director since this breach was revealed, as he became aware of it?

MR. EARNEST: I don't believe so, no.

[...]

Échantillon 5.

Press Briefing by Press Secretary Josh Earnest, 6/25/2015

[...]

Q: One last thing. Kathy Archuleta told Congress twice now, no one is personally responsible within the government for the hack. She said the perpetrators are the responsible party. I understand that part; I'm not asking you to disagree with that. But for those who feel anxious and who are trying to find out and get on a call line where they wait four or five hours to get a non-response about what's actually happened with their data, does the President -- or do you, speaking on behalf of the White House, believe no one is responsible for what was a hack in the first place, systems that were vulnerable, and then systems that were identified to have been vulnerable for seven consecutive years by inspectors general analyzing the systems at OPM?

MR. EARNEST: Well, Major, I can tell you that the President certainly feels responsible when it comes to making sure that the sensitive data of federal government personnel is properly protected. And that is certainly not too much for those federal employees to ask, and that's the expectation that the President has set out for his team. And the President is certainly willing to accept that among his many other responsibilities. Now, what –

Q: So this is on him?

THE PRESIDENT: What's also true is we're going to need some help from Congress, and we're going to need Congress to do their job. We've put forward some very specific proposals that we would like Congress to pass when it comes to cybersecurity that would improve the ability of both the federal government and the private sector to respond to these incidents.

Q: Understood. But if you look at the testimony who witnesses called -- and they were not hostile witnesses, they were not against the administration; some were former inspectors general -- they said these issues, these vulnerabilities could have been addressed even without cybersecurity legislation coming from Congress. Those were things that are dealing the government and private sector doing a lot more to share and integrate. But they said -- and again, they were not hostile witnesses -- they said these things could have been buttoned up internally; that it's a management and leadership issue within OPM, not cybersecurity legislation, that is the real culprit.

MR. EARNEST: Well, I think -- well, let me say a couple things about that. I think it's far too early to tell at this point exactly what could have been done differently to

ensure that we would be able to have prevented this particular intrusion. There's still an ongoing investigation. So it's too early to speak to that.
At the same time, the President and his team have acknowledged that there's more that the federal government, quite frankly, is working very hard to do right now to bolster our cybersecurity and to bolster our cyber defenses.
We're operating in a very dynamic environment against adversaries that have proven to be very innovative. And this is a significant challenge, but this is not a challenge that's unique to the federal government. This is a challenge that private sector entities are dealing with, and even some media companies have experienced these kinds of intrusions in a way that have been damaging.
So this is something that we all have -- that across the public and private sector, that we're all dealing with. Again, I would reiterate, though, that some of the information-sharing that we need Congress to act on is information-sharing that would benefit the federal government. If a private sector company is the victim of a particularly unique cyber-attack, we want to make sure that we can quickly communicate information about that attack not just to other private-sector actors, but also to the government as well, so that we can make sure that we're not vulnerable to the same kind of tactics that were used to penetrate someone else's system.
So that's why we've made that a real priority. And Congress has really fallen down on the job here, and we want them to act.

Q: Since you said the President feels he's responsible, has he told his team to give him metrics by which he can know when the cyber defenses have reached a certain level to remove vulnerabilities and deal with these endless wait times that people have, who are victims of this, trying to find out what they're supposed to find out when they call the number on the letter that they were sent to by OPM?

MR. EARNEST: Well, the President is serious about making sure that he's regularly updated on the efforts of agencies in the federal government to bolster their cyber defenses. And this is --

Q: Has he given them any marching orders?

MR. EARNEST: Well, I mentioned within the last couple of weeks here that this was actually an item on the agenda at a recent Cabinet meeting that the President convened, where every member of his Cabinet sat around the table, received a briefing about how important it is to take seriously these concerns about cybersecurity. And there is a mechanism -- I believe that DHS has established this mechanism -- for tracking the progress that each agency is making in bolstering their cyber defenses. And this is something that they are tracking very closely.
Some of this is also not just to obviously making sure that they're following through on this commitment, but also making sure that they're getting the resources that they need to take the steps that are necessary to protect their systems.

Q: How about the wait times?

MR. EARNEST: The wait times is a different issue. I don't know exactly how that's being tracked.

Q: -- a contractor and everything, but it's still a huge hassle.

MR. EARNEST: There's no doubt about that. And I know that the contractor has undertaken some steps under some pretty intense pressure from the federal government to try to streamline that process.
[...]

Byron.
Q: Thanks, Josh. The Director of National Intelligence, James Clapper, said today that China is the leading suspect in the OPM hack. If that's ultimately confirmed as true, what kind of response can we expect from the United States?

MR. EARNEST: Byron, at this point I'm not in a position to talk about any potential suspects in the ongoing investigation. I'd refer you to either DNI Clapper or to the FBI, who's leading the investigation, for the latest assessment. If they decide that it is actually in the interest of the investigation to be clearer about who they suspect may be involved, that will be a decision for them to make.
The other thing I will just point out is that I wouldn't guess at this point about what sort of response the United States may consider at this point against whoever is responsible for this particular incident. What is true is that if there is a response, it's probably not one we are likely to telegraph in advance. And two, you'll recall that earlier this year the President actually signed an executive order authorizing the Secretary of the Treasury to levy sanctions -- financial sanctions against individuals who carry out cyber-attacks or who benefit from them. That gives the U.S. government a whole set of new tools that didn't previously exist for responding to incidents like this.
So I'm not telling you that those tools will be deployed in response to this incident, but they certainly are available.

[...]

Échantillon 6.

Conference Call to Preview the Visit of President Xi Jinping of the People's Republic of China

MR. PRICE: Good afternoon, everyone, and thanks for joining this preview call to preview the visit of Xi Jinping, the President of the People's Republic of China. This call will be on the record but it will be embargoed until the conclusion of the call, so we would ask that you not tweet or otherwise use the contents of this call until its conclusion.

We have three senior administration officials on today's call. We have Ben Rhodes, the Deputy National Security Advisor for Strategic Communications. We have Caroline Atkinson, the Deputy National Security Advisor for International Economics. And we have Dan Kritenbrink, who is the Senior Director for Asian Affairs at the National Security Council.
So with that, I will turn it over to Ben Rhodes to kick us off.

MR. RHODES: Great. Thanks, Ned. Appreciate everybody getting on the call. I'll just make some opening comments about how President Obama has approached this relationship with China in office. I'll turn it over to Dan who can go through the agenda and some of the specific issues related to the visit. And then Caroline can speak to some of the economic issues that will come up around the visit.

[...]

Just to make a couple of other comments here -- again, we've approached this relationship knowing that we're not going to agree on everything, but with the strong belief that we benefit when we can advance cooperation. That includes on bilateral issues, but it also includes multilateral and global issues. We believe that the more China is invested in resolving global issues and supporting a rules-based international order, the better it will be for the United States and for the world. And the climate commitment that came out of last year's state visit is a direct indication of how sustained engagement can yield results in which the U.S. and China, again, are cooperating not just bilaterally but setting an example and helping provide momentum to global efforts as well.

[...]

The last thing I'd say is that the U.S.-China relationship is just one part of the broader rebalance to the Asia Pacific region. You've heard the President speak often about how America's interest in the 21st century will largely be defined by our engagement in the largest-emerging market in the world. A central pillar of our Asia rebalance is

this bilateral relationship with China. Other pillars of course include the U.S. alliances, which are the cornerstone of our approach to the Asia Pacific, and we've invested significantly in those alliances, as well as our emerging partnerships with countries such as the ASEAN countries.
So this is part of a broader Asia policy. But what I will say is that the countries of the Asia Pacific certainly believe that a good U.S.-China relationship, a stable U.S.-China relationship contributes to the stability and the prosperity of the region. So even as we are deepening those alliances, building those partnerships with emerging countries, working to complete the Trans-Pacific Partnership, which will be a landmark effort to advance America's economic interest and to cement our engagement in Asia, we see this bilateral relationship with China as fundamental to our Asia rebalance.
With that, I'll turn it over to Dan to go through the details of the visit.

[...]

And then of course, there will be a range of bilateral issues as well, including, we hope, further work at building out confidence-building measures between our two militaries, and some things we can do to improve people-to-people interaction between the American and Chinese people, building on last year's visa-related extension agreement.

I would close by just saying, as Ben said, there will also be I think a very robust discussion of the differences between our two countries. As the President has said, the national security advisor has said, we won't paper over those differences. We'll be very clear and candid about them. Some of those differences will include cyber, economic and trade issues, maritime issues and human rights. So I think you'll see that balanced approach on display during the state visit.
That's all I wanted to say.

MS. ATKINSON: Thank you, Dan, and thanks to everybody on the call. I just wanted to make a couple of points about the relationship with China in the economic sphere. Clearly, as Ben said, this is an extremely important and deep relationship. We have seen, this summer, that it's important that China demonstrate that its economic reforms are on track; that it will refrain from competitive devaluation; and that it will implement pro-growth fiscal policies that accelerate the transition to consumer-led growth. This is extremely important, we believe, for the acceleration of China's reform for continuing the growth that China wants and that is also in the interest of the global economy.

Secondly, the United States believes that it's time for China -- it's important that China should share responsibility for sustaining the rules-based international economic system. This system, which was put in place with a lot of work by the

United States and others, has benefitted China and enabled its rise. We believe that China recognizes this, and that it's important for us to work together to strengthen that international financial system, including through more balanced economic growth in China. Of course, the United States is in a relatively strong position at the moment in terms of our economic performance.
And finally, as Dan mentioned, there are some irritants on the bilateral economic relationship that can be threatened by China's policies that can be discriminatory and protectionist on technology, uneven enforcement of anti-monopoly law, and actions in the agricultural sphere where science-based approach is not yet fully in place.
So we believe that it's in China's interest and our interest that China move to reaffirm the protection of intellectual property and allow market forces to play a decisive role in the economy as they have said, and allow for fair competition and a level playing field for foreign firms in their domestic market.

Q You guys have talked a lot about cyber and we know that cyber will be probably a tense discussion. Can we expect that there will be an agreement at all on the cyber issue -- and/or will you say to Xi, will the President to President Xi that sanctions are pending?

MR. RHODES: I'll start, Jeff, and then see if Dan wants to add anything. I think cyber will certainly be a very important part of the agenda and the discussion. We made very clear to China our deep concerns about certain cyber activities. In particular, we focused on a Chinese government-sponsored, cyber-enabled theft of confidential business information and proprietary technology from U.S. companies. And so to be very clear here, this is not just a matter of whether or not countries conduct traditional espionage; it's a matter of whether our businesses can have the confidence that they can operate in China or operate globally without being subjected to cyber intrusions and that seek to steal their intellectual property.
This should be of interest to the Chinese as well. In the last several decades, as we've expanded this relationship, one of the key stakeholders for the U.S.-China relationship here in the United States has been the business community. But we are increasingly hearing concerns about activities that the Chinese have been engaged in. So we want to make very clear that this puts at risk China's ability to continue on its economic growth if businesses don't have confidence that they're not going to be subjected to cyber theft.

Our preference is to handle this through dialogue and through diplomacy, and through mutual understandings that we can reach. I don't want to suggest a particular formal agreement -- we'll have to see again what type of discussions the leaders have. What I do want to emphasize is that the area where we would like to reach a greater understanding with the Chinese is on the protection of intellectual property and the ability of businesses to operate without concern of cyber theft. And, again, this will be an ongoing dialogue.

Now, we've also made clear that we have other punitive measures available when we do see instances of cyber intrusions and cyber theft. In the past, the United States government has already engaged in law enforcement actions, for instance, that targeted Chinese entities who we believed were behind that type of activity. Sanctions remain the tool of the United States, and we would be prepared, if necessary, to pursue sanctions as a tool if we felt that there was a case that merited that type of punitive action.
So there's a range of options available to us, ranging from constructive dialogue and mutual understandings to more punitive measures to include sanctions. And I think we'll have the ability to lay that out for the Chinese. But I think we do so from the premise that it's in China's interest to ensure that businesses have the confidence that there is a level playing field in China and that they're not at risk from Chinese cyber actors.

Q Hi, there. It seems like the course of this relationship is always one step forward and then one step or two steps backwards, especially in Chinese actions in the cyber realm, maritime security and human rights. Do you feel like it's an inevitability that that's going to be the course of this relationship in the future? Do you have any optimism or confidence that China will be a better actor in cybersecurity? And if you do have some optimism, where does that come from? Thanks.

MR. RHODES: So, Michelle, I think that there's going to be aspects of the relationship that are cooperative and there are going to be aspects of the relationship that are competitive. And that's always been our understanding. And as a general matter, we welcome the peaceful rise of prosperous China. That can benefit our own interests. It can support U.S. jobs in economic activity. And it can contribute to the stability of the Asia Pacific region.

[...]

So there's a range of issues, I think, where I think we can say we've made progress. At the same time, we are going to have concerns and we're going to be open about those concerns. We talked about cyber. Again, the chief reason I think the Chinese have an interest in changing some of their behavior in the cyber realm is because if they're operating outside of established international rules and norms, they're ultimately going to alienate businesses, including U.S. businesses who have been critical to Chinese economic growth.
[...]

MR. KRITENBRINK: I completely agree with that. I mean, I think it's an exceptionally complex relationship; I think it always has been. I think we shouldn't lose sight of the fact that, as Ben very correctly pointed out, that we're cooperating in

a broad range of areas. I think you could argue that we're cooperating in more meaningful ways, on a more diverse set of issues than ever before. At the same time, the challenges that we face are exceptionally important and they're complex, and we intend to tackle those issues head on and deal with them in a forthright manner.
[...]

Q Hi, guys. Thank you for doing the call. I wanted to see if you could just talk a little bit about the relationship between President Obama and President Xi. We hear the relationship between Obama and Putin described sometimes as "businesslike." Considering their meeting at Sunnylands, what kind of relationship do he and Obama have? And can you talk a little bit about in their talks, perhaps, that private dinner or their other meetings, how President Obama will approach breaching some of these tougher issues if they do have a somewhat more friendly relationship? Thanks.

MR. RHODES: I think he's been able to develop a good relationship with President Xi. That doesn't mean we agree with everything President Xi does. But I think that they have been able to have constructive conversations.
And here's how I'd put it. The U.S.-China -- someone who's been in a lot of these meetings -- oftentimes, frankly, because we have such a long agenda, you end up sitting there and going through a list, and "here's our position on X-issue and here's your position." I think what's been distinct about their relationship, starting at Sunnylands, is far and away the most constructive engagements they've had have been in their private dinners.
You have the bilateral meetings, you work through the agenda, and that's necessary and very important. But both at Sunnylands and in China, President Obama commented afterwards that he felt the most constructive engagements were when they were able to talk for several hours over dinner without a formal agenda, and give a vision for where they want to take their country, give a vision for how they think the U.S. and China should operate together in the world, and kind of put aside the talking points and actually get a window into one another's world view.
And those world views are very different. And that's part of why I think the conversations are useful and important, because it provides a context for all these issues.
And so again, I think starting in Sunnylands and then in China, this ability to step back and offer a perspective of where we are in terms of our relationship and where our respective countries are, President Obama was able to hear from President Xi about his own domestic program, and was able to share some thoughts on his domestic program, as well. It doesn't mean that there's going to be perfect agreement, but I think they have an understanding as leaders of where they're coming from on these issues -- so that way, when there is a dispute, they're able to address it directly. And when there's an opportunity to make progress, we seize it.
So for instance, at Sunnylands there was a lot of talk about climate change, and there we had an important but more modest goal of dealing with the Montreal Protocol.

But those conversations I think led to the effort to have the breakthrough last year, where we announced these joint targets with respect to our missions. And I think that was rooted in President Obama's understanding that President Xi is ambitious, and that ambition can serve global interests.

I think it's a misnomer to say that we don't want China to play a large role on the world stage.

[...]

Q You mentioned some of the previous interactions these two Presidents have had, and presumably the issue of cyber has come up at Sunnylands and in China. And it seems like things have gotten progressively worse, even after those dialogues. So I'm wondering, though you say you want to fix things with dialogue, if the fact that things have gotten worse after previous encounters indicates that if there isn't something concrete, something deliverable, some kind of pact that comes out of this, sanctions are pretty likely. And then, secondly, I just want to know if you were able to see the Wall Street Journal interview that President Xi did. And in that interview, he said that the Chinese government does not engage in theft of commercial secrets in any form, nor does it encourage or support Chinese companies to engage in such practices. I wanted to know what your response was to his denial.

MR. RHODES: Well, candidly, cyber is an issue where we have not made the progress that we've wanted to make. We have not seen the types of steps that give our companies greater assurances. And we've been very forthright about that. And while our preference is resolving this through dialogue, we're not averse to punitive measures, including sanctions, if we feel like there are actors in China and entities that are engaged in activities that are sanctionable. So that remains very much a tool of U.S. policy and we'll have a mix of tools available, some of them more focused on dialogue and cooperation, but as necessary, we'd be willing to take punitive action. And we have in the past; you've seen some major law enforcement actions, for instance, that have been focused on Chinese entities.
And I just want to underscore this -- I didn't see the full interview from President Xi. What I would say is that we're drawing a very clear distinction between the fact that, look, there are activities that all governments engage in as it relates to national security, but what we don't engage in as the United States is the theft of trade secrets. And that's something that gets at the integrity of the global economy, and that's why we've been so focused on this.

MR. KRITENBRINK: Could I -- yes, one point. I think on this issue, certainly this has been an issue for the past few years. The President has raised it very directly. I think one indication that the Chinese side has taken seriously are concerns of the fact

that they sent Secretary Meng Jianzhu here as President Xi's special envoy to address these issues. And we had very candid and open discussions with him on that.
And you mentioned, President Xi's comments -- I mean, what I would say is, of course we would welcome a commitment on the part of the Chinese not to engage in this type of behavior. The focus of course has to be on actions not simply words. So I think we'll be looking very carefully at the actions of the Chinese state going forward.

MR. RHODES: Yes, and President Xi did say also, looking at this interview, that he wants to strengthen cooperation with the United States on this issue. I think this summit will be an opportunity for us to hear directly from him what form that takes, and then we'll be able to make a judgment based on those conversations.

Q Along the same line on this, can we rule out any action before the meeting? There had been some discussion of perhaps this could happen before or after the trip. It is now safe to say that there will be no action ahead of the meeting?

MR. RHODES: Yes, I would not anticipate -- if you're talking about sanctions -- I would not anticipate that type of action before the meetings, no.

[...]

We conduct over half a trillion dollars in economic activity with China. There is an enormous amount of U.S. jobs that are created and supported through our trade with China. China is a member of the U.N. Security -- a permanent member of the U.N. Security Council. China is the biggest country in the world, and also the biggest emerging power in the region of the world that is going to be a focal point for the United States.
So I think anybody who is President of the United States will find an interest to work through differences with China and to find areas of cooperating with China. It's not a coincidence that there's been bipartisan support for that type of policy for decades -- from Nixon and Ford to Carter to Reagan to Bush to Clinton to Bush to Obama. There have been differences of emphasis and differences on issues, but on the core premise that the United States of America benefits from engagement with China, I think that's clearly supported by bipartisan administrations.

What I would say is China needs to be mindful that its activities don't undermine its standing here in the United States. Congress has a very important role to play in U.S.-China policy. The stakeholders who supported the U.S.-China policy -- significantly our business community -- have an important role to play.

And so part of our message is, look, if you are not taking steps to address some of these concerns as it relates to particular trade irritants or cyber activities, you risk

eroding the support for the U.S.-China relationship that comes from the business community; you risk inviting responses from Congress.

So China does need to be mindful of the broad concerns in the United States on certain issues. And so I think that's an entirely valid point that, again, across the political spectrum, people are concerned about certain Chinese activities, and that is going to reflect itself not just in what this President does and the next President does, but in what Congress does and how different stakeholders in the United States see the relationship.

And the same is true around the world and in the region. The more China is invested in a rules-based international order, I think the more support the Chinese will find for their objectives in Asia and around the world. The more China is testing or going beyond the boundaries of that rules-based international order, I think the more countries are going to raise concerns.
And so that's very much the nature of the discussion, but I don't think people should discount the fact that engagement has yielded very concrete results, including an administration -- when you look at our signature initiatives -- be it the Iran nuclear deal or climate change -- China's cooperation was fundamental to that progress, as well.

MS. ATKINSON: Just then, to add, that in terms of the global economy, China is the second-largest economy, and what it does matters a lot for the rest of the world. And I think the way we see it is that this rules-based international order, which we have in the economic sphere as well, supported China's rise. And that was remarkable, but it's now time for China to embrace the responsibility that's commensurate with its size.
China can't be a free-rider on the international system. China needs to help to sustain the rules that enabled its rise and that will support a stronger and more stable global economy.
[...]

Q I kind of have to repeat the first question. Can you speak to reports that appeared in the New York Times this weekend stating that the United States and China are pursuing what's called the cyber arms control agreement? Basically relinquish the use of certain cyber-offensive capabilities against each other's critical infrastructure during peacetime.

MR. RHODES: Sure. What I'd say is we've had a number of very focused discussions with the Chinese, including on the recent trip from the Chinese minister. We believe very strongly that the U.S. and China both have an interest in investing in clear international norms as it relates to cyber activity. We're working together to try to arrive at common principles that could give us greater confidence that China is

acting in a manner that does not disadvantage our businesses, and that upholds and invests in those evolving international norms.

I don't want to suggest that we reached an arms control agreement here, but I do want to suggest that ultimately the goal here is we start from a common understanding that you have agreed-upon principles which we believe must include that cyber theft does not go forward. And then as the two largest economies in the world, I think we can lead an effort to develop international norms that govern cyber activity. And that is going to be something that is of interest to the United States and China and the whole world, and is an example of where we need to address bilateral differences but we can also, frankly, set a global framework that can deal with cyber issues going forward.

MR. KRITENBRINK: I think that's absolutely right. I would just say, as we've I think explained earlier in this call, the issue of cyber and particularly of the concerns that we have with various Chinese behaviors in the cyber realm will be a key focus of the discussions. I'd be reluctant to raise expectations about an agreement along the lines of what you've described. But certainly that would be, as Ben said, a long-term goal of working towards establishing those norms. But I think we're a long ways from getting there, but that certainly is the goal.

MR. RHODES: Great. Thanks, everybody, for joining the call.

Échantillon 7.

Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference

PRESIDENT OBAMA: Good afternoon, everybody. Please have a seat.
I want to once again welcome President Xi back to the White House. We first hosted him here three years ago when he was Vice President. So this is our sixth meeting. As a result of our efforts, our two nations are working together more closely across a broader range of critical issues -- and our cooperation is delivering results, for both our nations and the world.

Since I took office, American exports to China have nearly doubled and now support nearly one million American jobs. Chinese investment in the United States helps support jobs across our country. We partner to address global challenges, whether it's promoting nuclear security, combating piracy off the Horn of Africa, encouraging development and reconciliation in Afghanistan, and helping to end the Ebola epidemic in West Africa.

The historic climate change announcements that we made last year in Beijing have encouraged other countries to step up, as well, increasing the prospects for a stronger global agreement this year. And as a member of the P5+1, China was critical to both the sanctions regime that brought Iran to the negotiating table and to the talks that produced the comprehensive deal to prevent Iran from obtaining a nuclear weapon. So, greater prosperity and greater security -- that's what American and Chinese cooperation can deliver. That's why I want to say again, the United States welcomes the rise of a China that is peaceful, stable, prosperous, and a responsible player in global affairs. And I'm committed to expanding our cooperation, even as we address disagreements candidly and constructively. That's what President Xi and I have done on this visit -- during our working dinner last night and our meeting today.

Let me mention some specifics. First, with respect to our economic relationship, we agreed to step up our work toward a high-standard bilateral investment treaty that would help level the playing field for American companies. We've committed ourselves to a set of principles for trade in information technologies, including protection of innovation and intellectual property. President Xi discussed his commitment to accelerate market reforms, avoid devaluing China's currency, and have China play a greater role in upholding the rules-based system that underpins the global economy -- all of which are steps we very much support.

I raised once again our very serious concerns about growing cyber-threats to American companies and American citizens. I indicated that it has to stop. The United States government does not engage in cyber economic espionage for commercial gain. And today, I can announce that our two countries have reached a common understanding on the way forward. We've agreed that neither the U.S. or the Chinese government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage. In addition, we'll work together, and with other nations, to promote international rules of the road for appropriate conduct in cyberspace.

So this is progress. But I have to insist that our work is not yet done. I believe we can expand our cooperation in this area, even as the United States will continue to use all of the tools at our disposal to protect American companies, citizens and interests.

[...]

So, overall, we've had an extremely productive meeting. The particular work that has been done by our teams shows the extraordinary progress that we can make when we're working together. The candid conversations between President Xi and myself about areas of disagreement help us to understand each other better, to avoid

misunderstandings or miscalculations, and pave the way potentially for further progress in those areas.

And, President Xi, I want to thank you again for expanding your commitment to cooperation between our nations. I believe that it's another reminder that as we work to narrow our differences, we can continue to advance our mutual interests for the benefit not only of our two peoples, but for the benefit of the world.

Thank you very much.

PRESIDENT XI: (As interpreted.) President Obama, dear friends from the press, ladies and gentlemen, dear friends -- good morning. It's a great pleasure for me to meet with all of you together with President Obama. Let me begin by thanking again President Obama and the U.S. government for the gracious hospitality and thoughtful arrangements and warm reception accorded to me and the Chinese delegation. I also want to thank the American people for a warm welcome.

Yesterday and today, President Obama and I have had in-depth discussions on our respective domestic and foreign policies, important topics in bilateral relations, international and regional situation. Our meetings are constructive and productive, and we have reached extensive and important consensus.

During the discussions, President Obama shared with me the domestic agenda and foreign policy priorities that he has been working on. And I congratulated him on the progress that he has made in those areas. I appreciate President Obama's reaffirmation to me that the United States welcomes the rise of a peaceful, stable and prosperous China. It supports China to play a bigger role in the international arena. And the United States supports China's reform at opening up.

I indicated to President Obama that China is making all-around efforts to deepen comprehensive reform, to build law-based governance, to enforce strict party discipline, so as to achieve the grand goal of building a society of initial prosperity in all respects. The reform at opening up China will not stop.

China is firmly committed to the path of peaceful development. It is committed to growing friendship and cooperative relations with all countries in the world. To work with the United States to build the new model of major-country relationship without conflict, without confrontation, with mutual respect and win-win cooperation is a priority in China's foreign policy. We have spoken highly of the important progress made in China-U.S. relations since the Sunnylands summit in 2013. And we have agreed to follow the consensus, expand the practical cooperation in various areas at

the bilateral, regional, and global level, and manage differences and sensitive issues in constructive manner, and to advance the new model of major-country relationship between China and the United States.

We have agreed to deepen the practical cooperation in various areas at the bilateral scope. We have agreed to vigorously push forward the bilateral investment treaty negotiation, speed up the pace of the work so as to achieve a high standard and balanced agreement.

We will expand mutually beneficial cooperation in energy, environmental protection, science and technology, aviation, infrastructure, agriculture, health and other areas. The two governments and relevant agencies have signed many cooperation agreements, and our businesses have signed a series of commercial contact.

China and the United States are highly complementary economically and there is huge potential for further cooperation. For the United States to recognize China's market economy status and ease export control on civilian high-tech items, it will help expand the mutually beneficial cooperation between the two countries.

[...]

China and the United States are two major cyber countries and we should strengthen dialogue and cooperation. Confrontation and friction are not made by choice for both sides. During my visit, competent authorities of both countries have reached important consensus on joint fight against cyber-crimes. Both sides agree to step up crime cases, investigation assistance and information-sharing. And both government will not be engaged in or knowingly support online theft of intellectual properties. And we will explore the formulation of appropriate state, behavior and norms of the cyberspace. And we will establish a high-level joint dialogue mechanism on the fight against cyber-crimes and related issues, and to establish hotline links.

[...]

Mr. President, with 36 years of development, the interests of China and the United States are deeply interconnected, and we have greater responsibilities for world peace and human progress. There are broad areas that the two sides should and can work together. The Chinese side stands ready to work with the United States to uphold a spirit of perseverance, and advance bilateral relations to seek further progress to the better benefits of the Chinese and American people and the people in the world.

Thank you. (Applause.)

PRESIDENT OBAMA: Okay, we're going to take a few questions. We're going to start with Margaret Talev of Bloomberg.

Q Thank you, Mr. President. President Obama and President Xi, I'd like to talk to you about cyber. If I am an American business and I'm being hacked by Chinese pirates who are trying to steal my intellectual property, what firm assurances can you give us today that things are going to get better, and when? President Obama, are you satisfied enough about the steps that China is taking to hold off on imposing any new sanctions to this end? Or what do you still need to see? And, President Xi, could we expect prosecutions of Chinese people and organizations who have hacked American businesses? And if the U.S. did sanction anyone in China, would you respond with sanctions? Also, everyone will kill me if I don't ask -- what is your reaction to House Speaker John Boehner's decision to resign? (Laughter.) Will this make life better or worse for you? Are you concerned it will make it more difficult to avoid a government shutdown or raise the debt limit? And do you think Boehner could just waive the rules and get immigration reform through before he leaves? Thank you.

PRESIDENT OBAMA: I'll take them in order. With respect to cyber, this has been a serious discussion between myself and President Xi since we first met in Sunnylands. And the good news, from my perspective, is, is that in the lead-up to and then finalized during our meetings here today, we have, I think, made significant progress in agreeing to how our law enforcement and investigators are going to work together, how we're going to exchange information, how we are going to go after individuals or entities who are engaging in cyber-crimes or cyber-attacks. And we have jointly affirmed the principle that governments don't engage in cyber-espionage for commercial gain against companies. That all I consider to be progress.

What I've said to President Xi and what I say to the American people is the question now is, are words followed by actions. And we will be watching carefully to make an assessment as to whether progress has been made in this area. With respect to the various tools that we have to go after those who are attacking our companies or trying to extract trade secrets or data, we have traditional law enforcement tools, but -- as I indicated a while back -- through executive action, I've also instituted the ability to impose sanctions on individuals or entities where we have proof that they've gone after U.S. companies or U.S. persons.

And we did not, at our level, have specific discussions of specific cases. But I did indicate to President Xi that we will apply those and whatever other tools we have in our toolkit to go after cyber criminals, either retrospectively or prospectively. Those are tools generally that are not directed at governments; they are directed at entities or individuals that we can identify. And they're not unique to China. Those are tools that we're going to be using for cyber criminals around the world.

And President Xi, during these discussions, indicated to me that, with 1.3 billion people, he can't guarantee the behavior of every single person on Chinese soil -- which I completely understand. I can't guarantee the actions of every single American. What I can guarantee, though, and what I'm hoping President Xi will show me, is that we are not sponsoring these activities, and that when it comes to our attention that non-governmental entities or individuals are engaging in this stuff, that we take it seriously and we're cooperating to enforce the law.

The last point I'll make on the cyber issue -- because this is a global problem, and because, unlike some of the other areas of international cooperation, the rules in this area are not well developed, I think it's going to very important for the United States and China, working with other nations and the United Nations and other -- and the private sector, to start developing an architecture to govern behavior in cyberspace that is enforceable and clear.

It doesn't mean that we're going it prevent every cyber-crime, but it does start to serve as a template whereby countries know what the rules are, they're held accountable, and we're able to jointly go after non-state actors in this area.

[...]

PRESIDENT XI: (As interpreted.) Madam reporter has raised the cybersecurity issue. Indeed, at current, for the international community and for China and the United States, this is an issue all attach great importance to. With President Obama and I have on many occasions -- and this is a long history -- have exchange of views on this. I think it's fair to say we've reached a lot of consensus on cybersecurity, including some new consensus.

Overall, the United States is the strongest country in terms of cyber strength. China is the world's biggest cyber country in terms of the number of Web users. We have more than 600 million of netizens. Our two sides should cooperate because cooperation will benefit both, and confrontation will lead to losses on both sides. We are entirely able to carry out government department and expert levels of dialogue and exchanges to strengthen our cooperation in many respects and turn the cybersecurity between the two countries into a new growth source, rather than a point of confrontation between the two sides.

China strongly opposes and combats the theft of commercial secrets and other kinds of hacking attacks. The U.S. side, if has concerns in this respect, we can, through the exiting channels, express those concerns. The Chinese side will take seriously the U.S. provision of any information. Now, we have already, and in the future, we will still, through the law enforcement authorities, maintain communication and coordination on this matter, and appropriately address them.

So, all in all, we have broad, common interest in the field of the cyber. But we need to strengthen cooperation and avoid leading to confrontation. And nor should we

politicize this issue. During my current visit, I think it's fair to say that the two sides, concerning combatting cyber-crimes, have reached a lot of consensus. Going forward, we need to, at an early date, reach further agreement on them and further put them on the ground.

Thank you.

[...]

Échantillon 8.

FACT SHEET: President Xi Jinping's State Visit to the United States

On September 24-25, 2015, President Barack Obama hosted President Xi Jinping of China for a State visit. The two heads of state exchanged views on a range of global, regional, and bilateral subjects. President Obama and President Xi agreed to work together to constructively manage our differences and decided to expand and deepen cooperation in the following areas:

[...]

Cybersecurity : The United States and China agree that timely responses should be provided to requests for information and assistance concerning malicious cyber activities. Further, both sides agree to cooperate, in a manner consistent with their respective national laws and relevant international obligations, with requests to investigate cybercrimes, collect electronic evidence, and mitigate malicious cyber activity emanating from their territory. Both sides also agree to provide updates on the status and results of those investigation to the other side, as appropriate.

The United States and China agree that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.

Both sides are committed to making common effort to further identify and promote appropriate norms of state behavior in cyberspace within the international community. The United States and China welcome the July 2015 report of the UN Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International security, which addresses norms of behavior and other crucial issues for international security in cyberspace. The two sides also agree to create a senior experts group for further discussions on this topic.

The United States and China agree to establish a high-level joint dialogue mechanism on fighting cybercrime and related issues. China will designate an official at the ministerial level to be the lead and the Ministry of Public Security, Ministry of State Security, Ministry of Justice, and the State Internet and Information Office will participate in the dialogue. The U.S. Secretary of Homeland Security and the U.S. Attorney General will co-chair the dialogue, with participation from representatives from the Federal Bureau of Investigation, the U.S. Intelligence Community and other agencies, for the United States. This mechanism will be used to review the timeliness and quality of responses to requests for information and assistance with respect to malicious cyber activity of concern identified by either side. As part of this mechanism, both sides agree to establish a hotline for the escalation of issues that may arise in the course of responding to such requests. Finally, both sides agree that the first meeting of this dialogue will be held by the end of 2015, and will occur twice per year thereafter.

[...]

Échantillon 9.

XI Jinping. (2012, 16 décembre). De l'édification de la défense nationale et de l'armée. Propos tenus lors de la réunion élargie de la Commission militaire centrale. 16 décembre 2012.

Les membres de la Commission militaire centrale et les officiers de haut rang assument des responsabilités historiques importantes dans la direction de l'édification de la défense nationale et de l'armée. Nous devons à tout moment garder la tête froide, chérir les accomplissements des officiers et soldats des générations précédentes, mettre à profit les expériences précieuses accumulées au cours de l'histoire, et apprécier à leur juste valeur, les progrès accomplis dans l'édification de notre armée. Nous avons le devoir de nous dévouer corps et âme au Parti et au peuple, et de mener à bien l'édification de la défense nationale et de l'armée.

L'étude et l'application de l'esprit du XVIIIe Congrès du Parti doivent être considérées comme primordiales dans l'accomplissement de la tâche politique. Les divers échelons doivent suivre les dispositions prises par le Comité central du Parti et la Commission militaire centrale, pour mettre en place sans délai une campagne vouée à cette activité au sein de l'armée toute entière. Il faut étudier et appliquer de manière approfondie le concept de développement scientifique, ainsi que les pensées du Parti concernant l'édification de la défense nationale et de l'armée dans le contexte

actuel. Le concept de développement scientifique doit servir de principe directeur dans cette édification et ses particularités et ses règles doivent être parfaitement intégrées. Il faut faire le bilan des expériences précieuses de l'édification de la défense nationale et de l'armée par le président Hu Jintao, et s'assurer de l'application des principes et des mesures stratégiques qui furent déterminés sous sa direction.

La direction absolue de l'armée par le Parti ne saurait en aucun cas être remise en cause. Celle-ci garantit la nature et l'objectif de l'armée chinoise, le destin du socialisme, ainsi que la stabilité du Parti et de l'État sur le long terme. Elle est le fondement de l'existence et du développement de notre armée.

...

La Chine doit être capable d'accomplir militairement toute mission qu'elle se sera fixée. L'ensemble des forces armées doit réaliser clairement l'importance de son rôle dans le contexte plus large de sécurité nationale et de stratégie de développement. La souveraineté et la sécurité nationale doivent passer avant toute autre considération. Pour cela, l'armée doit insister sur l'importance primordiale de sa préparation au combat, augmenter de manière générale nos capacités en termes de dissuasion et de combat cybernétiques, et protéger les intérêts d'État en matière de souveraineté, de sécurité et de développement. L'armée toute entière doit accorder une importance stratégique aux exercices militaires, permettant d'augmenter continuellement ses capacités en situation de combat réel.

En conformité au principe de développement global chinois, nous devons œuvrer à renforcer l'esprit révolutionnaire de notre armée, et à la rendre plus moderne et plus standardisée. Il nous faut adopter une vision d'ensemble sur les tâches à accomplir dans les domaines politique, militaire, logistique et matériel, afin de mettre à niveau l'ensemble des capacités de nos forces armées. Le nouveau principe stratégique de défense active doit être appliqué de manière effective. L'innovation stratégique doit être encouragée et le rôle directeur de la stratégie militaire dans l'édification et les activités de l'armée, mis en valeur.

...

Nous soutiendrons cette évolution de manière rationnelle et feront tout pour accélérer la transformation du mode de développement de l'aptitude au combat. Nous approfondirons la réforme militaire, afin de construire un système moderne de forces armées aux caractéristiques chinoises.

...

Nous devons moderniser encore la défense nationale et nos forces armées.

...

Avec la direction déterminée du Comité central du Parti et de la Commission militaire centrale, associée au soutien énergique du peuple et aux efforts conjoints de l'armée toute entière, nous atteindrons cet objectif glorieux de modernisation de la défense nationale et des armées.

Échantillon 10.

Full text from President Xi Jinping's speech at the National Committee on U.S.-China Special Dinner for President Xi Jinping and Madame Peng Liyuan

Dr. Henry Kissinger; Gov. Jay Inslee of the state of Washington; Secretary of Commerce Penny Pritzker; Mayor Ed Murray of Seattle; Chairwoman Carla Hills of the National Committee on U.S.-China Relations; Chairman Mark Fields of the U.S.-China Business Council; ladies and gentlemen, good evening.

Thank you Dr. Kissinger for your kind introduction. Dr. Kissinger has always been able to come up with some new observations. His introduction has really given me a new perspective to look at myself.
It is great to be among so many friends, old and new in a state of Washington, and the City of Seattle, the first leg of my state visit to the United States. Let me begin by extending to you, and through you, to all the American people, my cordial greetings and best wishes.
I am no stranger to the state of Washington and the City of Seattle. Known as the Evergreen state, and the Emerald City, here you have got the majestic Mount Rainier and the charming Lake Washington. The film Sleepless in Seattle has made the city almost a household name in China. Besides, Washington is the leading state in U.S. exports to China and China is the No. 1 trading partner of the Port of Seattle. Washington and Seattle have become an important symbol of the friendship between Chinese and American people and the win-win cooperation between the two countries. As the Chinese saying goes, the fire burns high when everyone brings wood to it. It is the love and care and hard work of the national governments, local authorities, friendly organizations, and people from all walks of life in those countries that have made China-U.S. relations flourish. In particular, the national committee on U.S-China Relations, the U.S.-China Business Council, the U.S.-China Policy Foundation, the U.S. Chamber of Commerce, The China General Chamber of Commerce USA, the Committee of 100, the China Institute, the Council of Foreign Relations, the Asia Society, The Brookings Institution, and many other friendly groups and individuals that have made a tiring effort over the years to promote

friendly relations and cooperation between the two countries and brought this relationship to this far.

Let me pay high tribute and express my heartfelt gratitude to all the local governments, social organizations, universities, think-tanks, and people from all sectors of society who have dedicated themselves to the cause of China-U.S. friendship.

Ladies and gentlemen, dear friends. Since the founding of the People's Republic, especially since the beginning of reform and opening up, China has set out on an extraordinary journey. The Chinese of my generation have had some first-hand experience. Toward the end of the 1960s, when I was in my teens, I was sent from Beijing to work as a peasant in a small village, where I spent seven years. At that time, the villagers and I lived in earth caves and slept on earth beds. Life was very hard. There was no meat in our diet for months. I knew what the villagers wanted the most. Later, I became the village's party secretary and began to lead the villagers in production. One thing I wished most at the time was to make it possible for the villagers to eat meat to their heart's content. But it was very difficult for such a wish to come true in those years.

At the spring festival earlier this year, I returned to the village. It was a different place now. I saw black top roads. Now living in houses with bricks and tiles, the villagers had Internet access. Elderly folks had basic old-age care, and all villagers had medical care coverage. Children were in school. Of course, meat was readily available. This made me kindly aware that the Chinese dream is, after all, a dream of the people. We can fulfill the Chinese dream only when we link it with our people's yearning for a better life.

What has happened in [my village] is but a microcosm of the progress China has made through reform and opening up. In a little more than three decades, we have turned China into the world's second-largest economy, lifted 1.3 billion people from a life of chronic shortage, and brought them initial prosperity and unprecedented rights and dignity.

This is not only a great change in the lives of the Chinese people, but also a huge step forward in human civilization, and China's major contribution to world peace and development.

At the same time, we are civilly-aware that China is still the world's largest developing country. Our per capita GDP is only two-thirds that of global average and one-seventh that of the United States, ranking around 80th in the world. By China's own standard, we still have over 70 million people living under the poverty line. If measured by world bank standard, the number would be more than 200 million. Over 70 million citizens live on basic living allowances and the number of people with disabilities exceeds 85 million. During the past two years, I have been to many poor areas in China and visited many poor families. I wouldn't forget the look in their eyes longing for distant, happy life.

I know that we must work still harder before all our people can live a better life. That explains why development remains China's top priority. To anyone charged with the

governance of China, their primary mission is to focus all the resources on improving people's living standard and gradually achieve common prosperity. To this end, we have proposed the two centenary goals mentioned by Dr. Kissinger, namely to double the 2010 GDP and per capita income of the Chinese and complete the building of a moderately prosperous society by 2020 and to build a prosperous, strong, democratic ... harmonious, modernist socialist country that realizes the great renew of the Chinese nation by the middle of the century.

Whatever we do now is aimed at fulfilling these goals. To succeed in completing the building of a moderately prosperous society in all respects, we must comprehensively deepen reform, advance the law-based governance, and apply strict ... discipline. That is what our proposed 4-pronged strategy is all about.

Since you are all interested in the direction of China's development and foreign policy orientation, let me take this opportunity to share with you some of my thoughts in this regard. China's economy will stay on a steady course with fairly fast growth. The Chinese economy is still operating within a proper range. It grew by 7 percent in the first half of this year, and this growth rate remains one of highest in world. It has not come by easily, given the complex and volatile situation in world economy. At present, all economies are facing difficulties, and our economy is also under downward pressure. But this is only a problem in the course of progress. It will take ... steps to achieve stable growth, deepen reform, adjust structure, improve livelihood, and prevent risks while strengthening and innovating macro-regulation to keep the growth at medium-to-high rate.

Currently, China is continuing to move forward in this new type of industrialization, digitalization, urbanization, and agricultural modernization. With a high savings rate, a huge consumption potential, a hard working population, and a rising proportion of middle income people — now we have 300 million middle income earnings in China — China enjoys enormous space ... to grow in terms of market size and potential. China will focus more on improving the quality and efficiency of economic growth, and accelerating the shift of growth model and adjustment in economic structure. I will lay greater emphasis on innovation and consumption-driven growth — in this way, we will solve the problem of unbalanced, uncoordinated, and unsustainable development, and enable the Chinese economy to successfully transform itself and maintain strong momentum of growth.

Recent abnormal ups and downs in China's stock market has caused wide concern. Stock prices fluctuating accordance with your inherent laws and it is the duty of the government to ensure an open, fair, and just market order and prevent massive panic from happening. This time, the Chinese government took steps to stabilize the market and contain panic in the stock market, and thus avoided the systemic risk. Mature markets in various countries have tried similar approaches. Now, China's stock market has reached the phase of self-recovery, and self-adjustment. On the 11th of August, China moved to improve its RMB central parity quotation mechanism, giving the market a greater role in determining the exchange rates. Our efforts have achieved initial success in correcting the exchange rate deviation. Given the

economic and financial situation at home and abroad, there is no basis for continuous depreciation of the RMB. We will stick to the purpose of our reform to have the exchange rate decided by market supply and demand and allow the RMB to float both ways. We are against competitive depreciation or a currency war. We will not lower the RMB exchange rate to boost export. To develop the capital market and improve the market-based pricing of the RMB exchange, is the direction of our reform. This will not be changed by the recent fluctuation in the stock market.

The key to China's development lies in reform. Our reform is aimed at modernizing the country's governance system, and governance capabilities so that the market can play a decisive role in the allocation of resources. The government can play a better role and there is faster progress in building the socialist market economy, democracy, advanced culture, harmonious society, and soundly environment.

At the third of the 18th party central committee in 2013, we decided on an over-arching plan for deepening reform featuring over 330 measures. In 2014, 18 major reform items were by-and-large completed. In the first half of this year, we rolled out 70 key reform programs with their effects gradually becoming evident. When it comes to the toughest reforms, only those with courage will carry the day. We have the results and guts to press ahead, and take reform forward. We will stick to the direction of market economy reform and continue to introduce bold and result-oriented reform measures concerning the market, taxation, finance, investment and financing, pricing, opening up, and people's livelihood.

China will never close its open door to the outside world. Opening up is a basic state policy of China. Its policies that attract foreign investment will not change, nor will its pledge to protect legitimate rights and interests of foreign investors in China, and to improve its services for foreign companies operating in China. We respect the international business norms and practice of non-discrimination, observe the ... principle of national treatment commitment, treat all market players — including foreign-invested companies — fairly, and encourage transnational corporations to engage in all forms of cooperation with Chinese companies. We will address legitimate concerns of foreign investors in timely fashion, protect their lawful rights and interests, and work hard to provide an open and transparent legal and policy environment, an efficient administrative environment, and a level playing field in the market, with a special focus on IPR protection so as to broaden the space of cooperation between China and the United States and other countries.

China will follow the basic strategy of the rule of law in governance. Law is the very foundation of governance. We will coordinate our efforts to promote the rule of law in governance and administration, for the building of the country, the government and society on solid basis of the rule of law, build greater trust in judicial system, and ensure that human rights are respected and effectively upheld. China will give fair treatment to foreign institutions and foreign companies in the country's legislative, executive, and judicial practices. We are ready to discuss rule of law issues with the U.S. side in the spirit of mutual learning for common progress.

China is a staunch defender of cybersecurity. It is also a victim of hacking. The Chinese government will not, in whatever form, engage in commercial thefts or encourage or support such attempts by anyone. Both commercial cyber theft and hacking against government networks are crimes that must be punished in accordance with law and relevant international treaties. The international community should, on the basis of mutual respect and mutual trust, work together to build a peaceful, secure, open, and cooperative cyberspace. China is ready to set up a high-level joint dialogue mechanism with United States on fighting cyber crimes.

China recognizes the positive role played by foreign non-profit organizations. So long as their activities are beneficial to the Chinese people, we will not restrict or prohibit their operations, but will protect their operations through legislation and protect their legitimate rights and interests. On their part, foreign NPO's in China need to obey Chinese law and carry out activities in accordance with law.

China will continuing fighting corruption. As I once said, one has to be very strong if he wants to strike the iron. The blacksmith referred to here is the Chinese communist party. The fundamental aim of the party is to serve the people's heart and soul. The party now has over 87 million members and unavoidably, it has problems of one kind or another. If we let these problems go unchecked we will risk losing the trust and support of the people. That is why we demand strict enforcement of party discipline as the top priority of governance. In our vigorous campaign against corruption, we have punished both tigers and flies — corrupt official — irrespective of ranking, in response to our people's demand. This has nothing to do with power struggle. In this case, there is no House of Cards.

China is ready to cooperate closely with the international community in fighting corruption and tracking down fugitives. The Chinese people look to the U.S. for support and coordination so that corrupt elements will be denied — an overseas safe haven.

China will keep to the path of peaceful development. We have just celebrated the 70th anniversary of the victory of the Chinese people's resistance against Japanese aggression and the world anti-fascist war. An important lesson history teaches us is that peaceful development is the right path, while any attempt to seek domination or hegemony through force is against the historical trend and doomed to failure. The Chinese recognized as early as 2,000 years ago that though a country is now strong, varicosity will lead to its ruling. China's defense policy is defensive in nature and its military strategy features active defense. Let me reiterate here that no matter how developed it could become, China will never seek hegemony or engage in expansion.

To demonstrate our commitment to peaceful development, I announced not long ago that the size of China's military will be cut by 300,000. China is ready to work with other countries to build a new type of international relations with win-win cooperation at its core, replacing confrontation and domination with win-win cooperation and adopting a new thinking of building partnerships so as to jointly open a new vista of common development and shared security.

As far as the existing international system is concerned, China has been a participant, builder, and contributor. We stand firmly for the international order and system that is based on the purposes and principles of the UN charter.

A great number of countries, especially developing countries, want to see a more just and equitable international system. But it doesn't mean that they want to unravel the entire system or start all over again. Rather, what they want is reform and to improve the system to keep up with the times. This should serve the common interest of all countries and mankind as a whole.

China has benefitted from the international community and development, and China has in turn made its contribution to global development. Our Belt and Road initiative, our establishment of the Silk Road fund, and our proposal to set up the AAIB, are all aimed at helping the common development of all countries, rather than seeking some kind of spheres of political influence. The Belt and Road initiative is open and inclusive; we welcome participation of the U.S. and other countries, and international organizations.

We have vigorously promoted economic integration in the Asia Pacific and the Free Trade area of the Asia Pacific in particular because we want to facilitate the shaping of a free, open, convenient, and dynamic space for development in the Asia Pacific. We ... for an outlook of common, comprehensive, cooperative, and sustainable security because we want to work with other countries in the region and the rest of the international community to maintain peace and security in the Asia Pacific.

Ladies and gentlemen, dear friends. In our Sunnylands meeting in 2013, President Obama and I reached the important agreement to jointly build a new model of major country relationship between the two countries. This was a major strategic choice we made together on the basis of historical experience, our respective national conditions and the prevailing trend of world. Over past two years and more, the two sides have acted in accordance, with the agreement steadily moving forward by actual coordination and cooperation in various fields, and made important progress. We worked hand-in-hand to cope with aftermath of international financial crisis and promoted global economic recovery. We deepened pragmatic exchanges and cooperation in all fields, which brought about tangible benefits to the two people's. Last year, actual trade, two-way invesment stock, and total number of personnel exchanges all hit a record high.

We maintain close communication and coordination on such international and regional issues, as the Iranian nuclear issue, the Korean nuclear issue, south of Sudan, Afghanistan and the Middle East, as well as such global issues as fighting against Ebola and countering terrorism.

As an old Chinese saying goes, peaches and plums do not talk, yet a path is formed beneath them. These worthy fruits of cooperation across the Pacific Ocean speaks eloquently to the vitality and potential of China-U.S. relations.

This leads to the question: What shall we do to advance the new model of major country relationship between China and the U.S. from a new starting point and how we can work together to promote world peace and development. The answer is to

stick to the right direction of such a new model of relationship and make gradual, solid progress.

An ancient Chinese said, after taking into account the past, the future, and the normal practices, a decision can be made.

A number of things are particularly important for our efforts. First, we must read each other's strategic intentions correctly. Building a new model of major country relationship with the United States that features no confrontation, no conflicts, mutual respect and willing cooperation is the priority of China's foreign policy. We want to deepen mutual understanding with the U.S. on each other's strategic orientation and development path. We want to see more understanding and trust; less estrangement and suspicion in order to ... misunderstanding and miscalculation.

We should strictly base our judgement on facts, lest we become victim to hearsay, paranoid, or self-imposed bias. ... Should major countries time and again make the mistakes of strategic miscalculation, they might create such traps for themselves.

Second, we must firmly advance win-win cooperation. Cooperation is the only right choice to bring about benefits, but cooperation requires mutual accommodation of each other's interest and concerns, and the quest of the great common ground of converging interest. If China and the U.S. cooperate well, they can become a bedrock of global stability and a booster of world peace. Should they enter into conflict or confrontation, it would lead to disaster for both countries and the world at large. The areas where we should and can cooperate are very broad. For instance, we should help improve the global governance mechanism and work together to promote sustained growth of world economy and maintain stability in the global financial market.

We should conclude as soon as possible a balanced and high quality BIT, deepen the building of a new type of mill-to-mill relations, expand pragmatic cooperation on clean energy and environmental protection, strengthen exchanges in law enforcement, anti-corruption, health, and local affairs, and tap the corporation potential in infrastructural development. We should deepen communication and cooperation at the United Nations A-PEC, G-20, and other multi-electoral mechanisms, as well as our major international and regional issues and global challenges so as to make a bigger contribution to world peace, stability, and prosperity.

Third, we must manage our differences properly and effectively. As a Chinese saying goes, the sun and moon shine in different ways yet their brightness is just right for the day and night, respectively. It is precisely because of so many differences that the world has become such a diverse and colorful place, and that the need to broaden common ground and iron out differences has become so important. A perfect, pure world is non-existent, since disagreements are a reality people have to live with. China and the U.S. do not see eye-to-eye on every issue and it is unavoidable that we may have different positions on some issues. What matters is how to manage the differences and what matters most is that we should respect each other, seek common ground while reserving differences, take a constructive approach to understanding ... and spare no effort to turn differences into areas of cooperation.

Fourth, we must foster friendly sentiments among the peoples. People-to-people relations underpin state-to-state relations. Though geographically far apart, our peoples boast a long history of friendly exchanges. Some 230 years ago, Empress of China, a U.S. merchant ship, sailed across the vast oceans to the shores of China. Some 150 years ago, tens of thousands of Chinese workers joined their American counterparts in building the Transcontinental Pacific Railway. Some 30 years ago, China and the United States, as allies in World War II, fought shoulder-to-shoulder to defend world peace and justice. In that war, thousands of American soldiers laid down their precious lives for the just cause of the Chinese people.

We will never forget the moral support and invaluable assistance the American people gave to our just resistance against aggression and our struggle for freedom and independence. The Chinese people have always held American entrepreneurship and creativity in high regards.

In my younger years, I read the Federalist Papers by Alexander Hamilton and Common Sense by Thomas Paine. I was interested in the life story and thinking of George Washington, Abraham Lincoln, Franklin Roosevelt, and other American statement. I also read works of Henry David Thoreau, Walt Whitman, Mark Twain, and Jack London. I was most captivated by Ernest Hemingway's The Old Man and Sea, and its descriptions of howling wind, driving rain, roaring waves, small boat, and the old man and sharks. So when I visited Cuba for the first time, I paid a special visit to ... where Hemingway wrote the book, and in my second visit of Cuba, I dropped by the bar Hemingway frequented, and ordered his favorite rum with mint on the rocks — mojito.

i just wanted to feel for myself what had been on his mind and the very place he was as wrote those stories. I believe it's always important to make an effort to get deep a understanding of the cultures and civilizations that are different from out own.

The Chinese character Ren, or people, is in a shape of two strokes supporting each other. The foundation of the China-U.S. friendship has its roots in the people and its future rests with the youth. I want to announce here that China supports the initiative of sending a total of 50,000 Chinese and American students to study in each others' countries over the next three years. China and the U.S. will launch a year of tourism in 2016. China on its part will create more favorable conditions for closer people-to-people exchanges.

Ladies and gentlemen. Dr. Kissinger wrote in his book, World Order, that, and I quote, each generation will be judged by whether the greatest and most consequential issues of the human condition have been faced. And Martin Luther King said, 'the time is always right to do the right thing. Today we have come once again to a historical juncture. Let us work together to bring about an even better future for China-U.S. relations and make an even greater contribution the happiness of our two people's and well-being of the world."

Échantillon 11.

President Xi Jinping delivers keynote speech at the Second World Internet Conference, 16 décembre 2015

Welcome to the beautiful town of Wuzhen for this important discussion on the development of the Internet in the world. First of all, on behalf of the Chinese government and people and in my own name, I wish to express a warm welcome to all participants to the second World Internet Conference and express warm congratulations on the opening of the conference. I have work in Zhejiang for many years and visited Wuzhen on several occasions with my colleagues, I have been here five or six times, I like this place very much. During the second phase of the city renovation I was here, helping with the plan and supporting the efforts of the local government to restore the ancient residences, buildings to develop tourism here.

Today, coming back to Wuzhen, I find the town both familiar and new, actually I haven't been here for quite a number of years and this place is new in many ways. The first World Internet Conference Held here last year gave a strong boost to the development of online maker, online hospital, smart tourism and other Internet applications and new Internet related industries. And this has add a new fascinating dimension to the charm of this historical town. An Internet empowered and smart town, Wuzhen is an example of what can be achieved by combining tradition with modernity and Internet and integrating culture with science. It showcases the innovative development of the Internet in China and reflects the principal that global Internet development is indeed shared by all.

Looking at the history of the World civilizations, humanity has progressed along with agricultural, industrial and information revolutions. Each of these industrial and technological revolutions has had great and profound impact on the way of production and life. Today information technologies represented by Internet are representing rapid changes with each passing day. They have brought about new ways of social production, created new space for people's life, opened new horizons of state governors and enhanced our ability to understand and shape the world. Such abilities have been tremendously enhanced. The Internet has turned the world into a global village where distance no longer prevents people from interacting with each other. And communication is made easier than ever before. Indeed, thanks to the Internet, our world has become more colorful and people now live a fuller life.

China is going through a historic process of rapid application of information technologies. China attaches great importance to Internet development, since China was connected to the World Wide Web 21 years. We have incaping with the principles of proactive utilization, rational development, law based regulation and assurance of security, strengthened IT infrastructures, developed cyber economy and

made life better for our people through IT application. In the meantime we have conducted governance of cyberspace in accordance with law and ensured a clean environment for the cyberspace. Today, China is already home to 670 million Internet users and over 4.13 million websites. The Internet is now deeply integrated into China's economic and social development and the life of the Chinese people. The 5th plan of the 18th CPC central committee has put forward the concept of innovative coordinated green open and shared development. During the 13th plan period, China will vigorously implement the national cyber development strategy, the national Big Data strategy and the Internet plus action plan. We will develop an uplifting cyber culture, open more space for cyber economy, and promote the integration of Internet development with economic and social progress. Our goal is to ensure that more than 1.3 Billion Chinese people and people across of the world can all enjoy the benefits of Internet development.

Distinguished guests, dear friends, with the deepening of world multipolarity, economic globalization, cultural diversity and IT application, the Internet will only play a bigger role in the progress of human civilization. At the same time, however, such problems as unbalanced development, inadequate roles and inequitable order become more evident in the field of Internet. The information gap between different countries and regions is widening and the existing roles governing cyberspace partly reflect the desires and interests of the majority of countries. Infringement of individual privacy and intellectual property rights as well as cyber crimes happen from time to time around the world. Cyber surveillance, cyber attack and cyber terrorism have become a global scourge. In the face of these problems and challenges, the international community must enhanced dialogue and cooperation on the basis of mutual respect and trust, promote the transformation of the global Internet system and work together to foster a peaceful, secure, open and cooperative cyberspace. And put in place a multilateral democratic and transparent Internet governance system.

To make progress in the transformation of the global Internet governance system, the following principles must be upheld. One of the principles would be the respect of cyber sovereignty. The principle of sovereign equality enshrined in the charter of the United Nations is one of the basic norms in contemporary international relations. It covers all aspects of state-to-state relations, which also includes cyberspace. We should respect the right of individual countries to independently choose their own path of cyber development and model of cyber regulation and participate in international cyberspace governance on an equal footing. No country should pursue cyber hegemony, interfere in other countries internal affairs and engaged in or support cyber activities that undermine other countries national security and maintenance of peace and security. A secure stable and prosperous cyberspace is of great significance to all countries and the world. In the real world there are still lingering wars, shadows of terrorism and occurrences of crimes. Cyberspace should not become a battlefield for countries to wrestle with one another, still less should it

become a hot bath for crimes. Countries should work together to prevent and oppose the use of cyberspace for criminal activities such as terrorism, pornography, drug trafficking, money laundry and gambling. All cyber crimes, be they commercial cyber attacks or hacker attacks against government networks should be firmly combated in accordance with relevant laws and international conventions. No double standards should be allowed and upholding cyber security. We can not have just the security of one country while leaving the rest insecure, still less should one seek the so-called absolute security of itself at expanse of the security of others.

Promotion of openness and cooperation. As in old Chinese saying, when there is mutual care, the world will be in peace. When there is mutual hatred, the world will be in chaos. To improve the global Internet governance system and maintain the order of cyberspace we should firmly follow the concept of mutual support, mutual trust and mutual benefit and reject the old mentality of zero-sum game or winners taking all. All countries should advance opening up and cooperation in cyberspace and further substantiate and enhanced the opening up efforts. We should also built more platforms for communication and cooperation and create more convergent points of interests.

Growth areas for cooperation. A new highlinght for win-win outcome. Efforts should be made to advance complementarity of strenghts and common development of all countries in cyberspace, so that more countries and people will ride on the fast train of the information age and share the benefits of Internet development.

And another principle would be cultivation of good order. Like in the real world, freedom and order are both necessary in cyberspace. Freedom is what order is meant for, and order is the guarantee for freedom. We should respect Internet users rights to exchange their ideas and express their minds and we should also build a good order in cyberspace in accordance with law as it will help protect the legitimate rights and interests of all Internet users. Cyberspace is not a place beyond the rule of law. Cyberspace is virtual, but players in cyberspace are real. Everyone should abide by the law, with the rights and obligations of parties concerned clearly defined. Cyberspace must be governed, operated and used in accordance with law, so that the Internet can enjoyed sound development under the rule of law. In the meantime, greater efforts should be made to strengthen ethical standards and civilized behaviors in cyberspace. We should give full play to the rule of moral teachings and guiding the use of the Internet to make sure that the fine accomplishments of human civilizations will nourish the growth of cyberspace and help rehabilitate cyber ecology.

Distinguished guests, dear friends, cyberspace is the common space for activities of mankind. The future of cyberspace should be in the hands of all countries. Countries should step up communication, broaden consensus and deepen cooperation to jointly build a community of shared future in cyberspace. Recently, I have used this phrase ,

community of shared future, in quite a number of occasions. To this end, I would like to put forward five proposals. First, speed up the building of global cyber infrastructures and promote interconnectivity. The essence of the Internet is connectivity, and here lies in the value of information. We should strengthen the building of IT infrastructure for information to travel on a smooth road. Only in this way can we narrow the digital divide between different countries, regions and communities and ensure full flow of information resources. China is now implementing the broadbang China strategy. It is estimated that by 2020, broadband network in China will basically cover all the villages. The last kilometer of Internet infrastructure will be linked up thanks to this strategy and more people will have access to the Internet. China stands ready to work with all parties concerned to come up with more investments and technical support to jointly advance the building of a global cyber infrastructure and enable more developing countries and their people to share the development opportunities brought by the Internet. Second, build an online platform for cultural exchange and mutual learning. Cultures and civilizations are enriched through exchange and mutual learning and Internet is an important carrier to spread mankind fine cultures and promote positive energy. China is willing to build, through the Internet, a bridge of international intercultural interaction for fine cultures of the world to learn from each other and for people from all countries to share their feelings and enhanced mutual understanding.

We will work with all other countries to leverage the strength of Internet as a communication platform so that people of other countries will come to know more about China's fine culture and the Chinese people will learn more of theirs. Together, we will promote the prosperity and development of cyber culture, which will enrich people's mind and thinking and will enhance human civilization and progress. Third, promote innovative development of cyber economy for common prosperity. The world economy is on a difficult and tortuous path to recovery. The Chinese economy is also under a certain downward pressure. Solution lies in an innovation driven development, which will open new horizons of development.

China is now implementing the Internet Action Plan, advancing the building of digital China, developing the sharing economy and supporting Internet based innovation in all forms, with the view of improving the quality and efficiency of development. The openness of China's Internet has provided a big market for enterprises and business starters of al countries. China's door will never close. Our policy towards foreign investment will not change. Our protection of legitimate rights and interests of foreign invested enterprises will not change and the direction of providing better services to foreign companies and their investment, and business activity in China will not change. As long as they abide by China's law, we will warmly welcome enterprises and business starters from all countries to invest and do business in China. We are ready to step up cooperation with all countries through the development of cross-border e-comers and the building of information economy

demonstration zones we will be able to spur the growth of world wide investment and trade and promote global development of digital economy. Forth, maintain cyber security and promote orderly development. Security and development are like the two wings of a bird or the two wheels of a bicycle. Security ensures development and development is what security is aimed at. Cyber security is a global challenge and no country can stay aloof or immune from it. Maintaining cyber security is the shared responsibility of the international community. All countries should work together to contain the abuse of information technology, oppose cyber surveillance and cyber attacks and reject arms race in cyberspace.

China will work together with all other countries to step up dialogue and exchange and effectively manage defenses. We should push for the formulation of international cyberspace rules accepted by all parties as well as an international convention against terrorism in cyberspace and approve the legal assistance mechanism to fight cyber crimes and jointly uphold peace and security in cyberspace. Fifth, build an Internet governance system to promote equity and justice. International cyberspace governance should feature a multilateral approach with multiparty participation. It should be based on consultation among all parties, leveraging the role and various players including governments, international organizations, Internet companies, technology companies, non-governmental institutions and individual citizens.

There should be no unilateralism. Decisions should not be made with one party calling the shot or only a few parties discussing among themselves. All countries should step up communication and exchange, improve dialogue and consultation mechanisms on cyberspace and study and formulate global Internet governance rules so that the global Internet governance system becomes more fair and reasonable and reflects in a more balanced way the aspiration and interest of the majority of countries. This World Internet Conference is precisely for the purpose of building a platform to global Internet to be shared and governed by all and working together for the healthy development of the Internet.

Distinguished guests, dear friends, all good principles should adapt to changing times to remain relevant. While the Internet is invisible, Internet users are visible. The Internet is the common home of mankind. Making it better, healthier and safer is the common responsibility of the International community. Let us work hand in hand to promote an interconnected cyberspace shared and governed by all, and make contribution to a better future for the progress of all mankind. In conclusion, I wish the conference a complete success. Thank you.

Échantillon 12.

Foreign Ministry Spokesperson Hong Lei's Regular Press Conference on June 5, 2015

Q: First, the personal data of 4 million US federal employees was reportedly accessed by hackers. US government officials suspect that China is behind this attack. What is your comment?

A: On your first question, recently we have seen quite a lot of media reports or remarks of this kind. But are these reports or remarks scientific? Cyber attacks are usually conducted anonymously and across borders, making it hard to trace back. It is not responsible nor scientific to always use terms such as "likely" or "suspected" instead of conducting thorough investigations. It is the consistent position of China to firmly combat all forms of cyber attacks. China itself is a victim of cyber attacks. We are ready to carry out international cooperation on this issue and build a cyber space that is peaceful, secure, open and cooperative. We hope that the US side would discard suspicions, refrain from making groundless accusations, and show more trust and conduct more cooperation in this area.

Échantillon 13.

Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on July 10, 2015

Q: Recently there are allegations from Washington that Chinese hackers are responsible for security hackings into the US Office of Personnel Management. What is China's comment?

A: We have stated the Chinese government's principle and position on the issue of cyber security many times. All parties should adopt a constructive attitude on this issue. It is imperative to stop groundless accusations, step up consultations to formulate an international code of conduct in cyberspace and jointly safeguard peace, security, openness and cooperation of the cyber space through enhanced dialogue and cooperation in the spirit of mutual respect.

Échantillon 14.

Foreign Ministry Spokesperson Hua Chunying's Remarks on US Media Hyping Up Cyber Security Issue Related to China

Q: The US media has been playing up China-related cyber security issue in recent days. How do you think this will affect the China-US relations? How should the two countries properly address this issue?

A: The Chinese side has clarified its position on the cyber security issue on various occasions. The Chinese government staunchly upholds cyber security, firmly opposes and combats all forms of cyber attacks in accordance with law.

As shown in a report recently issued by relevant Chinese cyber security company, China has long suffered from massive cyber attacks from abroad and severe threats to national security and interests. Cyber security is a complicated global issue given the fact that cyber attacks are conducted anonymously and across borders. The Chinese side calls for all parties to seek a common solution through enhanced dialogue and cooperation. Groundless speculation, hyping up or accusation is not helpful to solve the problem nor conducive to any party's interests.

As major Internet countries, both China and the US share significant interests in cyber security. This should be a source of cooperation rather than confrontation for the two countries. We hope the US side can stop irresponsible attacks and accusations against China following a constructive spirit, create necessary conditions for bilateral cooperation in cyber security based on mutual respect and trust, and work together with the international community to build a cyber space that is peaceful, safe, open and cooperative.

Échantillon 15.

Full Text: Outcome list of President Xi Jinping's state visit to the United States

From September 22 to 25, 2015, at the invitation of President Barack Obama of the United States of America, President Xi Jinping of the People's Republic of China paid a state visit to the United States. During the visit, President Xi Jinping and President Obama had in-depth, candid and constructive talks. The two sides reached extensive consensus and arrived at a series of important outcomes. According to the briefing given by officials from the Foreign Ministry, the main consensus and outcomes reached by the two sides are as follows:

[...]

11. Technology is one of the pillars of the bilateral economic relationship between the China and the United States. Creating the conditions for expanded two-way trade and investment in the technology sector and avoiding measures that restrict it are critical to sustaining positive momentum in the economic relationship between our countries.

(1) Both countries affirm the value of adopting technology-product international standards that have been developed in an open, transparent, market-driven, and balanced manner that allow for due process. Furthermore, both countries recognize that industry's participation in standards development without undue government influence is fundamental to rapid innovation and technology development.

(2) Both countries affirm the importance of competition policy approaches that ensure fair and non-discriminatory treatment of entities and that avoid the enforcement of competition law to pursue industrial policy goals.

(3) Both countries commit that generally applicable measures to enhance information and communication technology cybersecurity in commercial sectors (ICT cybersecurity regulations) should be consistent with WTO agreements, be narrowly tailored, take into account international norms, be nondiscriminatory, and not impose nationality-based conditions or restrictions, on the purchase, sale, or use of ICT products by commercial enterprises unnecessarily.

(4) Both countries affirm that generally applicable measures regulating technology products in the commercial sector benefit from meaningful consultation with the private sector, governments, and other stakeholders to encourage innovative, flexible, and cost-effective solutions.

(5) China and the United States affirm the importance of developing and protecting intellectual property, including trade secrets, and commit not to advance generally applicable policies or practices that require the transfer of intellectual property rights or technology as a condition of doing business in their respective markets.

(6) Both countries affirm that states should not conduct or knowingly support misappropriation of intellectual property, including trade secrets or other confidential business information with the intent of providing competitive advantages to their companies or commercial sectors. Both countries affirm that states and companies should not by illegal methods make use of technology and commercial advantages to gain commercial benefits.

[...]

48. China and the United States agree that timely responses should be provided to requests for information and assistance concerning malicious cyber activities. Further, both sides agree to cooperate, in a manner consistent with their respective national laws and relevant international obligations, with requests to investigate cybercrimes, collect electronic evidence, and mitigate malicious cyber activity emanating from their territory. Both sides also agree to provide updates on the status and results of those investigation to the other side, as appropriate. China and the United States agree that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.

Both sides are committed to making common effort to further identify and promote appropriate norms of state behavior in cyberspace within the international community. China and the United States welcome the July 2015 report of the UN Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security, which addresses norms of behavior and other crucial issues for international security in cyberspace.

The two sides also agree to create a senior experts group for further discussions on this topic.China and the United States agree to establish a high-level joint dialogue mechanism on fighting cybercrime and related issues. China will designate an official at the ministerial level to be the lead and the Ministry of Public Security, Ministry of State Security, Ministry of Justice, and the State Internet and Information Office will participate in the dialogue. The U.S. Secretary of Homeland Security and the U.S. Attorney General will co-chair the dialogue, with participation from representatives from the Federal Bureau of Investigation, the U.S. Intelligence Community and other agencies, for the United States.

This mechanism will be used to review the timeliness and quality of responses to requests for information and assistance with respect to malicious cyber activity of concern identified by either side. As part of this mechanism, both sides agree to establish a hotline for the escalation of issues that may arise in the course of responding to such requests. Finally, both sides agree that the first meeting of this dialogue will be held by the end of 2015, and will occur twice per year thereafter.

BIBLIOGRAPHIE

Références :

Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce (ADPIC). (1994, 15 avril). Annexe 1C de « l'Accord de Marrakech instituant l'Organisation mondiale du commerce, signé à Marrakech, au Maroc, le 15 avril 1994 ». Récupéré de https://www.wto.org/french/tratop_f/trips_f/t_agm0_f.htm

Adelson, I., Ahmed, M.Z., Coyne, V., Han, L., Zhifan, J., Paisley, L.C. et Truong, K. (2014, juin). *U.S.-China Cybersecurity Cooperation*. School of International and Public Affairs, Columbia University.

Arpagian, N. (2015). *La cybersécurité*, 2e éd., Paris : Presses Universitaires de France.

Baldwin, J. R., Means, C. R. R., González, A., & Shenoy-Packer, S. (2014). *Intercultural communication for everyday life*. West Sussex, UK : John Wiley & Sons Inc.

Bauer, J.M. et Dutton, W. H. (2015). *The New Cybersecurity Agenda: Economic and Social Challenges to a Secure Internet*. Quello Center, Michigan State University. Récupéré de http://dx.doi.org/10.2139/ssrn.2614545.

BBC News. (2014, 19 mai). *US justice department charges Chinese with hacking*. Récupéré de http://www.bbc.com/news/world-us-canada-27475324

Berger, P.L. et Luckmann, T. (1966). *The social construction of reality : a treatise in the sociology of knowledge*. London : Penguin Books.

Burnham, P., Gilland, K., Grant, W. et Layton-Henry, Z. (2004). *Research Methods in Politics*. Houndmills : Palgrave Macmillan.

Burgman, P.R. Jr. (2016, 18 mai). Securing Cyberspace: China Leading the Way in Cyber Sovereignty. *The Diplomat*. Récupéré de http://thediplomat.com/2016/05/securing-cyberspace-china-leading-the-way-in-cyber-sovereignty/

Charte des Nations Unies. (1945, 26 juin). RT Can 1945 no 7.

China Law Translate. (2015, 6 juillet). *Cybersecurity Law (Draft)*. Récupéré de http://www.chinalawtranslate.com/cybersecuritydraft/?lang=en

Deibert, R.J. (2003). Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace. *Millennium - Journal of International Studies, 32* (501). DOI: 10.1177/03058298030320030801.

Desforges, A. (2014). Les représentations du cyberespace : un outil géopolitique. *Hérodote,* 1(152-153), pp. 67-81. DOI : 10.3917/her.152.0067

Dorna, A, (1995). Les effets langagiers du discours politique. *Hermès, La Revue*, 2 (16), pp. 131-146. Récupéré de http://www.cairn.info/revue-hermes-la-revue-1995-2-page-131.htm

Dorna, A. (2007). Pistes pour une étude contextuelle du discours politique populiste. *Bulletin de psychologie*, 6 (492), p. 593-600. DOI 10.3917/bupsy.492.0593

Douzet, F. (2013). Chine, États-Unis : la course aux cyberarmes a commencé. *Sécurité globale*, 1 (23), p. 43-51. DOI : 10.3917/secug.023.0043

Duchâtel, M. (2013). La politique étrangère de la Chine sous Xi Jinping. *Hérodote,* 3(150), p. 172-190. DOI: 10.3917/her.150.0172

Dunn Cavelty, M. (2012). The militarisation of cyberspace: Why less may be better. *2012 4th International Conference on Cyber Conflict*, Tallinn: NATO CCD COE Publications

Dunn Cavelty, M. (2013). From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review*, 15, pp. 105–122. DOI: 10.1111/misr.12023

Eisenach, J.A., Barfield, C., Glassman, J. K., Loyola, M., Tews, S. (2016). An American Strategy for Cyberspace : Advancing freedom, security, and prosperity. *American Entreprise Institute.* Récupéré de https://www.aei.org/publication/an-american-strategy-for-cyberspace-advancing-freedom-security-and-prosperity/

Entman, R. M. (1993, décembre). Framing: Toward Clarification of a Fractured Paradigm. *Journal of Communication*, 45(2), pp. 51-58.

Foucault, M. (1971). *L'ordre du discours: Leçon inaugurale au Collège de France prononcée le 2 decembre 1970.* Paris: Gallimard.

Foucault, M. (1977). La crise dans la tête. *L'ARC,* (no 70), 103 p.

Friedman, T. L. (2007). *The World Is Flat, 3.0 : A Brief History of the Twenty-First Century*. New York : Picador.

Gee, J. P. (2014). *An introduction to discourse analysis: Theory and method.* (4e éd.). Abingdon, Oxon ; New York : Routledge.

Gendron, A. et Rudner, M. (2012). *Évaluation des cybermenaces pesant contre les infrastructures du Canada.* Rapport préparé pour le Service canadien du renseignement de sécurité. Récupéré de http://www.securitepublique.gc.ca/cnt/cntrng-crm/plcng/cnmcs-plcng/rsrch-prtl/dtls-fr.aspx?d=PS&i=85395513

Goffman, E. (1956). *The presentation of self in everyday life*. Edinburgh: University of Edinburgh, Social Sciences Research Centre.

Hall, E.T. (1959). *The silent language*. New York: Doubleday.

Hall, S. (1997). « The Work of Representation ». Dans S. Hall (ed.) *Representation : Cultural Representations and Signifying Practices* (p. 1-47). London : Sage Publications.

Harold, S.W., Libicki, M.C., et Cevallos, A.S. (2016). *Getting to Yes with China in Cyberspace*. Santa Monica : RAND Corporation.

Hirschfeld Davis, J. (2015, 9 juillet). Hacking of Government Computers Exposed 21.5 Million People. *The New York Times.* Récupéré de http://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html?_r=0

Hirschfeld Davis, J. (2015, 10 juillet). Katherine Archuleta, Director of Personnel Agency, Resigns. *The New York Times*. Récupéré de http://www.nytimes.com/2015/07/11/us/katherine-archuleta-director-of-office-of-personnel-management-resigns.html?action=click&contentCollection=U.S.&module=RelatedCoverage&region=Marginalia&pgtype=article

Information Office of the State Council of the People's Republic of China (PRC). (2010, 8 juin). *The Internet in China.* Récupéré de http://www.china.org.cn/government/whitepaper/node_7093508.htm.

Inkster, N. (2016). *China's Cyber Power.* Abingdon : Routledge ; London : The International Institute for Strategic Studies.

Lampton, D. M. (2013). A New Type of Major-Power Relationship: Seeking a Durable Foundation for U.s.-China Ties. *Asia Policy.* 16 (1), 51-68.

Larousse. (2015). Hacker. Dans *Dictionnaire de français.* Récupéré le 10 novembre 2015 de http://www.larousse.fr/dictionnaires/francais/hacker/38812

Larousse. (2017a). Ontologie. Dans *Dictionnaire de français.* Récupéré le 30 janvier 2017 de http://www.larousse.fr/dictionnaires/francais/ontologie/56067

Larousse. (2017b). Interopérabilité. Dans *Dictionnaire de français.* Récupéré le 10 avril 2017 de http://www.larousse.fr/dictionnaires/francais/interop%C3%A9rabilit%C3%A9/43787

Larousse. (2017c). Déclaration. Dans *Dictionnaire de français.* Récupéré le 18 juin 2017 de http://www.larousse.fr/dictionnaires/francais/d%C3%A9claration/22224

Larousse. (2017d). Discours. Dans *Dictionnaire de français.* Récupéré le 18 juin 2017 de http://www.larousse.fr/dictionnaires/francais/discours/25859?q=discours#25733

Lee, N. (2013). *Counterterrorism and Cybersecurity : Total Information Awareness.* New York : Springer.

Li Yan. (2015, 21 septembre). Cyber Deal Expected to Halt Disputes. *China News Service*. Récupéré de http://www.ecns.cn/2015/09-21/181825.shtml.

Lieberthal, K. et Singer, P.W. (2012). *Cybersecurity and U.S.-China Relations.* Brooking Institutions, 21st Century Defense Initiative. Washington, D.C. : Brookings. Récupéré de https://www.brookings.edu/research/cybersecurity-and-u-s-china-relations/

Lu Wei. (2015, 14 février). « Cyber Sovereignty Must Rule Global Internet ». *The Huffington Post.* Récupéré de http://www.huffingtonpost.com/luwei/chinacybersovereigntyb6324060.html

Macdonell, D. (1986). *Theories of Discourse: An Introduction.* Oxford; New York: Basil Blackwell.

Mandiant (Firme). (2013). *APT1: Exposing one of China's cyber espionage units.* Alexandria, VA: Mandiant. Récupéré de https://www.fireeye.com/content/dam/fireeyewww/services/pdfs/mandiant-apt1-report.pdf

Maingueneau, D. (1997). *L'Analyse du discours.* Paris: Hachette.

Maingueneau, D. (2012). Que cherchent les analystes du discours ? *Argumentation et Analyse du Discours*, 9. [s.p.]. DOI : 10.4000/aad.1354

Maftei, J. (2015). Sovereignty in International Law. *Acta Universitatis Danubius. Juridica*, 11(1). Récupéré de http://journals.univ-danubius.ro/index.php/juridica/article/view/2798/2585

Ministry of Foreign Affairs of the People's Republic of China. (MFAPRC). Press and Media Service. (2015, 5 juin). *Foreign Ministry Spokesperson Hong Lei's Regular Press Conference on June 5, 2015.* [Communiqué]. Récupéré de http://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1270836.shtml

Ministry of Foreign Affairs of the People's Republic of China. Press and Media Service. (2015, 10 juillet). *Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on July 10, 2015.* [Communiqué]. Récupéré de http://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1280419.shtml

Ministry of Foreign Affairs of the People's Republic of China. Press and Media Service. (2015, 14 août). *Foreign Ministry Spokesperson Hua Chunying's Remarks on US Media Hyping Up Cyber Security Issue Related to China.* [Communiqué]. Récupéré de http://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1288809.shtml

Ministry of Foreign Affairs of the People's Republic of China. (2015, 26 septembre). *Full Text: Outcome list of President Xi Jinping's state visit to the United States.* [Communiqué]. Récupéré de http://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1300771.shtml

Moens, A. Cushing, S. et Dowd, A. (2015). Cybersecurity Challenges for Canada and the United States. *Fraser Institute.* Récupéré de https://www.fraserinstitute.org/sites/default/files/cybersecurity-challenges-for-canada-and-the-united-states.pdf

Mongeau, P. (2008). *Réaliser son mémoire ou sa thèse. Côté jeans & côté tenue de soirée*. Québec: Presse de l'Université du Québec

Nakashima, E. (2015, 9 juillet). Hacks of OPM databases compromised 22.1 million people, federal authorities say. *The Washington Post*. Récupéré de https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/

Nakashima, E. (2015, 21 juillet). U.S. decides against publicly blaming China for data hack. *The Washington Post*. Récupéré de https://www.washingtonpost.com/world/national-security/us-avoids-blaming-china-in-data-theft-seen-as-fair-game-in-espionage/2015/07/21/03779096-2eee-11e5-8353-1215475949f4_story.html

Obama, B. (2009, 29 mai). *Remarks by the President on Securing our Nation 's Cyber Infrastructure*. Notes pour une déclaration du président des États-Unis, M. Barack Obama, Washington D.C.: The White House. Récupéré le 13 avril 2017 de https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure

Obama, B. (2015, 13 janvier). *Remarks by the President.* Notes pour une déclaration du président des États-Unis, M. Barack Obama, au *National Cybersecurity Communications Integration Center*, Arlingtion, Virginia. Récupéré le 13 avril 2017 de https://obamawhitehouse.archives.gov/the-press-office/2015/01/13/remarks-president-national-cybersecurity-communications-integration-cent

Obama, B. (2015, 13 février). *Remarks by the President.* Notes pour une déclaration du président des États-Unis, M. Barack Obama, à l'occasion du *Cybersecurity and Consumer Protection Summit,* Université de Standford, Californie. Récupéré le 13 avril 2017 de https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit

OPM. Office of Communications. (2015, 9 juillet). *OPM Announces Steps to Protect Federal Workers and Others From Cyber Threats*. [Communiqué]. Récupéré

de https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats/

OPM. About. (s.d.). *Our Agency*. Récupéré de https://www.opm.gov/about-us/

OPM. Cybersecurity Resource Center. (s.d.). *Cybersecurity Incidents*. Récupéré de https://www.opm.gov/cybersecurity/cybersecurity-incidents/

Radu, R. (2014). « Power Technology and Powerful Technologies: Global Governmentality and Security in the Cyberspace ». Dans J.-F. Kremer and B. Müller (eds.), *Cyberspace and International Relations* (p.3-20), Springer-Verlag : Berlin Heidelberg. Récupéré de DOI: 10.1007/978-3-642-37481-4_1

Reuters. World News. (2013, 13 avril). *U.S., China agree to work together on cyber security*. Récupéré de http://www.reuters.com/article/us-china-us-cyber-idUSBRE93C05T20130413

Rushe, D. (2015, 5 juin). OPM hack: China blamed for massive breach of US government data. *The Guardian*. Récupéré de http://www.theguardian.com/technology/2015/jun/04/us-government-massive-data-breach-employee-records-security-clearances

Sanger, D.E. et Hirschfeld Davis, J. (2015, 4 juin). Hacking Linked to China Exposes Millions of U.S. Workers. *The New York Times*. Récupéré de http://www.nytimes.com/2015/06/05/us/breach-in-a-federal-computer-system-exposes-personnel-data.html

Saunders, P.C. (2013). « The rebalance to Asia: U.S.-China relations and regional security ». Washington, D.C. : Institute for National Strategic Studies, National Defense University. Récupéré de http://purl.fdlp.gov/GPO/gpo51503.

Schmidt, E. et Cohen, J. (2014). *The New Digital Age*. New York : Vintage Books.

Schmidt, M. S. et Sanger, D. (2014, 19 mai). « 5 in China Army Face U.S. Charges of Cyberattacks ». *The New York Times*. Récupéré de https://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html?_r=0

Segal, A. (2016). *The Hacked World Order*. New York : PublicAffairs.

Segal, A. et Tang, L. (2016). « Reducing and Managing U.S.-China Conflict in Cyberspace ». Chap. In Tanner, T. et Wang, D. (eds.) *U.S.-China Relations in Strategic Domains*. The national bureau *of* asian research, Special Report 57, pp.43-61.

Shi-Xu. (2005). *A cultural approach to discourse*. Basingstoke: Palgrave Macmillan.

Shull, A. (2014). *Global Cybercrime: The Interplay of Politics and Law*. Internet Governance Papers No. 8. Centre for International Governance Innovation. Récupéré de https://www.cigionline.org/publications/global-cybercrime-interplay-of-politics-and-law

Singer, P.W. et Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press.

White House (WH). (2011). *International Strategy for Cyberspace : Prosperity, Security, and Openness in a Networked World*. Washington D.C. : l'auteur.

White House. Office of the Press Secretary. (2015, 13 février). *Remarks by the President at the Cybersecurity and Consumer Protection Summit, Stanford University, California*. Récupéré de https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit

White House. Office of the Press Secretary. (2015, 9 juin). *Press Briefing by Press Secretary Josh Earnest, 6/9/2015*. [Communiqué]. Récupéré de https://www.whitehouse.gov/the-press-office/2015/06/09/press-briefing-press-secretary-josh-earnest-692015

White House. Office of the Press Secretary. (2015, 25 juin). *Press Briefing by Press Secretary Josh Earnest, 6/25/2015*. [Communiqué]. Récupéré de https://www.whitehouse.gov/the-press-office/2015/06/25/press-briefing-press-secretary-josh-earnest-6252015

White House. Office of Press Secretary. (2015, 22 septembre). *Conference Call to Preview the Visit of President Xi Jinping of the People's Republic of China*. [Communiqué]. Récupéré de https://www.whitehouse.gov/the-press-office/2015/09/23/conference-call-preview-visit-president-xi-jinping-peoples-republic

White House. Office of the Press Secretary. (2015a, 25 septembre). *Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference.* [Communiqué]. Récupéré de https://www.whitehouse.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint

White House. Office of the Press Secretary. (2015b, 25 septembre). *Fact Sheet: President Xi Jinping's State Visit to the United States.* [Communiqué]. Récupéré de https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xijinpings-state-visit-united-states

U.S. Department of State. Bureau of East Asian and Pacific Affairs. (2016, 6 décembre). *U.S. Relations With China.* Récupéré de https://www.state.gov/r/pa/ei/bgn/18902.htm

Ventre, D. (2011). *Cyberattaque et Cyberdéfense.* Paris: Hermès science publication/Lavoisier.

Wang, S. (2015, 11 juin). Commentary: U.S. unwarranted hacking accusations reveal its parochialism, stereotyped bias against China. *Xinhuanet.* Récupéré de http://news.xinhuanet.com/english/2015-06/12/c_134321564.htm

Westcott, N. (2008). *Digital Diplomacy: The Impact of the Internet on International Relations.* OII Working Paper No. 16. http://dx.doi.org/10.2139/ssrn.1326476

Wu, X. (2014). Agenda for a New Great Power Relationship. *The Washington Quarterly*, 37 (1), pp. 65-78. Récupéré de http://dx.doi.org/10.1080/0163660X.2014.89318

Xi Jinping. (2013, 7 juin). « Mettre en place un nouveau type de relations entre la Chine et les États-Unis ». Propos du président de la Chine M. Xi Jinping tenus lors d'une conférence de presse en compagnie du président américain Obama, le 7 juin 2013. Dans Xi Jinping, *La gouvernance de la Chine.* 2014, Beijing: Éditions en Langues étrangères.

XI Jinping. (2012, 16 décembre). « De l'édification de la défense nationale et de l'armée ». Notes pour la déclaration du président de la Chine, M. Xi Jinping, à l'occasion de la réunion élargie de la Commission militaire centrale, le 16 décembre 2012. Dans Xi Jinping, *La gouvernance de la Chine.* 2014, Beijing: Éditions en Langues étrangères.

Xi Jinping. (2015, 22 septembre). *Chinese President Xi Jinping Addresses the American Public.* Notes pour la déclaration du président de la Chine, M. Xi

Jinping, à l'occasion du dîner spécial pour le président Xi Jining et Madame Peng Liyuan, au National Committee on U.S.-China Relations, Seattle. Récupéré le 13 avril 2017 de https://www.ncuscr.org/content/full-text-president-xi-jinpings-speech

Xi Jinping. (2015, 16 décembre). *President Xi Jinping delivers a keynote speech at 2015 World Internet Conference.* Notes pour la déclaration du président de la Chine, M. Xi Jinping, à l'occasion de la cérémonie d'ouverture de la *Second World Internet Conference*, Wuzhen, Chine. Récupéré le 13 avril 2017 de http://news.xinhuanet.com/english/special/2015-12/16/c_134922743.htm

Xinhua (2015, 4 juin). U.S. allegations about hacking from China "not responsible, counterproductive": embassy. *Xinhuanet.* Récupéré de http://news.xinhuanet.com/english/2015-06/05/c_134300516.htm

Xinhuanet (2015, 12 août). Chinese embassy spokesman refutes U.S. media hype over "Chinese hacker" invasion. *Xinhuanet.* Récupéré de *http://news.xinhuanet.com/english/china/2015-08/13/c_134510320.htm*

Ressources complémentaires :

Austin, G. (2014). *Cyber Policy in China.* New York: John Wiley & Sons.

Austin, G. (2014b). Managing Asymmetries in Chinese and Amercian Cyber Power. *Georgetown Journal of International Affairs.*

Austin, G. (2015). « China's Security in the Information Age ». Chap. dans *Routledge Handbook of Chinese Security*, Routledge, pp. 355 - 355

Austin, G. (2016b). « China's Cyber Espionage: The National Security Distinction and U.S. Diplomacy ». *Asian Survey: a monthly review of contemporary Asian affairs,* [s.p.].

Austin, G. (2016c). Mapping and Evaluating China's Cyber Power. *Lau China Institute Policy Paper Series.* Récupéré de file:///Users/karipon114/Downloads/Greg_Austin_China's_Cyber_Power_Policy_Papers-Issue-2.pdf

Bardier, T. (2013, 6 décembre). Cyberchronique No 1 : Décomposition systémique d'une cyberattaque, dissymétries et antifragilité. *Cyberstratégie.* Récupéré de

http://www.cyberstrategie.org/?q=fr/cyberchronique-ndeg1-decomposition-systemique-cyberattaque-dissymetries-antifragilite

Betz, D.J. et Stevens, T. (2011). *Cyberspace and the State: Toward a Strategy for Cyber-Power*. Abingdon: Routledge.

Betz, D.J. et Stevens, T. (2013). Analogical reasoning and cyber security. *Security Dialogue, 44*(2), pp.147–164. DOI: 10.1177/0967010613478323

China's Leader in Online Legal Research (CLOLR). *National Security Law of the People's Republic of China.* (2015). Récupéré de http://lawinfochina.com/display.aspx?id=19663&lib=law

Global Commission on Internet Governance. (2016). One Internet. *Centre for International Governance Innovation & Royal Institute for International Affairs*, Récupéré de https://www.ourinternet.org/report

Min, K-S, Chai, S-W et Han, M. (2015). An International Comparative Study on Cyber Security Strategy. *International Journal of Security and Its Applications*, 9 (2), pp.13-20, Récupéré de http://dx.doi.org/10.14257/ijsia.2015.9.2.02

ONU. (2013, 13 septembre). Les cyberconflits et la sécurité nationale. *Le magazine des Nations Unies*, 1(2). [s.p.]. Récupéré de https://unchronicle.un.org/fr/article/les-cyberconflits-et-la-s-curit-nationale

State Council Information Office of the People's Republic of China. (2015). *China's Military Strategy*. Récupéré de https://news.usni.org/2015/05/26/document-chinas-military-strategy

White House. (2015). *National Security Strategy*. Washington D.C. : l'auteur.

U.S. Department of Defense (2015). *The Department of Defense Cyber Strategy*. Récupéré de http://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy

Ventre, D. (2013). « Le rapport Mandiant et la perception américaine de la menace chinoise ». *Sécurité globale*, 1(23), p. 53-64. DOI:10.3917/secug.023.0053