UNIVERSITÉ DU QUÉBEC À MONTRÉAL

LE DISCOURS DE L'ADMINISTRATION OBAMA SUR LA CYBERATTAQUE CONTRE SONY : UN POINT TOURNANT POUR LA CYBERSÉCURITÉ AMÉRICAINE ?

MÉMOIRE
PRÉSENTÉ COMME EXIGENCE PARTIELLE
DE LA MAÎTRISE EN COMMUNICATION

PAR
MARIE-ANNE GRENON

DÉCEMBRE 2015

« Dans toute société, la production du discours est 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, L'Ordre du discours.

« Chacun de nous impose sa perspective ou son schème, son cadre. »
Erwin Goffman, 1974, Les Cadres de l'expérience.

REMERCIEMENTS

Ce mémoire est le fruit de plusieurs mois de travail dont l'achèvement n'aurait toutefois jamais vu le jour sans l'appui de plusieurs personnes tout au long de mon parcours.

Je tiens d'abord à exprimer ma reconnaissance à l'égard du professeur Claude-Yves Charron, pour sa supervision exemplaire et sa disponibilité de tous les instants. Il a su orienter ma réflexion avec respect et rigueur. Merci d'avoir eu confiance en mes capacités; ce fut une source de motivation essentielle en vue de l'aboutissement de ce projet.

Je remercie tout spécialement ma mère Louise pour son soutien moral salutaire, et ce, depuis toujours. Merci également à la personne extraordinaire qu'est Bachir Sirois-Moumni. Ton épaule au quotidien, dans les joies comme les doutes, fut indispensable à cet accomplissement.

Par ailleurs, je souligne la présence indéfectible de mes amis, que je remercie du fond du cœur : Jo Van Der Coquelicot pour sa folie, avec qui, sur un coup de tête, je me suis inscrite à la maîtrise. Julie D. Bédard, Johanie, Lisa et Émilie, pour vos encouragements pendant la rédaction. Enfin, et non les moindres, Étienne pour son inspirante sagesse et Loulou Campagna pour son oeil de lynx.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

Tableau Page

RÉSUMÉ

Dans un contexte d'émergence de la cyberattaque en tant que problématique mondiale et de son impact sur les stratégies de sécurité, ce mémoire s'attache à la construction du discours de l'administration Obama relativement à la cyberattaque contre Sony de novembre 2014. Adoptant une posture constructiviste, l'objectif est de déterminer comment s'articule ce discours, avec quelles visées et s'il contribue ou non à marquer un point tournant pour la cybersécurité américaine.

L'orientation de cette recherche repose sur l'idée que le discours politique est construit en fonction d'un processus de sélection et d'omission de l'information, ce qui en altère la compréhension dans un but d'avancement des intérêts politiques. Une approche théorique et méthodologique en termes de cadrages (Entman, 1993) est privilégiée pour conduire une analyse de six discours de l'administration Obama.

La première partie exposera l'occultation singulière de l'annulation du film *The Interview* au profit des solutions multipolaires pour combattre un problème défini comme un affront à la liberté d'expression américaine. La deuxième s'interrogera sur la capacité du cadrage à favoriser le changement de politiques intérieures et étrangères aux États-Unis. Enfin, le discours à l'étude sera comparé à celui sur la cybersécurité dans le but d'y relever d'éventuelles évolutions, de la sémantique aux pratiques étatiques. À travers la capacité des acteurs politiques d'orienter le discours, nous reconnaitrons l'influence du cadrage pour altérer la compréhension de l'évènement Sony et ainsi structurer le monde social à l'avantage de l'administration Obama.

Mots clés : cyberattaque, cybersécurité, théorie des cadres, discours politique, administration Obama.

INTRODUCTION

Depuis l'avènement d'Internet, d'innombrables données se retrouvent disponibles dans le cyberespace. Avec la multiplication et la croissance exponentielles des systèmes d'informations, l'accès à ces renseignements devient de plus en plus rapide. Favorisant l'économie, facilitant nos vies et augmentant la productivité, ces avancées technologiques extraordinaires engendrent cependant un risque accru pour la sécurité des données des citoyens, des entreprises et des infrastructures indispensables de la société et de l'État. À cet effet, des individus malintentionnés ciblent de plus en plus la population en ligne pour commettre des actes malicieux, parfois de nature terroriste, par la voie des systèmes informatiques.

La prolifération de ces actes dans la première décennie du XXI[e] siècle constitue désormais une problématique mondiale généralement reconnue sous l'appellation cyberattaque. Selon une étude internationale menée par PwC[1], l'année 2014 se caractérise par une hausse de 48 % des cyberattaques à l'échelle de la planète. Les estimations sont au nombre de 42,8 millions pour cette même année, soit l'équivalent de 117 339 invasions par jour à la surface du globe. Les prévisions des experts ne

[1] Étude mondiale du cabinet d'expertise comptable français PwC, en collaboration avec les magazines CIO et CSO, réalisée en ligne du 27 mars 2014 au 25 mai 2014. Les résultats sont fondés sur les réponses de plus de 9700 employés de hauts niveaux dans le secteur de l'information et de la sécurité de plus de 154 pays. Pour plus d'information sur cette étude, on se réfère au document suivant : http://www.pwc.fr/cybersecurite-alors-que-les-incidents-augmentent-et-sont-toujours-plus-couteux.html.

sont guère rassurantes; elles devraient se multiplier et se sophistiquer, touchant de nouveaux sujets et objets dans des secteurs à ce jour insoupçonnés.

Dans sa forme, ses implications, ses conséquences et les transformations des rapports qu'elle engendre, la cyberattaque perpétrée contre Sony en 2014 en sol américain est sans précédent. Ce piratage massif se distingue notamment par le vol de données de plus de 47 000 employés, la profération de menaces terroristes et l'annulation momentanée de la sortie du film *The Interview*. Composante majeure de la stratégie de cybersécurité et du défi historique de la gouvernance d'Internet, le cas Sony soulève d'épineuses questions pour l'État américain. Ce dernier joue d'ailleurs un rôle prépondérant dans le règlement de ce nouveau type de conflit pour lequel il n'existe à ce jour aucun modèle de riposte.

Notre intérêt de recherche porte sur la construction du discours de l'administration Obama concernant le cas Sony. L'objectif est de démontrer que le discours est organisé en fonction d'un processus de sélection et d'omission de l'information qui altère la compréhension du cas Sony, dans le but de promouvoir certains intérêts politiques des États-Unis. Plus largement, il vise à situer le discours sur Sony en rapport avec celui sur la cybersécurité afin de déterminer s'il marque ou non, un point tournant pour la cybersécurité américaine.

Ce mémoire s'articulera autour de cinq chapitres. Dans le cadre du premier, nous présenterons le contexte d'évolution de la cyberattaque contre Sony et, plus largement, la transformation des rapports qu'elle engendre. La problématique d'ensemble permettra de saisir la confusion sémantique dans les discours autour du champ de la cyberattaque et l'importance particulière de l'événement Sony pour la cybersécurité américaine.

Le chapitre deux présentera le cadre de référence théorique basé sur le principe des cadres et cadrages d'Entman (1993, 2004) et appuyé par plusieurs auteurs monopolisant cette assise théorique, dont Riker (1996), Freedman (2003), Callaghan et Schnell (2005), Lakoff (2004, 2009) et Azpiroz (2013). Un bref passage théorique par les relations internationales, avec les travaux de Dunn-Cavelty (2012, 2013) sur le discours politique de la cybersécurité, sera présenté. À la lumière de la littérature, notre question de recherche prendra tout son sens : Comment s'articule le discours de l'administration Obama relativement à la cyberattaque contre Sony ? Viendront ensuite les questions sectorielles et l'hypothèse de recherche : le discours sur la cyberattaque contre Sony est construit de manière à promouvoir les solutions à la cyberattaque, ce qui tend de cette façon à favoriser le changement politique au pays, contribuant à marquer un point tournant pour la cybersécurité américaine. Enfin, la pertinence communicationnelle viendra clore ce premier chapitre.

Le chapitre trois abordera la méthodologie. Premièrement, le discours sera défini afin de rendre compte de sa complexité et des rapports de pouvoir qu'il évoque. L'échantillon composé de six discours politiques de l'administration Obama sera détaillé pour en établir la représentativité. Ensuite sera présentée notre méthode de collecte des données, soit l'analyse des cadres d'Entman, repris par Azpiroz (2013). La démarche de traitement des données fera l'objet de la dernière partie de ce chapitre.

L'exposé des résultats de la recherche, suivi de la discussion, seront traités respectivement dans les quatrième et cinquième chapitres. Les résultats de l'analyse du discours sur la cyberattaque contre Sony précéderont ceux du discours sur la cybersécurité. La discussion se concentrera d'abord sur la cyberattaque contre Sony. Puis, sur la relation entretenue entre les différents contenus visant à favoriser un changement de politiques. Plus largement, le discours sera comparé à celui portant

sur la cybersécurité pour expliquer la présence d'une évolution du cas Sony, du concept plus général de cyberattaque et des pratiques étatiques. Au terme de ce chapitre, nous serons en mesure de valider notre hypothèse de recherche.

CHAPITRE I

LA PROBLÉMATIQUE D'ENSEMBLE

1.1 La transformation des rapports à la cyberattaque

Dans cette première partie, nous nous intéresserons au contexte d'évolution de la cyberattaque contre Sony. Autant d'un point de vue circonstanciel qu'analytique, nous circonscrirons notre objet de recherche et le situerons dans le contexte plus large de la transformation des rapports qu'elle engendre. D'abord, nous présenterons l'événement Sony et tenterons de définir le concept de cyberattaque, ses attributs et ceux du cas à l'étude. Puis nous nous pencherons sur son rapport au contexte géopolitique et à la diplomatie, les options de riposte de l'État et l'évolution de la cybersécurité aux États-Unis. Mis en commun, ces éléments démontrent l'importance particulière de l'événement Sony dans la cybersécurité américaine.

1.1.1 Le cas Sony : rappel des faits

Dès la sortie de sa bande-annonce en juin 2014, le film *The Interview,* produit par Sony Entertainment Pictures (SPE)[2], la division hollywoodienne du géant japonais du

[2] Pour alléger le texte, nous privilégions l'emploi de Sony pour désigner la division Sony Entertainment Pictures en sol américain.

divertissement, crée la polémique. Classifié à titre de comédie[3] aux États-Unis, le scénario met en scène deux journalistes américains loufoques se rendant en Corée du Nord[4] pour officiellement interviewer le président Kim Jong-un, officieusement pour l'assassiner conformément aux ordres de la Central Information Agency (CIA). La Corée du Nord réagit avec colère, d'abord par une allégation publique, qualifiant le produit d'acte de guerre faisant la promotion du terrorisme contre le pays. En juillet 2014, l'ambassadeur nord-coréen au sein des Nations Unies formule une plainte officielle et demande l'interdiction de la sortie du film prévue en octobre. Connaissant le rôle de l'organisation internationale qui ne prévoit pas l'arbitrage de la censure cinématographique, la plainte demeure sans réponse. Pour ne pas froisser Pyongyang, Sony repousse la sortie du film au jour de Noël dans le but d'apporter certaines modifications à la facture visuelle[5].

Le 21 novembre 2014, les têtes dirigeantes de Sony, dont Michael Lynton et Amy Pascal, reçoivent un courriel d'extorsion signé God'sApstls. Le 24 novembre au matin, les employés sont avisés d'une intrusion dans le système informatique; leur écran d'ordinateur est figé sur un message d'avertissement intitulé « Hacked by GoP ». L'attaque s'orchestrera en sept étapes, dont la première est le vol de données

---

[3] D'emblée, on pourrait comparer *The Interview* à *Death of a President* (2006), un faux documentaire de fiction britannique prévoyant l'assassinat de George W. Bush. Or, *The Interview,* réalisé par Seth Rogen, relève davantage du grotesque et de l'humour adolescent bien connu chez l'auteur Evan Goldberg que de la satire politique. Ainsi, nous partageons la classification de comédie.

[4] Pour alléger le texte, nous privilégions l'appellation Corée du Nord plutôt que le nom officiel du pays, Democratic People's Republic of Korea (DPRK).

[5] Selon un échange de courriels rendus publics entre les dirigeants de Sony, la scène finale du film a été modifiée. Le 28 septembre 2014, Amy Pascal a écrit à Kazuo Hirai: « In shot #337 there is no face melting, less fire in the hair, fewer embers on the face, and the head explosion has been considerably obscured by the fire, as well as darkened to look less like flesh (...) » Propos rapportés par A. Sakoui et L. Shaw (2014).

confidentielles de l'entreprise qui avaient été rendues publiques sur la Toile. Il s'agit de 26 Go de renseignements sensibles, dont les informations personnelles de près de 47 000 employés et leur famille, incluant des acteurs, lesquelles se retrouvent accessibles en ligne : adresses, numéros d'assurance sociale, comptes bancaires, pseudonymes utilisés lorsque les artistes américains réservent à l'hôtel, jusqu'aux dossiers médicaux.

Une deuxième fuite est orchestrée le 3 décembre 2014, et expose des renseignements sur des certificats de sécurité et le détail d'authentifications pour divers comptes et accès. Une troisième fuite fait son apparition le 7 décembre avec, cette fois, l'information financière de l'entreprise. Puis, le 8 décembre est publiée l'archive des courriels reçus et transmis par Steve Mosko, président de Sony Pictures Television, et Amy Pascal, coprésidente de Sony Pictures Entertainment.

La plupart des étapes sont signées par un mystérieux collectif de pirates se faisant appeler Guardians of Peace (GoP). Émergent alors les premiers doutes de la communauté Web concernant l'implication possible de la Corée du Nord. Une rumeur à laquelle un porte-parole anonyme du gouvernement nord-coréen réplique : « The hostile forces are relating everything to the DPRK. I kindly advise you to just wait and see. » [6] Chargé de l'affaire, le Federal Bureau of Investigation (FBI) nie, le 9 décembre 2014, les rumeurs qui se veulent de plus en plus persistantes. Le FBI allègue : « There is no attribution to North Korea at this point. »[7]

---

[6] BBC. (2 décembre 2014). *North Korea refuses to deny Sony Pictures cyber-attack.* Récupéré de http://www.bbc.com/news/world-asia-30283573.

[7] Propos de Joe Demarest, l'assistant directeur de la division cyber du FBI, dans le cadre d'un panel lors de la conférence sur la cybersécurité le 9 décembre 2014. Propos rapportés par J. Finkle (2014) dans un article à ce sujet.

Dans la foulée des différentes fuites estimées à 235 gigaoctets[8], le 16 décembre 2014 marque l'étape la plus médiatisée : la menace physique. Le titre *The Interview* est pour la première fois mentionné. Dans un communiqué diffusé sur Internet, GoP profère des menaces terroristes contre les salles de cinéma qui envisagent de projeter le film :

> Warning : We will clearly show it to you at the very time and places "The Interview" be shown, including the premiere, how bitter fate those who seek fun in terror should be doomed to. Soon all the world will see what an awful movie Sony Pictures Entertainment has made. The world will be full of fear. Remember the 11th of September 2001. We recommend you to keep yourself distant from the places at that time. (If your house is nearby, you'd better leave.) Whatever comes in the coming days is called by the greed of Sony Pictures Entertainment. All the world will denounce the SONY.[9] (GoP, 2014)

Devant l'ampleur de cette menace désormais physique, d'importantes chaînes de cinéma américaines décommandent la projection du film. Finalement, le 17 décembre, Sony annule sa sortie.

Ce geste est décrit comme étant une atteinte à la liberté d'expression par la communauté hollywoodienne, et une vague de patriotisme se fait ressentir dans les

---

[8] Des informations confidentielles ont coulées notamment sur le plan d'affaires de Sony en vue de la production d'un nouveau long métrage de Spider-Man et sur le fait que l'actrice Jennifer Lauwrence gagnait moins que son partenaire masculin. Pour plus de détails, on se réfère à l'article de J. Cook (2014).

[9] La diffusion du message de Guardians of Peace a été faite sur le site Pastebin.com, une application Web qui permet de téléverser des documents pour affichage public. Or, suite à nos recherches, le fichier d'origine est actuellement introuvable Nous avons retracé sa transcription sur plusieurs sites Web, et retenons celle publiée sur le site Variety.

médias sociaux[10]. En ce qui concerne Obama, il prend immédiatement position et tranche publiquement sur la décision de Sony : « I think they made a mistake. »[11] Au même moment, la presse, dont le *New York Times*, rapporte les propos d'administrateurs américains, souhaitant garder l'anonymat, affirmant l'implication de la Corée du Nord[12].

Le lendemain, Sony reçoit un courriel de GoP autorisant désormais la diffusion du film *The Interview*, mais à certaines conditions :

> This is GOP. You have suffered through enough threats. *The Interview* may release now. But be careful. September 11 may happen again if you don't comply with the rules: Rule #1: no death scene of Kim Jong-un being too happy; Rule #2: do not test us again; Rule #3: if you make anything else, we will be here ready to fight.[13] (GoP, 2014)

---

[10] De Michael Moore à Stephen King, en passant par Steve Carrel jusqu'à Ben Stiller, Global News a répertorié près de 40 tweets de personnalités décriant la décision de Sony et la ramenant à une atteinte à la liberté d'expression. Pour de plus amples informations, se référer à l'article de John R. Kennedy (2014).

[11] Obama, B. (19 décembre 2014). *Remarks by the President in Year-End Press Conference*. Dernière conférence de presse de l'année à la Maison-Blanche. Récupéré de https://www.whitehouse.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference.

[12] Sanger, D. E. et Perltroth, (17 décembre 2014). U.S. Said to Find North Korea Ordered Cyberattack on Sony. *New York Times*. Récupéré de http://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html?_r=1.

[13] Pastebin. [s.d.] (18 décembre 2014). *Dear Sony from GOP*. Récupéré le 20 février 2014 de http://pastebin.com/m4YB2TJd.

Dans ce qu'il décrit comme la plus grave cyberattaque jamais commise aux États-Unis, le FBI affirme, [14] le 19 décembre, qu'il possède suffisamment de preuves pour attribuer la responsabilité au gouvernement nord-coréen. Par conséquent, il impute à ce dernier l'entière responsabilité de l'attaque informatique perpétrée en novembre, jusqu'aux menaces terroristes entourant *The Interview*. Ses conclusions reposent sur trois arguments relevant des similarités techniques entre l'attaque de Sony et les attaques antérieures attribuées à la Corée du Nord. Le premier argument est l'analyse du logiciel malveillant révélant « des liens » avec d'autres logiciels malveillants développés par « des acteurs nord-coréens ». (Traduction libre FBI, 2014) Le deuxième raisonnement est la découverte d'une série d'adresses IP communiquant avec celles « associées à des infrastructures nord-coréennes connues ». (Traduction libre, FBI, 2014) Quant au troisième argument, il est basé sur les outils utilisés par les pirates, en ce qu'ils sont qualifiés de « similaires » (Traduction libre, FBI, 2014) à ceux qui auraient déjà été identifiés lors d'offensives antérieures attribuées à la Corée du Nord.

De son côté, Pyongyang[15] s'empresse de nier toute implication par l'entremise de la Korean News Central Agency (KCNA), son agence de presse officielle, avant d'appeler à l'enquête conjointe pour trouver le coupable. Une proposition qui sera ignorée par Washington. L'État nord-coréen s'estime victime d'un cadrage de la part des États-Unis : « Whoever is going to frame our country for a crime should present concrete evidence. » (KCNA, 2014) Il signale que les résultats de l'enquête et la

---

[14] Federal Bureau of Investigation (19 décembre 2014). *Update on Sony Investigation.* [Communiqué] (202) 324-3691. Récupéré de http://www.un.org/News/fr-press/docs//2012/SGSM14567.doc.htm.

[15] Précisons que la Corée du Nord aurait des capacités non-négligeables en matière de piratage. Selon les experts, elle possèderait un réseau de mille huit cent informaticiens d'élites associés au Bureau 121, une unité du General Bureau of Reconnaissance sous le contrôle de l'armée nord-coréenne. La Corée du Sud accuse d'ailleurs souvent le Nord de pirater ses infrastructures essentielles.

tentative de cadrer le pays pour ce crime démontrent la tendance réfractaire des États-Unis envers la Corée du Nord. Si la politique hostile américaine persiste à son égard, le « pays du matin calme » fait miroiter la possibilité d'une « guerre désastreuse ». (Traduction libre, KCNA, 2014)

Pour sa part, Michael Lynton, président de Sony, proteste publiquement à l'accusation portée par Obama. Il soulève un manque de communication entre la presse, le public et l'État au sujet de l'événement. Certifiant n'avoir jamais souhaité l'annulation du film, il confie que « We are obviously both strong proponents of the First Amendment »[16] avant d'annoncer qu'il considère une sortie alternative du long métrage *The Interview*. De ce fait, le 23 décembre 2014[17], Sony confirme cette parution de *The Interview*. Le film prit l'affiche le jour de Noël dans certaines salles indépendantes des États-Unis et du Canada, en plus d'être disponible en ligne à un prix inférieur au marché.

1.2 La cyberattaque : variation sur la confusion sémantique

Pour définir la cyberattaque, il importe d'abord de prendre acte de ce que François-Bernard Huyghe (2014), chercheur à l'Institut de Relations Internationales et Stratégiques (IRIS), considère comme une dispersion ou une hybridation du concept. (Huyghe, 2014) Transdisciplinaire, il touche à l'informatique, à la communication, au

[16] Block, Melissa. (19 décembre 2014). Entrevue avec Michael Lynton. Récupéré de http://www.npr.org/sections/thetwo-way/2014/12/19/371966188/ceo-says-sony-pictures-did-not-capitulate-is-exploring-options.

[17] Dans la nuit du 23 décembre 2014, la Corée du Nord a subi une panne géante d'Internet d'une durée de plus de 9 heures consécutives, sans que le coupable ne soit identifié. Les présomptions pointent tantôt vers les États-Unis, tantôt vers la Chine qui, quant à elle, héberge les serveurs nord-coréens.

droit et souvent à la science politique, avec comme résultat une définition qui s'en trouve « variée »[18]. (Hathaway et al., 2012; Owens et al., 2009) En politique, le concept est du domaine de la défense nationale, des affaires étrangères, de l'application de la loi, de l'intelligence et du renseignement.

D'entrée de jeu, spécifions que la cyberattaque prend forme dans le cyberespace. Pour la chercheuse Alix Desforges (2014), ce lieu inédit prend un sens plus opérationnel dans les milieux universitaires et militaires, sans pour autant faire l'objet d'un consensus. Est-ce un espace géographique à contrôler, un territoire sans foi ni loi, ou une entité sans frontière ? On reconnaît que sa représentation s'exprime dans les différents enjeux qui lui sont relatifs. Puisque notre objet d'étude implique une cyberattaque contre une entreprise américaine imputée à l'État nord-coréen, nous considérons le cyberespace comme un « champ de confrontation à part entière »[19] entre différents acteurs. Si un bon nombre d'États mènent actuellement des opérations dans le cyberespace, on ne sait pas ce qui est acceptable et ce qui ne l'est pas, estime Matthijs Veenendaal, chercheur au Centre excellence de cyberdéfense de l'OTAN.

À l'image de son terrain, la définition de la cyberattaque subit également l'absence d'unanimité. Il tient cependant de l'évidence d'affirmer que le mot cyberattaque provient du préfixe cyber et du nom commun attaque. Issue de la cybernétique de Wiener, le préfixe sert à « former des mots liés aux nouvelles techniques de

---

[18] Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The Law of Cyber-Attack. *California Law Review*. 100(4): 817-885. Récupéré de http://www.californialawreview.org/articles/the-law-of-cyber-attack. Roscini, M. (2014). *Cyber Operations and the Use of Force in International Law*. Oxford: Oxford University Press.

[19] Cette expression est utilisée dans le *Livre blanc sur la défense et la sécurité nationale* (2013), un rapport d'une commission française présentant la stratégie du pays en matière de cybermenace d'ici les vingt ans à venir. Pour des informations supplémentaires, consultez le rapport en ligne.

communication numériques (Internet) » [20]. Retenons la tentative de définition de Daniel Ventre, spécialiste des cyberconflits et auteur de *Cyberattaque et Cyberdéfense,* « une agression contre les systèmes qui organisent, qui dirigent ». (Ventre, 2011)

Dans l'espace public, son sens est « obscur ». (Hathaway et al., 2012, Roscini, 2014) Pour l'État américain, la définition de la cyberattaque est « ambiguë ».[21] (Notre traduction, Whitehouse, 2014) Singer et Friedman, auteurs de *Cybersecurity and Cyberwar* (2014) y relèvent un problème d'ordre sémantique, car le discours implique un nouveau vocabulaire et de nouveaux cadres de référence. « Étant donné que le terme mélange des aspects informatiques très techniques avec des concepts plus généraux relevant du droit et du crime, même le terme le plus simple, tel qu'attaque, peut être chargé de sens. » (Traduction libre, Singer et Friedman, 2014)

Le souci, remarque l'experte en cybersécurité Myriam Dunn-Cavelty, c'est la nature sensationnaliste du discours qui crée une multiplication de significations et de nuances dans les termes propres au préfixe cyber[22], d'où l'existence de la confusion ou de la perte de sens lorsqu'ils sont mis ensemble. (Dunn-Cavelty, 2007; Fisher,

---

[20] Dictionnaire Web L'internaute. (2015). Récupéré de http://www.linternaute.com/dictionnaire/fr/definition/cyber/.

[21] Whitehouse (2014). *Judiciary Subcommittee on Crime and Terrorism Hearing on Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Crime and Terrorism.* [discours]. Session du Congrès du 15 juillet 2014. Récupéré de https://www.hsdl.org/?view&did=756247.

[22] On remarque d'ailleurs une utilisation de plus en plus de mots associés au préfixe cyber. L'attentat de Charlie Hebdo en France en 2015 s'est vu qualifié de cyberdjihadisme dans les médias. Les attaques de TV5 Monde et celle du compte du magazine américain *Newsweek.* Cette dernière, qui a été signée par un groupe s'autoproclamant Cybercalifat, a été présentée dans les médias comme originaire d'une cyberforce islamique.

2001). L'ONU[23] concède d'ailleurs qu'il importe d'assouplir le discours en matière de cyberattaque dans le but de créer des concepts clairs et justes pour définir les réalités du cyberespace. Les expressions fatalistes ou catastrophiques « worst case scenario » ou encore « cyber Pearl Harbor » sont largement entendues dans les discours.

Selon Ventre, cette dérive linguistique attribue au discours l'emploi de notions plus violentes. (Ventre, 2011). En effet, le terme cyberattaque est souvent associé, confondu ou substitué dans une prolifération lexicale le plus souvent à cybercrime, cyberterrorisme ou même à cyberguerre et, jusqu'à récemment, à cybermenace. Ce cafouillage semble d'ailleurs apparent dans les documents politiques consultés en préanalyse. De « cyberthreat » à « criminal attack » et à « cybervandalism » pour Obama. Avançant d'autres arguments, le sénateur américain John McCain rétorque qu'étant donné la gravité du geste, il devrait être considéré tel « an act of war », propos auquel réplique le président avec « No, I don't think it was an act of war. » (Obama, 2014) Enfin, dans une conversation entre les États chinois et américain sur le sujet, la Chine mentionne pour sa part du « cyberterrorisme ».

D'abord, définir la cyberattaque en fonction de ce qu'elle n'est pas nous apparaît une tentative de choix. Singer et Friedman distinguent attaque et cyberattaque. Pour eux, la différence réside dans deux fondements : « Le moyen (force kinésique comparativement à force digitale) et la cible (dommages physiques directs en comparaison avec dommages premiers aux ordinateurs et à l'information qui s'y trouve). » (Singer et Friedman, 2014).

---

[23] ONU (13 septembre 2013). Les cyberconflits et la sécurité nationale. *Le magazine des Nations Unies,* 1 (2). Récupéré de http://unchronicle.un.org/fr/article/les-cyberconflits-et-la-s-curit-nationale/.

La référence à cybercrime apparaît douteuse si l'on considère le crime dans sa définition classique, une infraction à la loi relevant d'un système juridique. Au nom de quelle loi la cyberattaque constitue-t-elle un crime ? Même si elle semble impliquer une infraction au droit et que le travail de reconnaissance au niveau législatif s'organise, aucune législation ne reconnaît actuellement le statut de crime ou d'attaque propre au cyberespace.

Quant à la référence au cyberterrorisme[24], fortement médiatisée, elle constitue souvent un abus de langage. (Ventre, 2011, 2015) Certes, le cyberterrorisme tend à être conceptualisé tel un nouveau champ de bataille. Cependant, la plupart des cyberattaquants ne sont pas des terroristes, car leur but est le vol ou la destruction de données. Pour Huyghe, c'est la finalité de la cyberattaque qui s'en distingue, car l'élément de proclamation ou de revendication propre au terrorisme est manquant. Un élément dont « la composante publique, voire publicitaire, du terrorisme (faire mourir pour faire savoir) semble ici faire défaut. » (Huyghes, 2014) On reconnaît que la menace terroriste peut toutefois être une technique utilisée[25] pour mener à terme les objectifs d'une cyberattaque. C'est le cas de notre objet à l'étude, avec la menace terroriste proférée à l'encontre des salles de cinéma ayant l'intention de diffuser *The Interview*, et contre les spectateurs et les personnes résidant à proximité des cinémas.

En regard de la réflexion ayant émergé au colloque de la Chaire Castex en 2011, la référence à cyberguerre, au sens clausewitzien, s'avère infondée. Pour le professeur

---

[24] Pour comprendre la complexité du cyberterrorisme et ses implications, se référer au chapitre 2 Understanding, Locating and Constructing Cyberterrorism de l'ouvrage Cyberterrorism, Understanding, Assessment, and Response (T. Chen, L. Jarvis, S. MacDonald, 2014).

[25] Suite à une recension des cyberattaques, nous n'avons point repéré de cyberattaque ayant pour technique l'attentat terroriste. Ce qui n'invalide pas pour autant le fait que cette technique ait existé et le risque qu'elle se produise dans le futur.

François Géré, « la cyberguerre n'a pas d'autonomie stratégique, elle ne peut exister par elle-même ». (Géré, 2011) En fait, elle se veut une interprétation de la guerre des hommes par les moyens du cyber. (Géré, 2011) À cet effet, la cyberattaque peut être un mode d'action de la guerre, mais ne constitue pas une forme de guerre en elle-même. (Géré, 2011) Au sens où le décrit Erik Gartzke de l'Université de Californie, pour être une guerre, le conflit sur Internet devrait pouvoir se substituer à une bataille. Or, cela ne s'est pas encore produit et ne risque pas de se produire de sitôt. (Gartzke, 2013)

De plus en plus, la cybermenace se taille une place de choix dans les discours des politiciens. (Dunn-Cavelty, 2014) Tout aussi vague que la cyberattaque, elle implique une « notion signifiant une utilisation malicieuse de l'information ou des technologies de communication comme cibles ou comme outils ». (Traduction libre, Dunn-Cavelty, 20XX) Par conséquent, cela engendre une perception croissante de peur et de menace dans la sphère publique. (Eriksson et Giacomello, 2014)

En somme, la cyberattaque est caractérisée par un flou sémantique qui engendre une confusion dans les discours à son sujet mais aussi, plus largement, sur la cybersécurité.

1.3 Des attributs à géométrie variable

Au-delà de sa définition, le concept de cyberattaque appelle à une mutation continuelle en raison de sa forme à géométrie variable. Il peut s'agir d'une tentative d'intrusion aléatoire dans un système informatique opéré par un adolescent, à partir des connaissances acquises à la suite de la lecture d'un manuel d'informatique. À l'autre pôle, il peut s'agir d'une attaque, selon un agenda prédéfini, en vue de saboter le système vital d'un État jugé ennemi. (Ventre, 2011) Entre les deux fourmille un

large spectre d'invasion aux multiples attributs[26] : acteurs, motivations, objectifs, dommages, méthodes, techniques, modes opératoires et attribution de responsabilité.

Minimalement, deux acteurs principaux sont impliqués lors d'une cyberattaque. Celui qui agresse, à l'offense, et celui qui subit, à la défense. Le terme pirate[27] est souvent employé pour définir l'internaute qui contourne ou détruit à des fins malveillantes, des éléments reliés à un réseau informatique. Sa référence est souvent en rapport avec le crime. Le terme hacker est davantage employé pour définir un passionné d'informatique dont la philosophie est basée sur le principe de la libre circulation de l'information. Enfin, à l'exemple du fondateur de Wikileaks Julian Assange, de l'ex-employé fédéral américain Edward Snowden, ou encore du collectif Anonymous, il peut s'agir d'un hacktiviste engagé dans ce qu'il considère comme d'intérêt public.

Quant aux motivations, elles peuvent être regroupées selon la nature de la volonté à perpétrer l'attaque. Cette dernière peut être idéologique[28] lorsque sa valeur se réalise par l'action de « punir des ennemis de son pays, arrêter un complot impérialiste ou réaliser la volonté de Dieu ». (Huyghe, 2014) Elle est économique si son but est

---

[26] Pour choisir les attributs les plus pertinents pour ce mémoire, nous nous inspirons des différents attributs de la cyberattaque identifiés par le chercheur iranien Medhi Khadivar (2015). Par l'étude de dix cyberattaques marquantes, l'auteur a crée une typologie de onze attributs qu'il regroupe en trois catégories: l'intention de l'attaque, son impact et son cheminement.

[27] Nous reconnaissons qu'il existe différents types de pirates, dont certains sont plus malicieux que d'autres; black hats, white hats, grey hats et script kiddies, notamment. Larousse (2015). Dictionnaire. Récupéré de http://www.larousse.fr/dictionnaires/francais/pirate/61126.

[28] Le piratage massif de la chaîne télévisuelle francophone TV5 Monde, en avril 2015, est à cette image. Revendiquée par un groupe djihadiste se réclamant de l'État Islamique (EI), la diffusion télévisuelle de onze canaux internationaux a été interrompue et les médias sociaux de la chaîne ont été pris d'assaut. La raison invoquée par le groupe : la dénonciation de l'intervention militaire des troupes françaises en Irak pour combattre l'EI. Ici, la volonté semble politique, souhaitant le retrait des troupes françaises contre ce dernier, et idéologique car elle intègre des valeurs religieuses.

d'affecter l'économie[29] d'un secteur privé ou public, ou politique si elle « implique des tactiques obéissant à une logique de puissance ». (Huyghes, 2014) La combinaison de plus d'une volonté est possible et la frontière entre les deux, ou les trois, peut être ardue à tracer.

Pour paraphraser Ventre, les objectifs visent tantôt à observer, déstabiliser, affaiblir ou paralyser son adversaire. (Ventre, 2011) Pour les atteindre, les auteurs possèdent une gamme de méthodes[30] et de modes opératoires qui se perfectionnent au rythme de la technologie. (Ventre, 2011) Il existe également des dommages, maîtrisés ou non, anticipés ou non, dont la nature et la polarisation de l'intensité sont extrêmement variables. (Ventre, 2011)

Le noyau dur du problème réside dans la nature stratégique du cyberespace qui ordonne la difficulté d'attribuer la responsabilité. Cette dernière se définit comme le fait de « déterminer l'identité ou la location d'un attaquant ou d'un intermédiaire de l'attaquant. ». (Wheeler et Larsen, 2008) L'élément inhérent à toute cyberattaque est l'ambiguïté. Celle « de sa source, du dommage qu'elle est censée produire, de ses finalités et de sa nature même ». (Huyghe, 2014) Cette ambiguïté[31] crée l'anonymat

[29] Prenons exemple sur la découverte, en février 2015, d'une cyberattaque échelonnée sur une période d'un an attribuée au groupe surnommé Carbanak. Visant une centaine de banques logées dans trente pays, ce stratagème aurait ainsi permis de dérober entre trois cent millions et un milliard de dollars, selon le *Financial Times*.

[30] Elles comprennent l'intrusion, l'usurpation, l'espionnage, le vol d'informations, le sabotage, jusqu'à l'acte terroriste. Pour ce faire, les techniques utilisées vont du harponnage, consistant à pêcher une victime en lui envoyant un courriel malveillant [*malware*], au déni de service, [DoS] visant la mise hors-ligne d'un serveur, jusqu'au Botnet, utilisant des ordinateurs dits zombis pilotés à distance. La simplicité du procédé de piratage apparait désarmante. L'histoire démontre qu'un simple manuel d'informatique suffit à individu non expérimenté, pourvu qu'il sache lire et soit motivé.

[31] Un constat que partagent les Américains Singer et Friedman (2014) ainsi qu'Eric Schmidt et Simon Cohen (2013), auteurs de l'ouvrage de référence *The New Digital Age: Reshaping The Future of People, Nations and Business.*

numérique, laquelle fait naître des hypothèses (Ventre, 2011) et des présomptions. (Huyghe, 2014) Dans l'état actuel des connaissances, il est très difficile d'attribuer la responsabilité d'une attaque. (Ventre, 2011) Lorsque cela s'avère possible, il est souvent question de déterminer l'ordinateur ou le réseau, moins souvent l'identité de l'individu derrière la machine. (Ventre, 2011) L'explication réside d'une part dans l'architecture d'Internet, qui n'a pas été conçue à des fins de traçage et, d'autre part, en raison de la vulnérabilité des systèmes d'informations, mais aussi de l'imprudence humaine envers leur protection.

S'il s'agit d'États, souvent la Corée du Nord, la Russie, l'Iran et la Chine (Ventre, 2011), ces derniers nient [32] être à l'origine des actes dont on les accuse. D'ailleurs, les acteurs habitués à être accusés ont aiguisé leurs argumentaires au fil des ans. (Ventre, 2011) Si les cyberattaques commises par des États peuvent être, selon Zeller, « distinguées par leur niveau de sophistication et leur modus operandi » [33] (traduction libre, Zeller, 2014), l'attribution demeure tout de même très ardue. Elle l'est davantage si la stratégie des attaquants entre en ligne de compte. Elle peut en être une de recherche d'anonymat, de faire accuser un tiers pour accentuer la confusion ou de faire savoir qu'ils en sont les auteurs, mais sans laisser de preuve formelle. (Huyghe, 2014)

---

[32] Prenons exemple sur trois cas probants. Les cyberattaques multiples envers les structures vitales (sites gouvernementaux et banques) de l'Estonie en 2007. Malgré les présomptions, la Russie, qui était alors en froid diplomatique avec le pays, a nié son implication. En 2009, le virus informatique Stuxnet en Iran où, malgré les présomptions, les États-Unis et Israël ont nié leur implication. Le piratage massif de l'Office of Personnel Management (OPM) en 2015, où ont été rendu public 21,5 millions de données personnelles d'employés ou d'ex-employés fédéraux américains. Malgré les présomptions des États-Unis, la Chine a nié son implication.

[33] Zeller, K. (17 décembre 2014). The Evidence That North Korea Hacked Sony Is Flimsy. *The Wired.* Récupéré de http://www.wired.com/2014/12/evidence-of-north-korea-hack-is-thin/.

En résumé, l'exposition des attributs de la cyberattaque nous permet de la considérer telle une forme d'invasion ou d'intrusion d'un système informatique, sans paramètres précis, dans une zone de non-droit où les limites d'actions et de réponses sont floues. Techniquement simple, elle revêt cependant une redoutable efficacité. Elle se configure avec des acteurs, des motivations, des objectifs, des méthodes, des techniques de même que des modes opératoires multiples. Elle se distingue des attaques dites traditionnelles par la difficulté d'attribution de responsabilité, ce qui vient ajouter à l'imprécision du concept, déjà miné par une confusion sémantique.

1.3.1 Sony : des attributs sans précédent

Dans le cas à l'étude, l'acteur impliqué à l'offense est un groupe de pirates se faisant appeler Guardians of Peace. À la défense, il s'agit de l'entreprise Sony et de l'État américain, ayant repris l'affaire par le biais de l'enquête du FBI.

La volonté des attaquants semble d'abord idéologique puisqu'elle touche la valeur de la liberté d'expression artistique américaine. On estime que la proposition de contenu du film *The Interview*, la dérision de l'État nord-coréen, va à l'encontre de l'idéologie des pirates. Puisque les États-Unis et la Corée du Nord se livrent une bataille politique depuis la fin de la guerre de Corée, et dans l'optique que la Corée du Nord soit réellement derrière l'attaque, la volonté apparaît politique.

Enfin, en regard du constat des dégâts financiers subis par la corporation estimés à 35 millions[34] de dollars américains, le caractère semble économique. Faute de pouvoir

[34] Sony fait figure de cas école pour l'estimation des coûts générés. Selon son évaluation en février 2015, Sony estimait les coûts à 35 millions de dollars. Cela pourrait être revu à la hausse en 2016, avec la parution du bilan financier de l'année 2015, car les coûts estimés sont principalement

relever les objectifs réels[35] des attaquants, il est possible d'en estimer certains : paralyser et affaiblir l'entreprise, et annuler le long métrage *The Interview*.

Quant aux méthodes utilisées, il s'agit en premier lieu de l'intrusion dans le système de Sony, en plus de constituer un vol de données, la mise en ligne illégale d'une portion d'entre elles, un acte de sabotage du système informatique et, enfin, la profération d'un acte terroriste. En matière technique, il s'agit principalement de l'utilisation de logiciels malveillants. Les modes opératoires permettent de qualifier l'attaque ciblée puisqu'elle vise Sony, de massive en raison des importants dommages causés, et qu'elle est orchestrée en sept fuites sur une période de trois semaines. Certaines étapes ont été signées par GoP ; par conséquent, l'attaque a été en partie revendiquée. On la qualifie en fait de publicisée et de largement médiatisée.

Quant aux dommages, nous les qualifions principalement de structurels. Après l'annulation du film et la mise en ligne de cinq longs métrages non diffusés, les préjudices sont financiers pour l'entreprise et les exploitants de chaînes de cinéma, en plus de toucher à la propriété intellectuelle. Dans le recours collectif actuel contre Sony pour vol de données, les dommages financiers peuvent aussi affecter les employés. En raison du stress lié à l'exposition de leurs informations personnelles sur la Toile, ils sont susceptibles de subir une atteinte sur le plan psychologique. Par la divulgation d'échanges de courriels entre cadres de Sony à caractère raciste contre le

---

engendrés par la restauration de son système informatique, et moins en termes de pertes de revenus dues aux films illégalement mis en ligne.

[35] En supposant que la Corée du Nord est réellement derrière l'attaque, on peut citer Kim Heun-kwan, professeur de sciences informatiques, formé en Corée du Nord mais ayant fui le pays depuis six ans. Selon ses estimations, « l'objectif ultime de la cyberstratégie du pays est de pouvoir attaquer les infrastructures de la Corée du Sud et des États-Unis ». (Heun-kwan, 2014)

président Obama, ils touchent à la réputation[36] individuelle et à celle de l'entreprise Sony. Enfin, n'oublions pas l'existence de dommages collatéraux. L'exemple du bédéiste québécois Guy Delisle, qui a vu son adaptation cinématographique Pyongyang annulée[37], démontre bien l'étendue possible des dommages hors frontières.

L'attribution de responsabilité pose un problème encore plus complexe dans le cas à l'étude. Rappelons que la Corée du Nord nie son implication. Une majorité d'experts[38] en cybersécurité affirment que la thèse nord-coréenne est discutable. Ils jugent la conclusion du FBI de faible portée,[39] premièrement en raison de la rapidité d'exécution de la mise en accusation. Deuxièmement, la preuve est uniquement basée sur l'observation de certaines similarités (logiciels utilisés au cours du hacking, adresses IP provenant de l'infrastructure numérique et outils des hackers) entre l'attaque de Sony et d'autres antérieurement imputées à la Corée du Nord. Allan Friedman croit que la confiance des États-Unis dans l'attribution qu'il qualifie de « surconfiance », est une stratégie diplomatique. En agissant de cette manière, le but est de décourager les autres pays de commettre de tels actes et de prouver que, malgré leur déni d'implication, ils seront indéniablement accusés. (Friedman, 2014)

---

[36] Cette révélation de courriels aura eu raison du poste de la coprésidente de Sony Picture, Amy Pascal; en février 2016, elle est contrainte de démissionner.

[37] Aux lendemains de l'annulation The Interview, une filiale de la 20th Century Fox ayant signé la distribution de l'adaptation de la bande dessinée *Pyongyang*, mettant en vedette Steve Carrel, dont le tournage était prévu en Serbie à compter de mars 2015, a décidé de se retirer du projet. Sans distributeur, le projet cinématographique a dû être annulé au grand désaroi de la communauté artistique.

[38] Nous retenons les experts américains suivants : Scott Borg, fondateur de l'Institut indépendant de recherches Cyber Consequences Unit; Sam Glines, président-directeur général de l'entreprise spécialisée en cyberattaque Norse; Marc Rogers, ex-hacker et Jeffrey Carr, président de l'entreprise de consultation en cybersécurité Taïa Global.

[39] Plusieurs experts ont employé le mot « flimsy » ou « tenuous » pour qualifier l'accusation.

En l'absence de détails fournis par le FBI et de réelles connaissances disponibles sur GoP, les auteurs présumés, les experts ont formulé des hypothèses multiples et parfois contradictoires. Il pourrait s'agir de plusieurs groupes, certains affiliés à Guardians of Peace[40] et d'autres pas, ayant indépendamment géré différentes étapes de l'attaque. Il pourrait aussi s'agir d'un groupe sans affiliation au régime des Kim, mais qui le serait devenu en cours d'attaque.

Au demeurant, les implications associées à ces attributs, particulièrement l'attribution de responsabilité controversée et l'annulation de *The Interview* sous la profération d'une menace terroriste à l'égard du peuple américain, font de la cyberattaque contre Sony un événement sans précédent.

1.4 Le rôle du contexte géopolitique et les ramifications diplomatiques

Le premier point commun aux cyberattaques « est le rôle que joue le contexte ». (Ventre, 2011) Dans le même ordre d'idées, selon Alix Desforges (2014), chercheuse à la Chaire Castex de cyberstratégie, « les conflits relatifs au cyberespace ne peuvent se comprendre en dehors de tout contexte géopolitique ». (Desforges, 2014) Prenons exemple sur le cyberespionnage de Google en 2009, connu sous le nom de l'affaire Aurora. Le géant des navigateurs Web a subi de l'espionnage informatique dont

[40] Le magazine *Wired* note d'ailleurs que la revendication de l'annulation du film par GoP n'est apparue que dans un second temps. Émerge donc un doute à savoir que l'annulation du film ait fait partie du plan initial des cyberattaquants. À cet effet, dans son blogue, l'expert en hacking Marc Roger estime que le film a été un prétexte pour les attaquants. « Ils ont vu là une opportunité pour rigoler et pour convaincre tout le monde que l'attaque était organisée par un gouvernement ». (Roger, 2014) D'autres croient à une guérilla marketing organisée par Sony afin de mousser la promotion du film. Une majorité s'entend sur l'aide de la Chine, en raison des serveurs informatiques nord-coréens hébergés en sol chinois. Enfin, les dernières avancées en date de février 2015, basées sur une étude linguistique du groupe Taïa Global, rapportent que les cyberpirates russes seraient plutôt au cœur de l'attaque.

l'objectif[1], dit-on, fut de recueillir des renseignements confidentiels et précieux sur son fonctionnement. Par le biais de la NSA, les États-Unis ont collaboré à l'enquête et ont attribué la responsabilité à l'Elderwood Gang, une organisation regroupant des espions chinois. Puis, l'entreprise a envisagé d'arrêter la censure de son moteur de recherche en Chine et, advenant l'impossibilité de le faire, a menacé de quitter le pays et de fermer ses bureaux locaux. À cet effet, Ventre explique que l'affaire Aurora est devenue le symbole de l'opposition entre Google et la Chine, et entre les États-Unis et la Chine. « Entre un modèle idéologique, celui de la liberté, des droits de l'homme, et le modèle chinois, celui de la répression et de la restriction des libertés ». (Ventre, 2011)

Généralement, dans un contexte donné, un événement survient dans le monde réel et crée une dynamique d'affrontement entre les acteurs sur le terrain diplomatique, politique ou militaire. (Ventre, 2011) Cette situation particulière est susceptible d'entraîner un prolongement de l'affrontement dans le monde virtuel. À cet effet, il existe un lien étroit entre cyberattaques et incidences politiques, ainsi qu'entre événements politiques et prolongements dans le cyberespace. (Ventre, 2011)

S'il importe à l'offensive, le contexte géopolitique joue un rôle tout aussi important à la défensive. L'attribution de responsabilité et, plus largement, la communication entourant la cyberattaque, ont de quoi occasionner des tensions dans les relations interétatiques (Ventre, 2011) et sont susceptibles de créer des ramifications diplomatiques complexes. (Paquay, 2014)

1.5 L'absence de modèle pour riposter à la cyberattaque

À l'heure actuelle, aucun accord international n'a été signé pour agir d'un point de vue juridique ou législatif en matière de cyberattaque. Plusieurs chercheurs du milieu

académique se penchent avec intérêt sur la question : acteurs gouvernementaux, organisations politico-militaires (OTAN), le Regroupement pour la règlementation d'Internet (The Global Commission on Internet Governance, ICAAN, UIT) et Think tanks (The Heritage Foundation, Centre for International Governance Innovation).

Martin Libicki, professeur et spécialiste américain, résume la présence de deux écoles de pensée. (Libicki, 2013) D'un côté, il y a ce que l'on pourrait appeler les règles de Las Vegas : ce qui se passe dans le cyberespace, reste dans le cyberespace. De ce fait, « aucune cyberattaque, même si elle cause des dommages conséquents, y compris la mort, ne mérite d'entraîner une réponse cinétique ». (Libicki, 2013) L'argument principal ici suggère qu'une riposte risquerait de provoquer des effets dévastateurs pour les populations. De l'autre, il y a le Manuel de Tallinn lancé en 2013 par un groupe d'experts sous la gouverne de l'OTAN. Cette perspective analyse comment le droit international, principalement en prenant comme terrain les conflits armés, s'applique au cyberespace. (Libicki, 2013) Pour eux, « la légitime défense autoriserait les nations à répondre violemment, tant qu'il y a une forme de proportionnalité entre les dommages causés par la cyberattaque initiale et la réponse cinétique. » (Libickie, 2013) Cette supposition s'est vue entérinée en septembre 2014, au sommet de l'OTAN sur la sécurité euroatlantique[41]. L'organisation a alors affirmé que la tâche

[41] L'OTAN, organisation transatlantique pour une défense collective solide, tient ce sommet à un moment charnière pour la sécurité, notamment pour discuter des menaces transnationales et multidimensionnelles qui compromettent la sécurité. Pour plus de détails, se référer au document suivant : Organisation du traité de l'Atlantique Nord (5 septembre 2014). *Déclaration du sommet du Pays de Galles*. [Communiqué].120. Récupéré de http://www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=fr.

lui incombait de décider, au cas par cas, des circonstances d'une invocation de l'article 5[42] à la suite d'un conflit dans le cyberespace.

Malgré cette avancée juridique, il revient actuellement au milieu politique d'interpréter et de fixer sa propre stratégie globale en matière de cyberattaque sur son territoire. « À l'État de choisir la doctrine d'emploi pour gérer la crise et la riposte. » (Huyghe, 2014) Si la riposte peut annoncer un retour à l'équilibre, à la paix, on redoute qu'elle puisse provoquer une escalade de la peur et de la violence. La gestion de la réponse est d'ailleurs tributaire d'un défi encore plus grand : la gouvernance du cyberespace. À ce sujet, le consensus en 2015 s'organise autour de l'idée suivante : elle « doit s'initier dans une approche multipartite et une coopération publique-privée »[43]. Quels que soient les futurs scénarios de cyberattaque, l'élaboration de la riposte risque d'être subordonnée aux développements de la gouvernance d'Internet.

1.6 L'évolution de la cybersécurité aux États-Unis

Les défis posés par la conflictualité croissante du cyberespace engendrent des conditions appelant une révision des paradigmes à partir desquels l'État structure la société. Cette nouvelle donne les incite à se constituer un arsenal défensif et offensif

[42] L'article 5 pose les conditions du droit à la légitime défense en cas d'attaque d'un de ses membres. Pour consulter l'article 5, se référer au pacte *Organisation du traité de l'Atlantique Nord.* (1949, mis à jour en 2008). *Traité de l'Atlantique Nord.* [Entrée en vigueur le 24 août 1949]. Récupéré de http://www.nato.int/cps/fr/natolive/official_texts_17120.htm.

[43] Le consensus actuel en matière de gouvernance du cyberespace est la recherche d'une stratégie globale à l'échelle mondiale. Cet accord se reflète dans les suggestions issues du Global Conference on Cyberspace (GCCS). Rencontre tenue aux Pays-Bas en avril 2015 lors de laquelle les différents participants, représentants des gouvernements, du secteur privé, de la société civile et de la communauté technique, ont conclu que la gouvernance devait s'initier dans une approche multipartite et une coopération publique-privée.

en matière de cybersécurité. Par ce terme, nous entendons l'annonce et la prise de mesures afin d'accélérer la protection des systèmes d'informations et d'accroître la sécurité en ligne de la population. Il s'agit aussi de prévenir les risques de cyberattaque de manière plus adéquate, de gérer les crises, de minimiser les conséquences et de se relever efficacement. Bref, l'objectif de la cybersécurité est de mettre au point une stratégie globale proposant des moyens de cyberdéfense adaptés aux menaces d'aujourd'hui.

Pour le théoricien américain des relations internationales Joseph Nye (2012), nous nous situons dans une nouvelle ère, où le cyberespace attribue la capacité de reconfigurer le pouvoir des gouvernements. Une époque où l'attaquant l'emporte sur la défense, où les petits acteurs souvent anonymes peuvent procéder à une déstabilisation, voire exercer un contrôle sur les grandes puissances étatiques. (Nye, 2012) Il n'est donc pas étonnant de constater que, depuis le milieu des années 2000, un nombre grandissant de nations, dont les États-Unis et la Chine, font de la cybersécurité une priorité à leur agenda. Par conséquent, nous assistons actuellement à une reconceptualisation des modalités de définition et d'application des normes encadrant la sécurité dans le cyberespace.

« Les États-Unis ont été parmi les premiers à assimiler la cybersécurité à une question de sécurité nationale et à élaborer des stratégies visant à lutter contre la série de menaces connexes. » (Porteous, 2010) Les premières traces de cybermenace dans le discours politique américain remontent à l'administration Reagan. (Dunn-Cavelty, 2007) À l'époque, la divulgation d'informations classifiées stockées dans les ordinateurs gouvernementaux suscitait déjà l'intérêt, en raison de la potentialité à être utilisées par des terroristes ou des éléments criminels. Le règlement des conflits relatifs au cyberespace était envisagé dans une perspective juridique où primait l'application de la loi. (Porteous, 2010)

Suite aux événements de septembre 2001, « les problèmes de cybersécurité ont repris une place centrale dans le discours national et au département de sécurité intérieure ». (Burch, 2015) L'accent était donné à la nécessité de se protéger contre la menace. En 2003, avec la parution de *The National Strategy to Secure Cyberspace* (Whitehouse, 2003), le gouvernement Bush affirme que les infrastructures vitales sont menacées de façon physique, mais aussi de manière virtuelle.

À la suite d'une révision de ses politiques en 2007, le pays « annonce la fin du rôle prépondérant joué par l'élément d'application de la loi. (Porteous, 2010) Il importait d'élaborer des stratégies d'action davantage opérationnelles devant « la menace de poursuites faible en raison de l'incertitude entourant l'attribution de responsabilité, des différences entre les législations des divers pays et le manque de coopération ». (Porteous, 2010)

Immédiatement après son élection à titre de 44^{e} président en 2008, Barack Obama commande un examen de la politique américaine sur la cybersécurité. Les conclusions amènent à la création du Cyberespace Policy Review en 2009, dont le but est de mieux protéger les systèmes informatiques américains contre les cybermenaces. La priorité est donnée à trois nouveaux outils : les organismes d'application de la loi, les Forces armées et le bureau de renseignement. (Porteous, 2010) Cet outillage permet de « mieux évaluer la menace, de donner l'alerte, de déterminer la vulnérabilité, de mener des enquêtes pour l'application de la loi et de réagir aux cyberincidents touchant les infrastructures essentielles ». (Parlement du Canada, 2010) C'est d'ailleurs à ce moment que les États-Unis ont commencé à suivre de très près des groupes de pirates chinois qui volaient des informations sensibles concernant la défense, l'énergie et l'informatique. (Traduction libre, Sanger, Perlroth et Shear, 2015)

Depuis ce virage annoncé, nous assistons à la montée du pouvoir donné aux services de renseignements, notamment au FBI et à la National Security Agency (NSA). Ces mesures ont eu pour effet de susciter un débat sur la question de la surveillance de masse. En 2013, les États-Unis ont vu leur image de défenseurs d'Internet se détériorer avec les révélations de l'ex-employé Edward Snowden. L'argument central[44] est basé sur l'estimation des conséquences d'une telle législation qui améliorerait les capacités de surveillance des autorités fédérales sur la population. À ce sujet, il subsiste une vive division[45] politique au sein du Congrès. D'un côté, il y a ceux souhaitant donner davantage de pouvoir à certains organes relevant de l'État et, de l'autre, ceux s'y opposant.

Au début 2014, des vérifications internes déterminent la présence de manquements de sécurité au niveau des systèmes informatiques de la fonction publique. L'administration Obama est alors fortement critiquée pour ses failles dans les structures vitales de la société : Internal Revenue Service, Nuclear Regulatory Commission, Department of Energy, Securities and Exchange Commission et Department of Homeland Security[46]. Dans le contexte des récentes intrusions envers

---

[44] Ce débat existe aussi ailleurs dans le monde; certaines instances gouvernementales poursuivent des buts de réformes similaires et, plus largement, dans l'opinion publique internationale. Au Canada, par exemple, avec le projet de loi C-51 du gouvernement Harper. Généralement reconnu sous l'appellation big data et surveillance dans le milieu académique ainsi qu'en référant à « Big Brother is watching you » du roman 1984 de George Orwell dans l'opinion publique.

[45] En résultante, les tentatives de réforme sur la vie privée sont souvent bloquées. Un exemple probant de cette bipartition est la proposition d'une nouvelle législation, le *Consumer Privacy Bill of Rights*. Introduite par Obama en 2012, mais rejetée au Congrès, cette loi vise à octroyer aux Américains le droit de décider comment leurs informations personnelles en ligne seront collectées et utilisées par les grandes entreprises.

[46] Sanger, Perlroth et Shear, (20 juin 2015). *Attack Gave Chinese Hackers Privileged Access to U.S. Systems*. New York Times. Récupéré de http://www.nytimes.com/2015/06/21/us/attack-gave-chinese-hackers-privileged-access-to-us-systems.html?_r=0.

des entreprises américaines, notamment Sony, Target et Home Depot, Obama a réaffirmé en 2015 la nécessité de proposer une stratégie de cybersécurité plus forte[47]. Dès janvier, il a demandé au Congrès de dorénavant considérer la cybermenace au même niveau qu'il juge le terrorisme. (Obama, 2015) Quatre nouvelles initiatives axées sur la sécurité des données mises en ligne, dont la réintroduction du *Consumer Privacy Bill of Rights,* ont aussi été annoncées. Plusieurs observateurs n'hésitent pas à reconnaître que la démarche gouvernementale est ambitieuse et, qu'en ce sens, la cybersécurité est devenue l'une des priorités centrales de l'administration en 2015.

Pour l'expert Geoff Sanders, le cas Sony représente un point tournant à cet effet, et « marque l'entrée dans le monde du cyberterrorisme. » (Traduction libre, Sanders, 2015) Plus nuancé, le général Watin-Augouard, fondateur du Forum International de la Cybersécurité (FIC), affirme qu'il ne s'agit pas encore de terrorisme, mais que « le stade de l'intimidation, voire de la menace, est dépassé »[48]. En raison du « continuum défense-sécurité, où cyberdéfense et lutte contre la cybercriminalité se composent, la cyberattaque de Sony marque un « tournant dans l'histoire de la cybersécurité [49] ».

Portant le chapeau de puissance hégémonique pour une majorité d'observateurs, la perspective des États-Unis façonne les discussions nationales et internationales en matière de cybersécurité dans les sphères techniques, commerciales et politiques.

---

[47] Obama, B. *Remarks by the President at the Federal Trade Commission.* Notes pour une allocution du premier ministre des États-Unis, Barack Obama, à l'occasion du Federal Trade Commission. 12 janvier 2015. *Constitution Center, Washington.* Récupéré de https://www.whitehouse.gov/the-press-office/2015/01/12/remarks-president-federal-trade-commission.

[48] Watin-Augouard. (1er janvier 2015). *Attaque contre Sony: pourquoi c'est un tournant dans l'histoire de la cybersécurité.* Solutions-numériques.com. Récupéré de http://www.solutions-numeriques.com/attaque-contre-sony-pourquoi-cest-un-tournant-dans-lhistoire-de-la-cybersecurite/.

[49] Op. cit.

(Dunn-Cavelty, 2014) En prenant en charge le volet cybersécurité dans les conflits, les États-Unis institutionnalisent la cyberdéfense et encouragent les autres pays à faire de même. (Ventre, 2015) Effectivement, à mesure qu'ils peaufinent leur stratégie d'actions, leurs plus proches alliés font de même. (Poteous, 2011)

Dans sa forme, ses implications et, plus largement, les transformations des rapports qu'elle engendre, la cyberattaque contre Sony est sans précédent pour l'État américain. Dans le contexte où il s'agit d'une nouvelle forme de conflit ayant un impact sur la cybersécurité et relevant du défi historique de la gouvernance du cyberespace, le cas Sony revêt une importance capitale dans l'étude du discours. La perspective de l'administration Obama suscite un intérêt de recherche très actuel pour comprendre le positionnement de l'État en la matière.

CHAPITRE II

LE CADRE DE RÉFÉRENCE THÉORIQUE

2.1 Le cadrage: une question de perspective

Selon une perspective constructiviste, nous abordons cette deuxième partie avec le principe de cadrage de Robert M. Entman (1993). De sa genèse à son évolution théorique, le concept sera explicité. Puis suivra son rôle dans la sphère politique, sa relation symbiotique avec les médias, l'immanence de la résonance culturelle, le contre-cadrage et le recadrage. S'ajouteront les conclusions d'études de Riker (1996), Callaghan et Schnell (2005), Lakoff (2004) et Azpiroz (2013), entre autres, ainsi qu'un passage sur les relations internationales avec Dunn-Cavelty (2012, 2013) à propos du discours politique de la cybersécurité. Le thème de recherche, nos questions sectorielles et la pertinence communicationnelle de ce mémoire viendront clore ce chapitre.

Mentionnons qu'un tel cadre théorique est nécessaire, voire indispensable à l'étude de notre objet, puisqu'il permet d'analyser le processus de communication par lequel les acteurs politiques construisent leur discours et altèrent la compréhension dans l'espace public.

2.2 Un processus de communication non statique

2.2.1 Le paradigme constructivisme

Fortement influencée par l'un des paradigmes principaux en sciences sociales contemporaines, le constructivisme, notre approche de la connaissance repose sur l'esprit de l'homme en tant que producteur d'une image de la vérité qui se retrouve en interaction avec cette réalité. L'interprétation de la réalité et ses distorsions dépendent de la façon dont l'homme les comprend. L'un des premiers ouvrages s'inscrivant sous le paradigme constructiviste est sans doute *La construction sociale de la réalité,* de Berger et Luckmann, en 1986. Inspirés notamment des écrits de Mead, Durkheim et Marx, le duo d'auteurs considère que la réalité est un construit social. La connaissance n'existe pas sous une forme donnée, elle se concrétise socialement. Appliqué à notre objet d'étude, ce paradigme permet d'envisager le langage employé pour décrire le monde comme étant socialement construit. Dans cette optique, nous considérons l'ensemble des discours à l'étude comme un construit social émanant du plan politique.

Pour mieux comprendre l'effet de la construction du discours sur le public et le sens qui lui est attribué par ce dernier, nous nous affilions au paradigme de l'interactionnisme symbolique. Ce courant a émergé au milieu du XX^{e} siècle avec George Herbert Mead et Herbert Blumer, au département de sociologie de l'Université de Chicago. Ce principe considère l'individu comme un acteur social dont les agissements à l'égard des choses sont accomplis en fonction du sens qu'il leur attribue. Ce sens, formé par l'interaction sociale avec autrui, confère un statut de producteur de ses propres actions et significations. Par un processus interprétatif, ce sens est amené à être modifié par l'individu dans son interaction, selon les circonstances et l'environnement. Aux fins de ce mémoire, nous comprenons que le

sens donné aux discours par le public américain est tributaire du processus interprétatif du public.

En résumé, on considère que le discours politique américain propose sa version de la réalité sur la cyberattaque contre Sony, et cette construction influence la perception de l'opinion publique, des médias et du plan politique.

2.2.2 La théorie des cadres : genèse et définition

En science sociale, la notion de cadrage aurait été introduite par l'anthropologue Gregory Bateson (1955). Il affirmait que les déclarations n'ont pas de significations intrinsèques, mais en acquièrent dans des cadres constitués par le contexte et le style. (Vliegenthart & Van Zoonen, 2011) L'édification du concept a été concrétisée par Erwin Goffman[50] dans *Les cadres de l'expérience* (1974). Goffman avance que selon cette œuvre majeure, pour donner un sens et accorder un degré de réalisme à une situation, les individus mobilisent des cadres. Par définition, un cadre est une avenue d'explication de ce qui se passe, et détermine ce qui est mis de l'avant dans un événement. (Goffman, 1974) Sa théorie implique un processus de sélection de l'information d'où émerge un cadre. Ce dernier guide la structure cognitive de sorte à percevoir une réalité implicite à ses racines culturelles. (Goffman, 1974) De la vie quotidienne au débat public, les cadres permettent au monde social de comprendre une situation puis de la raconter. L'être humain n'est pas conscient de la production

[50] Selon Cefaï et Gardella (2012), *Les cadres de l'expérience* a donné lieu à des interprétations variées, sinon contradictoires. La plus commune est celle que l'on peut imputer à une espèce d'interactionnisme symbolique, mais ils reconnaissent aussi un mixte original et déroutant entre « structuralisme » et «interactionnisme ».

de cadres, qu'il adapte et réadapte inconsciemment en fonction de la situation. (Goffman, 1974)

D'emblée, précisons qu'un cadre constitue un aspect d'un sujet, tandis qu'un cadrage s'exprime tel un résumé des cadres en présence, c'est-à-dire des différents aspects qui composent le sujet.

Dans la première phase de sa chronologie (1974 à 1990)[51], la notion de cadre a été introduite à titre de méthode de recherche pour analyser les médias. En examinant les articles de la presse écrite, Tuchman (1978), Gans (1979) et Gitlin (1980) ont contribué à fournir une base à la littérature. Le premier chercheur en communication ayant contribué à populariser la théorie est le professeur en communication, Robert M. Entman[52].

La deuxième phase (1991-1999) s'ouvre avec la parution de *Framing: Toward Clarification of a Fractured Paradigm* (1993). L'auteur y reconnaît l'abondance de perspectives conceptuelles et d'applications méthodologiques, à laquelle il réplique avec une réorganisation du concept dans une dimension médiatique. Parfois considérée en complément à l'agenda-setting, l'ouvrage d'Entman offre désormais une distinction assumée de ce modèle en proposant une définition plus exhaustive :

---

[51] Vicente and López (2009) reconnaissent trois phases dans le développement de la théorie des cadres : 1974-1990, 1991-1999 et 2000-...

[52] Robert Entman est professeur en médias et affaires publiques à l'Université George Washington et auteur prolifique d'études se référant au cadrage à titre de théorie et de méthode d'analyse.

> (...) to select some aspects of a perceived reality and make them more salient in a communicating text, in such a way to promote a particular problem definition, causal interpretation, moral evaluation, and/or treatment recommendation.

Dès lors, la troisième phase (2000-...) engendre de florissantes recherches[53] empiriques en communication, d'abord orientées vers la presse écrite selon une approche quantitative. (Azpiroz, 2014) Une multitude de définitions ont émergé, dont celle de Reese (2001) qui rend compte de la portée du concept : « Frames are organizing principles that are socially shared and persistent over time, that work symbolically to meaningfully structure the social world. »

À propos de cette définition, le doctorant Julien Auboussier offre un commentaire tout aussi ambitieux et éclairant. Pour le paraphraser, le cadre contribue à structurer l'organisation du monde et l'ordre social, et participe ainsi à la configuration d'un monde commun. (Auboussier, 2009)

Le cadrage prend en considération le rôle joué par les producteurs d'information dans la construction des textes écrits, de la psychologie à celui des milieux organisationnels. Qu'ils soient employés de l'État, d'un média ou d'un groupe social, les communicateurs[54] possèdent la capacité d'altérer la compréhension en attirant l'attention sur certains aspects de la réalité tout en délaissant d'autres facteurs. Comment s'orchestre cette capacité d'altération ? Par la « sélection de certains aspects d'une réalité perçue et par le fait de les rendre plus saillants dans une

[53] Nous retenons les chercheurs suivants : Scheufele (1999) ; Semetko et Valkenburg (2000); Reese (2001; 2007) : Entman (2004, 2010) : Choi, (2006, 2009, 2010); Seo et Lim (2007) et De Vreese (2005-2012).

[54] Par communicateurs, on croit comprendre qu'Entman fait référence au sens large des producteurs d'information : homme politique, rédacteur, journaliste, activiste, lobbyiste, etc.

communication écrite ». (Traduction libre, Entman, 1993) Par la sélection de l'information, on entend le processus de sélection volontaire de certaines informations et l'occultation d'autres. Par rendre saillant, on entend faire qu'une information soit plus visible, significative ou mémorable pour le public. Plus précisément, il s'agit de les rendre plus pertinentes en leur donnant davantage de poids et d'importance à nos yeux. (Entman, 1993) Comment cela s'opérationnalise-t-il ? À travers la présence de certains mots clés, phrases, images stéréotypées et sources qui réitèrent thématiquement des faits ou des jugements. (Entman, 1993) Aussi par l'agencement des mots, leur ordre et organisation dans le texte, leur répétition ou en les associant à des symboles culturellement familiers. (Entman, 1993) C'est dans la manière dont ces informations sont présentées à la conscience humaine que le cadrage parvient à l'influencer. (Entman, 1993) En tant que construction humaine variable en fonction de la conscience dans le temps et à travers les époques, nous comprenons que le cadrage est un « processus de communication non statique ». (De Vresse, 2005)

Si plusieurs niveaux[55] de cadrage coexistent, deux se distinguent cependant. (Reese, 2005) L'un s'attarde à la construction, aussi nommée configuration, du cadre (*frame-building*), à savoir par quel procédé le communicateur construit un cadre. La démarche d'Entman en fait partie, à l'image d'autres typologies, d'ailleurs. Le second niveau a trait aux effets du cadre sur les individus ou la société (*frame-setting*) en termes de « comportements et d'attitudes ». (Resse, 2005) Il s'agit d'analyser la façon dont le public, avec ses connaissances et ses prédispositions, interagit avec un cadre et quels en sont les effets sur l'opinion publique. (De Vresse, 2005) Pour le professeur en communication Shanto Iyengar (1991), ces effets sont compris comme

[55] Dietram A. Scheufele (1999) distingue trois processus : la configuration du cadre [frame-building], l'établissement du cadre [frame-setting] et les effets du cadrage sur l'individu [individual-level effects of framing].

étant des « altérations subtiles dans la définition ou la présentation des problèmes de jugement ou de choix et les changements résultant de ces altérations dans les décisions subséquentes ». (Iyengar, 1991) Sous cet angle, le cadrage facilite la construction cognitive du jugement, processus nécessaire pour appréhender un événement.

2.2.3 Le cadrage dans le discours politique

Les acteurs de l'État utilisent le langage, sous forme de discours oral ou écrit, pour influencer la manière dont une situation doit être interprétée. (Traduction libre, Callaghan & Schnell, 2005) L'origine du cadrage des problèmes associés à la sphère publique remonte à l'édification du débat public sur la gouvernance démocratique. (Callaghan et Schnell, 2005) À cet effet, dans ses études sur le cadrage, Riker (1996) remonte à aussi loin que 1787. Il y relève une confrontation dans l'histoire américaine concernant la ratification de la Constitution. Le cadrage « fédéraliste » estime qu'une gouvernance indépendante est nécessaire pour se prémunir contre une démocratie excessive. À l'opposé, « l'anti-fédéraliste » concède qu'un contrôle du gouvernement est nécessaire pour la démocratie en usant d'expressions clés telles que « Threat to liberty » et « Danger for Consolidation ». (Traduction libre, Riker, 1996)

Le milieu de la troisième phase (1999-...) est marqué par l'intégration d'un plus large corpus de textes et l'application de méthodes qualitatives et mixtes. Dans cette mouvance, l'étude de documents officiels d'État gagne en intérêt dans la communauté de chercheurs. La publication *Don't Think of an Elephant* (2004), du professeur de linguistique cognitive George Lakoff, contribue largement à considérer la théorie des cadres à titre d'outil de communication politique. On se questionne désormais à savoir comment le cadrage est composé par les politiciens et de quelle manière il influence les médias. (Traduction libre, Azpiroz, 2014)

Le cadrage place la communication politique à titre d'élément central de cette sphère, en tant que science et pratique. (Entman, 2005) Il est considéré comme le processus de communication « par lequel les acteurs politiques sélectionnent et établissent les priorités dans leur interprétation et leur explication de la réalité ». (Traduction libre, Entman, 2007) De son côté, Wilson ajoute l'importance de l'argument dans le cadrage, à savoir comment les politiciens construisent les arguments pour présenter un problème au public. (Wilson, 2009) Pour Kinder et Sanders, les cadres sont « inventés et utilisés par les élites politiques, souvent avec un œil sur l'avancement de leurs propres intérêts ou idéologies, et visent à faire des interprétations favorables ». (Kinder & Sanders, 1990) Ainsi, « le cadrage joue un rôle majeur dans l'exercice du pouvoir politique (...), (il) devient l'empreinte du pouvoir, il enregistre l'identité des acteurs ou des intérêts qui ont participé à dominer le texte ». (Traduction libre, Entman, 1993) L'existence du cadre n'est pas à elle seule suffisante pour orienter un débat, une perception, ou occulter une facette d'un problème. Pour demeurer performant, le cadre doit bénéficier à un côté de la médaille plutôt qu'à un autre. (Entman, 2004) Un discours sur une problématique opposant deux pays, dont le portrait serait détaillé en pesant le pour et le contre tout en nuance, apparaîtrait en ce sens moins convaincant pour le public.

Dans le domaine de l'administration publique, le cadrage mène conséquemment à une double vie. Il existe dans la construction du discours des élites et dans le processus cognitif utilisé par le public pour donner un sens à la politique. (Kinder et Sanders, 1990)

2.2.4 La relation d'interdépendance média-politique

Un des points centraux de la pensée d'Entman figure dans le statut particulier du cadrage politique par rapport aux médias. La « Maison-Blanche, ses partisans et ses

détracteurs colportent leur message à la presse dans l'espoir d'un gain d'influence politique ». (Entman, 2004) En effet, le pouvoir du cadrage politique vient de sa capacité à façonner le discours pour les médias et l'opinion publique. Cette autorité demeure cependant tributaire de l'acceptation par les instances médiatiques, mais aussi des autres leaders d'opinion. (Pan et Kosicki, 1993) Dès lors, l'État ne jouit pas d'un pouvoir absolu et d'une influence directe sur les médias. À cet effet, Riker offre une définition plus nuancée du cadrage, un « processus central par lequel les politiciens et les journalistes exercent leur influence politique entre eux et sur le public ». (Riker, 1986) En ce sens, nous croyons que les médias et le gouvernement entretiennent une relation « symbiotique ». (Norris, Kern et Just, 2003)

Plusieurs auteurs mobilisant la théorie des cadres ont fait état de la relation d'interdépendance entre politique et média. Par une méthode d'analyse comparée, l'influence du cadrage politique sur les discours médiatiques a été observée. Les conclusions de l'article de *The U.S. Press Construction of North Korea As Part of the Axis of Evil*, du professeur en communication Jinbong Choi, présente la perception de la Corée du Nord à travers quatre journaux américains. Sur la question de la politique internationale vis-à-vis la Corée du Nord, « la presse rapporte un point de vue similaire à celui du gouvernement américain ». (Traduction libre, Choi, 2006) Dans *The Representation of North Korean National Image in National Newspapers in the United States* (2010), Choi relève la présence d'un cadre dominant anti-Corée du Nord dans la couverture médiatique, véhiculant une image négative du pays.

Dans *News as Propaganda: A Comparative Analysis of US and Korean Press Coverage of the Six-Party Talks 2003–2007* (2013), le professeur en communication Yong Jang Won présente une analyse comparative des cadres dans la presse américaine et coréenne. Ses conclusions démontrent que la couverture médiatique est certes interconnectée à la relation au système médiatique mais aussi à l'intérêt

national, sous le cadre de l'idéologie dominante caractéristique à chaque gouvernement. (Won, 2013)

Dans leur analyse de contenu, les doctorants Jeongsub Lim et Hyunjin Seo (2009) démontrent une forte connexion du *New York Times* au Pentagone. Trois cadres sont identifiés comme étant mis à l'avant-plan dans le discours politique (menace militaire, droits humains et dialogue) pour expliquer les problématiques nord-coréennes. Ces trois mêmes cadres se reflètent dans l'argumentaire déployé par la presse, tout comme leur fluctuation est à l'image de celle du plan politique. Lorsque le discours étatique réduit la magnitude du cadre des droits humains, par exemple, les doctorants observent, au cours du mois suivant, le même schéma dans les pages du journal. (Lim et Seo, 2009)

Enfin, citons l'ouvrage phare *Framing Terrorism: The News Media, the Government and the Public* (2003) de Norris, Kern et Just. Les conclusions de l'interaction entre le gouvernement et les journalistes dans la couverture américaine du terrorisme démontrent que le cadrage médiatique tend à promouvoir un consensus appuyant l'utilisation de la force par l'État. (Norris, Kern et Just, 2003)

Dans le but d'offrir un modèle théorique pour l'étude comparative du cadrage dans la presse et en matière politique, Entman défend un nouveau modèle dans Projection of Power (2004). Un modèle systémique permettant l'étude de la création et de l'évolution du cadrage : le Cascading Network Activation.[56] (Annexe A) Ce dernier décrit l'influence des idées en matière d'affaires étrangères, en tant que processus

[56] Ce modèle a été développé en réaction à l'*indexing* et à l'*hegemony,* deux modèles de communication politique considérant les médias comme étant soumis au plan politique, en lien avec la politique étrangère. Jugeant ces deux modèles obsolètes, il a développé le *Cascading Activation.*

descendant de l'administration jusqu'au public. (Entman, 2003) Nous faisons ici référence à la métaphore de la cascade où, en amont, il existe le système étatique, suivi des élites lui étant rattachées, des médias, de la formation du cadre et, en aval, du public. Son application permet d'étudier la distance entre les versions de la Maison-Blanche et les façons dont les médias communiquent à leur sujet. Ainsi, le modèle prouve que la Maison-Blanche ne détient pas un contrôle sur le discours en matière d'affaires étrangères, puisque les médias peuvent défier sa perspective en présentant un point de vue divergent.

En clarifiant les hiérarchies, le modèle reconnaît la présence d'une double direction dans la cascade. Lorsqu'il arrive en aval, au public, le processus d'influence peut remontrer vers le haut, jusqu'à l'État. Puisque le public s'informe la plupart du temps auprès des médias et non auprès du service de presse du Pentagone, Entman reconnaît une certaine supériorité des médias dans leur capacité d'influencer le public. Les médias prendraient davantage en considération la position du public dans la construction de leurs nouvelles. (Entman, 2004)

À la double direction, Entman reconnaît une compétition entre les deux systèmes. Basés sur une dynamique compétitive, le cadre de la dominance et celui de la contestation s'opposent, se façonnent et se transforment. Qui, entre les médias et l'État, remporte le concours du cadrage et obtient le plus d'influence ? Parfois, note l'auteur, le cadre de l'État est si dominant dans le discours médiatique que les cadres alternatifs dissidents peuvent difficilement se tailler une place dans les discours médiatiques. Tenant compte de la liberté de la presse en Amérique, Entman note qu'il est cependant rarissime d'être témoin d'une telle dominance. (Entman, 2004) Quelques cas font figure d'exceptions, affirme l'auteur, le cadrage du 11 septembre en aura été une dans les premiers mois suivant l'événement. En théorie, lorsque survient une crise, les médias devraient offrir de deux à trois cadres dits contestataires

à celui de l'État. En d'autres termes, les médias devraient proposer différentes manières de présenter le problème, sa cause, son évaluation et sa solution avec une magnitude et une résonance culturelles différentes de celles de l'État. Or, cet idéal qu'Entman nomme le contre-cadrage, s'applique de façon moins importante. La réalité semble variable et se situe quelque part entre la domination complète et un certain degré de contestation. (Entman, 2004)

2.2.5 La résonance culturelle: une condition sine qua non

Pour saisir la portée de la théorie des cadres, il est essentiel d'intégrer la culture, car elle occupe un rôle de premier plan dans la construction des discours. (Entman, 1993) En effet, pour qu'un cadre soit performant, le communicateur, le texte lui-même et son lectorat doivent correspondre à la culture partagée et être compris en ce sens. (Entman, 1993) Communément, cette idée est nommée résonance culturelle. Considérant la culture comme un stock de connaissances, Entman la décrit de la façon suivante : « La culture doit être définie comme des cadres communs empiriquement démontrables, exhibés à la fois dans le discours et dans la pensée des personnes appartenant à un groupe social. »

D'ailleurs, dans ses analyses sur la guerre froide, il reconnaît que les communicateurs, lorsqu'ils composent leurs textes, sont influencés par le contexte culturel. Nécessairement, ils prennent appui sur des normes et comportements jugés légitimes pour être compris du public. Ils prélèvent « des fragments du présent pour les articuler au stock de connaissances » (Auboussier, 2009) Socialement partagés[57]

[57] Auboussier reconnaît que le stock de connaissance est partagé inégalement. Nous estimons en ce sens que le degré d'adhérence dans le monde social face à un cadrage est inégal. À l'intérieur d'une culture donnée, le degré de résonnance est donc variable d'un individu à un autre, d'un groupe social à un autre.

et persistants au fil du temps, les cadres travaillent symboliquement à structurer de façon significative le monde social. (Resse, 2001) Pour Auboussier, l'idée que le cadre n'existe que s'il est partagé et, qu'en ce sens, le cadre est situé entre la production et la réception. (Auboussier, 2009) Avant de s'inscrire dans le discours et d'être interprété par le public, le cadre existe comme pré-élaboration cognitive. (Auboussier, 2009) À cet effet, une proposition de discours dont les idées font ombre ou affront à la culture du public, apparaît risquée, et son degré d'adhérence minimisé.

En somme, le contexte culturel, avec ses codes, ses connaissances et croyances, et le cadrage, dans sa construction et son interprétation, sont intrinsèquement liés. Par conséquent, les études menées selon la théorie des cadres ne peuvent être effectuées sans la prise en compte du contexte culturel.

2.2.6 L'absence de carte blanche : contre-cadrage et recadrage

Intrinsèquement lié à son environnement, le cadrage comporte plusieurs facteurs susceptibles d'interagir entre eux pour restreindre ou favoriser la performance d'un cadre. D'abord, au niveau humain, les élites politiques n'ont pas carte blanche pour construire les cadres selon leur libre arbitre individuel. (Callaghan & Schnell, 2005) Certes, tel que déjà mentionné, leur capacité à créer des cadres performants est reliée à la condition de résonance culturelle. Or, elles dépendent aussi de leur statut, de leur crédibilité et des ressources de leur organisation. (Callaghan & Schnell, 2005) En outre, au niveau institutionnel, elles dépendent du gouvernement américain. Avec le Congrès, le cadrage des problèmes est contrôlé de près par les leaders des parties et le comité de conférence. (Cox et McCubbin, 1993) Ainsi, la latitude du président peut être contrainte par la réticence du Congrès. (Entman, 2004) Prenons l'exemple du débat entourant la légalisation de l'avortement aux États-Unis. D'un côté, l'avortement constituait une question de droit de la femme et de liberté individuelle,

avec une définition du problème mentionnant « third-trimester procedures ». De l'autre, on appelait au droit du fœtus avec l'expression « partial birth abortion ». (Terkildsen et Schnell, 1997) Pour un même problème, on note deux cadrages susceptibles d'activer respectivement différentes valeurs (conservatisme moral, comparativement à traditionalisme religieux). Un tel principe a pour effet de produire différents degrés de soutien chez les politiciens. (Traduction libre, Terkildsen et Schnell, 1997)

Un élément jugé important par Callaghan et Schnell (2005) réside dans la capacité des élites politiques à prendre en considération les autres cadres en présence. Car aucun thème propre à un cadrage n'émerge sans la présence latente d'un contre-thème. (Gamson, 1992) Callaghan et Schnell expliquent cette idée en termes de cadrages et contre-cadrages, auxquels ils attribuent l'expression compétition de cadres. Jouant un rôle significatif dans la communication politique, cette concurrence a lieu entre les différents groupes proposant des cadrages opposés. L'étude sur le contrôle des armes à feu aux États-Unis, suite aux attaques du 11 septembre, illustre bien cette idée. Les partisans de la loi avancent que le terrorisme est favorisé par un laxisme juridique au niveau du contrôle des armes à feu avec l'expression « Guns cause Terrorism ». Les opposants, quant à eux, estiment que les Américains peuvent combattre le terrorisme par l'utilisation responsable des armes à feu en tant qu'outils de défense nationale. L'arme devient ici une solution « Guns stop Terrorism ». (Callaghan et Schnell, 2001)

Il existe cependant des problèmes dont la nature est susceptible de n'offrir a priori aucun contre-cadrage; les affaires étrangères (Callaghan et Schnell, 2005), et ce, spécialement lorsque la Maison-Blanche joue le rôle de premier plan dans la diffusion de l'information. Par exemple, en temps de guerre ou de crise internationale, la Maison-Blanche est souvent amenée à jouer ce rôle. En conséquence, l'habileté du

président à cadrer le problème devient plus prononcée en raison de sa mainmise sur l'information. (Entman, 2004)

Cette emprise semble toutefois de courte durée. Le contrôle du cadrage par un seul joueur apparaît ardu en raison du processus même de cadrage qui repose sur le « *check-in balance* ». (Callaghan et Schnell, 2005) Cette idée de poids et contrepoids fait partie intégrante du concept et contribue à générer un discours aux perspectives diverses, qui profite à l'un, et qui nuit à l'autre. En ce sens, on partage la conception soutenant que « le cadrage trace les frontières d'un débat politique ». (Callaghan & Schnell, 2005)

Au contre-cadrage s'ajoute le recadrage. Callaghan et Schnell l'illustrent avec l'analyse des propos de Bush, au lendemain du 11 septembre. Bush a d'abord utilisé l'expression « Operation Infinite Justice » pour appuyer la solution militaire soulevée pour répondre à l'attaque terroriste. Deux semaines plus tard, lors d'un dévoilement public, cette expression a été remplacée par « Operation Enduring Freedom »[58]. (Callaghan et Schnell, 2005) Donald Rumsfeld, à l'époque secrétaire de la Défense, a justifié ce changement en raison de l'objection du monde musulman. L'expression originale était liée à une finalité de la confession islamique, la justice infinie, que seul Dieu pouvait promulguer. Ce changement est considéré chez les auteurs comme un recadrage visant à justifier la solution militaire proposée par l'État américain. (Callaghan et Schnell, 2005) Le mot « Freedom » remémore aux Américains une démocratie précieuse et contribue à légitimer un recours aux Forces armées. En effet, des sondages ont révélé que 71 % des Américains croyaient fermement que le but de

[58] ND (25 septembre 2001) *Infinite Justice, out - Enduring Freedom, in Tuesday*. Dans BBC News. Récupéré de http://news.bbc.co.uk/2/hi/americas/1563722.stm.

la guerre en Afghanistan était de défendre le « freedom and democracy ». (Callaghan et Schnell, 2005) Précisons que ce cas-ci présente un recadrage avoué en point de presse. D'ordinaire, il est rarement publicisé.

2.3 Panorama des recherches sur le cadrage dans les discours politiques

Dans la prochaine partie, nous présentons les travaux de recherches ayant analysé le cadrage et son application dans le discours politique. Puisqu'aucune étude sur le cadrage politique d'une cyberattaque ou autre cyberévénement n'a pu être recensée, les sujets touchent à la sécurité nationale, au terrorisme et à la cybersécurité. Ces thèmes s'avèrent les plus susceptibles d'entretenir un lien théorique avec le nôtre.

2.3.1 L'évolution du cadre aux É.-U. : de guerre froide à War on Terror

Dans l'oeuvre phare *Framing Terrorism: The News Media, the Government and the Public (2003)*, le trio d'auteurs Norris, Kern et Just identifie deux cadres d'influence auxquels a adhéré la Maison-Blanche. Le premier, celui de la guerre froide, remonte au temps de la guerre du même nom jusqu'aux années 1990. Mis de l'avant pour offrir une compréhension des conflits internationaux, il a toutefois perdu sa cohérence intellectuelle et la constance de sa puissance narrative des suites de la chute du mur de Berlin et à la dislocation de l'URSS. (Traduction libre, Norris, Kern et Just, 2003) Le deuxième cadre, le « War on Terror », est arrivé subitement et tient son nom de l'expression formulée par Bush dans son discours post-11 septembre 2001.

La venue du War on Terror a offert une avenue et un vocable aux politiciens américains et aux journalistes pour construire un nouveau discours. Ce dernier a contribué à donner « du sens à une multitude d'histoires variées; la sécurité

internationale, les guerres civiles et le conflit mondial ». (Norris, Kern et Just, 2003) Il a revêtu plusieurs fonctions. Cognitives d'une part, en unissant des faits, des événements et des acteurs disparates désormais impliqués dans la lutte au terrorisme. Évaluatives, d'autre part, en nommant les assaillants, en identifiant les victimes et en attribuant le blâme, en allouant aux leaders politiques la capacité de communiquer un message simple et cohérent au public, en forgeant la perception en termes de dichotomie, les amis opposés aux ennemis. (Traduction libre, Norris, Kern et Just, 2003) Sa principale fonction est celle de la solution avec l'explication et la justification des hostilités envers les dirigeants de l'Afghanistan, de l'Irak et de la Corée du Nord. C'est d'ailleurs à ce moment que Bush a identifié certains pays soutenant le terrorisme, dont celui au nord du 38^{e} parallèle, avec le qualificatif « axis of evil[59] ». Avec du recul, l'analyse rend compte de répercussions majeures engendrées par le War on Terror dans l'espace public. Il a ouvert le débat sur la « définition du terrorisme, les rôles sociaux et politiques, l'éthique des opérations, la complicité de l'État, les dangers des futures activités terroristes et l'échec de la démocratie ». (Traduction libre, Norris, Kern et Just, 2003)

Dans *Framing American Politics* (2005), Callaghan et Schnell s'interrogent sur l'évolution des politiques américaines en temps de « War on Terror ». Leur analyse fait état d'un discours politique émanant de l'idée de la « défense de la liberté ». (Callaghan et Schnell, 2005) Il s'agit d'une valeur à forte résonance culturelle, car profondément intégrée dans la société américaine. Les auteurs ont découvert que le cadre de la liberté favorise la promotion d'un but caché de l'État : « un plan gouvernemental pour s'introduire dans la sphère privée et, ainsi, dans les droits constitutionnels ». (Callaghan et Schnell, 2005) Cerné de cette manière, le problème a

[59] L'expression formulée par Bush a été répétée dans les discours subséquents et reprise par les médias du monde entier pour désigner, parfois à tort, des pays soutenant le terrorisme.

permis d'altérer le débat public sur la révision des politiques intérieures destinées à prévenir le terrorisme, de sorte qu'il a été plus aisé de modifier certaines lois concernant la « sécurité dans les aéroports, l'immigration, la surveillance électronique, le tribunal militaire, le contrôle des armes à feu, etc. ». (Callaghan et Schnell, 2005) C'est pourquoi est introduite l'idée qu'avec un cadrage autre, le débat et les modifications de lois auraient pu être davantage ardus en raison d'une opposition plus virulente.

De leur côté, Lewis et De Reese reconnaissent le War on Terror comme « un puissant cadre idéologique ». Pour identifier les effets du cadrage sur l'évolution des lois aux États-Unis post-11 septembre, ils ont évalué les cadres selon la typologie d'Entman. Leur analyse démontre que le cadre de la solution est mis de l'avant tandis que les trois autres sont, à différents degrés, occultés. De nature militaire, la solution appelle à l'octroi de pouvoirs spéciaux au président et à l'allégeance politique du peuple envers l'État et son rôle de protecteur de la nation. En se concentrant uniquement sur les mesures à prendre pour vaincre la terreur et en écartant les autres problèmes en présence, le cadrage sert à justifier les nouvelles politiques de sécurité américaines et ses interventions armées à l'étranger, en Irak et en Afghanistan. (Lewis et Reese, 2009)

Générant des conclusions du même ordre, George Lakoff avance que le War on Terror a donné le feu vert à l'administration Bush pour consolider son pouvoir. À ce stade élevé de performance, le cadrage a bénéficié au gouvernement pour faire avancer son programme politique avec une proportion réduite de détracteurs dans l'espace public. À cet effet, il remarque une faible critique quant à l'intervention militaire en Afghanistan, ou encore à l'utilisation des fonds de retraite pour financer la guerre en Irak. (Lakoff, 2004) La faible critique liée à ces décisions est attribuable à la présence du cadre de la définition du problème en termes de sentiment

patriotique. (Lakoff, 2004) En ces temps incertains, la peur d'être accusé d'antipatriotique a largement influencé le processus cognitif des détracteurs potentiels, une démarche nécessaire à la construction de leur perception face aux nouvelles politiques. (Lakoff, 2004)

Jugé contre-productif face à la réelle menace terroriste (traduction libre, Lakoff, 2005), le War on Terror s'est disloqué au milieu des années 2000. Organisé autour du terme « war », il caractérisait une nation sous attaque militaire selon Lakoff, à laquelle on doit appliquer des solutions militaires. Devant la menace terroriste, la guerre n'est pas automatiquement prescrite et les solutions diplomatiques, économiques et politiques devraient d'abord être favorisées. (Lakoff, 2004) Dans cette mouvance, le War on Terror a été remplacé par « Global Struggle Against Violent Extremism ». (Lakoff, 2005) Un cadre plus réaliste, dont la mission reste toutefois imprécise, qui permet d'accorder une plus grande latitude à l'État pour réagir avec une force excessive devant une violence extrême. (Lakoff, 2005) L'effritement du War on Terror au profit d'un autre cadre d'influence permet d'affirmer l'importance du facteur dans l'évolution du cadrage politique. S'ils se transforment, se réinterprètent et disparaissent au fil des années, certains cadres d'influence majeure sont pourtant rarement oubliés. Après une décennie d'abandon, la mémoire collective se souvient toujours du sens de l'expression War on Terror.

2.3.2 Le discours de Bush post-11 septembre 2001 d'après Entman

Pour relever les cadres post-11 septembre conduisant à l'annonce imminente de guerres, Entman a étudié le très attendu discours de Bush en janvier 2002, le State of the Union. Le cadrage présente un problème défini simplement comme un « act of war » causé par un ennemi qualifié de « evil ». Pendant les mois subséquents, Entman remarque que les mots « war » et « evil » sont rendus saillants, car répétés à plusieurs

reprises dans les discours du président et de son administration. L'auteur conclut que le mot « evil » appelle à des pensées et des sentiments de danger, de menace et de peur, conscients et inconscients, à propos des attentats new-yorkais. De plus, il promeut le respect de l'autorité présidentielle dans sa responsabilité à protéger la nation. Avant d'annoncer une guerre, Entman avance qu'il était vital pour l'État de transmettre un cadre sans équivoque et émotionnellement convaincant au peuple américain. (Entman, 2004) En effet, selon l'auteur, la présence de ce cadrage a accru le sentiment de peur des Américains.

Quant aux solutions identifiées, elles visent à unir le pays derrière la nécessité de la guerre contre le terrorisme et l'intervention militaire pour renverser le gouvernement afghan. Plutôt que d'appeler pour les sacrifices de la population civile, en proposant, par exemple, une hausse d'impôts pour couvrir les coûts, Bush a fait tout le contraire. Il a invité les Américains à s'unir et à consommer davantage, en plus de réclamer auprès du Congrès une réduction d'impôts. En proposant des solutions qui ne sont pas impopulaires à l'Américain moyen, Bush a gagné en respect, alors qu'il suggérait la pénible idée de la guerre.

2.3.3 Le discours de Bush sur le War on Terror suivant l'opinion d'Azpiroz

Avec un échantillon composé d'un seul et unique discours, la doctorante espagnole Maria Azpiroz s'est penchée sur la perspective de Bush en février 2005, dans *Framing as a Tool for Mediatic Diplomacy Analysis: Study of George W. Bush's Political Discourse in the « War on Terror »*. Sa méthodologie est basée sur la typologie des fonctions du cadrage d'Entman.

Ainsi, Azpiroz met d'abord en lumière le contexte historique et politique de l'époque basé sur la guerre contre le terrorisme, une stratégie de politique étrangère axée sur la

lutte contre le terrorisme international. La première initiative militaire était la guerre en Afghanistan, avec le soutien de plusieurs. Toutefois, la décision de Bush d'intervenir en Irak a trouvé un soutien moins politique et populaire. Renouvelant son deuxième mandat de président, Bush s'est rendu en Europe avec l'objectif de rétablir de bonnes relations avec les membres de l'Union européenne et de l'OTAN.

Les conclusions démontrent une nette prédominance de la fonction évaluative basée sur un jugement moral, comme par exemple entretenir de bonnes relations euro-américaines et de faire avancer le démocratie dans les pays du Moyen-Orient. La fonction solution se distingue également par l'amélioration des relations américaines avec l'Union européenne et au sein de l'OTAN, de même que par l'évolution de l'OTAN et le défi que le terrorisme et le statu quo de la tyrannie et le désespoir au Moyen-Orient représentent. (Traduction libre, Azpiroz, 2013) Dans ce dernier cas, Bush présente également des solutions spécifiques proposées selon différents problèmes : le conflit israélo-palestinien, la consolidation de la démocratie en Afghanistan et en Irak, le développement iranien des armes nucléaires, etc. En revanche, la définition du problème et la cause demeurent plus rares. Le problème est présenté comme une situation de crise dans la relation entre les États-Unis, l'Union européenne et l'OTAN. Tous trois sont confrontés au défi commun de l'instabilité et du terrorisme au Moyen-Orient. Ce déséquilibre est attribuable, selon l'auteur, au fait qu'en 2005, la guerre contre le terrorisme avait déjà été détaillée maintes fois, et la cause jugée inutile à mettre de l'avant.

La saillance de ce contexte se présente sous forme de mots clés, les plus répétés étant : démocratie, liberté, paix, valeurs, sécurité, alliance et terreur (avec leurs dérivés). Azpiroz y relève des images spécifiques non seulement en raison de leur répétition, mais aussi eu égard à leur contenu symbolique ou à leur forte résonance culturelle. De plus, les expressions les plus remarquables, qui transportent des

charges symboliques importantes, correspondent normalement à certains mots clés. Tel est le cas avec l'utilisation du terme « libération » pour faire référence à l'intervention militaire en Irak. (Traduction libre, Azpiroz, 2013) Une grande partie des opposants à cette guerre, que leurs voix soient médiatiques, politiques ou universitaires, ont commenté ce choix de mot. Pour eux, le terme « invasion » associé à l'intervention militaire en Irak était plus justifié que le mot « libération ». (Traduction libre, Azpiroz, 2013) Or, Bush a préféré ce dernier, puisqu'il entretenait une résonance plus forte selon les valeurs américaines inscrites dans la Constitution.

Enfin, Azpiroz relève plusieurs allusions et références à l'histoire américaine et européenne, venant appuyer la valeur de la liberté en la rendant plus significative. Par exemple, Bush concède que le progrès de la liberté a contribué à accroître la paix dans le monde lors de Seconde Guerre mondiale et de la guerre froide. L'auteur y voit un moyen efficace de déclencher une résonance culturelle avec le public, tout en encourageant la compréhension et l'acceptation du message.

2.3.4 Le code Obama d'après Lakoff

Estimant qu'ils constituent un objet de recherche prolifique dans les études en communication, notre attention fut portée sur les discours de Bush. Loin de bénéficier d'une telle littérature, le cadrage des discours de l'actuel président Barack Obama est brièvement abordé par George Lakoff. En observant différents textes officiels sur plusieurs sujets, Lakoff dégage ce qu'il nomme le « code Obama ». La perspective générale du président pour discourir de sujets critiques s'oriente sur ce que signifie le fait d'être un Américain, d'être patriotique, d'être un citoyen et de partager tous ensemble les sacrifices et les victoires du pays. (Lakoff, 2009) Puisqu'elle est basée sur les valeurs communes à forte résonance culturelle, l'affiliation dont parle l'État va au-delà de l'idéologie politique. (Lakoff, 2009) La nécessité de s'affilier pour

combattre les problèmes de la société reste donc plus susceptible d'être comprise et acceptée par le public. Cela particulièrement en temps de crise, où la vision est moraliste et l'idée de l'unité du peuple omniprésente. (Lakoff, 2009) Quoique le propos de Lakoff présente un portrait général du cadrage d'Obama, voire en surface, ses conclusions indiquent que le patriotisme et l'idée de s'unir traversent autant les époques que les différentes administrations.

2.3.5 Le discours sur la menace relative à la cybersécurité selon Dunn-Cavelty

Considérant que notre objet de recherche, le discours sur la cyberattaque, s'inscrit dans le domaine plus large de la cybersécurité, nous retenons les travaux de Myriam Dunn-Cavelty[60]. Son intérêt de recherche porte sur les risques politiques et l'incertitude dans les normes de sécurité, ainsi que l'évolution de la sécurité nationale et internationale en raison des cyberincidents. Dans une perspective constructiviste axée sur les relations internationales, l'auteure s'est penchée sur la représentation de la menace relative à la cybersécurité dans les discours politiques. Considérant son assise théorique issue des sciences politiques, nous relevons des similitudes entre les résultats de Dunn-Cavelty et ceux des auteurs présentés, monopolisant la théorie des cadres. Les conclusions confèrent davantage de pertinence à ce mémoire.

Dans *The Militarisation of Cyberspace: Why Less May be Better* (2012), la cybersécurité est présentée comme l'une des questions de sécurité nationale les plus pressantes de notre époque. En raison de cyberattaques sophistiquées et très médiatisées, la cybersécurité constitue une préoccupation stratégique et militaire pour de nombreux États. (Dunn-Cavelty, 2012) L'auteur avance que le discours politique

[60] Pour en savoir davantage sur les travaux de Dunn-Cavelty, consulter son site Web : http://www.myriamdunn.com/index/Welcome.html.

sur la cybersécurité fait fausse route à trois égards. D'abord, le discours évoque l'image de l'ennemi alors qu'en fait, il n'y a pas d'adversaire identifiable, puisqu'il est souvent impossible de le reconnaître. Puis il met l'accent sur des mesures propres au domaine de la sécurité nationale, plutôt que sur des solutions économiques et entrepreneuriales. Enfin, il présente de manière erronée l'État comme pouvant exercer un contrôle sur le cyberespace. Cela a pour effet de créer une atmosphère d'insécurité et de tensions dans le système international, non sans effet sur la mauvaise interprétation de la nature et du degré du cyber-risque, mais aussi de la faisabilité des différentes mesures de protection dans un monde complexe où le risque est interdépendant. (Traduction libre, Dunn-Cavelty, 2012) En guise de conclusion, l'auteur rappelle la nécessité d'une juste représentation de la cybersécurité, en fonction d'une information qui revêt à la fois qualité et équilibre.

En 2012, Dunn-Cavelty critiquait le manque de solutions économiques proposées pour une gestion plus efficace du problème. En 2015, Ventre avance que ce type de mesures est de plus en plus privilégié. Lorsque les dirigeants politiques prennent la parole en matière de cyberdéfense, « ce n'est pas seulement une question de sécurité, mais également d'économie ». (Ventre, 2015) La présence d'enjeux économiques est désormais en filigrane du discours politique. Une économie, une industrie est en train de se créer, des relations entre l'armée et le secteur industriel, des passerelles entre les deux mondes. » (Ventre, 2015)

Dans *From Cyber-Bombs to Political Fallout: Threat Representations with discourse* (2013), Dunn-Cavelty identifie différentes représentations de menaces associées au cyberespace dans les propos de différents acteurs : des hackers, en passant par les experts, jusqu'aux politiciens. Chez ces derniers, elle cherche à savoir comment ces types de menaces sont représentés dans le discours politique, à titre de problèmes de sécurité nationale, et comment ces représentations peuvent façonner les pratiques de

cybersécurité d'un gouvernement. Particulièrement riche en métaphores, cette figure de style est utilisée comme un puissant mécanisme pouvant façonner les perceptions. (Dunn-Cavelty, 2013) De cette façon, lorsqu'ils parlent de cybermenace, les acteurs politiques utilisent un réservoir de représentations à différents degrés et de multiples manières. (Dunn-Cavelty, 2013) « Le plus souvent, elles sont utilisées pour mobiliser et pour prouver qu'il est essentiel de poser plus d'actions, avec plus d'énergie, dans le but de contrôler le cyberespace (...) ». (Lawson, 2012) Dunn-Cavelty explique que la nécessité d'avoir recours constamment à la mobilisation provient du fait qu'il existe peu de données fiables sur le niveau réel du risque et qu'aucun cyberévénement n'a causé à ce jour des dommages apocalyptiques. (Dunn-Cavelty, 2013) Conséquemment, les acteurs politiques sont convaincus qu'une action plus immédiate reste nécessaire, et ils pointent des situations potentiellement graves (Dunn-Cavelty, 2013) pour tenter d'encourager le changement politique.

Avec la présentation du panorama des études sur la théorie des cadres et, plus globalement, à celle sur la cybersécurité, nous avons démontré que l'étude du cadrage peut s'opérer de manière générique, constituant une ligne de parti, par exemple, ou spécifique, faisant l'objet d'un discours unique dans un contexte particulier. Les propos de l'État américain se distinguent par l'importance octroyée au cadre de type solution. Détourner l'attention du problème, de sa cause ou de son évaluation, oriente la teneur du débat vers les solutions proposées. Si d'autres cadres sont mis de l'avant parallèlement à la solution, leur contenu fait souvent référence aux valeurs américaines, principalement la liberté[61] et le patriotisme. Ces valeurs, soit l'appel à la mobilisation à l'effet de s'unir dans le but de résoudre un problème, viennent appuyer

[61] Le concept de liberté ou plus spécifiquement celui de la liberté d'expression revient souvent dans les études présentées. Ce mémoire aurait bénéficié de références théoriques portant sur le discours de la liberté d'expression lors de cyberattaques. Or il n'a pas été possible d'en repérer. Dans le champ communicationnel, la littérature sur la liberté d'expression associée au cyberespace est relativement récente. Elle se consacre davantage à analyser le rôle de la technologie dans le changement sociétal en contexte non-démocratique ou encore le débat sur un Internet libre de censure.

l'idée de l'urgence d'agir et mettre en place des solutions. Ces valeurs partagent la caractéristique de posséder un haut degré de résonance culturelle auprès du peuple américain. Un concept essentiel à la compréhension du discours et pour lequel plus le degré est élevé, plus l'adhésion aux idées proposées augmente. Avec un tel cadrage, certaines annonces de mesures politiques qui, d'ordinaire, seraient moins bien perçues, le sont davantage, et ce, encore plus en temps de crise ou de guerre. Nous comprenons que le cadrage est un puissant processus de communication fournissant des outils aux acteurs politiques afin d'orienter leur discours dans l'intention de favoriser le changement des normes intérieures et étrangères.

2.4 Questions centrale et sectorielles

Au contact de la littérature, l'orientation de notre questionnement de recherche prend forme. La problématique d'ensemble a permis de saisir que dans sa forme, ses implications, ses conséquences sans précédent et la transformation des rapports qu'elle engendre, la cyberattaque contre Sony revêt une importance particulière pour la cybersécurité américaine. De plus, nous avons démontré que l'État américain endosse le rôle d'acteur principal dans le règlement de ce conflit. Pour sa part, la revue de la littérature a permis de démontrer que le cadrage dans le discours politique est une conception de l'homme qui se veut un puissant outil pour orienter les discours selon les intérêts politiques. En ce sens, notre intérêt porte sur celui de l'administration Obama. À cet effet, nous formulons la question centrale suivante : comment s'articule le cadrage de la cyberattaque contre Sony dans le discours de l'administration Obama ?

Nous postulons que le cadrage de l'administration Obama sur la cyberattaque de Sony s'articule à travers l'omniprésence de solutions, tend à favoriser le changement

de politiques et contribue à marquer un point tournant pour la cybersécurité américaine.

Dans le même ordre d'idées, trois questions sectorielles, dont la première comporte des sous-questions, appuient notre démarche :

1. Quel est le cadrage de la cyberattaque contre Sony dans le discours de l'administration Obama ?

   Comment le problème est-il défini ? Quelles sont ses causes ? Que suggèrent ses évaluations ? Quelles solutions sont proposées ? Quels cadrages sont ignorés et quels sont ceux mis de l'avant ?

2. Comment le cadrage de la cyberattaque contre Sony tend-il à favoriser le changement politique ?

3. Comparativement au cadrage générique de la cybersécurité, comment le cadrage de la cyberattaque contre Sony contribue-t-il à marquer un point tournant dans la cybersécurité américaine ?

Cette recherche offre une perspective communicationnelle sur un nouveau phénomène, la cyberattaque, pour lequel la littérature reste à ce jour sous-développée dans le champ communicationnel. (Kadhivar, 2015) Toutes disciplines confondues, nous n'avons pu relever l'existence de recherches visant à analyser le discours de communication politique ayant trait à une cyberattaque, et ce, du point de vue d'un État qui en accuse un autre. Analyser la construction du cadrage facilite la compréhension du discours politique en termes de définition du problème, de causes, d'évaluation morale et de solutions. Dans le contexte où la cyberattaque est devenue un enjeu de cybersécurité mondial, susceptible d'affecter la stabilité géopolitique et la diplomatie, mais aussi la sécurité des citoyens du monde, il devient pertinent de se pencher sur une telle analyse. Cette dernière constitue un point de départ névralgique pour comprendre le positionnement de l'État en matière de cyberattaque et, plus largement, en matière de cybersécurité.

CHAPITRE III

LA MÉTHODOLOGIE

3.1 L'analyse de discours et l'approfondissement des cadres

Dans cette troisième partie, nous tenterons d'avancer une définition non exhaustive du discours. Subséquemment à une approche herméneutique sera explicitée la méthode de collecte des données, celle de l'analyse des cadres d'Entman (1993). La composition du corpus et enfin la démarche de traitement des données, termineront ce chapitre. Cette méthodologie nous semble la plus pertinente puisqu'elle nous permet d'identifier, de décrire, d'extraire et d'analyser les différents cadres en présence dans le discours, pour ensuite les comparer et les interpréter en regard de l'aspect théorique.

3.2 Le discours : a priori historique, rapports de force et procédures de contrôle

Constituant à la fois une notion polysémique et un élément de controverse dans les sciences sociales, le discours pourrait à lui seul faire l'objet d'un mémoire. Par conséquent, nous proposons une définition non exhaustive. Instable dans sa forme et critiqué dans sa construction théorique et méthodologique, le discours reçoit une définition très variée en fonction des approches et des courants de pensée. Les approches se trouvent aussi bien en sciences du langage que dans les sciences politiques, la rhétorique, l'histoire, les sciences de l'éducation, la sociologie et la

communication. Le discours est tantôt associé aux conversations entre individus, aux débats télévisés, aux contenus politiques, à la presse écrite ou à la publicité, et ce, dans une perspective allant de critique à pragmatique. (Maingueneau, 1996) Il est généralement admis que le discours peut être conceptualisé en tant que texte ou pratique discursive dans un but de production, de distribution ou de consommation. Dans le cadre de ce mémoire, nous privilégions une conceptualisation en tant que pratique sociale liée à l'idéologie et au pouvoir.

Pour l'aborder sous cet angle, on s'inspire fortement de l'école française[62] mise sur pied dans les années 1970, où s'articule la linguistique aux travaux sur l'idéologie, la psychanalyse et le marxisme. En raison de son influence unique sur l'analyse de discours, trois éléments de la théorie du philosophe français Michel Foucault apportent une clarification pertinente dans le cadre de ce mémoire : les formations discursives, l'intertextualité et l'ordre du discours.

D'abord, le discours se définit chez Foucault dans un large triptyque, « tantôt domaine général de tous les énoncés, tantôt groupe individualisable d'énoncés, tantôt pratique réglée rendant compte d'un certain nombre d'énoncés ». (Foucault, 1969) Plus précisément, le philosophe définit le discours comme « un ensemble d'énoncés en tant qu'ils relèvent de la même formation discursive » (1969).

[62] Nous partageons également l'assise théorique anthropologique plutôt associée à l'école américaine.

Par formation discursive[63], il entend un vaste concept pour lequel il existe un a priori historique[64] :

> Un ensemble de règles anonymes, historiques, toujours déterminées dans le temps et dans l'espace qui ont défini à une époque donnée, et pour une aire sociale, économique, géographique ou linguistique donnée, les conditions d'exercice de la fonction énonciative. (Foucault, 1969)

Avant tout, Foucault s'intéresse à la question du savoir/pouvoir en analysant certains événements du contexte social en tenant compte de leur dimension historique. Il suppose l'existence de l'édification de la réalité à travers l'acte langagier. Dans *L'Archéologie du savoir* (1969), il questionne d'ailleurs largement l'existence d'un moment fondateur d'un texte en s'associant au concept d'intertextualité[65]. Par essence, l'intertextualité implique une « coprésence » plus ou moins explicite entre deux ou plusieurs textes. (Genette, 1982) Le processus de création d'un texte est immanent à un ensemble d'écrits, émanant de différents individus, à diverses époques

---

[63] Par formation discursive, nous retenons la définition reprise par le philosophe français et spécialiste de l'analyse du discours, Michel Pêcheux. En rejoignant les propos de Foucault, Pêcheux en fait une distinction en raison de son association au marxisme althussérien. Il avance que toute « formation sociale implique l'existence de positions politiques et idéologiques qui ne sont pas le fait d'individus mais de formations entretenant entre elles des rapports d'antagonisme, d'alliance ou de domination ». (Pêcheux, 1990) Qualifiées d'idéologies, ces formations « incluent une ou plusieurs formations discursives inter-reliées, qui déterminent ce qui peut être dit à partir d'une position donnée dans une conjoncture donnée ». (Pêcheux, 1990)

[64] Dans sa proposition d'une nouvelle approche de la sociologie de la connaissance, la sociologue Reiner Keller (2007) observe que Berger et Luckmann affirment l'existence d'un « a priori historique (et social) des systèmes symboliques (...), car ils sont le résultat ou l'effet pervers d'une production historique collective ». (Keller, 2007) Cette conception est partagée par Michel Foucault. (Keller, 2007) À cet effet, il est « rarement considéré que Foucault suivait dans ses études historiques une démarche analytique en affinité avec la tradition qualitative en sociologie ». (Kendall et Wickham, 1999) Nous nous appuyons donc sur les propos de Keller pour s'inscrire en continuité théorique avec Michel Foucault.

[65] L'édification de l'intertextualité a été introduite par Julia Kristeva, dans *Sèmiôtikè* (1969).

et en des lieux distincts. Tous les discours seraient de ce fait interdépendants. (Foucault, 1969) En nous appuyant sur l'intertextualité, nous sommes d'avis que les textes de l'administration Obama, considérés comme les éléments constitutifs d'un discours, ont préexisté au moment de leur formulation. En ce sens, le discours politique sur la cyberattaque contre Sony ne constitue pas de nouveaux propos ayant émergé pendant la cyberattaque. Malgré le statut de phénomène relativement récent de la cyberattaque et la nature sans précédent de l'événement Sony, le discours à leur sujet ne serait pas nouveau en soi. Il puise spontanément son sens dans l'historique des discours préexistants, ceux caractérisant la relation conflictuelle États-Unis-Corée du Nord, ou encore ceux de la guerre au terrorisme depuis le 11 septembre 2001, pour se réactiver en fonction de la cyberattaque contre Sony. Déjà comprise et acceptée par le public, la préexistence est caractérisée notamment par le cadre du « War on Terror » et le cadre anti-Corée du Nord, explicité au chapitre II.

Parmi les divers écrits, Foucault reconnaît la relation du texte à son contexte de production. Régi par des procédures de contrôle, le discours est conditionné par un ensemble de règles associées à un contexte de production. Il en résulte une altération dans le contenu du discours. Le philosophe en fait d'ailleurs un postulat central dans *L'Ordre du discours* (1971) :

> Dans toute société, la production du discours est 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)

Par ailleurs, tout discours s'articule en rapport avec un pouvoir qui détermine les procédures de contrôle pour former des énoncés socialement acceptables[66]. Sous l'angle foucaldien, la notion de pouvoir relève « de la multiplicité des rapports de force qui sont immanents au domaine où ils s'exercent, et sont constitutifs de leur organisation (...) ». (Foucault, 1976) Les stratégies dans lesquelles prennent effet ces rapports de force sont une forme terminale du pouvoir et non le pouvoir lui-même. (Foucault, 1976) En ce sens, nous comprenons qu'il existe de multiples rapports de force au sein de l'État, où s'imbriquent des stratégies impliquant des relations de conflit à travers lesquels se manifestent différentes formes et aspects de pouvoir. Le discours politique à l'étude est intrinsèquement lié à une représentation de la réalité défendant des formes de pouvoir propres à l'administration Obama.

L'analyse du discours foucaldien est comprise par Mainguenau comme « l'étude de vastes configurations, où se mêlent textes, institutions et comportements. » (Maingueneau, 2012) Cette conception demeure cependant « très loin du train-train quotidien empirique » et est dépouillée d'appareil méthodologique (Keller, 2007) pour mener une analyse.

Pour approfondir les rapports de force qui sous-tendent le discours, nous nous référons au concept de communication politique. Dominique Wolton la conceptualise en opposition à l'idée classique qui la réduit à une stratégie pour faire passer un message. (Wolton, 1995) Il s'agit plutôt d'un espace fragile d'affrontements discursifs. C'est le terrain où « s'échangent les discours contradictoires des trois acteurs qui ont la légitimité de s'exprimer publiquement sur la politique : les hommes politiques, les journalistes et l'opinion publique au travers des sondages ». (Wolton,

[66] Cette conception rejoint l'idée d'Entman, à savoir que pour être performant, un discours doit avoir un certain degré de résonance culturelle.

1989) Dans la communication, « il y a toujours mobilisation de ressources différentes, contradictoires, qui s'opposent dans un jeu dynamique, dont l'enjeu est toujours le pouvoir ». (Wolton, 1995) Cet enjeu repose sur la maîtrise de l'interprétation de la réalité dans une perspective qui est toujours liée à la prise de pouvoir, ou à son exercice. (Wolton, 1995) En effet, les acteurs politiques ont recours à divers procédés rhétoriques et à des stratégies de persuasion et de séduction (Charaudeau, 2005) dans le but d'influencer l'opinion sociétale. Pour y arriver, le procédé reconnu s'organise sur la sélection des thèmes et des problèmes sur lesquels se règlent les affrontements cognitifs et idéologiques du moment. (Wolton, 1995) Cette proposition rejoint fortement notre cadre de référence théorique : le cadrage.

À titre d'instrument de l'accès au pouvoir, la communication politique joue un rôle central lors d'une crise impliquant un positionnement de l'État. En effet, lors d'une cyberattaque, par exemple, la communication politique a un « impact sur la manière de gérer l'incident, sur la sécurité et parfois sur la dimension économique, politique ou sociale ». (Ventre, 2013) Cette communication est également susceptible de créer un climat de peur au sein de la population et d'influencer les rapports entre États (Ventre, 2013) et à l'intérieur même de l'État. Ventre s'interroge sur la nature du message à communiquer lorsque survient une cyberattaque. Comment l'exprimer ? Quoi dire ? Assurer une communication large ou restreinte ? (Ventre, 2011) Sous quel angle doit-on définir le problème ? En ce sens s'orchestre nécessairement une stratégie de communication politique de la part de l'État qui se traduit dans ses discours.

Dans cette optique, le discours confère un sens aux diverses situations. En regard de son a priori historique, des rapports de force et des procédures de contrôle qu'il suscite, il contribue à structurer le monde social. Son analyse devient fondamentale pour approfondir la compréhension d'une réalité perçue, autant par ses évidences que

par ses subtilités. Cela est vrai particulièrement lors de l'émergence de nouveaux phénomènes venant troubler l'ordre social, où entrent en jeu des rapports de force associés à différentes formes de pouvoir.

3.3 La méthodologie qualitative : analyse des cadres

Notre choix s'arrête sans surprise sur une méthode qualitative, celle de l'analyse de discours. S'inscrivant en constance directe avec notre cadre de référence théorique, alors que nous considérons que le cadrage par les acteurs politiques se déploie généralement dans leurs discours, nous sélectionnons la méthodologie de l'analyse des cadres d'Entman (1993).

Constituant un pôle dominant en sciences sociales, principalement en journalisme, l'analyse des cadres permet d'étudier les discours oraux ou écrits de tous acabits, pourvu qu'ils soient sous forme de verbatim. À large spectre, l'objet de cette méthodologie peut constituer « un problème, un événement ou des acteurs, aussi bien des individus, des groupes ou des nations ». (Entman, 1993, 2004, 2010) La cyberattaque de Sony, événement problématique impliquant différents acteurs, dont deux nations, est en parfaite adéquation avec le modèle méthodologique sélectionné. De plus, comme le suggère Norris, un événement impliquant la Corée du Nord et les États-Unis est susceptible de faire l'objet d'une telle analyse. (Norris, Kern et Just, 2003)

Nous nous intéressons uniquement à la construction du cadre et du cadrage, et non à l'analyse de leurs effets en termes de comportements et d'attitudes au sein de l'opinion publique. Certes, la perspective de l'administration Obama à propos du cas Sony influence la compréhension des politiciens, des médias et des Américains. Bien que l'analyse des cadres propose une méthodologie pour en rendre compte, nous ne

pouvons considérer l'analyse de l'effet des cadres[67] pour des raisons de circonscription de l'objet d'étude. Il en est de même du modèle en cascade d'Entman. De ce fait, notre analyse se concentre uniquement sur le premier système du modèle, l'État américain.

Indépendamment des sujets, l'analyse qualitative du cadrage est effectuée selon une matrice [68]. Celle d'Entman vise à identifier comment le producteur de discours structure son propos selon quatre fonctions : la définition du problème, sa cause, son évaluation et sa solution. (Entman, 2003) Le premier cadre, la définition du problème, s'exprime par la sélection et la saillance de certains des aspects pour identifier le problème. Souvent, en termes d'effets ou de conditions illustrant une problématique, il détermine la teneur des autres cadres. Sa présence justifie fréquemment les autres cadres, souvent celui de la solution. Ensuite, le diagnostic de la cause détermine ce qui crée le problème. Quant à l'évaluation, elle implique un jugement moral et s'exprime souvent par la présentation des acteurs sous la dichotomie simpliste des bons versus les méchants. La dernière fonction, celle qui mène à la solution, implique des justifications et la proposition d'effets potentiels observables suite à l'application ou non de la solution. Elle est généralement proposée en vue de faire la promotion des actions du gouvernement. (Entman, 2003) Introduisons brièvement ce modèle par les résultats de l'étude d'Entman sur le cadrage des événements du 11 septembre 2001 dans la presse américaine :

---

[67] Prenons l'exemple de Dietram A. Scheufele quant aux niveaux d'effet du cadrage sur l'individu dans *Framing as a Theory of Media Effects* (1999).

[68] Un nombre limité de typologies des cadres existe pour effectuer une telle analyse. Nous reconnaissons notre intérêt envers Semetko et Valkenburg (2000) proposant une matrice d'analyse d'événements en période de crise. Composée de cinq cadres (attribution de responsabilité, conflit, intérêt humain, valeur morale et conséquence économique), cette matrice aurait été pertinente à notre objet d'étude. Nous privilégions cependant la typologie d'Entman, reprise par Azpiroz, pour sa renommée auprès de la communauté de chercheurs.

> The problematic effect was the death of thousands of civilians in an act of war against America; the cause was terrorists; the moral judgment condemned the agents of this assault as evil; and the remedy quickly became war against the perpetrators. (Entman, 2003)

Dans ce cas type, la définition du problème et la solution dépendent l'une de l'autre et sont mises de l'avant dans le but d'unir le pays derrière la guerre contre le terrorisme, tandis que la cause et l'évaluation sont laissées pour compte. (Entman, 2003)

En résumé, la typologie d'Entman constitue un point de départ névralgique pour comprendre la perspective de l'État par rapport au phénomène de la cyberattaque de Sony et la cybersécurité. Cela rejoint un point de vue qualitatif, puisque cette étude vise à identifier et à extraire les différents cadres en présence dans six discours formulés à partir d'un même sujet. Ils sont ensuite résumés en termes de cadrage propres au motif, pour finalement être interprétés.

Nous sommes conscients de l'utilisation fréquente de la méthode quantitative ou mixte en analyse des cadres. En généralisant des résultats statistiques visant la neutralité et l'élimination de la subjectivité, la méthode quantitative s'inscrit moins, selon notre humble avis, en adéquation avec notre approche herméneutique qui sera présentée dans la prochaine section.

Une seconde typologie apparaît pertinente pour ce mémoire. Dans *News Framing* [69] (2005), le Néerlandais Claes H. De Vreese distingue deux types de cadrages : ceux dits spécifiques à un thème et ceux dits génériques. Les premiers renvoient à un thème, à un phénomène et à un acteur spécifique. Les seconds font référence aux

[69] Malgré que cette distinction soit appliquée au cadrage des médias par De Vreese, nous croyons qu'il est possible de l'appliquer au cadrage politique.

cadres généraux applicables à divers thèmes, phénomènes ou acteurs. En regard de notre objet d'étude, nous considérons le cadrage de la cyberattaque contre Sony comme étant spécifique, prenant forme à l'intérieur de celui plus générique de la cybersécurité.

En vue d'expliquer la méthode de l'analyse des cadres, la littérature réfère parfois à la métaphore du photographe. Avant de prendre une photographie, le professionnel sélectionne un cadre pour capter l'image qui s'offre à lui. Par exemple, il zoome inconsciemment sur un objet en particulier et tourne volontairement l'appareil vers la droite afin d'occulter un objet qu'il juge disgracieux. Le résultat est une image cadrée selon l'œil du photographe. Ne connaissant pas la dimension complète du cliché qui s'offre dans son champ visuel à l'instant même du déclic de l'appareil, l'individu a une version cadrée de la photographie. Pour saisir cette étendue et les raisons pour lesquelles tel objet a été occulté, tandis que l'autre a été mis en avant, nous devons appliquer une méthode qui prend à la fois en compte les cadres, le contexte de production, mais aussi la subjectivité de l'analyste.

3.4 L'approche herméneutique

Notre approche de l'analyse de discours n'est pas à proprement critique, même si Maingueneau croit que « toute étude du discours possède par nature une dimension critique ». (Maingueneau, 2012) Pour identifier et analyser les cadres en présence, nous nous basons sur l'approche herméneutique dans le sens où l'a d'abord conçue Martin Heidegger (1990) : un processus d'interprétation lié au soi. Réactualisée par le philosophe Hans-Georg Gadamer (1991), pour qui la méthode propre aux sciences exactes à elle seule ne suffit pas, sa conception de l'herméneutique suggère d'approfondir l'expérience de la compréhension et de l'interprétation à travers la subjectivité de l'être. Appliquée aux recherches empiriques sur l'analyse des cadres,

l'approche herméneutique figure parmi les cinq approches méthodologiques proposées par Matthes and Kohring en 2008 :

> The hermeneutic approach identifies frames by providing an interpretative account of texts linking up frames with broader cultural elements. Studies are based on small samples that reflect the discourse on a particular issue or event. Frames are described in detail and there is not quantification. The main criticism to this approach points to the difficulty of explaining how frames were extracted from the texts. (Matthes et Kohring, 2008)

Quoique cette méthode est susceptible de créer un « processus de catégorisation complexe ou une influence excessive de l'analyste »[70] (Vicente et López, 2009), elle se révèle être la plus pertinente. On reconnaît, tout comme l'a réalisé Azpiroz dans ses recherches, que l'analyse qualitative des cadres, jumelée à l'approche herméneutique, a l'avantage d'intégrer une compréhension profonde du cas à l'étude. (Azpiroz, 2013)

3.5 Création du corpus et sélection de l'échantillon

S'il nous était impossible d'étudier la totalité du champ discursif de la cyberattaque contre Sony, nous proposons d'extraire un sous-ensemble représentatif de l'événement, constitué d'une seule perspective, celle de l'État américain. Conduite sur le moteur de recherche de la Maison-Blanche et de Google, sous les expressions « Sony attack », « Sony hack » et « Sony cyber attack », les déclarations de l'administration Obama ont été examinées sur une période de cinq mois : du 24

[70] Vicente, M. et López, P. (2009). Resultados actuales de la investigación sobre framing: sólido avance internacional y arranque de la especialidad en España. *Zer. Revista de Estudios de Comunicación*, (14), 13-34.

novembre 2014, jour de la cyberattaque, au 24 avril 2015. Six d'entre elles ont soulevé notre intérêt et constituent notre échantillon. Elles sont présentées sous forme de tableau.

Tableau 3.1
Présentation de l'échantillon

#	Nature	Titre	Communicateur(s)	Date
1	Déclaration	Pas de titre	Bernadette Meehan, porte-parole du Conseil national de sécurité	17/12/2014 Au lendemain de la profération de menace terroriste, le jour même de l'annulation du film.
2	Remarque	« Remarks by the President in Year-End Press Conference »	Barack Obama et les journalistes	19/12/2014 Quelques heures après l'accusation de la Corée du Nord par le FBI.
3	Remarque	« State of Union » talk-show télévisé sur CNN	Barack Obama et l'animatrice Candy Crowley	21/12/2014
4	Déclaration (Ordre exécutif)	« Authorizing the imposition of sanctions against the Government of North Korea and the Workers' Party of Korea. »	Jacob J. Lew, secrétaire du Trésor	02/01/2015
5	Remarque	« Remarks by the President at the Cybersecurity and Consumer Protection Summit. »	Barack Obama	13/02/2015
6	Déclaration (Ordre exécutif)	« Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities. »	Barack Obama	02/04/2015

Pour constituer l'échantillon de la cyberattaque de Sony, le choix se porte sur la totalité [71] des communications politiques rendues publiques par l'administration Obama sur le sujet, entre le 17 décembre 2014 et le 2 janvier 2015. La première communication officielle du gouvernement, en réponse à la cyberattaque contre Sony, fut celle du Conseil de sécurité nationale. La dernière conférence de presse de l'année

[71] Nous considérons qu'une citation ou une référence courte relative au cas Sony ne constitue pas une communication politique suffisamment substantielle pour être intégrée au corpus.

du président, au cours de laquelle plusieurs questions des journalistes portaient sur l'événement Sony. L'entrevue télévisuelle du président au populaire talk-show « State of the Union » sur CNN, où l'animatrice l'a interrogé à maintes reprises sur le sujet. Pour terminer, l'annonce officielle d'un ordre exécutif[72] visant à sanctionner la Corée du Nord pour les méfaits qu'elle aurait commis à l'encontre de Sony. Représentatif, cet échantillon au nombre de quatre permet de relever les différents cadrages, leurs thèmes et leurs contenus, mais aussi la possible confusion sémantique associée au champ de la cyberattaque.

Au sujet des procédures analytiques subséquentes, deux échantillons vont au-delà de la cyberattaque de Sony, à la fois dans leur contenu qu'en fonction du continuum temps. Puisque la dernière partie du mémoire vise à contextualiser notre objet d'étude dans l'optique plus large de la cybersécurité, deux communications politiques portent sur ce sujet. Le premier est le discours inaugural d'Obama au Cybersecurity and Consumer Protection Summit. Il s'agit d'un Sommet organisé par la Maison-Blanche à l'Université Stanford, visant le renforcement de la coopération entre les grandes entreprises de technologies et le gouvernement. Le deuxième discours est l'annonce de l'ordre exécutif Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities, proposant de nouvelles procédures législatives pour assurer une meilleure cybersécurité au pays. Correspondant aux mois de février et avril 2015, ces deux déclarations sont sélectionnées dans un but comparatif afin de rendre compte d'un recadrage potentiel sur la cyberattaque de Sony et concernant le concept plus général de ce que représente une cyberattaque.

---

[72] L'ordre exécutif (Executive Order, en anglais) est entré en fonction sous George Washington. Il s'agit d'une directive signée par le président, la plus haute autorité du pouvoir exécutif. Impliquant parfois la loi, l'ordre exécutif permet au président de prendre des décisions importantes sans le consentement du Congrès. En ce sens, elle est parfois controversée. C'est d'ailleurs par ordre exécutif que le président George W. Bush a créé la juridiction d'exception des commissions militaires de Guantanamo dans le cadre du « War on Terror ».

La moitié de l'échantillon recueille les propos directs du président Obama, tandis que dans l'autre moitié se trouvent des textes dits officiels, approuvés ou signés par le président, et diffusés par les organes de presse de la Maison-Blanche. En ce sens, notre utilisation de l'expression « administration Obama » inclut le président et ses proches collaborateurs. Nous estimons qu'ils suivent tous sensiblement une certaine ligne de parti en matière de communication politique sur la cyberattaque et la cybersécurité. Dans le cas contraire, nous en serions témoins au moment de la présentation des résultats. Par ce choix diversifié d'échantillons de nature officielle et médiatique, le corpus a l'avantage de présenter une perspective globale de l'administration Obama, à la fois spécifique sur l'événement Sony, et générique relativement à la cybersécurité.

3.6 Traitement des données

3.6.1 L'identification : thèmes, cadres et cadrages

D'emblée, rappelons que le cadrage est connu comme étant la capacité des acteurs à « altérer la compréhension en attirant l'attention sur certains aspects de la réalité tout en délaissant d'autres ». (Entman, 2003)

Commençons par identifier les thèmes en question. Spécifiquement, un thème est une idée, un sujet qui domine en entier ou en partie un discours. Suite à une lecture approfondie de chaque allocution, émergera dans l'esprit du lecteur un ou plusieurs thèmes. Le texte sera donc découpé en fonction des thèmes.

La deuxième étape vise à identifier les cadres, soit les informations sélectionnées et celles qui sont délaissées pour chacun des quatre cadres, et ce, pour chacun des

thèmes abordés. Cette identification se déroule par un processus d'interrogation du texte. Pour s'inscrire dans la même démarche méthodologique que celle d'Azpiroz[73] (2013), s'appuyant sur le modèle d'Entman (1993), nous reprenons les interrogations suivantes :

1. Quel est le problème ?
2. Qu'est-ce qui cause le problème ?
3. Quels acteurs sont présentés et quels sont leurs rôles ? Qui sont les bons et les mauvais ?
4. Quelles solutions sont avancées pour pallier le problème ?
5. Quelles sont les composantes langagières ?

Le principe de présentation et des réponses aux interrogations est structuré sous forme de tableaux. Le résultat est un nombre de tableaux équivalent au nombre de thèmes relevés dans chaque discours. Dans la ligne verticale sont indiquées les quatre premières interrogations. La ligne horizontale, quant à elle, vise à répertorier si le cadre est présent ou non. Il en résulte la réponse à la question ou, le cas échéant, une case vide exprimant l'absence de réponse.

Les cadres recommandés sont ceux contenant le plus d'informations, et les cadres exclus sont ceux comportant peu ou pas d'information. À ce stade, nous serons en mesure d'identifier le cadrage en présence pour chaque échantillon, à savoir quels aspects sont sélectionnés et omis pour définir le problème, sa cause, son évaluation et sa solution.

[73] Pour en savoir davantage sur les travaux d'Azpiroz, se référer à sa recherche Framing as a tool for mediatic diplomacy analysis: study of George W. Bush's political discourse in the "War on Terror" (2013).

Comme le précise Entman (1993), une seule phrase peut contenir les quatre cadres, tandis qu'il est probable qu'un article entier n'en représente aucun. Or un discours peut contenir un, plusieurs ou la totalité des quatre cadres. Le texte sera jugé lorsque soumis au cadrage s'il répond aux critères à au moins deux des quatre cadres possibles tel que l'entend Entman (1993). En fait, pour être considéré comme un échantillon théorique valable, le discours doit répondre aux normes d'au moins deux cadres. Dans le cas contraire, l'échantillon est jugé invalide.

3.6.2 La saillance dans les cadres

Lorsqu'un cadre met de l'avant un aspect, celui-ci est rendu saillant dans le texte par la mise en relief de composantes langagières. Ces dernières sont connues comme étant des formes symboliques où se matérialise le cadre. « C'est ainsi qu'il devient saisissable pour l'analyste, qu'il offre prise à sa reconnaissance pratique. » (Auboussier, 2009) Par « rendre saillant », Entman réfère au processus voulant attribuer une certaine pertinence en accordant plus de poids et d'importance aux structures du langage. (Entman, 1993) Le fait de les rendre « plus visibles, significatives ou mémorables pour le public ». (Traduction libre, DeLuca & Delicath, 1999) L'identification des composantes langagières est la raison de l'existence de la cinquième question du modèle d'Azpiroz. La dernière colonne du tableau regroupe les structures du langage à partir desquelles il est possible d'identifier la saillance qui forme un cadre. Nous avons relevé les principaux éléments de la saillance des différents auteurs, principalement chez Entman. Nous les présentons sous forme de grille de référence non exhaustive, susceptible d'évoluer en cours d'analyse :

Tableau 3.2
Éléments de saillance

Type de saillance	Contenu de saillance
Sélection	Mots clés et dérivés, phrases clés, images stéréotypées et sources qui réitèrent thématiquement des faits ou des jugements.
Visible	Répétition, caractères gras.
Agencement	Idées similaires structurées les unes à la suite des autres.
Ordre	Structure globale du texte proposant début, milieu et fin.
Signification	Donner du sens à l'aspect en l'associant aux symboles culturels familiers, à des événements historiques ou mémorables. Tous liens avec la résonance culturelle.
Degré/Portée	Accentuer la gravité ou l'intensité.
Simplicité	Expliquer en termes simples, en évitant les complexités.
Sous-entendu	Prêter une attention particulière aux choix de mots, aux temps de verbes et à la prospective.

3.6.3 Le facteur contextuel

Facteur fortement induit par les auteurs présentés (Entman, Azpiroz, Foucault), l'étude du discours doit s'opérer en référence au contexte. D'abord, nous devons avoir à l'esprit la situation politique d'adversité entre les deux nations impliquées dans la cyberattaque. Les États-Unis revendiquent la démocratie, et la Corée du Nord s'autoproclame socialiste[74]. Entretenant des relations conflictuelles depuis la guerre de Corée en 1953, plusieurs facteurs contextuels sont généralement explicités. Nous faisons référence à l'état de belligérance et l'absence de relations diplomatiques officielles depuis la fin de la guerre de Corée. La désignation du pays par le président Bush comme faisant partie de l'axe du mal, favorisait son isolement. Une politique

[74] Suite à la lecture de *Les Origines du totalitarisme* (1951) de Hanna Arendt, nous tenons à préciser que le régime nord-coréen s'apparente davantage, à notre humble avis, à un système totalitaire qu'à un système socialiste.

étrangère américaine dite hostile à l'égard du pays basée sur des sanctions économiques dites draconiennes. Enfin, des pourparlers intermittents à six sur le programme nucléaire nord-coréen ont eu lieu, parallèlement à trois essais nucléaires entre 2006 et 2013. Des actes vivement condamnés par la communauté internationale ont tôt fait de cristalliser le pays dans son statut d'ennemi des États-Unis, voire d'adversaire public. Malgré ces facteurs aggravants, il est généralement reconnu que les États-Unis favorisent le dialogue et font preuve d'une ouverture certaine pour l'amélioration de leurs relations américano-nord-coréennes.

Dans le contexte au sens foucaldien, les rapports de force impliquant des formes de pouvoir politique sur l'échiquier mondial, sont largement investis par les États-Unis. Par sa position privilégiée dans la communauté internationale et son statut de défricheur de la cybersécurité, le pays jouit d'une grande latitude pour donner le ton et poser des balises en la matière. (Dunn-Cavelty, 2007, Porteous, 2011, Ventre, 2015) En ces temps où la menace associée au cyberespace est grandissante et où la gouvernance d'Internet est une priorité, le contexte de production est bousculé par l'urgence de mettre en place une règlementation. De plus, les États-Unis sont en droit d'imposer des sanctions au gouvernement de Kim Jong-un, la situation inverse étant quasi impossible. En ce sens, nous croyons que le contexte politique actuel favorise la position des États-Unis.

Par ailleurs, dans le contexte « d'espace discursif » américain[75] (Wolton, 2005), il existe un cadrage médiatique et politique généralement défavorable à l'égard de la Corée du Nord. (Choi, 2006, Song, 2011, Won, 2013) Dans son analyse des

[75] Puisque le discours de l'État américain fait l'objet de notre étude, notre brève description de l'espace discursif concerne uniquement ce discours. Loin de vouloir minimiser l'apport de la Corée du Nord dans la conflictualité, notamment par son programme nucléaire, et l'existence de sa vision qui semble stéréotypée face à l'Amérique, nous nous concentrons sur l'espace discursif américain.

politiques étrangères des États-Unis entre 1994 et 2002 à l'égard du régime des Kim, Étienne Lévesque (2006) relève que l'État américain entretient une vision stéréotypée de son ennemi. Il en va de même selon la doctorante Jiyoung Song, qui dénonce l'orientation négative des plans politique et médiatique, tout en invitant à tenir davantage compte du contexte sociohistorique nord-coréen dans toutes analyses, qu'elles soient académiques, médiatiques ou politiques. (Song, 2011) Cela a certes des échos en termes de résonance culturelle sur l'opinion publique. Quand une situation amène les États-Unis à accuser un tiers, la Corée du Nord apparaît être un ennemi de choix.

Au-delà de ces éléments contextuels, nous pourrons faire des liens spontanés avec le contexte spécifique associé à un discours.

3.6.4 La mise en relation entre les cadres

Un cadrage est déterminé par la mise en relation des cadres de chaque échantillon. Les similarités et divergences entre les échantillons seront résumées pour dresser un portrait global du cadrage propre à la cyberattaque contre Sony. Des pistes théoriques explicatives, en lien avec la littérature et le contexte, émergeront de manière objective et subjective.

Au terme de cette unité de traitement, nous serons en mesure de répondre à la première question sectorielle que nous tenons à rappeler ici: quel est le cadrage de la cyberattaque contre Sony dans le discours de l'administration Obama ? En outre, les sous-questions seront également répondues.

Il est pertinent de reconnaître que l'analyse des cadres outrepasse largement l'identification des cadres sous l'angle de leur sélection et de leur omission. Sa richesse méthodologique réside dans la mise en relation entre les différents cadres, car ces liens sont susceptibles d'orienter le discours à divers égards, et ce, en termes d'appui, de négation ou d'ignorance. Dans le cas présent, l'hypothèse prévoit un cadrage de type solution qui tend à favoriser le changement de politiques. Dans le panorama des études présentées au chapitre II, nous avons repéré certains liens récurrents entre les cadres. Trois d'entre eux nous apparaissent significatifs dans notre manière d'aborder le traitement de nos données. Nous les exposons ainsi dans le but de guider notre analyse :

- Le cadre de type solution est souvent prôné dans le discours de l'État américain et souvent appuyé par le cadre de la définition du problème.
- Ainsi mis de l'avant, il peut détourner l'attention du problème, de sa cause ou de son évaluation, pour orienter la teneur du débat vers les solutions proposées.
- Si d'autres cadres sont mis de l'avant avec celui de la solution, leur contenu fait souvent référence aux valeurs américaines, principalement la liberté, la démocratie et le patriotisme.

L'ensemble de ces éléments servira de point de départ pour la mise en relation entre les cadres de la cyberattaque contre Sony afin de répondre à la deuxième question sectorielle : comment le cadrage de la cyberattaque contre Sony tend-il à favoriser le changement politique ?

Dans le but d'approfondir notre compréhension du discours sur la cyberattaque de Sony et pour le situer dans une optique plus large, nous le comparons à celui de la cybersécurité. Le cadrage de ce dernier sera d'abord identifié, mais de manière plus succincte que son homologue. Pour ce faire, les pistes théoriques de Dunn-Cavelty

(2012, 2013) seront ici mises à profit. Une fois présentés sous forme de résumé, nous pourrons ensuite relever les similitudes et les divergences entre les deux cadrages à l'étude. Nous espérons ainsi être témoins d'un recadrage au sens où l'entendent Callaghan et Schnell (2005). Nous verrons s'il s'agit d'une évolution ou d'un changement dans le propos concernant la définition, la cause, l'évaluation et la solution de la cyberattaque de Sony, ou encore d'un concept de cyberattaque au sens plus général. L'accent sera aussi donné aux différents indicateurs de temps, à ce qui marque une scission entre l'événement Sony et l'après-Sony. Nous serons alors en mesure de répondre à la dernière question sectorielle : comparativement au cadrage de la cybersécurité, comment le cadrage de la cyberattaque contre Sony contribue-t-il à marquer un point tournant dans la cybersécurité américaine ?

CHAPITRE IV

PRÉSENTATION DES RÉSULTATS

4.1 L'omniprésence de la définition du problème et de la solution

Ce chapitre présente les résultats de l'analyse. Nous identifions ici les thèmes et leurs cadres respectifs pour les quatre échantillons associés à la cyberattaque de Sony et les deux échantillons relatifs à la cybersécurité.

4.2 L'identification des cadres de la cyberattaque de Sony

4.2.1 Conseil de sécurité nationale

La première communication de l'administration sur l'événement Sony propose deux thèmes : la décision de Sony (Tableau B.1) et la cyberattaque contre Sony (Tableau B.2). Le premier décrit le problème de manière claire et succincte : « Attempt to threaten or limit artists freedom of speech or of expression. » Il s'agit d'une valeur profonde de la société américaine : la liberté. Qualifié de « serious », l'accent est mis sur le fait que les « American artists and entertainers » et que « U.S. respects theirs to produce and distribute content of their choosing ». La cause est vague, étant attribuée à la mention « Sony announcement regarding *The Interview* ». En termes d'évaluation, le gouvernement des États-Unis se dit « aware of Sony's

announcement », tout en s'y dissociant complètement : « U.S. has no involvement in such decision. » De manière implicite, cette dissociation pose un jugement moral, à savoir que Sony est en défaut. De ce fait, aucun moyen d'y remédier n'est proposé.

Quant au vocabulaire associé au concept de cyberattaque, il est peu diversifié, sans doute en raison du caractère expéditif de la déclaration. Le mot « attack » est répété deux fois, juxtaposé aux termes « criminal », « breaches », « seek to gain access » et « attempt to threaten or limit ».

Dans le second thème, l'ensemble des paramètres proposés pour définir le problème de la cyberattaque de Sony demeure simple, parfois vague. Défini de manière succincte et imprécise, il s'agit de « breach » et d'« attack », affectant toutes les sphères de la société : « U.S. companies, U.S. Consumers and U.S. infrastructure, in U.S. and elsewhere. » Il est causé par la présence de « criminal and foreign countries » et de « perpetrators » cherchant à s'infiltrer dans les réseaux américains publics et privés. En disant prendre en charge l'entreprise victime et de collaborer avec le FBI, l'État se présente comme un bon acteur dans les circonstances. Alors que l'attribution de responsabilité de l'attaque n'a pas encore eu lieu, on propose déjà une gamme de solutions basée sur l'engagement du gouvernement à traduire les coupables devant la justice. Cet aspect est rendu saillant de plusieurs manières. Premièrement, il est émis de façon plus visible avec la présence de mots clés, au temps présent ou au futur, appelant à l'action : « closely monitor », « support, assistance », « investigation », « investigating », « considering », « justice », « provide », « update » et « working tirelessly ». Deuxièmement, en répétant à dix reprises en six phrases consécutives le nom du pays « United States », son abréviation « U.S. » ou la référence au gouvernement avec l'emploi du « we ». Troisièmement, l'agencement dans le texte; les phrases se suivent, l'ordre dans le texte est respecté, et la première phrase donne le ton : « U.S. closely monitors all report breaches. » Enfin,

quatrièmement, on remarque l'utilisation de caractères gras dans le texte : « (...) **will provide an update at the appropriate time. We are considering a range of options in weighing a potential response** ». Malgré le caractère flou des cinq moyens suggérés, nous sommes convaincus que le gouvernement est engagé à riposter à la cyberattaque. En définitive, c'est le cadre solution qui est mis de l'avant, tandis que les trois autres cadres qui ont été formulés brièvement sont délaissés.

4.2.2 Conférence de presse

Dans sa dernière conférence de presse de l'année, le président accorde une place prépondérante aux deux thèmes déjà présentés, en plus de celui ayant trait à la cybersécurité. La thématique de la décision de Sony (Tableau B.3) oriente l'essentiel de son propos sur les conséquences de la décision, soit la censure. « We cannot have a society in which some dictator someplace can start imposing censorship here in the U.S. » Dans une prospective basée sur le scénario du pire, l'État attire l'attention sur l'impossibilité de laisser opérer la censure en sol américain :

> (...) imagine what they start doing when they see a documentary that they don't like, or news reports that they don't like. Or even worse, imagine if producers and distributors and others start engaging self-censorship (...)
>
> Imagine if instead of it being a cyber threat, somebody had broken into their office and destroyed a bunch of computers and stolen disks. Is that what it takes for suddenly you to pull the plug on something? (Obama, 2014)

Pour donner davantage d'accent à l'impossible censure, deux événements sportifs fortement ancrés dans l'imaginaire américain sont cités :

> We can't start changing ours patterns of behaviour any more than we stop going to a football game because there might be possibility of a terrorist attack : any more than Boston didn't run its marathon this year because of the possibility that somebody might try to cause harm. (Obama, 2014)

On fait appel à une valeur fondamentale, soit l'identité américaine, en répétant la même idée : « So that's not who we are » et « That's not what American is about ». Alors que la sortie du film *The Interview* a bel et bien été annulée, cette affirmation identitaire induit toutefois l'idée inverse, celle de la non-capitulation devant la censure. Curieusement, en aucun cas le mot annulation ou encore le titre du film n'est mentionné. Par conséquent, cet aspect de la définition du problème est occulté.

Quoiqu'elle n'est pas explicitée, à la lecture de la documentation y ayant trait, on comprend que le motif est attribuable à l'entreprise Sony. L'évaluation est perceptible dans le jugement moral avec « Yes, I think they made a mistake », et de prescription morale avec « I wish they had spoken to me first ». Nonobstant le fait qu'à deux reprises il se dit empathique à l'égard de l'entreprise, Obama présente Sony comme un acteur qui n'est pas dans son camp, qui ne partage pas ses valeurs. Bref, il prétend que le gouvernement aurait mieux agi : « I would have told them, do not get into a pattern in which you're intimidated by these kinds of criminal attacks. »

Enfin, la solution est amenée simplement en une seule phrase : « We'll engage with not just the film industry, but the news industry and the private sector. We already have. We will continue to do so. » L'engagement face au problème, un rôle que le gouvernement se doit d'endosser en raison même de sa responsabilité à protéger, ne constitue pas une réponse typique à l'imposition de censure.

La seconde thématique, la cyberattaque de Sony (Tableau B.4), présente le problème simplement, sous l'angle d'une « attack » ayant entraîné « a lot of damages ». Cela

est sans doute justifiable par le fait qu'il a déjà été brièvement défini en début de discours par Obama, puis repris dans la question du journaliste. À l'origine de ce qui a provoqué l'attaque, on cite le FBI pour confirmer que la Corée du Nord est en cause. Dans son appréciation, le président présente les bons, le gouvernement américain, et les mauvais, qu'il n'hésite pas à dévaloriser : l'État nord-coréen. D'ailleurs, il tend même à ridiculiser ce dernier. Avec sarcasme, on laisse présager la nature saugrenue du régime :

> I think it says something interesting about NK that they decided to have the sate mount an all-assault on a movie studio because of a satirical movie. (Laughter) I think it gives you some sense of what of the kind of regime we're talking about here. (Obama, 2014)

Se distinguant fortement des trois autres par la densité des informations sélectionnées, le cadre de la solution met l'accent sur un État qui s'implique en affirmant : « engaged on these issues ». Cet aspect sélectionné se concrétise avec la répétition à cinq reprises de la même structure grammaticale, l'accent étant donné à la riposte : « We will respond. We will respond proportionally, and we'll respond in a place and time and manner that we choose. » Obama s'approprie par deux fois l'autorité présidentielle de décider de la nature de la riposte en fonction de celles qui lui seront proposées : « I will make a decision on those based on what I believe. » Tel un justicier, il décrit un degré de riposte « appropriate » et « proportionnal ». Au niveau sémantique, alors que le problème présentait une « attack », les solutions proposées le sont plutôt par rapport à un « crime ». Le lecteur ignore quelles méthodes seront appliquées, mais il est convaincu que des mesures seront prises par l'administration et que ce seront les bonnes.

À noter que le troisième thème identifié, la cybersécurité, sera traité dans la section 4.3.1 prévue à cet effet.

4.2.3 Entrevue télévisée

Dans le populaire talk-show *State of the Union*, les deux thèmes récurrents composent le discours (Tableau B.6). À nouveau, le problème de la décision de Sony sous l'angle de la conséquence ayant entraîné une action de censure est le premier cadre en importance : « If we set a precedent in which dictator in another country can disrupt, through cyber (...) we start censorship ourselves, that's a problem. » Ce cadre est présenté comme un affront à la valeur fondamentale de « free speech » et de « right of artistic expression ». Pour ajouter à l'impossibilité de laisser la censure s'imposer, Obama prend exemple sur une situation hypothétique qui est intolérable :

> It's a problem not just for the entertainment industry, it's a problem for the news industry. CNN has done critical stories about North Korea. What happens if, in fact, there is a breach in CNN's, you know cyberspace? Are we going to suddenly say, well, we'd better not report on North Korea ? (Obama, 2014)

Sans doute attribuable au sujet déjà posé dans la question de l'intervieweuse, la mention directe au titre du film *The Interview* est une fois de plus occultée. Deuxième cadre en importance, l'évaluation présente un gouvernement qui se dit « pretty sympatic to Sony ». Néanmoins, il sous-entend que l'entreprise a fait une erreur : « Had they talk to me directly about this decision, I might have called the movie theater chains and distributors and asked them what the story was. » Pour la première fois, Obama minimise la dichotomie bon versus méchant : « The key here is not to suggest that Sony was a bad actor. » Il prescrit ensuite l'importance de s'adapter : « It's making a broader point that all of us have to adapt to the possibility of cyber attacks. » Pour Obama, la cause, attribuée brièvement à Sony, et la solution qui se veut absente, sont toutes deux occultées.

Le second thème relevé est celui de la cyberattaque contre Sony, qui, parfois, bascule[76] vers la cybersécurité (Tableau B.7). D'entrée de jeu, Obama précise qu'il ne considère pas l'attaque de Sony à l'exemple d'un « act of war », mais plutôt comme étant du « cybervandalism ». Nous supposons qu'il tient à recadrer le propos qui a largement circulé dans les médias, la Corée du Nord ayant qualifié *The Interview* d'acte de guerre. La problématique est définie en termes très larges : « disrupt our lives in all sort of ways ». On accorde un degré élevé de considération avec l'emploi à quatre reprises de « very costly », « very expensive » et « very seriously ». Pour la première fois, le fondement est défini au niveau macro, alors qu'un environnement « in this new world so much digitalized » qui octroie la capacité d'attaque d'un large corpus « state actors », les « others countries » et les « non state actors ». On perçoit certes la dichotomie bon versus méchant, mais l'estimation du discours est occultée.

Largement invoqué en avant-plan, l'objectif vise l'engagement du gouvernement de répondre à la cyberattaque, duquel émanent dix solutions partageant la même structure grammaticale : le pronom « we » suivi d'un verbe au temps présent appelant à l'action gouvernementale : « respond », « work », « go », « start », « do » et « going ». Ces verbes et leurs dérivés forment également les mots clés en présence. Allant dans tous les sens, les moyens demeurent imprécis. Seulement deux d'entre eux sont concrètement applicables. Le besoin du Congrès de proposer une loi en matière de cybersécurité et l'étude de la possibilité de remettre la Corée du Nord sur la liste des États soutenant le terrorisme (en référence au « Axis of Evil » formulé par Bush). Au-delà des méthodes de résolution, l'accent est mis sur la mobilisation, notamment à travers le partenariat « public-private ». Il nécessite de travailler plus fort, et les actions doivent être plus énergiques qu'à l'ordinaire « a lot more to guard against

[76] La frontière entre ces deux thèmes est parfois difficilement percevable. Nous avons choisi de les regrouper en un seul sujet, en précisant toutefois la présence d'un glissement.

them » et « a much better job of guarding against that ». Pour la première fois, et ce, deux fois de suite, Obama assure avec espoir la possibilité de vaincre le problème, alléguant « we can manage ». En se référant à l'idée du système judiciaire, il avance qu'un problème relevant du cyber doit être traité tel un crime commis dans le monde physique.

4.2.4 Ordre exécutif (*Sanctioning*)

Deux semaines seulement après l'accusation officielle du FBI, l'esprit est à la réprimande au Pentagone. Considérant que le but d'ordre exécutif est de sanctionner la Corée du Nord, nous relevons sans surprise un seul thème dans cette déclaration : la cyberattaque de Sony (Tableau B.8).

Deuxième cadre en importance, le contexte de la problématique est présenté de manière claire en énumérant différents aspects : la cible, le contexte, la gravité et l'implication. Pour la première fois, on distingue les deux cibles visées : « targeting Sony Pictures and the threat against movie theaters and moviegoers ». Cette précision est sans doute attribuable à la portée des sanctions annoncées, où l'étendue du problème se doit d'être justifiée. On rappelle d'ailleurs le contexte marqué par des « numerous provocations » antérieures de la Corée du Nord. L'importance est donnée aux mots et à leur répétition, exprimant la gravité des actions nord-coréennes : « cyber attacks », « threat », « threaten », « destructive, destabilizing conduct », « intimidate », « undermine », « destabilizing», destructive actions » et « repressive actions ». L'implication est décrite en termes de menace à la liberté d'expression : « U.S. business and artists exercising their right of freedom of speech », « attempts to undermine our values », mais aussi la sécurité nationale et la cybersécurité.

Prévisible, le diagnostic du problème vise le « Government of North Korea and the Workers' Party of Korea », mentionné à trente-trois reprises sous les dérivés « North Korea » ou « North Korean ». S'il est évident qu'on présente deux acteurs principaux en fonction du mal versus le bien, le jugement caractéristique de la fonction appréciation est ici laissé pour compte. Il n'est pas surprenant de le constater puisqu'il s'agit d'un document officiel du Trésor, où il est rarissime de constater la présence de moralité.

Premier cadre en importance, la solution propose la signature d'un ordre exécutif visant l'imposition de sanctions au gouvernement et au parti dit fautif. La référence à l'autorité du président se chiffre au nombre de dix, « pursuant to the authorities of this new E.O. » et « under the authority of the President's ». À l'aide d'un « broad and powerful tool », le but des sanctions est d'exercer une pression financière « to hold North Korea accountable », « isolate key North Korean entities » et « disrupt the activities (...) ». L'effet souhaité est d'empêcher le pays de s'engager dans un processus commercial avec les États-Unis. Plus de la moitié de l'article est destiné à la nomenclature en caractères gras des cibles visées : trois entités, avec la description de leurs activités, et dix individus incluant leurs prénom, nom et titre. Avec cette description détaillée, appartenant d'ordinaire au mystérieux, les actions du gouvernement des États-Unis apparaissent ciblées, énergiques, voire grandioses. Étrangement, cette sanction vise l'isolement économique, en continuité avec l'historicité des sanctions américaines imposées à la Corée du Nord.

4.3 L'identification des cadres de la cybersécurité

4.3.1 Conférence de presse

Étant donné que le thème de la cybersécurité[77] est à l'ordre du jour, revenons à la conférence de presse d'Obama (Tableau B.5). Le problème est exposé simplement et succinctement, « issues of cybersecurity », en précisant son degré d'intensité « is so urgent », « enormous damage », « serious » et « utmost seriousness ». La faute est attribuée au « digital world » qui offre aux « hackers » des possibilités d'agir. Pour appuyer cette description, le président a recours à la métaphore du « Wild West » pour définir le cyberespace. Deuxième cadre en importance, l'évaluation présente un ennemi aux multiples visages : « non-state actor », « weak state », « state actor » et « hackers ». L'évolution future de leurs capacités est précisée, « are going to be better » et « (...) are going to be sophisticated », tout comme leurs dommages potentiels qui seront « costly » et « serious ». Le ton laisse transparaître une certaine crainte face au futur. Une idée qui est cependant rapidement rééquilibrée par le positionnement de l'État, tel un chien de garde, dans la prévention de ces types d'attaques.

Si elle est substantielle, la fonction évaluative ne fait cependant pas le poids devant la solution qui remporte haut la main le premier titre. Le « first place » et « our first order business » sont donnés à la mise en place de meilleures pratiques et à la prévention des attaques. L'espoir face à l'ouverture du Congrès est mentionné à deux reprises. On espère que ce dernier soit préparé à travailler de pair avec l'administration pour créer une « strong cybersecurity lays that allow for information-

[77] Du début à la fin de son discours, les propos d'Obama s'entrecoupent à plusieurs endroits d'idées touchant la cyberattaque de Sony et la cybersécurité. En alternant ainsi entre les deux thématiques, il est parfois difficile d'identifier quelles idées appartiennent à quelle thématique. Nous tenons à le spécifier par souci de transparence.

sharing » entre le secteur privé et le secteur public. Toutefois, on rappelle avec rationalité que « a lot more needs to be done. We are not even close to where we need to be ». Les prévisions sont sombres et l'idée de la menace est imminente. Si cette priorité n'est pas mentionnée à l'agenda, « this is going to be affecting our entire economy in ways that are extraordinarily significant ». En définitive, le temps est venu pour l'État américain de jouer un rôle de leader sur le plan de la cybersécurité : « to start setting up some very clear rules of the road in terms of how the Internet and cyber operate ».

4.3.2 Sommet

Ce discours inaugural d'Obama est présenté dans le cadre d'un Sommet dont l'intérêt porte sur la protection du consommateur et l'économie en ligne. Les quatre fonctions du cadre sont mises de l'avant, avec une prédominance du moyen suivi de la description du problème (Tableau B.9). Le problème de « cyber threat » est principalement traité sous l'angle économique. Il s'agit d'ailleurs de la problématique, la « most serious » auquel le pays a été confronté jusqu'à maintenant. Dans la conceptualisation de ce nouveau problème, l'idéologie doit être tenue à distance : « This is not a Republican or Democratic issue », « This sould not be an ideological issue ». « I want to emphasize : this is not a Democratic issue, or a Republican issue » et « This is not a Liberal or Conservative issue ». Une place est accordée au concept de cyberattaque, aussi présenté sous l'angle économique. Obama se montre désolé pour les compagnies victimes : leurs secrets, leur propriété intellectuelle et leur taux d'employabilité. Pour l'une des rares fois, un des attributs du cas Sony est explicité en mentionnant les dommages causés sur les plans structurel, économique et humain. « North Korean cyber attack on Sony Pictures destroyed data and disabled thousands of computers, and exposed the personal

information of Sony employees » et « these attacks are hurting American companies and costing American jobs ».

L'origine est majoritairement technologique, attribuable à la présence en ligne de tous : État et consommateurs. La métaphore du « Wild West » est mieux définie; il s'agit d'un lieu où l'on demande à l'État d'être le « sheriff ». Les ennemis sont multiples, tantôt un « Hacker from China and Russia », parfois des « Foreign government and criminals ». L'évaluation du gouvernement américain est effectuée dans la confiance « we've boosted our defense », « we're making progress » et « taken a new step », tout en avouant une transparence certaine : « Government has to be constantly self-critical. »

Près des deux tiers du discours sont consacrés à la proposition et à l'explication des solutions. Elles reposent en grande partie sur la mobilisation des secteurs public et privé. L'administration ne peut agir seule; les grandes entreprises technologiques doivent impérativement s'impliquer face au problème. Pour ce faire, Obama propose quatre axes stratégiques offensifs : « a shared mission », « to focus on our unique strenghts », « constantly evolve » et celui qu'il juge de plus important : « protecting the privacy of civil liberty of the American people ». La priorité est de ce fait accordée au respect de la valeur fondamentale de la liberté. Quatre mesures concrètes sont soumises pour mieux se préparer aux menaces : « a single national standard », une législation « Consumer Privacy Bill of Rights », où l'on en profite pour appeler deux fois le Congrès à s'unir, la création du « Cyber Threat Intelligence Integration Center » et, enfin, un ordre exécutif pour promouvoir le partage d'informations entre le public et le privé. En filigrane, la protection des données personnelles des citoyens sur la Toile reflète ces propos.

On appelle à s'unir, à rassembler les forces des secteurs public et privé : « as true partners, together, cooperation across border » et « All of us working together ». L'emploi des verbes s'oriente aussi en ce sens : « improve », « working », « build stronger defense », « disrupt more attacks », « make cyberspace safer ». Enfin, les trois derniers paragraphes sont consacrés à la métaphore de la cathédrale : « The processus of technological developement is like building a cathedral (...) Everything is tied to everything else. » Connaissant l'importance de la tradition religieuse aux États-Unis, cette métaphore est associée à une forte résonance culturelle.

En résumé, ce discours est à l'image du titre de l'article du journal français *Le Monde :* « Obama tend la main à une Silicon Valley méfiante. »[78]

4.3.3 Ordre exécutif (*Blocking*)

Plus de quatre mois après que GoP ait menacé la liberté américaine, le Pentagone annonce la signature d'un second ordre exécutif autorisant la création d'une nouvelle autorité pour répondre à la menace générale face à la cybersécurité (Tableau B.10).

Le problème est défini selon un nouveau terme : « malicious ». Il sert à qualifier les « cyber actors » et les « cyber enabled activities » (un nouveau préfixe en caractères gras) et les « cyber threats ». Il fournit une précision étonnante sur le caractère problématique relié à la cybersécurité :

---

[78] Untersinger, M. (13 février 2015) Cybersécurité : Barack Obama tend la main à la Silicon Valley méfiante. *Le Monde.* Récupéré de www.lemonde.fr/pixels/article/2015/02/13/cybersecurite-barack-obama-tend-la-main-a-la-silicon-valley-mefiante_4576356_4408996.html.

> The malicious **cyber-enabled activity** must have the purpose or effect of significantly harming or compromising critical infrastructure; misappropriating funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain; knowingly receiving or using trade secrets that were stolen by cyber-enabled means for commercial or competitive advantage or private financial gain; disrupting the availability of a computer or network of computers (for example, through a denial of service attack); and attempting, assisting or providing material support for any of the above activities. (Obama, 2015)

Dans ce court texte, « malicious » et « cyber » sont respectivement répétés à huit reprises, tandis que « threat » l'est à six. L'État est confronté à un problème dont le degré est inégalé « one of the most serious challenge » et « the most significant cyber threats that we face ». Sa portée considère tout le monde : « Our critical infrastructure, our companies and our citizens » et vise tous les secteurs : « National security, foreign policy, economic, health, financial ». Une référence indirecte à Sony est faite avec la mention « As we have seen in recent months », à propos des cybermenaces qui peuvent toucher les compagnies.

En regard du but avoué de cette déclaration, annoncer une nouvelle autorité pour contrer la menace, le cadre de la solution se hisse naturellement au premier rang. L'accent est mis sur l'autorité présidentielle, et le mot « authority » est plusieurs fois mentionné. Cette nouvelle autorité s'organisera selon une « comprehensive strategy » avec des « targeted tools », dans le but d'imposer des sanctions individuelles ou de groupe aux coupables, et ce, au niveau du « diplomatic engagement, trade policy tools, and law enforcement mechanism » qu'organisera l'autorité. Les verbes employés appellent à l'action défensive plutôt qu'offensive : « to counter », « to combat », « to respond » et « to control ». Le gouvernement se présente comme étant outillé pour contrôler la menace. Pour leur part, les principes du fondement et de l'évaluation ont été écartés.

Tout bien considéré, le discours à l'étude démontre la présence des deux premiers thèmes : la décision de Sony et la cyberattaque contre Sony, pour lesquels sept cadres sont mis de l'avant. Quatre pour la solution et trois pour la signification du problème (Annexe C, Tableau sommaires des cadrages). Les deux thèmes se distinguent respectivement par un cadrage différent. La décision de Sony d'annuler le film *The Interview* est cadrée en fonction du caractère de la problématique, tandis que la cyberattaque l'est eu égard à la résolution du problème. La cause et l'appréciation sont exclues. Pour sa part, le troisième thème, soit la cybersécurité, propose huit cadres. Trois pour la solution, suivi de deux pour la description de la difficulté. Quoique moins performants, nous en retrouvons deux pour l'évaluation et un pour la cause.

CHAPITRE V

DISCUSSION

5.1 Les solutions : vers le changement de politiques

Dans un premier temps, nous dressons le portrait global du cadrage de la cyberattaque contre Sony. Pour ce faire, nous explorerons la sélection et l'omission des informations qui composent chacun des quatre cadres, tout en proposant des pistes interprétatives théoriques. Par la suite, nous procéderons à la mise en relation entre les cadres pour démontrer comment le cadrage tend à favoriser le changement de politiques aux États-Unis. Enfin, pour approfondir notre compréhension du cadrage de la cyberattaque et dans le but de le situer dans une optique plus large, nous le comparons à celui de la cybersécurité. Au terme de ce chapitre, nous serons en mesure de valider notre hypothèse.

5.2 Le cadrage de la cyberattaque contre Sony

5.2.1 La décision de Sony : un problème d'atteinte à la liberté d'expression

Le problème est d'abord défini de manière vague : « announcement regarding *The Interview* », « such decision », « announcement » et, enfin, « decision ». On relève une mention unique du titre *The Interview* et deux références à « satirical movie ». Ce

sera d'ailleurs la seule fois où le titre du film sera mentionné, et ce, dans la totalité du corpus. Nous croyons que *The Interview* est un aspect central de la problématique. Dans son ensemble, cette omission nous semble plutôt intrigante. La possibilité que le titre ait été déjà mentionné dans la question des journalistes ou de l'animatrice de CNN, justifiant la non-reprise par Obama dans sa réponse, n'est ici point observable. À une référence près, par la mention « the movie », on constate l'absence du titre ou son annulation. Cette omission sur le plan politique apparaît encore plus marquée en regard de la couverture médiatique. Dans les médias américains, l'annulation du film a fait couler beaucoup d'encre. Suite à une observation de la couverture médiatique, nous pouvons affirmer qu'elle semble orientée vers cet aspect. Les titres d'articles de presse le démontrent : « Sony Cancels *The Interview* (...) »[79], « Sony Canceled the Release of *'The Interview'*. »[80], « *The Interview* New York Premiere Canceled in Wake of Hacker Threats. » et « Sony Just Canceled The Dec. 25 Release Of *'The Interview'* »[81]. D'autre part, on insinue la victoire des attaquants : « *The Interview* is Canceled. The Terrorists Won. »[82], « Sony Cancels North Korea Movie in Apparent

---

[79] Roger, K. (18 décembre 2014) Sony Canceled 'The Interview.' But What Are We Actually Missing? *New York Times*. Récupéré de http://www.nytimes.com/2014/12/18/us/sony-canceled-the-interview-but-what-are-we-actually-missing.html.

[80] Edger, G. (18 décembre 2014) Sony canceled the release of 'The Interview.' Here's how it could come out. *Washington Post.* Récupéré de https://www.washingtonpost.com/lifestyle/style/sony-canceled-the-release-of-the-interview-heres-how-it-could-come-out/2014/12/19/119e3328-8791-11e4-a702-fa31ff4ae98e_story.html.

[81] Arnold, B. Kelley, M.-B.Weisman A. (17 décembre 2014). Sony Just Canceled The Dec. 25 Release Of *'The Interview'*. *Business Insider.* Récupéré de http://www.businessinsider.com/reports-top-movie-theater-chains-just-caved-to-sony-hackers-2014-12#ixzz3kzdNPGVL.

[82] Mendelson, S. (18 décembre 2014). 'The Interview' Is Canceled. The Terrorists Won. So Now What Should Sony Do? *Forbes*. Récupéré de http://www.forbes.com/sites/scottmendelson/2014/12/18/put-the-interview-on-vod-dont-give-it-away-for-free/.

Win for Pyongyang Hackers. »[83]. Cette différence dans la sélection de l'aspect présenté, illustre parfaitement le cadrage tel que le décrit Entman : « (...) qu'ils soient employés de l'État ou d'un média, ils possèdent la capacité d'altérer la compréhension en attirant l'attention sur certains aspects de la réalité tout en délaissant d'autres ». (Entman, 1993) Si l'administration Obama ne parvient pas à définir le problème en regard de l'annulation du film *The Interview*, sous quel aspect porte-t-elle son attention ? Sur la conséquence du problème formulée en termes d'affront à la liberté de parole et d'expression artistique américaine. Elle demeure simple à comprendre et est déjà intégrée depuis des siècles dans l'imaginaire du peuple. D'ailleurs, cet aspect du problème est rendu saillant de six manières.

Premièrement, par les expressions clés associées au concept de liberté : « free speech », « rights of artistic expression », « artist freedom of speech or of expression », « rights to produce and distribute », « content of their choosing », « censorship » et « self-censorpship ». Obama a recours à deux concepts, lesquels ne sont pas de même nature. La liberté d'expression (freedom of expression) est un droit individuel d'expression de soi, reconnu tel un droit humain inaliénable. (Traduction libre, Patching et Hirst, 2014) Il est présenté ici sous l'angle artistique. Tandis que la liberté de parole (freedom of speech) est un « droit d'exiger une voix politique pour exprimer ce que certains veulent réprimer ». (Traduction libre, Patching et Hirst, 2014) C'est un droit « sujet au domaine juridique, à l'éthique et aux restrictions idéologiques ». (Traduction libre, Patching et Hirst, 2014) Cette déclinaison du concept, accompagnée d'expressions clés, rend plus visible l'idée de la liberté.

---

[83] Kelsey, E., Richwine, L. et Shina-Roy P. (18 décembre 2014) *Sony cancels North Korea movie in apparent win for Pyongyang hackers. Reuters.* Récupéré de : http://www.reuters.com/article/2014/12/18/us-sony-cybersecurity-theaters-idUSKBN0JV2MA20141218.

Deuxièmement, par la répétition de ces expressions caractérisées par leur simplicité grammaticale et en les citant les unes à la suite des autres dans le texte, on les rend plus visibles. Alors que nous avons affaire à un film qui fut annulé en raison d'une menace terroriste, l'exemple suivant démontre la simplicité de l'État dans sa manière d'aborder le problème : « We believe in free speech. We believe in rights of artistic expression. »

Troisièmement, par le recours à l'imaginaire du public, parfois même plus directement sous la forme interrogative, on rend la liberté plus significative. En effet, Obama présente huit situations réelles ou hypothétiques de censure pouvant affecter la liberté dans le quotidien des Américains. Ces situations de censure sont présentées comme étant intolérables pour le peuple, et sont formulées à la forme négative, accentuant ainsi leur caractère inadmissible.

Par ailleurs, quatrièmement, on répète sous diverses formes que les Américains ne seront pas intimidés par la peur de la menace ou la mise en danger de leur liberté. On rend ainsi la crainte plus réelle. En toute transparence, l'État avoue même que le temps est venu de le démontrer concrètement « Sometime this is a matter of setting tone and being very clear that we're not going to be intimidated (...). » L'idée est aussi rendue mémorable en faisant une comparaison avec le marathon de Boston et avec les matchs de football, des événements qui remémorent aux Américains le fait qu'ils ne capitulent pas devant la menace. C'est ce qu'Entman reconnaît comme étant une association à des caractères culturellement familiers. (Entman, 1993) En effet, le sport est un puissant symbole culturel aux États-Unis.

Ensuite, comme cinquième point, la valeur du patriotisme est fortement mise en avant-plan. L'identité américaine ne se laisse pas atteindre. En fait, elle est inatteignable : « So that's not who we are. That's not what American is about. » Cela

rejoint un des points de vue de Lakoff relativement au code Obama, pour qui le discours du président oriente le propos sur « ce que signifie le fait d'être un Américain, d'être un citoyen et de partager tous ensemble les sacrifices et les victoires du pays ». (Lakoff, 2009) Ce cadrage de l'État rime d'ailleurs avec la « vague de patriotisme » selon Hirst (2015) qui a émergé chez le public suite à l'annulation du film, notamment dans la communauté hollywoodienne. Rappelons qu'à travers les médias sociaux, l'acte a été vivement décrié comme étant une atteinte à la liberté d'expression artistique. On ignore cependant qui, du public ou d'Obama, a évoqué en premier l'atteinte à la liberté d'expression, puisqu'ils se sont tous deux exprimés sur le sujet le 17 décembre 2014. Chose certaine, nous sommes en présence d'un cadrage politique qui reflète dans une large proportion l'idée exprimée par le public.

Finalement, le discours se concentre sur un sous-entendu : l'atteinte à la liberté n'a pas eu lieu. Dans son discours du 21 décembre, Obama emploie désormais la conjonction « if » pour sous-entendre que la décision concernant l'atteinte à la liberté n'a pas été prise, ou du moins qu'elle peut être réversible. « If we set a precedent in which dictator in another country can disrupt (...) we start to censorship ourselves, that's a problem ». En effet, à la lecture de certains extraits du discours qui composent ce cadre, nous avons une nette impression que le film n'a pas été annulé, alors que ce fut le cas. Quoiqu'il en soit, les cyberattaquants n'ont pas réussi leur coup, alors qu'ils ont réussi à faire annuler le film. Cela est certes favorisé par ce que nous avons auparavant déjà relevé : l'omission quasi complète de l'annulation du film *The Interview* et des références associées. Nous croyons qu'il serait effectivement problématique pour l'État de reconnaître que la Corée du Nord, par la menace informatique, peut influencer le droit du Premier Amendement aux États-Unis. Sur le plan symbolique, cela marquerait les esprits tout en étant nuisible à l'image des États-Unis, défenseur de la liberté d'expression. Si les cadres en politique sont souvent

créés avec un œil sur l'avancement de l'intérêt politique et visent à faire des interprétations qui lui sont favorables (Kinder et Sanders, 1990), l'intérêt de l'État américain nous apparaît évident : il souhaite la sortie du film *The Interview*. La sortie sera en fait annoncée deux jours plus tard par Sony, alors que l'entreprise se positionne par le fait même comme un défenseur de la liberté. Le film sera projeté tel que prévu, le jour de Noël. La liberté d'expression sera ainsi respectée, et les Américains pourront en jouir en visionnant *The Interview*.

La menace à la liberté n'est pas un nouveau cadrage sur le terrain politique américain; elle remonte à 1787 avec la présence du cadre du « Threat of Liberty ». (Riker, 1996) Ce concept est profondément intégré dans la société américaine, notamment en raison de son inscription dans la Constitution des États-Unis et le débat public suscité plus récemment par son Premier Amendement. En ce sens, la définition d'un problème sous forme d'une défense en termes de « freedom and liberty » est une valeur à forte résonance culturelle. (Callaghan et Schnell, 2005) Le recours à cette valeur par l'État américain est donc un moyen de déclencher une forte résonance culturelle. En maximisant son degré de saillance de six manières différentes, la valeur revêt encore plus d'importance.

Quant à l'origine du problème de la décision de Sony, elle est délaissée. Le diagnostic est posé sur l'entreprise Sony sans plus de détails. Une seule piste d'explication de la décision est présente dans le discours : Sony est une corporation et doit obéir à des obligations d'affaires. Cette indication demeure toutefois vague puisqu'elle s'appuie sur le fait évident que Sony est une entreprise. Il est intéressant de rappeler qu'en aucun cas le titre du film ou sa référence n'est mentionné.

Quant à l'évaluation du problème, le gouvernement se dissocie entièrement de la décision de Sony. Bien que le président se dit à trois reprises compatissant à l'égard

de Sony, il l'accuse sans équivoque : « Yes, I think they made a mistake. » En affirmant sur tous les fronts que l'État aurait mieux fait que Sony dans les circonstances, que Sony aurait d'abord dû discuter avec le président, ce dernier induit que l'entreprise ne partage pas la valeur de la liberté. Cela valide les propos de George Lakoff, à savoir que « le cadrage d'Obama appelle à l'affiliation au-delà du plan politique, avec ceux qui partagent les mêmes valeurs autour d'un problème en particulier ». (Lakoff, 2009) En ce sens, ce cadre appuie la description du sujet problématique, puisqu'il présente le gouvernement comme étant un acteur à la défense de la liberté. Rappelons que « pour être performant, un cadre doit bénéficier à un côté de la médaille plus qu'à un autre ». (Entman, 2004) Le cadre de l'évaluation est visiblement performant, car il bénéficie au gouvernement des États-Unis et nuit à l'image générale de Sony.

Une idée paradoxale est soulevée dans le discours d'Obama lorsqu'il affirme pour la première fois, le 21 décembre : « The key here is not to suggest that Sony was a bad actor. It's making a boarder point that all of us have to adapt to the possibility of cyberattacks. » Un qualificatif a aussi été ajouté. Effectivement, Obama se dit désormais « pretty sympatic ». Nous comprenons ces deux éléments comme un léger recadrage de l'appréciation à l'égard de Sony. Nous l'attribuons au rappel de l'animatrice au sujet de Michael Lynton, président de la division Sony. L'animatrice précise que ce dernier s'est dit « kind of disappointed » par les propos d'Obama, l'accusant d'avoir commis une erreur. Rappelons que Lynton s'était défendu publiquement en affirmant que le président avait mal compris la problématique, que la cause n'était pas Sony, mais plutôt les chaînes de cinéma. En ce sens, il y a présence d'un cadrage de contestation, ce qui crée une compétition de cadrages entre les différents acteurs. (Entman, 2004) En l'occurrence, il s'agit d'un cas précis de recadrage politique qui survient lorsqu'une élite gouvernementale prend en « considération les autres cadrages en présence ». (Callaghan et Schnell, 2005)

À cet égard, tentons un croisement avec le modèle en cascade[84] d'Entman. Dans les premiers jours de la crise, la perspective de l'administration présente Sony comme étant fautive. Des suites de la sortie publique de Michael Lynton, qui a bénéficié d'une couverture médiatique, la perspective est recadrée pour être légèrement plus favorable. L'influence des médias a sans doute fait remonter la cascade jusqu'à la Maison-Blanche et ainsi favorisé le recadrage. Cela porte à croire que le cadrage proposé par l'État au sujet de la décision de Sony n'est pas dominant dans le discours médiatique. Les médias semblent ici avoir joué « leur rôle » comme l'avance Entman, en offrant un cadrage contestataire à celui de l'État.

Tous les discours convergent vers l'absence de solution pour résoudre le problème de la liberté d'expression. L'omission des moyens de résolution s'explique en prenant en considération que la censure selon l'administration n'a pas sa raison d'être aux États-Unis. Elle ne doit tout simplement pas exister. Rien ne sert alors d'y apporter des solutions. De plus, cette omission laisse ainsi toute la place aux multiples méthodes proposées que nous aborderons dans la prochaine partie.

En définitive, la décision de Sony est présentée par l'administration Obama telle une problématique intolérable d'atteinte à la liberté d'expression, tout en occultant l'annulation du film *The Interview*. Quoiqu'elle ne fait pas le poids devant l'importance accordée à la définition du problème, l'évaluation présente Sony comme étant fautif tandis que l'État concède qu'il aurait mieux agit. La cause et la solution sont pour leur part écartées.

---

[84] Puisque nous n'avons pas conduit d'analyse des cadres dans le discours médiatique sur la cyberattaque de Sony, nous ne pouvons l'affirmer avec certitude. Nous nous permettons toutefois de tracer ce parallèle de façon plus subjective qu'objective.

5.2.2 La cyberattaque de Sony : l'omniprésence de solutions

D'emblée, précisons que, comparativement au thème précédent, la perspective de l'État américain sur la cyberattaque de Sony est moins unidirectionnelle. Plusieurs aspects sont sélectionnés, et leur contenu est plus variable.

Le positionnement du problème est simple. Dès les premiers instants, l'État est confronté à une « attack » et à une « breach ». Avec l'association du préfixe cyber à un nouveau vocabulaire, on crée l'appellation « act of cyber vandalism », tout en précisant qu'il ne s'agit pas d'un « act of war ». Au tournant de l'année, les mots « cyberattack » et « threat » sont employés. Jamais le sens de ces termes et leur implication ne sont nettement définis. Le problème demeure par conséquent fortement nébuleux et, en ce sens, on reconnaît la présence d'une confusion sémantique.

À l'exception des cibles visées, « Sony », « movie theaters » et « moviegoers », on note l'omission quasi complète des attributs de la cyberattaque : motivations, objectifs, méthodes, modes opératoires et techniques. Tout comme les données rendues publiques, l'annulation du film de même que les dégâts structurels, financiers et humains. La vulnérabilité des infrastructures technologiques favorisant l'offensive d'attaque est amenée discrètement à une seule reprise lorsqu'il est question de l'amélioration des systèmes informatiques des entreprises américaines avec « harden their site ».

Nous expliquons cette omission par la confusion sémantique du champ de la cyberattaque rendant complexe une communication juste et efficace du sujet, et à l'absence d'espace discursif disponible pour définir le problème puisque déjà présenté sous l'angle de l'atteinte à la liberté d'expression. De son propre aveu, l'État

américain reconnaît l'ambigüité du concept de cyberattaque. (Whitehouse, 2014) Sachant que le concept général de la cyberattaque est marqué par la confusion sémantique (Hathaway et al., Roscini, Ventre, Singer et Friedman, Dunn-Cavelty, Huyghes) et que cette confusion marque aussi le discours de la cyberattaque contre Sony, nous croyons qu'elle est susceptible de freiner l'État dans sa fonction communicative. Lorsque le sens d'un concept est ambigu, il porte à croire que la tendance est à la retenue, voire à l'omission. En raison du niveau de complexité d'une cyberattaque, nous croyons qu'il est davantage bénéfique pour l'État d'occulter cet aspect et de sélectionner un contenu plus performant. En ce sens, l'administration Obama a choisi de définir le problème sous l'angle de l'atteinte à la liberté de parole et d'expression artistique. L'État en profite d'ailleurs pour appuyer le cadre de la signification du problème propre à la thématique de la décision de Sony. À cet effet, il rappelle qu'il s'agit d'un problème de « freedom of speech » pour les artistes, qui heurte les valeurs américaines.

Avant même l'accusation du FBI, le diagnostic est déjà orienté vers les « Foreign countries » et les « State actors ». Puis vient l'accusation officielle de la « North Korea » et, en janvier, on pointe avec plus de précision le « Governement of North Korea and the Workers' Party of Korea ». Évoluant timidement au rythme de l'attribution de responsabilité, la raison demeure toutefois en coulisse.

Présent chez la majorité des experts en cybersécurité, et relégué par certains médias, le cadre contestataire met de l'avant la présence de sérieux doutes quant à la responsabilité de la Corée du Nord. De nombreuses hypothèses circulent d'ailleurs, tel que relevé dans notre problématique d'ensemble. Cependant, en aucun cas le discours politique à l'étude ne fait état de ce cadre contestataire. Ni les détails sur l'enquête du FBI ni les considérations techniques sur la difficulté d'attribution, voire

son impossibilité, ne sont avancés. Jamais le doute ou le questionnement n'est soulevé ou insinué.

Une première piste d'explication s'exprime en regard de la résonance culturelle. En effet, la cause n'a point besoin d'explication, puisqu'une Corée du Nord fautive entretient un fort retentissement aux États-Unis. La perception négative à l'égard du pays est déjà structurée de façon significative sur le plan politique et dans les médias. Jumelée à la gravité sans précédent de l'attaque contre Sony, la Corée du Nord endosse à nouveau son rôle d'ennemi de choix auprès du public. Une deuxième piste émerge d'après l'intérêt américain d'éviter des ramifications diplomatiques complexes avec la Chine, le Japon et la Corée du Nord. À cet effet, Maxime Paquay, journaliste à la Radio Télévision Belge Francophone et à France 2, suggère que si les États-Unis communiquent en détail à propos de la responsabilité de la Corée du Nord, une confrontation plus directe entre les deux pays pourrait éclater. (Paquay, 2014) De son côté, le *New York Times* relève que pendant qu'Obama attribuait publiquement l'attaque de Sony à la Corée du Nord, il discutait devant le Congrès, en audience privée, de l'implication de la Chine. Or, blâmer publiquement son partenaire chinois pourrait « affecter la coopération sur le programme nucléaire iranien et créer des tensions avec les autres pays asiatiques. » (Traduction libre, Sanger, Perlroth et Shear, 2015) Sur un échiquier similaire, Sony représente un symbole de l'entrepreneuriat japonais. (Paquay, 2014) Le Japon est actuellement en négociations avec Pyongyang sur un sujet chaud : la libération de prisonniers japonais datant de la guerre de Corée. En raison de l'accusation, la Corée du Nord pourrait décider, dans un contexte de représailles, d'entraver le processus de négociations avec les Japonais. (Paquay, 2014) Cette situation pourrait placer les États-Unis dans une position inconfortable face à leur allié japonais. Bref, il semble que l'État américain ait tout avantage à ne pas attiser le feu déjà ardent.

Que la Corée du Nord soit derrière l'attaque ou non, c'est du moins ce que souhaite laissé supposer l'administration Obama, alors que c'est l'inverse dans le discours nord-coréen. Visiblement, l'un des deux discours politiques rapporte un mensonge. Or, l'important ici pour l'État américain n'est pas de faire accéder à une meilleure lisibilité du monde, mais de se présenter comme protecteur de sa nation face à l'ennemi nord-coréen.

Malgré que l'évaluation n'est pas mise de l'avant, elle reflète ce que nous avons relevé dans la littérature, soit la dichotomie bon versus méchant. (Entman, 2003, Norris, Kern et Just, 2003) Il dit prendre en charge l'entreprise victime, collaborer avec le FBI et endosser sa responsabilité à protéger le peuple. Inversement, la Corée du Nord n'obtient aucun crédit favorable. Lorsqu'il n'est pas occulté, le pays est jugé avec sarcasme ou dévalorisé en raison de son système non démocratique. La présence d'un État protecteur est de bon augure face à son l'ennemi nord-coréen.

Alors que l'attribution de responsabilité n'a pas encore eu lieu, l'État émet déjà des solutions. Sous l'aspect d'un gouvernement engagé pour répondre à la cyberattaque, la saillance s'organise de plusieurs manières, entre autres par la présence de mots clés ou phrases clés appelant à l'engagement au moment actuel : « is working tirelessly », « investigating », « engage », « working up », « today's action », « the action taken today », ou encore « ongoing government commitment ». On remarque la répétition à dix-sept reprises de la même structure grammaticale, soit « we'll » ou « I'll » suivi d'un verbe appelant à l'action conjugué au temps futur. Aussi, par l'ordre mentionné du début à la fin du discours, et l'agencement de ces mentions dans le texte, ils se suivent presque toujours, l'engagement est ainsi plus visible. Cela se fait par un appel aux actions plus dynamique : « we have to do more », « we have to do a much better job » et au fait de s'unir à tous les niveaux, notamment entre le secteur public-privé et avec le Congrès. On l'illustre par l'emploi répété dans tous les discours du « we »,

évoquant l'appartenance à la société américaine. En effet, le sentiment patriotique tend à minimiser la critique des décisions politiques dans l'espace public. (Lakoff, 2004) De plus, par le recours à l'autorité présidentielle, par Obama lui-même ou en référence à son autorité, on rend l'aspect significatif. En temps de crise, la Maison-Blanche est souvent amenée à jouer un rôle de premier plan. (Brody, 1991 et Entman, 2004) Sa mainmise sur l'information devient à cet égard plus prononcée, et les stratégies proposées s'en trouvent optimisées.

La vingtaine de moyens proposés se dit en réponse à une menace à la sécurité nationale, très rarement à l'économie. Leur nature reste vague, parfois même secrète. Dans les deux premiers discours on annonce que les solutions seront « proportional » et « appropriate » mais on laisse planer une certain mystère : « it's not something that I will announce here today » et « we'll respond in a place and time and manner that we choose ». Admettant que l'ordre exécutif est la première mesure appliquée, l'État sous-entend qu'il n'y en aura d'autres sans pour autant préciser leur nature et leur portée. Sachant qu'il n'existe pas de modèle pour riposter à une cyberattaque, nous constatons que le gouvernement américain se range du côté des dernières avancées de l'OTAN en la matière : « la légitime défense autoriserait les nations à répondre violemment, tant qu'il y a une forme de proportionnalité entre les dommages causés par la cyberattaque initiale et la réponse cinétique. »[85] Nonobstant l'emploi du terme « crime », nous comptons une seule référence directe à une solution judiciaire, et ce, uniquement dans la première communication « bring the perpetrators (...) to the justice ».

[85] Libicki, M. (1er et 2e trimestres, 2014) De Tallinn à Las Vegas. Une cyberattaque d'importance justifie-t-elle une réponse cinétique ? *Hérodote* (152-153). Récupéré de http://www.herodote.org/spip.php?article627.

Trois solutions suggèrent des mesures ciblées : la demande faite au Congrès, qui se précise au fil du temps, pour s'unir dans le but de faire passer une nouvelle loi visant à protéger les consommateurs Web ; l'étude de la possibilité, tout en pesant les mots utilisés, de remettre la Corée du Nord sur la liste des États soutenant le terrorisme; l'annonce d'un ordre exécutif imposant des sanctions économiques à la Corée du Nord, présentée tel un « commitment to hold North Korea accountable ».

En résumé, l'omniprésence de mesures pour riposter à la cyberattaque de Sony, lesquelles sont basées essentiellement sur l'engagement du gouvernement, rend saillant de manière extraordinaire le cadre de la solution. Parallèlement, les trois autres cadres sont laissés de côté. La définition du problème s'articule à travers une confusion sémantique, de la « breach » au « cyber vandalism ». La cause est attribuée à l'État nord-coréen, tandis que l'évaluation est réalisée selon la dichotomie bon versus méchant.

5.3 Les liens entre les cadres ou comment favoriser le changement de politiques

Pour conduire notre interprétation, notre point d'ancrage est la mise en relation des cadres en entre eux, principalement les deux en importance. Tel que l'a démontré notre panorama des études au chapitre II, le cadrage de type solution est souvent invoqué dans le discours de l'État américain. (Dunn-Cavelty, 2013, Azpiroz, 2013, Lewis et Reese, 2009, Callaghan et Schneel, 2005, Lakoff, 2004) C'est également ce que révèlent les résultats de notre analyse. Dans leur omniprésence, les moyens de résolution détournent l'attention du problème, de sa cause et de son évaluation. Cela a pour effet d'orienter le débat vers les solutions proposées par l'État. (Lewis et Reese, 2009) Puisqu'elles appellent au patriotisme, les avenues suggérées possèdent un fort degré de résonance culturelle, ce qui renforce leur incidence. La nature des principes de résolution reste pourtant très vague car ces dernières proposent l'engagement du

gouvernement à résoudre le problème, à l'exception de deux d'entre elles. Elles sont rendues saillantes par leur application concrète, et impliquent respectivement un changement des politiques en vigueur.

Du fait d'impliquer un amendement aux politiques intérieures, l'une d'elles se formule en tant que souhait : Obama espère la collaboration du Congrès afin de faciliter l'adoption du *Consumer Privacy Bill of Rights.* Une proposition de loi qui divise le Congrès depuis 2012 dont l'une des raisons invoquées est la menace au droit à la vie privée. L'engagement du gouvernement exige cependant une grande confiance de la population et du secteur privé à son égard. En proposant la révision d'une loi controversée comme solution à la cyberattaque de Sony, Obama attise le débat public sur la surveillance de masse. À la virulente question du respect de la vie privée face à l'intrusion de l'État, le président, conscient de cette brèche à sa réputation, appelle à la transparence et à la confiance « Government has to be constantly self-critical and we have to be able to have an open debate about it ». Si les discours sont cadrés conformément aux intérêts politiques, le débat peut-il véritablement être transparent ? À cet effet, nous croyons que l'État américain propose une loi disant protéger la population, alors qu'en concomitance, il fait aussi la promotion d'un plan « pour s'introduire dans la sphère privée et dans les droits constitutionnels ». (Callaghan et Schnell, 2005) En ce sens, les implications législatives jugées essentielles par l'administration Obama, démontrent que la cyberattaque de Sony sert de prétexte pour l'avancement de l'agenda démocrate.

La seconde solution qui pour sa part envisage un changement de politiques étrangères, vise l'imposition de sanctions économiques au gouvernement nord-coréen et à des membres du Parti du travail de Corée. En fait, ces sanctions visent les entités et certains de leurs officiels, les empêchant d'accéder au système financier américain. En d'autres termes, l'Amérique n'est plus autorisée à commercer avec la Corée du

Nord. Rappelons un élément contextuel pertinent, isolé de la communauté internationale, le pays croule déjà sous les sanctions économiques des États-Unis depuis la guerre de Corée. La solution à une nouvelle problématique, la cyberattaque, s'inscrit en continuité avec l'historique de politiques étrangères américaine à l'égard du pays. À cet effet, John Park, spécialiste de l'Asie du Nord-Est à la Harvard School, qualifie ces sanctions de hautement symboliques en s'interrogeant ainsi : « How do you sanction the world most heavily sanctionned country ? »[86] Appelant à l'octroi de pouvoirs spéciaux au président, l'ordre exécutif nous apparaît davantage une démonstration de force destinée à illustrer la supériorité de l'État américain sur l'État nord-coréen.

Malgré l'absence de consensus et de normes internationales sur la cybersécurité, les États-Unis prennent le pas et donnent l'exemple en ripostant à la cyberattaque. Cette méthode coup de poing nous semble à la fois s'inscrire dans la logique de punition nord-coréenne à l'américaine, et à la fois tel un véhicule pour l'État servant à transmettre à la communauté internationale les priorités américaines en matière de politiques étrangères. (Norris, Kern et Just, 2003)

Sachant que l'autorité présidentielle est maximisée en temps de crise (Entman, 2004), nous estimons qu'elle est également accentuée lors d'une cyberattaque. D'abord en raison de la confusion sémantique associée au champ de la cyberattaque, de sa complexe définition et de son caractère sans précédent, le degré de résonance culturelle attribué à une cyberattaque semble faible. L'imaginaire populaire n'a pas de référent adéquat, les unités de sens se dégageant du concept apparaissent donc

[86] Allen, N. (2 janvier 2015). Entrevue avec John Park. *Barack Obama targets North Korea with fresh sanctions over Sony cyber-attack.* Telegraph. Récupéré de http://www.telegraph.co.uk/news/worldnews/asia/northkorea/11322791/Barack-Obama-targets-North-Korea-with-fresh-sanctions-over-Sony-cyber-attack.html.

limitées. Puis, en raison de l'absence de modèle de riposte, les solutions proposées n'ont pas de point comparatif. En ce sens, nous croyons que, dans ce cas de figure, la tendance à se fier à l'autorité présidentielle dans sa capacité à proposer des moyens qui se veulent appropriés et proportionnels, est maximisée.

En orientant le débat public sur les solutions annoncées, on peut estimer que ces deux méthodes seraient d'ordinaire moins bien perçues. (Lewis et Reese, 2009) Cela fait en sorte que le cadrage facilite la révision d'une politique intérieure controversée et l'application d'une politique extérieure hostile souvent critiquée dans l'espace public.

La théorie démontre que lorsque d'autres cadres accompagnent celui de la solution, leur contenu fait souvent référence aux valeurs américaines. (Lakoff, 2004, Entman 2004, Callaghan et Schnell, 2005, Azpiroz, 2013) Le cadre solution est davantage performant lorsqu'il s'accompagne d'un problème relatif à la liberté. (Lakoff, 2004) C'est exactement ce que reflètent nos résultats. La cyberattaque de Sony met de l'avant des solutions au problème d'atteinte à la liberté de parole et d'expression artistique, en plus de faire appel au patriotisme. Le recours à ces valeurs bénéficie d'un fort degré de résonance culturelle auprès du public. (Lakoff, 2004, Callaghan et Schnell, 2005) En effet, la liberté et le sentiment d'appartenance constituent des valeurs socialement partagées et persistantes depuis plus de deux siècles aux États-Unis. Pour paraphraser Reese, ces valeurs ont travaillé symboliquement à structurer de façon significative la société américaine. (Resse, 2001) L'atteinte à ces principes est d'ailleurs répétée et traitée avec un haut degré d'intensité par l'État. L'emploi d'une telle intensité sert d'ailleurs à justifier des résolutions orientées vers le changement politique. (Dunn-Cavelty, 2012) Le recours à la liberté permet aussi de minimiser le débat, ou à tout le moins d'édulcorer l'argumentaire de certains détracteurs. (Callaghan et Schnell, 2005, Lakoff, 2004) En ce sens, cadrer un problème sous la liberté est tel un bouclier face à la contestation, et permet d'autoriser

des solutions politiques pour enrayer son intolérable affront. Alors qu'en réalité, ni les sanctions économiques, ni le *Consumer Privacy Bill of Rights* ne permettent d'empêcher les valeurs américaines d'être brimées. C'est pourtant l'idée inverse qui teinte le discours.

Par ailleurs, la liberté possède la particularité d'être simple à comprendre, comparativement à la complexité technique d'une cyberattaque ou encore aux rapports de force décisionnels entre Sony et les chaînes de cinéma. Le recours à cette valeur en tant que problématique simple facilite la tâche des politiciens qui se doivent de communiquer un message simple et cohérent au public. (Norris, Kern et Just, 2003) Plus le problème est défini simplement, plus il voit son degré d'adhérence augmenté. Pour paraphraser Entman, plus la résonance est forte, plus grande sera l'adhérence au discours par le public. En sélectionnant l'aspect de la liberté pour expliquer la décision de Sony, la garantie de l'acceptation était presque assurée. De plus, l'évaluation fait référence au gouvernement en tant que défenseur de la liberté, tandis qu'il présente Sony comme y faisant défaut. Il vient donc fortement appuyer les deux cadres en importance.

Nous reconnaissons donc l'influence du cadrage pour altérer la compréhension de l'évènement Sony et ainsi structurer le monde social à l'avantage de l'administration Obama. La première partie de notre hypothèse, incluant les deux premières questions sectorielles, peut conséquemment être validée : le cadrage s'articule à travers l'omniprésence de solutions et tend à favoriser le changement de politiques intérieures et extérieures aux États-Unis. Nous tenons cependant à ajouter un élément essentiel qu'initialement nous n'avions pas intégré à l'hypothèse : le cadre de la définition du problème, définit en terme d'affront à la liberté de parole et d'expression artistique américaine, vient fortement appuyé le cadre de la solution.

5.4 Le cadrage de la cybersécurité

Dans cette section, notre objectif sera de situer le discours de la cyberattaque contre Sony dans une optique plus large, en le comparant à celui de la cybersécurité. La comparaison du contenu des cadres sera réalisée en portant une attention particulière aux similitudes et aux différences. Cela a pour but de relever une potentielle évolution sur le phénomène à l'étude dans les communications politiques post-Sony.

5.4.1 Le recadrage de la cyberattaque

À l'image de ce que nous avons relevé précédemment, le caractère du problème relatif à la cybersécurité est principalement formulé en termes vagues : « threat », « cyber threat », « attack », « kind of criminal attack » et « crime », validant ainsi l'existence d'une confusion sémantique. La sécurité nationale est certes menacée, mais elle est occultée par une nouvelle cible, soit la menace à l'économie, celle du pays, des entreprises et des familles américaines. Cette intégration de la dimension économique, que Dunn-Cavelty estimait en 2012 comme étant essentielle pour une meilleure gestion de la cybersécurité, quoique plutôt absente dans les discours politiques, est dans ce cas-ci intégrée au discours. Cette présence corrobore les propos de Ventre affirmant que la cybermenace à l'économie teinte depuis peu les discours politiques. (Ventre, 2015)

Au même titre que la cyberattaque, la cybersécurité est présentée comme un des problèmes les plus pressants de notre époque. Elle représente aussi une urgence tel que le relève Dunn-Cavelty (2012), qui s'organise de manière plus directe : « urgent », « one of the most serious challenge, « the most significant cyber threat that we have faced », « utmost seriousness » et « most serious ».

Cela dit, on note une évolution notable de la signification du problème dans le dernier échantillon à l'étude, daté du 2 avril 2015. Désormais, le problème de la cyberattaque est défini avec un vocable nouveau basé sur l'utilisation du préfixe cyber, « malicious cyber-enabled activity ». Les attributs de ce problème sont concrètement définis en termes d'objectifs, d'effets, de méthodes et de techniques. Puisqu'il s'agit de la seule et unique fois où l'échantillon est détaillé et que l'on nomme le problème, on se questionne sur l'apparition de cette précision. Nous croyons que le fait de donner des balises claires pour identifier un cyberévénement sert majoritairement à soutenir la mise sur pied de la nouvelle autorité pour riposter à leur présence. En d'autres termes, à nouveau le cadre de la définition du problème sert à justifier celui de la solution. De plus, cette précision donne un sens au concept de cyberattaque, et dénoue par conséquent un nœud sémantique.

Par ailleurs, cette avancée teinte également les propos du cas Sony. Loin de présenter un portrait global de la situation, le discours apporte toutefois un certain éclaircissement en spécifiant les dommages structurels, économiques et humains.

Pour la première fois, l'État cherche à occulter ouvertement la dimension politique du problème, car indépendamment de l'allégeance, le problème touche tout le monde, « companies, critical infrastructures, citizens », et tous les secteurs de la société, du commerce jusqu'à la santé. Cette tendance des acteurs gouvernementaux à évacuer la politique dans leurs discours sur la cybersécurité est aussi soulevée par Dunn-Cavelty.

Le diagnostic, antérieurement attribuable à la présence de l'ennemi nord-coréen, est plutôt posé ici au niveau macrotechnologique. Le « digital world » est en cause, car il offre des occasions d'agir aux « hackers » et aux « malicious actors ».

Quant à l'évaluation du gouvernement, elle subit un recadrage au cours des mois. En décembre, on estime que « a lot more needs to be done. We are not even close to where we need to be ». En février, on avance « we're making progress », « taken a new step », alors qu'en avril le gouvernement se dit être en contrôle de ses moyens pour protéger ses citoyens, « we all know what we need to do ». Comme le prescrit le cadrage de la cyberattaque, on aborde la prospective de situations potentiellement graves en se référant au cyberterrorisme. Cette nécessité de présenter un avenir risqué a pour but d'encourager le changement politique. (Dunn-Cavelty, 2013) Toutefois, pour chaque propos sombres, on rééquilibre constamment avec la promesse d'un avenir meilleur, basé sur l' « empowerment », l'innovation et le progrès technologique.

5.4.2 Vers des solutions plus concrètes

En ce qui a trait au premier cadre en importance de la cyberattaque de Sony, la solution, il se trouve dans une proportion encore plus marquée dans le discours sur la cybersécurité. L'aspect sélectionné est d'ailleurs le même : un gouvernement engagé tous azimuts pour prévenir et combattre le problème. Cet engagement est rendu saillant de manière fortement similaire. Cela se fait par la présence de mots clés, surtout de verbes appelant à l'engagement au temps présent. À la défense, surtout. Par le degré d'importance accordé à la solution : « first place », « first order business », « priority ». Mais aussi par leur organisation pêle-mêle dans le texte, faisant fi d'une structure de texte classique, c'est-à-dire sujet amené, posé et divisé.

On note le même appel à s'unir pour faire face au défi, et ce, surtout à l'offense. Le souhait d'une action nécessaire et urgente est perceptible, ce qui a pour effet d'encourager, selon Dunn-Cavelty, le changement politique. Ce que nous observons cependant varie considérablement de la tendance constatée par l'auteur, celle d'un

gouvernement se positionnant comme seul acteur pouvant agir dans le contrôle du cyberespace. (Dunn-Cavelty, 2012) L'État reconnaît plutôt l'impossibilité de réaliser ce défi en solo, et met l'accent sur la nécessité de coopération entre les secteurs public et privé. Il n'est pas surprenant de constater cet appel du gouvernement à l'union avec le secteur privé, car pour opérer des changements à la sécurité des systèmes, l'État a besoin des grandes entreprises de technologies (Intel, Apple, Microsoft, American Express, Google, Facebook). (Untersinger, 2015) De plus, une tension[87] subsiste entre l'État et les entreprises depuis les révélations d'Edward Snowden. Certaines d'entre elles n'auraient pas apprécié avoir été espionnées par l'administration. D'un autre côté, de hauts fonctionnaires de l'administration ont sévèrement critiqué certaines applications de Google et Apple. Une myriade d'autres tensions coexistent et contribuent à gangrener la relation du secteur public et du secteur privé. Bref, nous comprenons cet appel à l'union comme particulièrement stratégique de la part de l'administration Obama.

Au manque de clarté des solutions à la cyberattaque, les solutions à la cybersécurité se distinguent par leur niveau de précision. Elles possèdent des titres ciblant leur domaine d'application à large spectre : loi, diplomatie et outils politiques. Quatre axes stratégiques sont annoncés pour sécuriser les informations personnelles en ligne des Américains. Le même nombre de mesures mises en place est annoncé. La première vise la priorité donnée à la création du Cyber Threat Intelligence Integration Center. Ce centre aura pour mission de concentrer toutes les informations au sujet des menaces de type électronique. Une seconde annonce est faite sous décret présidentiel qui prescrit l'obligation pour les entreprises de déclarer qu'elles ont été attaquées. La

[87] Pour comprendre les tensions existantes, nous nous sommes librement inspirés du texte de Martin Untersinger intitulé *Cybersécurité : Barack Obama tend la main à la Silicon Valley méfiante* dans le quotidien Le Monde. Martin Untersinger est journaliste spécialisé dans les impacts du numérique dans la société et auteur d'*Anonymat sur Internet : comprendre pour protéger sa vie privée* (2013).

finalité de cette proposition a pour but de favoriser la remontée d'informations concernant le secteur informatique du secteur privé vers les autorités américaines. Du même coup, elle vise l'immunité des entreprises qui partageront des informations privées avec le gouvernement fédéral. La troisième annonce, déjà mentionnée dans le cadrage de la cyberattaque de Sony, requiert la collaboration du Congrès en vue de l'adoption du *Consumer Privacy Bill of Rights*. Répété à quatre reprises, l'appel est cette fois davantage présent et formulé de manière plus directe. Enfin, il y a formation d'une autorité spéciale pour imposer des sanctions aux « malicious cyber actors » impliqués dans des « malicious cyber enabled activities. En définitive, depuis janvier 2015, nous sommes témoins de nouvelles solutions impliquant le changement de politiques intérieures et extérieures. Globalement, elles cherchent l'amélioration de la communication en temps de crise par la restructuration des échanges d'informations sur la cybersécurité et la protection de la vie privée des citoyens en ligne. Nous comprenons cela comme un changement de stratégie de cybersécurité.

À l'instar du discours sur la cyberattaque, on relève la présence de la même métaphore : celle du « shérif » dans le « Wild West » pour illustrer le cyberespace, et une nouvelle, celle de la construction d'une cathédrale pour le progrès technologique. Elles apparaissent ici tel que le remarque Lawson, employées pour mobiliser et pour prouver qu'il est nécessaire de poser un plus grand nombre d'actions, en y consacrant davantage d'énergie, dans le but de contrôler le cyberespace (...) » (Lawson, 2012) On reconnaît à cette figure de style le statut de puissants mécanismes activement utilisés dans le discours pouvant façonner les perceptions. (Dunn-Cavelty, 2013)

De plus, le discours fait état de phrases clés associées à l'idée d'un temps nouveau, d'une ligne franchie depuis peu, que nous croyons fortement reliée à l'événement Sony : « As we seen in recent months », « We have to work together like never before », « to start setting up some very clear rules of the road in terms of how the Internet

and cyber operate. » Le discours de la cybersécurité à l'étude illustre bien le « continuum défense-sécurité » de Watin-Augouard (2015). En effet, nous sommes à la fois en présence d'une cyberdéfense. L'État américain se défend suite à l'attaque de Sony en imposant de nouvelles règles, tout en étant l'acteur central d'une lutte offensive contre une nouvelle entité, les « cyber-enabled activities ».

Sachant que sur le continuum temps le discours sur la cybersécurité à l'étude prend forme après l'événement Sony, nous avons relevé la présence d'évolutions où l'objet du propos est plus concret et plus précis. Principalement, il s'agit du recadrage du concept de la cyberattaque, de l'existence de nouvelles pratiques étatiques et d'une scission notable dans le discours entre l'avant et l'après Sony. En ce sens, nous avons répondu à notre troisième et dernière question sectorielle, à savoir que le discours de la cyberattaque contre Sony, en tant qu'événement impliquant un positionnement stratégique de l'État, contribue à marquer un point tournant pour la cybersécurité aux États-Unis.

Nous sommes à présent en mesure de valider notre hypothèse d'ensemble : le cadrage du discours de l'administration Obama sur la cyberattaque de Sony s'articule à travers l'omniprésence de solutions, et tend à favoriser le changement de politiques américaines intérieures et extérieures, ce qui contribue à marquer un point tournant pour la cybersécurité aux États-Unis.

CONCLUSION

Notre problématique a démontré que dans sa forme, ses implications et les transformations des rapports qu'elle engendre, la cyberattaque contre Sony est sans précédent pour l'État américain. Dans le contexte où il s'agit d'une nouvelle forme de conflit ayant une influence considérable sur la cybersécurité, nous avons souhaité analyser comment l'administration Obama articule son discours sur la cyberattaque de Sony. Dans une perspective constructiviste basée sur la théorie et l'analyse des cadres d'Entman (1993-2005), l'objectif principal de ce mémoire fut de mener une analyse du discours politique américain sur la cyberattaque de Sony. Pour ce faire, le processus de sélection et d'omission de l'information conduit par l'État américain dans la construction de ses discours a été examiné. Nous avons pu relever comment le propos est abordé et de quelle façon il est orienté de manière à altérer la compréhension du public sur la cyberattaque de Sony selon une visée d'intérêts politiques. Devenue tangible par l'extraction des cadres et leur mise en relation, la perspective de l'administration Obama a dès lors pu être interprétée.

D'abord, dans la partie initiale, nous avons démontré que l'État articule sa perspective sur le phénomène selon deux thèmes principaux : la décision de Sony et la cyberattaque en elle-même. En regard de la typologie d'Entman, c'est le cadre de solution qui a imposé son importance, suivi de la définition du problème. L'annulation du film *The Interview* et la complexité technique de la cyberattaque ont été occultées pour se concentrer sur le problème d'atteinte à la liberté de parole et d'expression artistique causée par la décision de Sony, suite aux menaces attribuées à la Corée du Nord. Déjà intégré dans l'imaginaire et simple à comprendre, l'affront à

la valeur de la liberté appelle à une résonance culturelle des plus fortes aux États-Unis. Pour combattre ce problème, l'administration Obama met de l'avant une vingtaine de solutions à caractère patriotique, valeur aussi à fort degré de résonance. En faisant abstraction des causes et des évaluations, les solutions envahissent l'espace discursif et s'imposent de facto comme valables. Proposées à une menace nouveau genre, caractérisées par la confusion sémantique et l'absence de modèle de riposte, les solutions appellent davantage le public à se fier à l'autorité présidentielle et, ainsi, à adhérer plus aisément aux deux seules solutions politiques concrètement applicables. La demande de collaboration au Congrès en vue de l'adoption du *Consumer Privacy Bill of Rights* et l'imposition de sanctions économiques à la Corée du Nord. À la lumière de ces interprétations, la première partie de l'hypothèse fut validée : le discours sur la cyberattaque de Sony oriente l'attention sur l'omniprésence de solutions et tend à favoriser le changement de politiques intérieures et extérieures aux États-Unis.

En outre, nous avons situé notre objet d'analyse dans son contexte plus large, en le comparant au discours de la cybersécurité. Puisqu'il met de l'avant les deux mêmes cadres, ce discours s'est inscrit en continuité avec celui de la cyberattaque. Il s'en est distingué cependant en proposant l'intégration d'une nouvelle cible de la menace, soit à l'économie américaine plutôt qu'uniquement à la sécurité nationale. Un nouveau vocable pour désigner une cyberattaque, « cyber-enabled activity », contribuant ainsi à diminuer la confusion sémantique associée au champ de la cyberattaque. De nouveaux axes stratégiques et des solutions plus concrètes et davantage ciblées basées sur un continuum défense-sécurité. Enfin, par la présence de marqueurs de temps entre l'avant et l'après Sony a révélé l'existence d'un réorientation où l'État déploie désormais une énergie jamais égalée auparavant. Cette avancée substantielle dans le discours de la cybersécurité a permis de valider la dernière partie de notre hypothèse :

le discours sur la cyberattaque contre Sony contribue à marquer un point tournant pour la cybersécurité américaine.

Nos résultats reflètent dans une large proportion, bien que le sujet ne soit pas le même, plusieurs des orientations théoriques présentées dans la littérature. Par ailleurs, nous n'avons pas la prétention d'affirmer que nos résultats sont généralisables au reste des discours préexistants sur les cyberattaques, étant donné le caractère sans précédent du cas Sony et le contexte de développement ultra rapide des stratégies américaines de cybersécurité.

Considérant les paramètres précis attribués à cette recherche, nous avons été dans l'obligation de passer sous silence plusieurs facteurs explicatifs qui ont sans aucun doute joué un rôle significatif dans l'évolution de la cyberattaque et, plus largement, de la cybersécurité aux États-Unis. Cette étude n'a pas la prétention de proposer une perspective globale sur le discours politique de l'État américain ayant trait au concept de cyberattaque et de cybersécurité, pas plus qu'elle ne s'inscrit dans une logique d'interprétation de la véritable politique américaine en matière de conflits relatifs au cyberespace. Elle visait plutôt une tentative de compréhension de la construction du discours politique sur un cas précis de cyberattaque.

Nous regrettons que cette recherche n'ait pu intégrer d'autres perspectives politiques en négociation et en conflit. Il aurait été opportun de la situer dans son contexte d'affrontements discursifs politiques, par exemple, avec les républicains, ou encore avec l'administration nord-coréenne. Notre analyse de cas se limitait toutefois au seul discours de l'administration Obama. L'interprétation aurait d'ailleurs été approfondie en fonction d'une littérature plus développée sur le discours politique de la cyberattaque. Toutefois, cette dernière demeure à ce jour très fragmentaire, d'où la pertinence de l'analyse de cas du présent mémoire.

Nous avons constaté un degré élevé de difficulté quant à l'évaluation de la perception de l'État américain dans la construction de son discours. Lorsqu'il est question de souligner l'influence de la perception d'une entité sur la construction de ses dires, nous savons pertinemment que nous naviguons en eaux troubles. D'abord, parce qu'il nous est ardu de saisir ce qui occupe l'esprit des communicateurs en filigrane du discours, nos interprétations des effets escomptés du cadrage sont donc parfois à la limite de la supposition. Ensuite, car nous sommes prédisposés à interpréter certains arguments avancés par l'État selon notre propre subjectivité.

Autres pistes de recherche

Dans une approche systémique, une étude comparative visant à analyser le cadrage propre aux autres systèmes du modèle en cascade d'Entman (élite, média, opinion publique) s'avère des plus pertinentes. Il serait ainsi possible de relever la compétition entre les cadres des différents systèmes et les recadrages possibles dans le temps. Nos résultats démontent certes la tendance du discours à favoriser le changement de politiques. Or, s'il a été démontré que le discours influence les perceptions, nous n'avons pas été en mesure d'adopter une approche de réception active pour analyser comment les perceptions ont été influencées. L'effet du cadrage politique sur l'opinion publique et sur les médias gagnerait à être analysé pour rendre compte de la portée de la théorie des cadres.

La problématique de la cyberattaque touche le cœur du fonctionnement de l'État en ce qu'elle menace la protection de ses citoyens et de ses entreprises, mais aussi son infrastructure. Elle engendre un lot de questionnements sur la capacité de l'État à respecter sa responsabilité de protéger. À cet effet, on reconnaît « qu'il existe une contradiction indéniable dans la stratégie nationale et internationale en matière de cybersécurité ». (Wines, 2010) Plusieurs pays et la communauté internationale sont

présentement amenés à collaborer ensemble pour lutter contre la cybermenace, alors que certains États, dont les États-Unis, représentent une cybermenace entre eux et pour leurs citoyens. Déjà durement critiqué pour espionnage informatique massif depuis l'affaire Snowden, notamment, le Pentagone n'a pourtant pas d'autre choix que d'inspirer confiance et de mettre en pratique des moyens d'améliorer la cybersécurité.

Tenant compte de ce paradoxe, nous pouvons nous demander quelles seront les prochaines stratégies de l'administration Obama pour assurer le pas de deux entre le respect de la vie privée et la responsabilité de protéger contre les cyberattaques. Dans un autre ordre d'idées, sur le plan géopolitique, comment les cyberattaques influenceront-elles l'évolution des discours et des stratégies sur la cybersécurité nationale et internationale des différentes administrations américaine, nord-coréenne, chinoise et russe ?

ANNEXE A

FIGURE « CASCADING ACTIVATION »

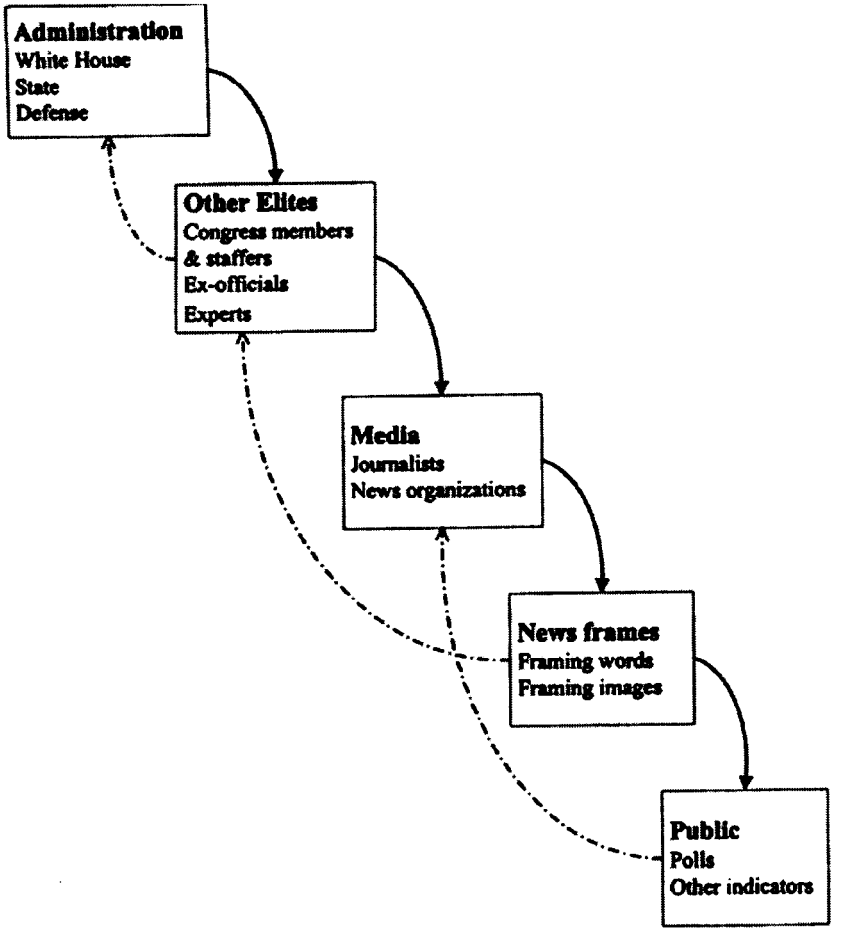

Figure A. 1 Modèle développé par Robert Entman (2003) Cascading Activation : Contesting the White House's Frame After 9/11

ANNEXE B

TABLEAUX D'ANALYSE DES CADRAGES

Tableau B.1
Conseil de sécurité nationale
Thème: Décision de Sony

Cadres	**Questions**	**Réponses**	**Composantes langagières**
Définir le problème ** Cadre mis de l'avant **	Quel est le problème?	Sony announcement regarding The Interview, such decision The U.S. respects artists' and entertainers' rights to produce and distribute content of their choosing. We take very seriously any attempt to threaten or limit artists' freedom of speech or of expression.	The Interview : mentionné pour la seule et unique fois du corpus! Liberté d'expression : valeur écrite dans la Constitution américaine, mot-clés, répétition et organisation.
Diagnostique/ Cause	Qu'est-ce qui cause le problème?	Sony	
Évaluation basée sur le jugement moral	Quels acteurs sont présentés et quels sont leurs rôles ? Qui sont les bons et les mauvais?	US : We are aware of Sony announcement, U.S. has no involvement in such decision.	Référence à l'annulation du film *The Interview* mais on ne mentionne ni le mot film, ni le titre US induit qu'il n'appuie pas Sony dans sa décision. Sous-texte: Sony a fait une erreur, U.S. auraient fait mieux. Sony : mauvais US: bon.
Solution avancée	Quelles solutions sont avancées pour régler le problème?	-N/D	
-	Notes		

Tableau B.2
Conseil de sécurité nationale
Thème: Cyberattaque

Cadres	Questions	Réponses	Composantes langagières
Définir le problème	Quel est le problème?	- Attack. - Breachs affecting US companies, U.S Consumers and U.S infrastructure, in U.S. and elsewhere	Présente en terme de criminel et pays étrangers. Breach: imprécise.
Diagnostique/ Cause	Qu'est-ce qui cause le problème ?	- We know that criminals and foreign countries regularly seek to gain access to government and private sector network. (here /elsewhere) - Perpetrators	Pas de détail, vague.
Évaluation basée sur le jugement moral	Quels acteurs sont présentés et quels sont leurs rôles ? Qui sont les bons et les mauvais?	US FBI lead investigation Sony Picture Entertainement	Pas de jugement, mais dichotomie bon vs mauvais.
Solution avancée ****** **Cadre mis de l'avant** ******	Quelles solutions sont avancées pour régler le problème?	- The US government has offered Sony Picture Entertainment support and assistance in respond to the attack - FBI has the lead for the investigation - U.S. is investigating attribution and **will provide an update at the appropriate time**. *(en gras dans le texte)* - U.S. government is working tirelessly to bring the perpetrators of this attack to justice. - **We are considering a range of options in weighing a potential response** *(en gras dans le texte)*	On ne cite pas la Corée du Nord, l'attribution n'a même pas eu lieu, mais on évoque déjà que l'on considère des solutions. Mot-clés engagement : closely monitor, support, assistance, investigation, provide, update, we know, working tirelessly, justice. U.S ou référence : we est répété 10X. US will Référence à la justice.
-	Notes	Vocabulaire possible confusion : Attack X2, breaches, seek to gain access	Reste vague dans l'utilisation des appellations.

Tableau B.3
Conférence de presse
Thème: La décision de Sony

Cadres	Questions	Réponse	Composantes langagières
Définir le problème ****** **Cadre mis de l'avant** ******	Quel est le problème?	-Imposing censorship in US -We cannot have a society in wich some dictator someplace can start imposing censorship here in the U.S. -Because if somebody is able to intimidate folks out of releasing a satirical movie, imagine what they start doing when they see a documentary that they don't like, or news reports that they don't like. Or even worse, imagine if producers and distributors and others start engaging self-censorship because they don't want to offend the sensibility of somebody whose sensibilities probably need to be offended. So that's not who we are. That's not what American is about. -We can't start changing ours patterns of behaviour any more than we stop going to a football game because there might be possibility of a terrorist attack : any more than Boston didn't run its marathon this year because of the possibility that somebody might try to cause harm. So let's not get into that way of doing business. -Image if instead of it being a cyber-threat, somebody had broken into their office and destroyed a bunch of computer and stolen disk. Is that what takes for suddenly you to pull the plug on something?	Ne nomme pas le film. Saillant: Liberté d'expression: plusieurs mot-clés, répétition et organisation à la suite les unes aux autres. 6 mises en situation/imaginaire + forme interrogative. Censure intolérable+ forme négative. Référence au sport. Américains ne plient pas .
Diagnostique/ Cause	Qu'est-ce qui cause le problème ?	Sony	
Évaluation basée sur le jugement moral	Quels acteurs sont présentés et quels sont leurs rôles ? Qui sont les bons et les mauvais?	-Again, I'm sympatic that Sony as a private company was worried about liabilities and this, and that and other. Yes, I think they (Sony) made a mistake. I wish they (Sony) had to spoken to me first. I would have told them, do not get into a pattern in wich you're intimidates by these kinds of criminal attack.	Sony a fait une erreur, U.S. auraient fait mieux. Sony : mauvais US: bon.
Solution avancée	Quelles solutions sont avancées pour régler le problème	We'll engage with not just the film industry, but the news industry and the private sector. We already have. We will continue to do so.	
-	Quelles sont les composantes langagières ?	-Référence au marathon de Boston/match de football. -Vocabulaire : criminal attack, cyber-threat, attack, terrorist attack.	

Tableau B.4
Conférence de presse
Thème : Cyberattaque de Sony

Cadres	Questions	Réponses	Composantes langagières
Définir le problème	Quel est le problème?	Attack, crime NK: They caused a lot of damage.	Pas mentionné autre qu'avec le mot "attack" dans l'attribution de la cause.
Diagnostique/ Cause	Qu'est-ce qui cause le problème ?	North Korea The FBI announced today and we can confirm that North Korea is engaged in this attack. We have no indication that North Korea was acting in conjunction with another country.	
Évaluation basée sur le jugement moral	Quels acteurs sont présentés et quels sont leurs rôles ? Qui sont les bons et les mauvais?	North Korea: I think it says something interesting about NK that they decided to have the sate mount an all- assault on a movie studio because of a satirical movie. (Laughter) I think gives you some sense of what of the kind of regime we're talking about here. U.S. government : engage on these issues	Essaie de ridiculiser l'État NK ? (il rit en parlant de l'État nord-coréen)
Solution avancée ** **Cadre mis de l'avant** **	Quelles solutions sont avancées pour régler le problème?	- We will respond. - We will respond proportionally, and we'll respond in a place and time and manner that we choose. - It's not something that I will announce here today. - We just confirmed that it was NK; we have been working up on a range of options. They will be presented to me. - I will make a decision on those based on what I believed *is proportional and appropriate* to the nature of the crime.	Nature des mesures vagues/secrètes mais convainue de l'action. Répétition: we will respond 3X consécutif. 5X we'll ou I'll appelant à l'action. Décision juste: proportional and appropriate Référence au crime. Appropriation de l'autorité présidentielle. Recours we/ I
-	Notes	Crime, attack	

Tableau B.5
Conférence de presse
Thème : La cybersécurité

Cadres	Questions	Réponse	Composantes langagières
Définir le problème	Quel est le problème?	Issue of cybersecurity is so urgent.	Ne dit pas que nos systèmes sont vulnérables.
Diagnostique/ Cause	Qu'est-ce qui cause le problème ?	Digital word = opportunities for hackers. Sort of the Wild West.	
Évaluation basée sur le jugement moral ** **Cadre mis de l'avant (2)** **	Quels acteurs sont présentés et quels sont leurs rôles ? Qui sont les bons et les mauvais?	-Weak state can engage in these kind of attacks, you've got non-state actor that can do enormous damage. -Hackers are going to be better. State actors and non state actors (...) are going to sophisticated and many of them can do some damage. - Hackers to engage cyber assaults Private & public -Next attacks; there are going to be costly, there are going to be serious. We take them with the utmost seriousness.	Prédit le futur.
Solution avancée ** **Cadre mis de l'avant (1)** **	Quelles solutions sont avancées pour régler le problème? -	-This points to the need for us to work with the international community to start setting up some very clear rules of the road in terms of how the internet and cyber operate. -Now, our first order business is making sure that we do everything to harden site and prevent those kind of attacks from taking place. -a lot more needs to done. We are not even close to where we need to be. -I hope the Congress is prepared to work with us on is strong cybersecurity lays that allow for information-sharing across private sectors plateforms, as well as the public sector. -Incorporating best practices and preventing these attacks from happening in first place. -Again, this is a part of the reason why it's going to be so important for Congress to work with up and get a actual bill passed that allows for the kind of informational sharing we need. -If we don't put in place of the kind of architecture that can prevent these attacks from taking place, this is not just going to be affecting movie, this is going to be affecting our entire economy in ways that are extraordinarily significant.	Nature de riposte floue. Riposte tributaire du jugement du Président. Prédit de potentielles attaques. Congrès: demande la collaboration sans mentionner qu'il y a divergence au sein du Congrès. To work, Prevent taking place.
-	Notes	Vocabulaire: Crime, Attacks, Hackers, Kind of criminal attacks, Cyber threat, attack	

Tableau B.6
Entrevue télévisée
Thème: Décision de Sony

Cadres	Questions	Réponse	Composantes langagières
Définir le problème ** **Cadre mis de l'avant** **	Quel est le problème?	-But what i was laying out was a principle that i think this country has to abide by We believe in free speech. We believe in the right of artistic expression and things that power that might not like. -If we set a precedent in wich dictator in another country can disrupt, through cyber (...) (if) we start censorship ourselves, that's a problem. -It's a problem not just for the entertainment industry, it's a problem for the news industry. CNN has done critical stories about North Korea. What happens if, in fact, there is a breach in CNN's, you know cyberspace? Are we going suddenly say, well, we'd better not report on North Korea? -The Boston marathon suffered an actual grievous attack that killed and maimed a number of people. Ad the next year, we had a successful a Boston Marathon as we've ever had. -Sometimes this is a matter of setting tone and being very clear that we're not going to be intimidated by some ... cyber hackers.	Aucune mention The Interview. If/conditionnel. Its a problem X3. Liberté d'expression: plusieurs mot-clés, répétition et organisation. 2 mises en situation : imaginaires + interrogatives. Censure/intolérable/forme négative. Patriotisme
Diagnostique/ Cause	Qu'est-ce qui cause le problème ?	Sony	
Évaluation basée sur le jugement moral	Quels acteurs sont présentés et quels sont leurs rôles ? Qui sont les bons et les mauvais?	-I was pretty sympatic the fact that they've got business considerations they've got to make. Had they talk to me directly about this decision. I might have called the movie theater chains and distributors and asked them what the story was. - Sony: The key here is not to suggest that Sony was a bad actor. It's making a broader point that all of us have to adapt to the possibility of cyber attacks.	Recadrage Sony US: aurait fait mieux. .
Solution avancée	Quelles solutions sont avancées pour régler le problème?		Américains ne plient pas devant la peur de la menace.
-	Notes	Référence au sport, au Marathon de Boston qualifié de grievous attack. Vocabulaire de la cyberattaque: Can disrupt through cyber, breach (cyberspace), cyber hacker.	

Tableau B.7
Entrevue télévisée
Thème : Cyberattaque de Sony (avec glissement sur la cybersécurité)

Cadres	Questions	Réponse	Composantes langagières
Définir le problème	Quel est le problème?	I don't think it was an act of war. I think it was an act of cyber vandalism that was very costly, very expensive. We take it very seriously. When other countries are sponsoring it, we take it very seriously. disrupt our live in all sorts of ways.	4X very. Nouveau mot cybervandilsm.
Diagnostique/ Cause	Qu'est-ce qui cause le problème ?	Environment in this new world so much digitalized that both state and non state actors. Other countries.	
Évaluation basée sur le jugement moral	Quels acteurs sont présentés et quels sont leurs rôles ? Qui sont les bons et les mauvais?	ND	Pas de qualificatif: minimiser l'importance du rôle de l'ennemi, pour accorder plus de place aux solutions.
Solution avancée ** **Cadre mis de l'avant** **	Quelles solutions sont avancées pour régler le problème?	We will respond *proportionally* as I said. We have to do a lot more to guard against them. We need Congress to pass a cyber security law. We have got to work with private and public sector as to work together to harden their sites. We have to threat it like we would threat the incidence of crime in our countries. I think there is something that we can manage. We can manage through, as long as public-private sector is working together. We have to go after the wrongdoer. We can't start changing how we operate. We have to do a much better job of guarding against that. We're going to review those (put North Korea back on the list of states that sponsor terrorism) through a process that's already in place.	We can manage X2. Mots clés engagement, Répétition, agencement we 10X suivit d'un verbe. 11 références au we ou I urgence d'action. Patriotisme. Solution floue sauf Congrès. Omission: CN.
-	Notes	Contre la menace. Vocabulaire cyberattaque : Not an act of war, cyber. vandalism.	

Tableau B.8
Ordre exécutif *(Sanctioning)*
Thème: Cyberattaque

Cadres	Questions	Réponses	Composantes langagières
Définir le problème ** **Cadre mis de l'avant (2)** **	Quel est le problème?	- Government of DPRK numerous provocations, particularly the recent cyber attack targeting Sony and the threat against movie theaters and moviegoers. - Destabilizing, destructives and repressive actions particularly undermine its effort to U.S. cyber-security and intimidate U.S business/artiste exercising their right of freedom of speech. - Destructive and destabilizing conduct. - Attempt to undermine our values or threaten the N-S.	Destabilizing X2, destructives X2, repressive. Liberté d'expression: right of freedom of speech, values.
Diagnostique/ Cause	Qu'est-ce qui cause le problème ?	- Government of North Korea and the Workers' Party of Korea	
Évaluation basée sur le jugement moral	Quels acteurs sont présentés et quels sont leurs rôles ?		Dichotomie claire bon vs mauvais.
Solution ** **Cadre mis de l'avant (1)** **	Quelles solutions sont avancées pour régler le problème?	- Obama signed an E.O. authorizing the imposition of sanctions against the GNK and the WPK to hold N-K accountable. We will employ *a broad set of tools to defend U.S. businesses and citizen* (Secretary of treasury) - The action taken today under the authority of the president new E.O. will further *isolated* key NK entities and *disrupt* the activities of close to a dozen critical NK operatives. We will continue *to use this broad and powerful tool to expose the activities of NK officials/entities*. This step reflect the ongoing commitment of the U.S. *to hold N-K accountable*. Today's action are driven by our commitment to hold NK accountable - (...) *escalated financial pressure* on the Governement including its agencies, instrumentalities, and controlled entities, by . (...) that would deny designated persons access to the U.S. financial system and prohibit U.S. person from engaging in transactions or dealing with it. -3 entities for being controlled entities of the Government of North Korea: (voir liste des nom dans le corpus) -Apply sanctions against officials of the NKG/WPK, and persons determined to be owned or controlled by, or acting for on behalf of, or to hve provide material support for the GNK, WPK or any other person (...) -10 Individuals for their status as officials of GNK	Tool, set of tools. Nature : +/- en lien avec la cyber attack /cybersécurité. Mot-clé action : Action taken today, apply, today's actions, ongoing commitments. Step. North Korea et dérivés : 33X. Autorité présidentielle : portée de E.O. répété plus de 10X.
	Quelles sont les composantes langagières ?	Référence à plusieurs Vocabulaire : Cyber-attack, threat	

Tableau B.9
Sommet
Thème: Cybersécurité

Cadres	Questions	Réponses	Composantes langagières
Définir le problème **Cadre mis de l'avant** (2)	Quel est le problème?	Cyberthreats : are challenge to our national security + matter of public safety+ America's economic security, a direct threat to the economic security of American families, a most serious economic national security challenge that we face as a nation + Children X 2 protect them + A threat to Americain's economy security + This is not a Republican or Democratic issue+This sould not be an ideological issue. + And that's one thing I want to emphazing : This is not a Democratic issue, or a Republican issue. This is not a Liberal or Conservative issue. + American companies are being targeted, their trade secrets stolen, intellectual property ripped off. + North Korean cyber attack on Sony Pictures destroyed data and disabled thousand of computers, and exposed the personal information of Sony employees. These attacks are hurting Americain companies and costing American jobs.	Référence à Sony en parlant des compagnies attaquées et du data des citoyens rendu public. Menace à l'économie et ce n'est pas un problème politique. (Lakoff, même valeur).
Diagnostique/ Cause **Cadre mis de l'avant** (3)	Qu'est-ce qui cause le problème ?	Much of our critical infrastructure un on net connected on the Internet.+ As a nation, we do more business online than ever before.+ As consumer, we do more online than ever before.+ As a nation we do more business online than ever before. High-technology industries support millions of American job. All this give us an enormous competitive advantage in the global economy. +Technologies + Hacker from China and Russia. + Foreign government and criminals.+ Cyber world= wild, Wild Est	Pas de mention de la Corée du Nord.
Évaluation basée sur le jugement moral **Cadre mis de l'avant** (3)	Quels acteurs sont présentés et quels sont leurs rôles ? Qui sont les bons et les mauvais?	We've boosted our defense in government, we're sharing more information with the private to help those companies defense themselves, we're working with industry to use what we call a cybersecurity framework to prevent, respond and recover from attacks.+ We're making progress, I've recently announced new actions to keep up this momentum.+ We've also taken a new step to strengthen our cybersecurity.+ To well-being of our children+ Government has to be constantly self-critical and we have to be able to have an open debate about it (intruding own privacy)	

Cadres	Questions	Réponses	Composantes langagières
Solution avancée **Cadre mis de l'avant** (1)	Quelles solutions sont avancées pour régler le problème?	We have to preserve the one of greatest engine for creativity and innovation in human history.+ I want more American succeeding in our digital world. I want young people like you to unleash the new wave of innovation, launch the next startups (...) (empower individual) + First, this has to be a shared mission (Government and industry working together as true partner)+ Second, we have to focus on our unique strengths (Government/private sector do it together) + Third, we're going to have a constantly evolve (attacks are getting more and more sophisticated every day)+ Fourth, and the most important, in all our work we have to make sure we are protecting the privacy of civil liberty of the American people. (reforms)+ We are calling on Congress not to engage in politics but make work to make sure that our security is safeguarded and that we have to fund the Department of Homeland Security.+ We'll called for a single national standard+ We'll be proposing legislation that we call Consumer Privacy Bill of Rights+ I'm once again calling on Congress to together and get this done.+ This week, we announced the creation of our new Cyber Threat Intelligence Integration Center +. I'm signing a new e.o. to promote even more information sharing about cyberthreats (between private sector & government) + We all know what we need to do. We have to build stronger defense and disrupt more attacks. We have make cyberspace safer. We have to improve cooperation across the board. + All of us working together to do what none of achieve alone.	Sur les 28 paragraphes: 17 sont consacrés à la proposition de solutions. Mobilisation + unir. On s'adresse directement aux acteurs. à tous, aux Américains, aux étudiants, aux compagnies en en nommant 9, aux industries, au Congres, aux républicains, aux démocrates, aux enfants, aux law teacher. We suivi d'un verbe appelant a l'action : 14 fois. 2X appel au Congrès
-	Notes	Positif + Comparaison au terrorisme + Métaphore : Wild West. (...) we'are asked to be the sheriff Cathedral (3 paragraphes) .	

Tableau B.10
Ordre exécutif *(Blocking)*
Thème : Cybersécurité

Cadres	Questions	Réponses	Composantes langagières
Définir le problème **Cadre mis de l'avant** (1)	Quel est le problème?	Threat posed by **malicious cyber actors.** **Cyber threat** pose one of the **most serious economic and national security challenges** to the U.S. These **threats** can emanate from a range of sources and target our critical infrastructure, our companies and our citizens. The malicious **cyber-enabled activity** must have the purpose or effect of significantly harming or compromising critical infrastructure; misappropriating funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain; knowingly receiving or using trade secrets that were stolen by cyber-enabled means for commercial or competitive advantage or private financial gain; disrupting the availability of a computer or network of computers (for example, through a denial of service attack); and attempting, assisting or providing material support for any of the above activities. **(...) the most significant cyber threat that we face.** (...) engage **in malicious cyber enabled activities** that create a significant **threat to** the national security, foreign policy, or economic, health, financial stability of U.S. **to counter the threat posed** by **malicious cyber actors the most serious malicious cyber threats** that we face.	L'utilisation de "our" pour unir/mobiliser. Focus sur la définition de la menace, du danger qui guette les États-Unis. Significant malicious : flou mais une nomenclature est pour une fois posée.
Diagnostique/ Cause	Qu'est-ce qui cause le problème ?	Malicious cyber actors	
Évaluation basée sur le jugement moral	Quels acteurs sont présentés et quels sont leurs rôles ?	Malicious versus United State + Administration	
Solution avancée **Cadre mis de l'avant** (2)	Quelles solutions sont avancées pour régler le problème?	Provide a new authority to respond to the treat+ Pursuising a comprehensive strategy to **control** them.+ This E.O offers a targeted tool for countering. + Authorizes to impose sanctions on individuals or entities. + Employ the authorities of my office and this Administration, including diplomatic engagement, trade policy tools, and law enforcement mechanism. + A new Authority to **combat**	We À chacune des six solutions proposées, on rappelle son but : contrer la menace.
-	Notes	The most significant. Most serious malicious cyber threat that we face (répété 2 X). Threat. Nouveau préfixe: cyber-enabled activity, respond, confront, countering, counter, combat.	Dynamique de défense face à la menace + aucune mention de l'amélioration de nos systèmes informatiques.

ANNEXE C

TABLEAU SOMMAIRE DES CADRAGES

Les trois thèmes relevés et leur(s) cadrage(s) respectif(s)

Thèmes	Tableau	Cadre Problème	Cadre Cause	Cadre Évaluation	Cadre Solution
Décision de Sony	Tableau B.1 Conseil de sécurité nationale 17 décembre 2014	X			
	Tableau B.3 Conférence de presse 19 décembre 2014	X			
	Tableau B.6 Entrevue télévisée 21 décembre 2014	X			
Cyberattaque de Sony	Tableau B.4 Conférence de presse 19 décembre 2014				X
	Tableau B.1 Conseil de sécurité nationale 17 décembre				X
**Glissement sur la cybersécurité	Tableau B.7 Entrevue télévisée 21 décembre 2014				X
	Tableau B.8 Ordre exécutif (*Sanctioning*) 2 janvier 2015				X
Cybersécurité	Tableau B.5 Conférence de presse 19 décembre 2014			X (2)	X (1)
	Tableau B.9 Sommet 13 février 2015	X (2)	X(4)	X (3)	X (1)
	Tableau B.10 Ordre exécutif *(Blocking)* 2 avril 2015	X(1)			X (2)

ANNEXE D

ÉCHANTILLONS 1 À 6

Échantillon 1. Déclaration du National Security Council

"The U.S. government closely monitors all reports of breaches affecting U.S. companies, U.S. consumers, and U.S. infrastructure. We know that criminals and foreign countries regularly seek to gain access to government and private sector networks – both in the United States and elsewhere.

"The U.S. government has offered Sony Pictures Entertainment support and assistance in response to the attack. The FBI has the lead for the investigation. The United States is investigating attribution and **will provide an update at the appropriate time**. The U.S. government is working tirelessly to bring the perpetrators of this attack to justice, and **we are considering a range of options in weighing a potential response**.

"We are aware of Sony's announcement regarding ''The Interview.' The United States respects artists' and entertainers' right to produce and distribute content of their choosing. The U.S. government has no involvement in such decisions. We take very seriously any attempt to threaten or limit artists' freedom of speech or of expression."

Échantillon 2. *Remarks by the President in Year-End Press Conference.*

(...)

Q Thank you, Mr. President. I'll start on North Korea -- that seems to be the biggest topic today. What does a proportional response look like to the Sony hack? And did Sony make the right decision in pulling the movie? Or does that set a dangerous precedent when faced with this kind of situation?

THE PRESIDENT: Well, let me address the second question first. Sony is a corporation. It suffered significant damage. There were threats against its employees. I am sympathetic to the concerns that they faced. Having said all that, yes, I think they made a mistake.

In this interconnected, digital world, there are going to be opportunities for hackers to engage in cyber assaults both in the private sector and the public sector. Now, our first order of business is making sure that we do everything to harden sites and prevent those kinds of attacks from taking place. When I came into office, I stood up a cybersecurity interagency team to look at everything that we could at the government level to prevent these kinds of attacks. We've been coordinating with the private sector, but a lot more needs to be done. We're not even close to where we need to be.

And one of the things in the New Year that I hope Congress is prepared to work with us on is strong cybersecurity laws that allow for information-sharing across private sector platforms, as well as the public sector, so that we are incorporating best practices and preventing these attacks from happening in the first place.

But even as we get better, the hackers are going to get better, too. Some of them are going to be state actors; some of them are going to be non-state actors. All of them are going to be sophisticated and many of them can do some damage.

We cannot have a society in which some dictator someplace can start imposing censorship here in the United States. Because if somebody is able to intimidate folks out of releasing a satirical movie, imagine what they start doing when they see a documentary that they don't like, or news reports that they don't like. Or even worse, imagine if producers and distributors and others start engaging in self-censorship because they don't want to offend the sensibilities of somebody whose sensibilities probably need to be offended.

So that's not who we are. That's not what America is about. Again, I'm sympathetic that Sony as a private company was worried about liabilities, and this and that and the other. I wish they had spoken to me first. I would have told them, do not get into a

pattern in which you're intimidated by these kinds of criminal attacks. Imagine if, instead of it being a cyber-threat, somebody had broken into their offices and destroyed a bunch of computers and stolen disks. Is that what it takes for suddenly you to pull the plug on something?

So we'll engage with not just the film industry, but the news industry and the private sector around these issues. We already have. We will continue to do so. But I think all of us have to anticipate occasionally there are going to be breaches like this. They're going to be costly. They're going to be serious. We take them with the utmost seriousness. But we can't start changing our patterns of behavior any more than we stop going to a football game because there might be the possibility of a terrorist attack; any more than Boston didn't run its marathon this year because of the possibility that somebody might try to cause harm. So let's not get into that way of doing business.

Q Can you just say what the response would be to this attack? Would you consider taking some sort of symbolic step like watching the movie yourself or doing some sort of screening here that –

THE PRESIDENT: I've got a long list of movies I'm going to be watching. (Laughter.)

Q Will this be one of them?

THE PRESIDENT: I never release my full movie list.

But let's talk of the specifics of what we now know. The FBI announced today and we can confirm that North Korea engaged in this attack. I think it says something interesting about North Korea that they decided to have the state mount an all-out assault on a movie studio because of a satirical movie starring Seth Rogen and James Flacco [Franco]. (Laughter.) I love Seth and I love James, but the notion that that was a threat to them I think gives you some sense of the kind of regime we're talking about here.

They caused a lot of damage, and we will respond. We will respond proportionally, and we'll respond in a place and time and manner that we choose. It's not something that I will announce here today at a press conference.

More broadly, though, this points to the need for us to work with the international community to start setting up some very clear rules of the road in terms of how the Internet and cyber operates. Right now, it's sort of the Wild West. And part of the problem is, is you've got weak states that can engage in these kinds of attacks, you've got non-state actors that can do enormous damage. That's part of what makes this

issue of cybersecurity so urgent.

Again, this is part of the reason why it's going to be so important for Congress to work with us and get a actual bill passed that allows for the kind of information-sharing we need. Because if we don't put in place the kind of architecture that can prevent these attacks from taking place, this is not just going to be affecting movies, this is going to be affecting our entire economy in ways that are extraordinarily significant. And, by the way, I hear you're moving to Europe. Where you going to be? (...)

Q Thank you, Mr. President. I wanted to ask about Cuba. What would you say to dissidents or democracy advocates inside Cuba who fear that the policy changes you announced this week could give the Castro regime economic benefits without having to address human rights or their political system? When your administration was lifting sanctions on Myanmar you sought commitments of reform. Why not do the same with Cuba? And if I could just follow up on North Korea. Do you have any indication that North Korea was acting in conjunction with another country, perhaps China?

THE PRESIDENT: We've got no indication that North Korea was acting in conjunction with another country. (...)

Q I want to follow on that by asking, under what conditions would you meet with President Castro in Havana? Would you have certain preconditions that you would want to see met before doing that? And on the hack, I know that you said that you're not going to announce your response, but can you say whether you're considering additional economic or financial sanctions on North Korea? Can you rule out the use of military force or some kind of cyber hit of your own?

THE PRESIDENT: I think I'm going to leave it where I left it, which is we just confirmed that it was North Korea; we have been working up a range of options. They will be presented to me. I will make a decision on those based on what I believe is proportional and appropriate to the nature of this crime. (...)

Échantillon 3. Le président Obama en entrevue à "State of Union" sur CNN

CANDY CROWLEY, HOST: First of all, happy holidays. Thank you for joining us.

BARACK OBAMA, PRESIDENT OF THE UNITED STATES: Happy holidays, Candy.

CROWLEY: Thank you. I want to just start out talking about Sony and North Korea...

OBAMA: Right.

CROWLEY: - because the chairman of Sony which had your news conference...

OBAMA: Right.

CROWLEY: - and said he didn't think you understood what actually happened, that Sony was committed to putting the movie out, but the movie theaters came to them and said, yes, we're not going to run it, that he's not had a digital entity come to him to ask that, listen, how about putting it on YouTube and he said, maybe.
He said he was kind of disappointed in what you said.

OBAMA: Well, look, I was pretty sympathetic to the fact that they've got business considerations they've got to make. And, you know, had they talked to me directly about this decision, I might have called the movie theater chains and distributors and asked them what that story was.

But what I was laying out was a principle that I think this country has to abide by. We believe in free speech. We believe in the right of artistic expression and things that powers that be might not like.

And if we set a precedent in which a dictator in another country can disrupt, through cyber, you know, a company's distribution chain or its products and, as a consequence, we start censoring ourselves, that's a problem.

And it's a problem not just for the entertainment industry, it's a problem for the news industry. CNN has done critical stories about North Korea.

What happens if, in fact, there is a breach in CNN's, you know, cyberspace?
Are we going to suddenly say, well, we'd better not report on North Korea?
So the key here is not to suggest that Sony was a bad actor. It's making a broader

point that all of us have to adapt to the possibility of cyber attacks. We have to do a lot more to guard against them.

My administration has taken a lot of strides in that direction, but we need Congress to pass a cyber security law. We've got to work with the private sector and the private sector has to work together to harden their sites.
But in the meantime, when there's a breach, we have to go after the wrongdoer. We can't start changing how we operate.

CROWLEY: I wonder if maybe it was fear of lawsuit as opposed to fear of North Korea...

OBAMA: Which is possible.

CROWLEY: - that - there's that threat right there that - that people are looking at their theater thinking, you know, anything happens here, I'm - I'm done.

OBAMA: You know, that's possible. But, look, as I said, you know, the Boston Marathon suffered an actual grievous attack that killed and maimed a number of people. And that next year, we had a successful a Boston Marathon as we've ever had.

You know, sometimes this is a matter of setting a tone and being very clear that we're not going to be intimidated by some, you know, cyber hackers.
And I expect all of us to remember that and operate on that basis going forward.

CROWLEY: Do you think this was an act of war by North Korea?

OBAMA: No, I don't think it was an act of war. I think it was an act of cyber vandalism that was very costly, very expensive. We take it very seriously. We will respond proportionately, as I said.

But, you know, we're going to be in an environment in this new world where so much is digitalized that both state and non-state actors are going to have the capacity to disrupt our lives in all sorts of ways. We have to do a much better job of guarding against that. We have to treat it like we would treat, you know, the incidence of crime, you know, in our countries. When other countries are sponsoring it, we take it very seriously. But, you know, I think this is something that we can manage...(COUGHING)

OBAMA: But that's something that I think we can manage through, as long as public-private sector is working together. **(...)**

CROWLEY: And, finally, will you put North Korea back on the list of states that sponsor terrorism and will you take Cuba off?

OBAMA: We're going to review those through a process that's already in place. We've got very clear criteria as to what it means for a state to sponsor terrorism. And we don't make those judgments just based on the news of the day. We look systematically at what's been done and based on those facts, we'll make those determinations in the future.

CROWLEY: And the - do you lean a direction of those? It seems given what North Korea - what we know North Korea has done in terms of its cyber attacks?

OBAMA: I'll - I'll wait to review what, you know, what the findings are.

CROWLEY: Right. And it would be hard to have relationships with Cuba, wouldn't it, if they were still on the terror (INAUDIBLE)?

OBAMA: I think so.

CROWLEY: Yes.

OBAMA: But a - but we'll take a look at it. (...)

Échantillon 4. Annonce d'un ordre exécutif *Treasury Imposes Sanctions Against the Government of The Democratic People's Republic Of Korea*

Action Targets the Government of North Korea in Response to Recent Provocations

WASHINGTON – In response to the Government of the Democratic People's Republic of Korea's numerous provocations, particularly the recent cyber-attack targeting Sony Pictures Entertainment and the threats against movie theaters and moviegoers, President Obama today signed an Executive Order (E.O.) authorizing the imposition of sanctions against the Government of North Korea and the Workers' Party of Korea. This step reflects the ongoing commitment of the United States to hold North Korea accountable for its destabilizing, destructive and repressive actions, particularly its efforts to undermine U.S. cyber-security and intimidate U.S. businesses and artists exercising their right of freedom of speech.

Pursuant to the authorities of this new E.O., Treasury today has designated three entities and 10 individuals for being agencies or officials of the North Korean government.

"Today's actions are driven by our commitment to hold North Korea accountable for its destructive and destabilizing conduct. Even as the FBI continues its investigation into the cyber-attack against Sony Pictures Entertainment, these steps underscore that we will employ a broad set of tools to defend U.S. businesses and citizens, and to respond to attempts to undermine our values or threaten the national security of the United States," said Secretary of the Treasury Jacob J. Lew. "The actions taken today under the authority of the President's new Executive Order will further isolate key North Korean entities and disrupt the activities of close to a dozen critical North Korean operatives. We will continue to use this broad and powerful tool to expose the activities of North Korean government officials and entities."

Targeting the Government of North Korea and the Workers' Party of Korea

The E.O. signed today escalates financial pressure on the Government of North Korea, including its agencies, instrumentalities, and controlled entities, by authorizing targeted sanctions that would deny designated persons access to the U.S. financial system and prohibit U.S. persons from engaging in transactions or dealings with it.

The E.O. authorizes the Secretary of the Treasury, in consultation with the Secretary of State, to apply sanctions against officials of the Government of North Korea and the Workers' Party of Korea, and persons determined to be owned or controlled by, or acting for or on behalf of, or to have provided material support for the Government

of North Korea, Workers' Party of Korea, or any other person whose property and interests in property are blocked pursuant to the Order.

Designations under the New E.O.

The following three entities are designated under the E.O. signed by the President today for being controlled entities of the Government of North Korea:

· **Reconnaissance General Bureau (RGB):** RGB is North Korea's primary intelligence organization and is involved, inter alia, in a range of activities to include conventional arms trade proscribed by numerous United Nations Security Council Resolutions. RGB was previously listed in the annex to E.O. 13551 on August 30, 2010. RGB is responsible for collecting strategic, operational, and tactical intelligence for the Ministry of the People's Armed Forces. Many of North Korea's major cyber operations run through RGB.

· **Korea Mining Development Trading Corporation (KOMID):** KOMID is North Korea's primary arms dealer and main exporter of goods and equipment related to ballistic missiles and conventional weapons. KOMID, a North Korean state-owned entity, was previously listed in the annex to E.O. 13382 on July 1, 2005 for its role in North Korea's proliferation of weapons of mass destruction. It was also sanctioned by the United Nations in April 2009. KOMID has offices in multiple countries around the world and facilitates weapons sales for the North Korean government.

· **Korea Tangun Trading Corporation** is subordinate to the Second Academy of Natural Sciences and is primarily responsible for the procurement of commodities and technologies to support North Korea's defense research and development programs, including materials that are controlled under the Missile Technology Control Regime (MTCR) or the Australia Group. Tangun Trading Corporation was designated by the Department of State pursuant to E.O. 13382 in September 2009 and was designated by the United Nations in 2009. The identifier information for this designated entity is also being updated to include several aliases it uses to operate internationally. The new aliases for Korea Tangun Trading Corporation include Ryung Seng Trading Corporation, Ryungseng Trading Corporation, and Ryungsong Trading Corporation.

The following 10 individuals are designated under the E.O. signed by the President today for their status as officials of the North Korean government:

· **Kil Jong Hun** and **Kim Kwang Yon** are officials of the North Korean government and represent the southern African interests of KOMID. Kil Jong Hun is KOMID's Representative in Namibia and an official of the North Korean

government.

· **Jang Song Chol** is a KOMID representative in Russia and an official of the North Korean government. He is working with individuals in Sudan who are procuring materials from him.

· **Yu Kwang Ho** is an official of the North Korean government.

· **Kim Yong Chol** is a KOMID Representative in Iran and an official of the North Korean Government.

· **Jang Yong Son** is a KOMID Representative in Iran and an official of the North Korean government.

· **Kim Kyu** is the KOMID External Affairs Officer and an official of the North Korean government.

· **Ryu Jin** and **Kang Ryong** are KOMID officials operating in Syria and are officials of the North Korean government.

· **Kim Kwang Chun** is a Korea Tangun Trading Corporation representative in Shenyang, China and an official of the North Korean government.

Échantillon 5. *Remarks by the President at the Cybersecurity and Consumer Protection Summit*

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 6. *Annonce d'un ordre exécutif Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities*

Today, I issued an Executive Order that provides a new authority to respond to the threat posed by malicious cyber actors. Cyber threats pose one of the most serious economic and national security challenges to the United States, and my Administration is pursuing a comprehensive strategy to confront them. As we have seen in recent months, these threats can emanate from a range of sources and target our critical infrastructure, our companies, and our citizens. This Executive Order offers a targeted tool for countering the most significant cyber threats that we face.

This Executive Order authorizes the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, to impose sanctions on individuals or entities that engage in malicious cyber-enabled activities that create a significant threat to the national security, foreign policy, or economic health or financial stability of the United States. The malicious cyber-enabled activity must have the purpose or effect of significantly harming or compromising critical infrastructure; misappropriating funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain; knowingly receiving or using trade secrets that were stolen by cyber-enabled means for commercial or competitive advantage or private financial gain; disrupting the availability of a computer or network of computers (for example, through a denial of service attack); and attempting, assisting or providing material support for any of the above activities.

I intend to employ the authorities of my office and this Administration, including diplomatic engagement, trade policy tools, and law enforcement mechanisms, to counter the threat posed by malicious cyber actors. This Executive Order supports the Administration's broader strategy by adding a new authority to combat the most serious malicious cyber threats that we face.

RÉFÉRENCES BIBLIOGRAPHIQUES

Arnold, B. Kelley, M.-B.Weisman A. (2014, 17 décembre). Sony Just Canceled The Dec. 25 Release Of 'The Interview'. *Business Insider*. Récupéré de http://www.businessinsider.com/reports-top-movie-theater-chains-just-caved-to-sony-hackers-2014-12#ixzz3kzdNPGVL

Auboussier, J.P. (2009). *L'antimondialisation dans la presse écrite française : évènement, problème public et discours social.* (Thèse de doctorat). Université Lumière Lyon 2. Récupéré de http://theses.univ-lyon2.fr/documents/getpart.php?id=lyon2.2009.auboussier_jp&part=158045#Noteftn190

Azpíroz, M-L. (2014). Framing and Political Discourse Analysis: Bush's trip to Europe in 2005. *Observatorio (OBS*) Journal*, 8(3), 075-96.

Bardier, T. (2013, 16 décembre). Décomposition systémique d'une cyberattaque, dissymétries et antifragilité. *Cyberstratégie*. Récupéré de http://www.cyberstrategie.org/?q=fr/cyberchronique-ndeg1-decomposition-systemique-cyberattaque-dissymetries-antifragilite

Block, Melissa. (19 décembre 2014). Entrevue avec Michael Lynton. *NPR*. Récupéré de http://www.npr.org/sections/thetwo-way/2014/12/19/371966188/ceo-says-sony-pictures-did-not-capitulate-is-exploring-options.

British Broadcasting Corporation. (2014, 2 décembre). *North Korea refuses to deny Sony Pictures cyber-attack.* BBC. Récupéré de http://www.bbc.com/news/world-asia-30283573

Burch, J. (2015, mars). Brave New World: The Future of Cyberspace & Cybersecurity. *Homelandsecurity*. Récupéré de http://inhomelandsecurity.com/brave-new-world-the-future-of-cyberspace-cybersecurity/

Cefaï, D. et Gardella, E. (2012). Comment analyser une situation selon le dernier Goffman. Récupéré de http://www.academia.edu/3252243/Comment_analyser_une_situation_selon_le_dernier_Goffman_De_Frame_Analysis_à_Forms_of_Talk

Charaudeau P. (2005). *Le discours politique. Les masques du pouvoir*. Paris: Vuibert.

Chen, T., Jarvis, L., MacDonald, S. (2014, juin). *Cyberterrorism, Understanding, Assessment, and Response*. New York: Springer. 215 p.

Choi, J. (2005). *Framing North Korea as an "axis of evil : A comparative analysis of North K o r e a in the U.S. and South Korean newspapers*. PhD dissertation, Université du Minnesota.

Choi, J. (2006, 16 juin). *Framing the National Image of North Korea in the U.S. News Media*. Communication présentée dans le cadre de International Communication Association meeting à Dresden du 19 au 23 juin 2006. Récupéré de http://citation.allacademic.com/meta/p92479_index.html

Choi, J. (2009). *Framing North Korea: How do American and South Korean newspapers fram North Korea*? Séoul: CommunicationsBooks.

Choi, J. (2010). The Representation of North Korean National Image in National Newspapers in the United States. *Public Relations Reviews*, 36, 392-394.

Cook, J. (2014, 16 décembre). Sony Hackers Have Over 100 Terabytes Of Documents. Only Released 200 Gigabytes So Far. *Business Insider*. Récupéré de http://www.businessinsider.com/the-sony-hackers-still-have-a-massive-amount-of-data-that-hasnt-been-leaked-yet-2014-12

Cox G. et Cubbings, M. (1993). *Legislative Leviathan: Party Government in the House*. Berkeley: University of California press.

De Vresse, C.H. (2005). News framing: Theory and typology. *Information Design Journal*. 13(1). 51-62.

Dearing, J.W. et Rogers E. (1996). *Agenda Setting*. Californie: Sage publications.

Département du Trésor. (2015, 1er janvier). Treasury Imposes Sanctions Against the Government of The Democratic People's Republic Of Korea. Gouvernement des États-Unis. Annonce d'un ordre exécutif pour sanctionner la Corée du Nord. Récupéré de http://www.treasury.gov/press-center/press-releases/Pages/jl9733.aspx

Desforges, A. (2014, 28 avril) Les représentations du cyberespace : un outil géopolitique. *Hérodote*. 152, 67-79. Récupéré de http://www.herodote.org/IMG/pdf/Desforges.pdf

Dictionnaire Web L'internaute. (2015). Récupéré de http://www.linternaute.com/dictionnaire/fr/definition/cyber/.

Dunn-Cavelty, M. (2013, mars). From Cyber-Bombs to Political Fallout: Threat Representations with discourse. *International Studies Review* (Impact Factor: 0.74). 15(1).

Dunn-Cavelty, M. (2012, juin). *The militarisation of cyberspace: Why less may be better*. Communication présentée à Cyber Conflict Conference, à Tallin, du 5 au 8 juin 2012. (p.1 à 13). Tallin. Récupéré de http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6243971&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6243971

Dunn-Cavelty, M. (2007). Cyber-Terror - Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate. *Journal of Information Technology and Politics, Vol. 1, No. 4, pp. 19-3*

Edger, G. (2014, 18 décembre). *Sony canceled the release of 'The Interview.' Here's how it could come out.* Washington Post. Récupéré de https://www.washingtonpost.com/lifestyle/style/sony-canceled-the-release-of-the-interview-heres-how-it-could-come-out/2014/12/19/119e3328-8791-11e4-a702-fa31ff4ae98e_story.html.

Entman, Robert M. (2008). Theorizing Mediated Public Diplomacy: The U.S. Case. *The International Journal of Press/Politics*, 13 (2), 87-102.

Entman, R. M. (2004). *Projections of Power: Framing News, Public Opinion, and U.S. Foreign Policy*. Chicago: University of Chicago Press.

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

Federal Bureau of Investigation. (2014, 19 décembre). *Update on Sony Investigation.* [Communiqué] (202) 324-3691. Récupéré de http://www.un.org/News/fr-press/docs//2012/SGSM14567.doc.htm

Finkle, J. (2014, 9 décembre). FBI official says 'no attribution' to North Korea in Sony hack probe. *Reuters.* Récupéré de http://www.reuters.com/article/2014/12/09/us-sony-cybersecurity-fbi-idUSKBN0JN1MF20141209

Foucault M. (1966). *Les Mots et les Choses.* Paris : Gallimard.

Foucault M. (1969). *L'Archéologie du savoir.* Paris : Gallimard.

Foucault M. (1971). *L'Ordre du discours.* Paris: Gallimard.

Gadamer, H. G. (1991). *Écrits II: herméneutique et champ de l'expérience humaine,* Paris : Aubier.

Gans, H.J. (1979). *Deciding What's News.* London: Constable.

Gartzke, E. The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. *MIT Press Journal.* International Security, Automne 2013, 38 (2). Récupéré de http://www.mitpressjournals.org/doi/abs/10.1162/ISEC_a_00136#.VWD9LWChCQs

Gennette, G. (1982). *Palimpsestes (La littérature au second degré).* Collection poétique. Paris : Seuil.

Géré, F. (2011, 29 novembre). De la cybersécurité à la cyberstratégie. Dans Cyberstratégie : un nouveau domaine de la pensée stratégique. Acte de colloque organisé par l'Alliance géostratégique et l'Écoles de Saint-Cyr Coëtquidan à Paris le 25 novembre 2011. Paris : École militaire.

Gitlin, T. (1980). *The Whole World Is Watching: Mass Media in the making and unmaking of the new Left.* Los Angeles and London: University of California Press.

Goffman, E. (1974). *Frame Analysis.* Boston: Northeastern Press.

France. Élysée. (2013, 29 avril). *Livre blanc sur la défense et la sécurité nationale.* Rapport de la commission sur le Livre blanc sous la présidence de Jean-Marie Guéhenno. [Document PDF]. Paris: Gouvernement Français. Récupéré de http://www.elysee.fr/assets/pdf/Livre-blanc-sur-la-Defense-et-la-Securite-nationale.pdf.

Hathaway, O. A., Crootof, R., Levitz, P. et Perdue, W. (2012). The Law of Cyber-Attack. *California Law Review*. 100(4): 817-885. Récupéré de Available at: http://scholarship.law.berkeley.edu/californialawreview/vol100/iss4/2

Heidegger, M. (1990). *Être et Temps*. (trad. François Vezin) Paris : Gallimard

Heung-k. K. (2014, 19 décembre). Cyberattaque contre Sony : un exercice nord-coréen ? *ICI Radio-Canada*. Récupéré de https://www.cgionline.org/articles/cyberattaque-contre-sony-un-exercise-nord-coreen

Hottot, K. (2015, 4 février). Sony redresse le cap, malgré l'attaque de Sony Pictures. *Nextinpact*. Recupéré de http://www.nextinpact.com/news/92967-sony-redresse-cap-malgre-attaque-sony-pictures.htm

Huygue, F-B. (2014, 27 décembre). *La lutte contre les attaques informatiques*. Le site de François-Bernard Huyghe. Récupéré de http://www.huyghe.fr/actu_620.htm

Iyengar, S. (1991). *Is anyone responsible?* Chicago: University of Chicago Press.

Jordan B. (2014, 29 décembre). Experts: North Korea May Not Have Hacked Sony After All. *Defensetech.org*. Récupéré de http://defensetech.org/2014/12/29/experts-north-korea-may-not-have-hacked-sony-after-all/#ixzz3Vi0FYBjj

Kadivar, M. (2014, novembre). Cyber-Attack Attributes. *Technology Innovation Management Review, Edition Cybersecurity*, 2 (3). Récupéré de http://timreview.ca/issue/2014/november

Kahneman, D., et Tversky, A. (1984). Choice, values, and frames. *American Psychologist. 39,* 341-350.

Keller, R. (2007). L'analyse de discours du point de vue de la sociologie de la connaissance. Une perspective nouvelle pour les méthodes qualitatives. *Recherche Qualitative*, Hors série (3); 287-306. Récupéré de http://www.recherche-qualitative.qc.ca/documents/files/revue/hors_serie/hors_serie_v3/Keller-FINAL2.pdf

Kelsey, E., Richwine, L. et Shina-Roy P. (2014, 18 décembre). *Sony cancels North Korea movie in apparent win for Pyongyang hackers*. Reuters. Récupéré de : http://www.reuters.com/article/2014/12/18/us-sony-cybersecurity-theaters-idUSKBN0JV2MA20141218.

Kempf, O. (2013, 13 février). Stratégie du cyberespace. *La revue géopolitique.* Récupéré de http://www.diploweb.com/Strategie-du-cyberespace.html

Kendall, G. et Wickham, G. (1999). *Using Foucault's Methods*. London: Sage

Kennedy, John R. Global News. (18 décembre, 2014). Hollywood reacts to Sony decision to cancel The Interview release. *Global News*. Récupéré de http://globalnews.ca/news/1733720/hollywwod-reacts-to-sony-decision-to-cancel-the-interview-release/

Kinder, D.R. et Sanders, L.M. (1990). Mimicking Political Debate with Survey Questions: The Case of White Opinion on Affirmative Action for Blacks. *Social Cognition.* 8, 73-103.

Korean Central News Agency. (2014, 20 décembre). *DPRK Foreign Ministry Rejects U.S. Accusation against Pyongyang over Cyber Attack.* Récupéré dans l'onglet Past News de http://www.kcna.co.jp/index-e.htm

Kristeva. J. (1969). *Sèmiôtikè. Recherche sur une sémanalyse*. Paris : Seuil.

Kuypers, J.A. (2006). *Bush's War: Media Bias and Justifications for War in a Terrorist Age.* Lanham, MD: Rowman & Littlefield

Kyodo. (2014, 17 décembre). *Cyberattacks detected in Japan doubled to 25.7 billion in 2014. Japan Times.* Récupéré de http://www.japantimes.co.jp/news/2015/02/17/national/crime-legal/cyberattacks-detected-in-japan-doubled-to-25-7-billion-in-2014/

Lakoff, G. (2004). *Don't Think of an Elephant! Know Your Values and Frame the Debate*. Vermont: Chelsea Green Publishing

Lakoff, G. (2005, 31 juillet). War on Terror, Rest in Peace. Alternet. Récupéré de http://www.alternet.org/story/23810/war_on_terror,_rest_in_peace

Lakoff, G. (24 février 2009). George Lakoff on The Obama Code. *Five Thirty Eight.* Récupéré de http://fivethirtyeight.com/features/george-lakoff-on-obama-code/

Larousse (2015). Dictionnaire. Récupéré de http://www.larousse.fr/dictionnaires/francais/pirate/61126

Lévesque, E. (2007). Les velléités nucléaires nord-coréennes dans la ligne de mire des États-Unis: une explication décisionnelle des crises de 1994 et 2002. (Mémoire de maîtrise). Université du Québec à Montréal.

Lewis S.C. et S. D. Reese. (2009). What is The War on Terror ? Framing Through The Eyes of Journalists. *Journalism and Mass Communication Quaterly*, 89 (1), 85-102

Libicki, M. (1er et 2ième trimestre, 2014). De Tallinn à Las Vegas. Une cyberattaque d'importance justifie t-elle une réponse cinétique ? *Hérodote* (152-153). Récupéré de http://www.herodote.org/spip.php?article627

Lim, J., et Seo, H. (2009). Frame flow between government and the news media and its effects on the public: Framing of North Korea. *International Journal of Public Opinion Research. 21*(2), 204-223.

Maingueneau, D. (1996). *Les termes clé de l'analyse de discours*. Paris : Seuil

Maingueneau, D. (2012). Que cherchent les analystes du discours ? *Argumentation et Analyse du discours*. Numéro 9. Récupéré de http://aad.revues.org/1354?lang=fr

McDougal. (2013, septembre). The Journal of Pan African Studies. 6 (4). Récupéré de http://www.jpanafrican.com/docs/vol6no4/6.4-ready1.pdf

Mead, G. H. (1963). *L'esprit, le soi et la société.* (trad. J. Cazeneuve). Paris : Presses Universitaires de France.

Mendelson, S. (18 décembre 2014). *'The Interview' Is Canceled. The Terrorists Won. So Now What Should Sony Do*? *Forbes*. Récupéré de http://www.forbes.com/sites/scottmendelson/2014/12/18/put-the-interview-on-vod-dont-give-it-away-for-free/.

Nye, J. S. (2012, 10 avril). Cyber Guerre et Paix. *Project Syndicate : The World's opinion page*. Récupéré http://www.project-syndicate.org/commentary/cyber-war-and-peace/french

Obama, B. *Remarks by the President.* Notes pour une allocution du premier ministre des États-Unis, M. Barack Obama, à l'occasion de la du Cybersecurity *and* Consumer Protection Summit. Université de Standford, Californie. 13 février 2015. Récupéré de https://www.whitehouse.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit

Obama, B. *Remarks by the President at the Federal Trade Commission.* Office of the Press Secretary. Notes pour une allocution du premier ministre des États-Unis, M. Barack Obama, à l'occasion du Federal Trade Commission. Constitution Center. Washington, 12 janvier 2015. Récupéré de *https://www.whitehouse.gov/the-press-office/2015/01/12/remarks-president-federal-trade-commission*

Obama, B. (2014, 21 décembre). CNN's Candy Crowley interviews President Barack Obama. *CNN Press Room.* Récupéré de http://cnnpressroom.blogs.cnn.com/2014/12/21/cnns-candy-crowley-interviews-president-barack-obama/

Obama, B. *Remarks by the President in Year-End Press Conference.* Notes pour une allocution du premier ministre des États-Unis, M. Barack Obama, à l'occasion de la dernière conférence de presse de l'année. Maison Blanche. 19 décembre 2014. Récupéré de https://www.whitehouse.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference

Organisation du traité de l'Atlantique Nord. (2014, 5 septembre). *Déclaration du sommet du Pays de Galles.* [Communiqué].120. Récupéré de http://www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=fr

Organisation des Nations Unis. (2013, 13 septembre). Les cyberconflits et la sécurité nationale. *Le magazine des Nations Unies,* 1(2). Récupéré de http://unchronicle.un.org/fr/article/les-cyberconflits-et-la-s-curit-nationale/

Organisation du traité de l'Atlantique Nord. (1949, mis à jour 2008). *Traité de l'Atlantique Nord.* [Entré en vigueur le 24 août 1949]. Récupéré de http://www.nato.int/cps/fr/natolive/official_texts_17120.htm

Owens, W. A., Dam, K., & Lin, H. S. (2009). *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber-attack Capabilities.* Washington : National Academies Press.

Pan, Z. et Kosicki, M-G. (1993). Framing Analysis: An Approch To New Discourse. *Political Communication.* 10 (1), 55-75

Paquay, M. (2014, 18 décembre). Piratage de Sony: de la cyberattaque au cyberterrorisme. *RTBF*. Récupéré de : http://www.rtbf.be/info/monde/detail_piratage-de-sony-de-la-cyberattaque-au-cyberterrorisme?id=8603146

Pastebin. [s. d.] (2014, 18 décembre). *Dear Sony from GOP*. Récupéré de http://pastebin.com/m4YB2TJd

Pêcheux, Michel. (1969). *Analyse automatique du discours.* Paris : Dunod

Pfau, M., Compton, J. A., Parker, K. A., Wittenberg, E. M., An, C., Ferguson, M., et al. (2004). The traditional explanation for resistance based on the core elements of threat and counterarguing and an alternative rationale based on attitude accessibility: Do these mechanisms trigger distinct or overlapping processes of resistance? *Human Communication Research,* 30, 329–360.

Porteous, H. (2010, 8 février). Cybersécurité et renseignement de sécurité : l'approche des États-Unis. Division des affaires internationales, du commerce et des finances. Récupéré de http://www.parl.gc.ca/Content/LOP/ResearchPublications/prb0926-f.htm

Reese, S. (2001) A bridging model for media research. *Reese Stephan (et al.) (dir.), Framing Public Life: Perspectives on Media and our Understanding of the Social World.* Mahwah : Lawrence Erlbaum, p. 7-31

Riker, W. H. (1986). *The art of political manipulation.* New Haven: Yale University Press.

Roger, K. (18 décembre 2014). *Sony Canceled 'The Interview.' But What Are We Actually Missing? New York Times*. Récupéré de http://www.nytimes.com/2014/12/18/us/sony-canceled-the-interview-but-what-are-we-actually-missing.html.

Rogers, M. (18 décembre 2014). Why the Sony hack is unlikely to be the work of North Korea. *Marc's Security Rambling*. Récupéré de http://marcrogers.org/2014/12/18/why-the-sony-hack-is-unlikely-to-be-the-work-of-north-korea/

Roscini, M. (2014). *Cyber Operations and the Use of Force in International Law.* Oxford: Oxford University Press.

Rüdiger F., Hoare J., Köllner P. et Pares S. (2013). *Korea 2013 Politics, Economy and Society.* Leiden and Boston: Brill.

Sanders, G. (2014, 18 décembre). Are We Prepared for the Future of Cyber-Attacks? *Tech.co.* Récupéré de http://tech.co/sony-pictures-hack-cyber-attacks-2014-12

Sanger, D. E. et Perltroth, (2014, 17 décembre). U.S. Said to Find North Korea Ordered Cyberattack on Sony. *New York Times*. Récupéré de

Scheufele, D. A. (1999, mars). Framing as a Theory of Media Effects. *Journal of Communication*, 49 (1), 103–122.

Shaw, L. et A. Sakoui. (2014, 9 décembre). Sony CEO Hirai Cleared Scenes in Film on N. Korea's Kim. *Bloomberg*. Récupéré de http://www.bloomberg.com/news/articles/2014-12-10/sony-ceo-hirai-cleared-scenes-in-film-on-n-korea-s-kim

Schmidt E. et Cohen J. (2013). The New Digital Age: Reshaping the Future of People, Nations and Business. (2e éd.). New York: Knoff

Singer P.W. et Friedman A. (2013). *Cybersecurity et Cyberwar*. Oxford : Oxford University Press.

Song J. (2011). *Human Rights Discourse in North Korea Post-Colonial, Marxist and Confucian Perspectives.* Routledge

Terkildsen N. et Schnell, F. (1997). How Media Frames Move Public Opinion : An Analysis of the Women's Movement. *Political Reseach Quarterly*, 59 (4), 879-900. Récupéré de http://www.unc.edu/~fbaum/teaching/PLSC541_Fall06/Terkildsen_Schnell_1997.pdf

Tuchman, G. (1978). *Making news.* New York: Free Press.

Untersinger, M. (13 février, 2015). Cybersécurité : Barack Obama tend la main à la Silicon Valley méfiante. *Le Monde. Récupéré de* www.lemonde.fr/pixels/article/2015/02/13/cybersecurite-barack-obama-tend-la-main-a-la-silicon-valley-mefiante_4576356_4408996.html

Ventre (21 janvier, 2015). Le cyberespace, un champ de bataille aux limites encore floues. *Reuters*. Récupéré de http://fr.reuters.com/article/technologyNews/idFRKBN0KU28520150121?pageNumber=2&virtualBrandChannel=0

Ventre, D. (2011). *Cyberattaque et Cyberdéfense*. Paris : Hermès science publication/Lavoisie R.

Vicente, M. et López, P. (2009). Resultados actuales de la investigación sobre framing: sólido avance internacional y arranque de la especialidad en España. *Zer. Revista de Estudios de Comunicación,* 14, 13-34.

Watin-Augouard. (2015, 1er janvier). *Attaque contre Sony: pourquoi c'est un tournant dans l'histoire de la cybersécurité.* Solutions-numériques.com. Récupéré de http://www.solutions-numeriques.com/attaque-contre-sony-pourquoi-cest-un-tournant-dans-lhistoire-de-la-cybersecurite/.Wheeler, D. A. et Larsen, G. N. (2013, octobre). *Techniques for Cyber Attack Attribution* (IDA Paper P-3792). Institute for Defense Analysis :Virginie.

White House (2015, 2 avril). *Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities.* Annonce d'un ordre exécutif pour bloquer certaines personnes engagées dans un acte de "cyber-enabled activity". Washington: The White House Récupéré de https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m

White House (2014, 15 juillet). Discours d'ouverture du One hundred thirteenth Congress, second session : *Judiciary Subcommittee on Crime and Terrorism Hearing on Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks.* Washington: The White House. Récupéré de https://www.hsdl.org/?view&did=756247

White House (2014, 17 décembre). Non-titré. Statement, National Security Council. Déclaration de Bernadette en réponse à la cyberattaque de Sony. Récupéré de http://www.businessinsider.com/the-white-house-responds-to-new-sony-hacking-information-2014-12

White House. (2003). *The National Strategy to Secure Cyberspace.* Washington: The White House. Récupéré de : https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

Wilson, W.J. (2009). *More than just race.* New York, NY: W.W. Norton &Company.

Wines, M. (25 janvier 2010). China Issues Sharp Rebuke to U.S. Calls for an Investigation on Google Attacks, *New York Times.*

Wolton, D. (1989, juillet). Communication politique : Les médias, maillon faible de la communication politique. *Hermès 4.* Récupéré de : http://documents.irevues.inist.fr/bitstream/handle/2042/15407/HERMES_1989_4_165.pdf

Wolton, D. (1995). Les contradictions de la communication politique. *Hermes.* Récupéré de : http://documents.irevues.inist.fr/bitstream/handle/2042/15211/HERMES_1995_17-18_107.pdf..?sequence=1

Won. Y. J. (2013). News as propaganda: A comparative Analysis of US and Korean Press Coverage of the Six-Party Talks 2003–2007. *International Communication Gazette*, 75(2), 188-204.

Zeller, K. (2014, 17 décembre). The Evidence That North Korea Hacked Sony Is Flimsy. *The Wired.* Récupéré de http://www.wired.com/2014/12/evidence-of-north-korea-hack-is-thin