UCL Université catholique de Louvain

Faculté des sciences économiques, sociales, politiques et de communication (ESPO)
Ecole des Sciences Politiques et Sociales (PSAD)

Le renseignement comme instrument de « *soft power* »

National Security Agency : de la surveillance de masse à la guerre de l'information

Travail réalisé par
Gauthier Vandenbussche – NOMA : 0993-14-00

LSPRI2900A – Mémoire Deuxième Partie
Michel Liégeois

Promoteur - Lecteur(s)
Michel Liégeois - Louis Jean Le Hardy de Beaulieu

Année académique 2019-2020
Master [120] en sciences politiques, orientation relations internationales, à finalité spécialisée

Avant-propos

Au terme de cette recherche, je tiens à remercier les personnes suivantes qui m'ont permis de réaliser ce mémoire :

Monsieur Michel Liégeois, promoteur de ce mémoire, professeur à l'Université catholique de Louvain (UCL), pour ses conseils avisés, mais également pour son implication et sa disponibilité tout au long de l'année, lors de la réalisation et de la rédaction de ce document, et ce, malgré les circonstances actuelles ;

Madame Nathalie Delobbe pour son aide dans sa relecture attentive et ses conseils avisés ;

Mes parents, Charles Vandenbussche et Sandrine Staelens, pour leur soutien indéfectible durant tout mon parcours académique ;

Ma petite-amie, Maëlle Borrey, qui m'a soutenu, encouragé et conseillé tout au long de mes études et de ce mémoire ;

Mais également mes amis et tous ceux qui m'ont apporté du soutien pendant toutes ces années.

Je déclare sur l'honneur que ce mémoire a été écrit de ma plume, sans avoir sollicité d'aide extérieure illicite, qu'il n'est pas la reprise d'un travail présenté dans une autre institution pour évaluation, et qu'il n'a jamais été publié, en tout ou en partie. Toutes les informations (idées, phrases, graphes, cartes, tableaux, …) empruntées ou faisant référence à des sources primaires ou secondaires sont référencées adéquatement selon la méthode universitaire en vigueur.

Je déclare avoir pris connaissance et adhérer au Code de déontologie pour les étudiants en matière d'emprunts, de citations et d'exploitation de sources diverses et savoir que le plagiat constitue une faute grave.

Gauthier Vandenbussche

Lexique des abréviations

ADM	Arme de Destruction Massive
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
BND	Bundesnachrichtendienst
CIA	Central Intelligence Agency = Agence Centrale du Renseignement (américain)
COMINT	Communications intelligence : renseignement des transmissions
DCI	Director of Central Intelligence
DGSE	Direction Générale de la Sécurité Extérieure (français)
DNI	Director of National Intelligence
EADS	European Aeronautic Defence and Space company : Consortium aéronautique et de défense européen
ELINT	Electronic intelligence : renseignement d'origine électronique
GAFA	Google, Apple, Facebook, Amazon
GC&CS	Governement Code and Cypher School
GCHQ	Government Communications Headquarters) = Quartier Général des Communications du Gouvernement (britannique)
IMINT	Imagery intelligence : renseignement satellitaire
ISNU	Israeli SIGINT National Unit
JSA	Joint Signal Activity
KGB	Komitet Gossoudarstvennoï Bezopasnosti = Comité pour la Sécurité de l'État (soviétique)
LBDSN	Livre Blanc sur la Défense et la Sécurité Nationale
MASINT	Maeserument and signature intelligence : renseignement des signatures
NSA	National Security Agency = Agence Nationale de Sécurité (américain)
NSC	National Security Council
ONU	Organisation des Nations unies

OSINT	Open source intelligence
OTAN	Organisation du traité de l'Atlantique nord
PROTINT	Protected intelligence
PSP	Programme de surveillance du président
RFA	République Fédérale allemande
SIGINT	Signal intelligence : ROEM, renseignement d'origine électromagnétique
UKUSA	United Kingdom + United States of America

Table des matières

1. Introduction

Au lendemain de la Seconde Guerre Mondiale, le monde est séparé en deux pôles guidés chacun par une grande puissance : les États-Unis et l'Union soviétique. Cette guerre froide n'est pas une guerre "traditionnelle" puisqu'elle ne se réalise pas via des confrontations directes (notamment en raison de la dissuasion nucléaire) mais au moyen de conflits indirects (guerre de Corée, guerre du Vietnam, …). A une ère où le conflit se fait dans l'ombre, les services de renseignement vont prendre une importance croissance. En effet, à partir du moment où une seule bombe nucléaire peut détruire une ville entière, les techniques d'espionnage vont devenir primordiales. C'est ainsi que la CIA (Central Intelligence Agency) et la NSA (National Security Agency) sont créées respectivement en 1947 et en 1952 côté américain ainsi que le KGB (*Komitet Gossoudarstvennoï Bezopasnosti*, Comité pour la Sécurité de l'État) en 1954 côté soviétique. Ces services n'ont fait que gagner de plus en plus d'ampleur au fur et à mesure des années.

Lorsque vint la fin de la guerre froide, les États-Unis s'imposent en tant que superpuissance dans le monde entier et veulent créer un consensus international autour de leur puissance. Pour cela, les services de renseignement américains vont former des alliances avec d'autres pays. Cependant, c'est avec l'attentat du 11 septembre, qui a surpris tout le monde, que fût signé *l'US Patriot Act* en octobre 2001[1], permettant aux services de renseignement américains d'espionner n'importe qui sous prétexte d'une potentielle liaison au terrorisme. Avec la révolution d'internet, le renseignement technique va prendre de plus en plus de place dans le monde du renseignement américain. Mais c'est surtout grâce à des lanceurs d'alerte comme Edward Snowden que les pratiques du renseignement électromagnétique sont dénoncées car elles ne respectent ni la protection de la vie privée, ni même les alliés des États-Unis qui se font espionner par les agences américaines.

Comme nous le verrons, les collectes de masse de la NSA ont déjà été dénoncées et analysées[2] suite aux informations dévoilées par Edward Snowden en 2013. Cependant, si les agences américaines du renseignement faisaient de la

[1] Bush, Georges. US Patriot Act, 107-56 § 215 (2001).
[2] MacAskill, Ewen, et Gabriel Dance. « NSA files : decoded ». *The Guardian*. 1 novembre 2013.

surveillance de masse pour lutter contre le terrorisme, il existe d'autres raisons que l'antiterrorisme qui ne sont que partiellement exploitées.

En effet, plusieurs questions subsistent : Quels États participent également à cette collecte massive d'informations ? Le renseignement a-t-il été utilisé comme un instrument de géopolitique ou de géoéconomie ? Par le biais des réseaux de renseignement, les États-Unis ont-ils réussi à maintenir leur puissance ? Ces questions peuvent se formuler en une seule : **Dans quelles mesures les renseignements collectés par des collaborations établies dans le milieu du numérique et du renseignement par la *National Security Agency* représentent-ils des instruments de *« soft power »* au service du gouvernement des États-Unis afin d'influencer d'autres États ?**

Ce mémoire se focalisera donc sur la *National Security Agency* et comment la Maison blanche a utilisé ces renseignements pour influencer les États du monde entier. Ce mémoire aura ainsi pour but de démontrer que les agences de renseignement américaines, et la NSA en particulier, ont réussi à créer un réseau de collectes d'informations, non pas uniquement dans un but de lutter contre le terrorisme, mais d'augmenter le rayonnement et l'influence de la puissance américaine. Ainsi, l'analyse sera portée avant tout sur le concept de puissance et donc sur la perspective réaliste des relations internationales telle que décrite par Henry R. Nau[3].

Dans ce mémoire, nous allons nous concentrer sur la puissance américaine mais seulement sur l'un de ses aspects, le *soft power* américain. Cependant, on ne va pas considérer le *soft power* dans toutes ses dimensions ici mais seulement, dans le but de comprendre comment le renseignement américain peut représenter un instrument de persuasion sur d'autres États. Nous allons également nous intéresser à l'usage du renseignement comme instrument de *soft power* et à la manière dont il a été utilisé dans la dimension de *smart power* par le gouvernement Obama. Ensuite seulement, nous nous intéresserons plus particulièrement à la NSA.

[3] Nau, Henry R. *Perspectives on international relations : power, institutions, and ideas*. 4th éd. Los Angeles: Sage, 2015.

1.1. La démarche

Vis-à-vis de la question de recherche, il est désormais possible de définir un ensemble d'hypothèses afin de répondre à la question. La phase de recherche préétablie permet donc de formuler 3 hypothèses :

Grâce aux liens entre certaines grandes entreprises américaines spécialisées dans les infrastructures liées à Internet et la NSA, le gouvernement américain a pu installer une dynamique d'influence envers certains États, aujourd'hui dépendants de ces infrastructures.

Cette première hypothèse tente de mettre en lien la révolution technologique ainsi que le développement de certaines entreprises liées au cyber auxquels la NSA a dû faire face.

En fournissant divers programmes de collectes de données à certaines agences ou via divers accords de coopération de transfert de données et/ou de métadonnées, la NSA a pu accéder à toute information collectée par celles-ci et le gouvernement américain a pu ainsi créer un lien de dépendance et d'influence vis-à-vis de ces États.

Notre deuxième hypothèse tentera de démontrer que les liens entre la NSA et certaines agences de renseignement étrangères permettent aux Etats-Unis d'exercer une influence sur celles-ci, ainsi que sur leur gouvernement.

La NSA, en créant des virus ou des « *backdoors* » et en les implantant dans des systèmes au sein des États, parfois alliés des États-Unis, ceci leur a permis de leur donner un avantage stratégique, permettant ainsi aux États-Unis de freiner la montée en puissance de certains États de manière préventive.

La dernière hypothèse, qui s'éloigne légèrement du concept de *soft power*, essaiera d'identifier si la NSA a les capacités et la volonté de lancer des cyberattaques sur certains Etats, à des fins coercitives ou d'influence.

Plusieurs théories peuvent être utiles afin d'appréhender ces hypothèses. En effet, vu que ce travail portera essentiellement sur la *perspective réaliste*, celle-ci sera expliquée dans les termes utilisés par Henri R. Nau[4]. Cette théorie et les concepts sous-

[4] Nau, Henry R. *Perspectives on international relations : power, institutions, and ideas*. 4th éd. Los Angeles: Sage, 2015.

jacents seront primordiaux puisque nous sommes dans un jeu de puissances. La perspective réaliste permettra également de servir de base pour expliquer le concept de *« soft power »* de Joseph Nye[5].

Les théories de *l'uni-multipolarité* dans le livre *« The Lonely Superpower »*[6] ainsi que *la guerre des civilisations* dans *« The Clash of the Civilizations »*[7] de Samuel Huntington seront également exploitées afin d'expliquer le contexte de la puissance américaine après la guerre froide et s'il existe aujourd'hui une peur des puissances moyennes au sein des États-Unis (*multilatéralisme*).

Les théories du renseignement vont également être expliquées et mises en parallèle avec les concepts de la perspective réaliste et de la notion de « *soft power* ». L'architecture particulière du renseignement américain sera ensuite démontrée et on observera les changements liés notamment au 11 septembre dans *l'Intelligence community* américaine. Le changement de paradigme du renseignement lié à la révolution numérique et ses conséquences sur le renseignement d'origine électro-magnétique seront également explicitées avant de commencer la phase analytique.

Durant la phase analytique qui consistera à vérifier nos hypothèses, plusieurs critères vont être pris en compte. Tout d'abord, nous allons nous intéresser aux possibilités exploitées par la NSA dans le domaine du numérique et les liens qu'elle a tissé avec certaines entreprises américaines spécialisées dans le domaine de l'Internet. Ensuite, les alliances entre services de renseignement seront mises en avant afin de comprendre avec qui la NSA traite pour vérifier s'il existe une dépendance des autres agences vis-à-vis de l'agence américaine. Ces analyses permettront ensuite de déterminer si le renseignement peut être effectivement utilisé comme un outil d'influence, de "force douce", ce qui correspond notamment aux critères du *soft power*.

Enfin, une analyse finale sera faite quant à la politique de collecte de renseignement de la NSA après l'affaire Snowden mais aussi sur les relations entre la NSA et la Maison blanche depuis l'élection de Donald Trump à la présidence des États-Unis. Un chapitre sera également consacré à l'avenir du renseignement face à

[5] Nye, Joseph S. « Soft Power ». *Foreign Policy*, nº 80 (1990): 153-71.
[6] Huntington, Samuel P. « The Lonely Superpower ». *Foreign Affairs* 78, nº 2 (1999): 35-49.
[7] Huntington, Samuel P. « The Clash of Civilizations? » *Foreign Affairs* 72, nº 3 (1993): 22-49.

l'augmentation de la connectivité numérique mondiale et aux prochaines potentielles utilisations du renseignement dans la lutte géopolitique entre les grandes puissances. Ce travail se terminera évidemment par une conclusion reprenant en compte les résultats des analyses faites tout au long de ce mémoire.

2. La perspective réaliste

Afin d'évaluer l'implication de la NSA dans la dynamique d'influence des États-Unis, il est primordial de présenter dans un premier temps le concept de perspective réaliste. Il s'agit en effet d'une des approches les plus utilisées en relation internationales et les différents principes qui en découlent auront toute leur importance pour comprendre correctement les mécanismes de renseignement et d'influence mis en place par les États-Unis.

L'approche réaliste des relations internationales est une bonne première base pour dresser le portrait des relations internationales. En effet, cette approche dite "réaliste" des relations internationales affirme que dans les conditions anarchiques de la politique mondiale, où il n'existe aucune autorité politique au-dessus des États, ces derniers doivent donc compter sur leurs propres forces pour préserver leur indépendance. L'utilisation de la force n'est envisagée que comme dernier recours (*ultima ratio*). Pour les « réalistes », le monde n'est composé que d'États souverains qui visent à préserver leur sécurité et qui, pour ce faire et si besoin, sont prêts à utiliser la force. Cette théorie se vérifie au long des siècles passés où la guerre a été un élément constant des affaires internationales[8].

Bien qu'il existe différents types de « réalistes », il y a un consensus pour considérer que la politique mondiale est régie par des politiques de puissances et que l'équilibre des puissances est un élément central des relations internationales. Cependant, il ne faut pas se limiter à une conception trop étroite de la notion de puissance, et c'est en utilisant par exemple les idées ou les idéologies que l'on peut prendre en compte l'ensemble des ressources qui permettent de mesurer et de comparer les puissances entre elles.

[8] Nye Joseph S, « L'équilibre des puissances au XXIe siècle », *Géoéconomie*, 2013/2 (n° 65), p. 26.

Si d'autres approches, telles que les approches libérale, constructiviste ou critique existent et permettent d'expliquer certains phénomènes, c'est la perspective réaliste qui sera principalement utilisée ici pour comprendre l'importance du renseignement dans la stratégie de *soft power* du gouvernement américain.

La perspective réaliste se concentre sur les conflits et la guerre, non pas parce que cette perspective favorise la guerre ou estime que la guerre est nécessaire, mais parce qu'elle part de postulat qu'étudier la guerre permettra de l'éviter à l'avenir. Selon la perspective réaliste, la guerre est une conséquence de l'anarchie, qui résulte elle-même de la répartition décentralisée du pouvoir dans le système international[9]. Les réalistes estiment en effet que les organisations internationales telles que l'ONU, ne représentent pas une centralisation du pouvoir et n'ont qu'un faible pouvoir d'influence parce que seuls les États sont souverains. Chaque État est vu comme un acteur indépendant, rationnel et veut assurer son intégrité. Dans sa recherche de sécurité, chaque État peut en ultime recours user de la force.

Dans l'exercice du pouvoir et de la souveraineté, les États se menacent inévitablement. En effet, en l'absence de pouvoir centralisé, la communication entre deux acteurs qui n'ont pas de relations diplomatiques peut être compliquée, notamment dans l'interprétation de certaines actions. Les États ne peuvent pas être sûrs des intentions des autres. La méfiance est donc le mot d'ordre dans cet environnement anarchique.

Afin de mieux comprendre cet environnement, différents concepts qui découlent de la perspective réaliste vont être expliqués, tel que le dilemme du prisonnier, l'équilibre des forces et le dilemme de sécurité.

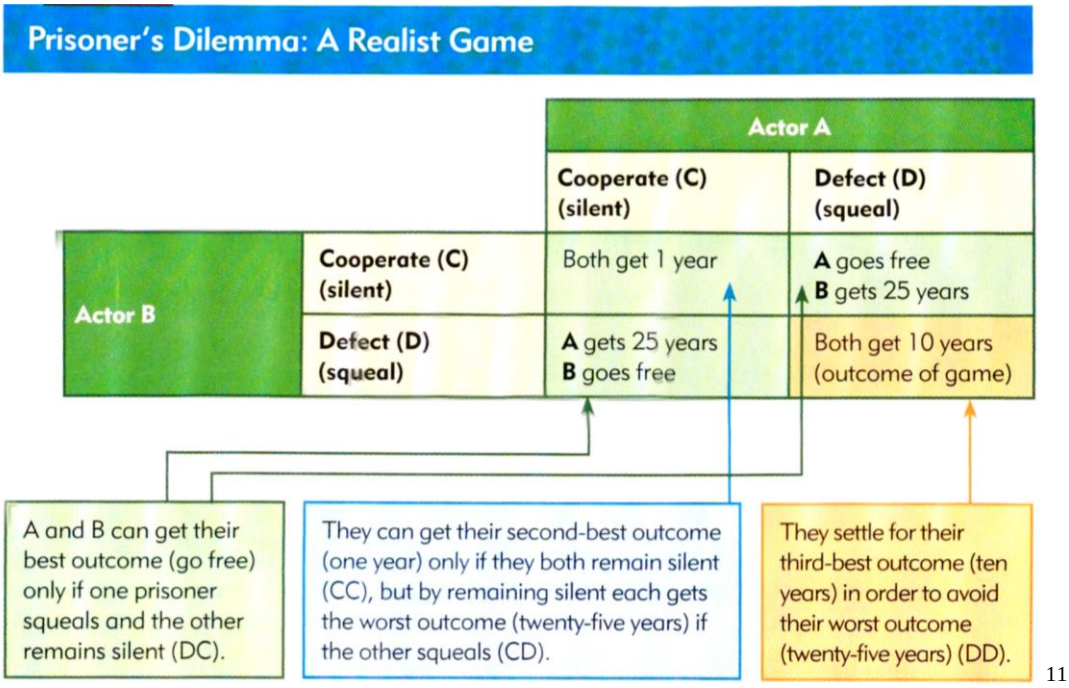
2.1. Le dilemme du prisonnier

Le dilemme du prisonnier est un scénario dans lequel deux individus ont potentiellement commis un délit et sont interrogés séparément par la police car elle n'a pas de preuve pour les inculper. La police interroge les deux suspects de manière à ce qu'il n'y ait aucune communication entre eux. Afin de les convaincre de parler et ainsi, constituer des preuves pour pouvoir les inculper, la police leur propose deux choix qui aboutissent à trois conséquences différentes (voir la figure 1 ci-dessous). Soit l'acteur

[9] Nau, Henry R. *Perspectives on international relations : power, institutions, and ideas*. 4th éd. Los Angeles : Sage, 2015, p. 37.

A parle (*Defect*) et son acolyte, l'acteur B, garde le silence (*Cooperate*), alors B aura 25 années de prison et A repartira libre. Soit les acteurs A et B gardent le silence et n'auront qu'un an de prison. Soit A et B se dénoncent respectivement et auront 10 ans de prison[10].

Figure 1 : Principe du dilemme du prisonnier



[11]

En regardant de manière raisonnée la figure 1 et, sachant que les détenus cherchent à avoir la peine la plus légère possible (1 an de prison), la réponse la plus logique serait de garder le silence. Seulement, sans communication entre eux, il suffit qu'un des deux acteurs décide de parler et il repart libre tandis que l'autre doit purger 25 années de prison. Ne pouvant pas se faire confiance l'un l'autre, les deux acteurs choisiront l'option de parler de peur d'écoper de 25 années de prison. Le dilemme du prisonnier amène donc les deux acteurs à parler et seront condamnés à 10 années de prison.

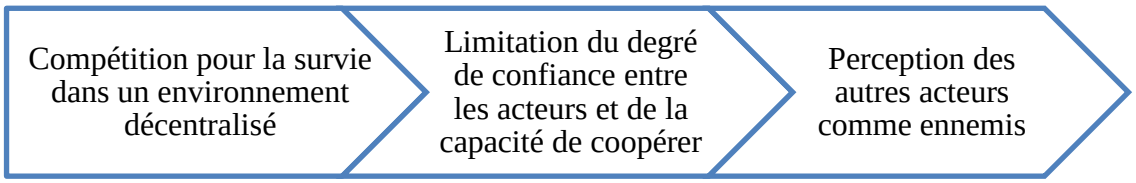
Le point de vue réaliste fait valoir que ce type de dilemme définit la logique de nombreuses situations dans les affaires internationales. En effet, en principe, les États souhaitant la paix, devraient adopter des stratégies de désarmement mutuel qui

[10] Nau, Henry R. *Perspectives on international relations : power, institutions, and ideas*. 4th éd. Los Angeles : Sage, 2015, p. 28-29.
[11] *Ibid*, p. 29.

favorisent la coopération (garder le silence dans le scénario du dilemme du prisonnier) afin d'éviter de menacer les autres en se militarisant (ce qui correspond à parler). Cependant, dans un système anarchique où la méfiance est mot d'ordre, comme c'est le cas dans la perspective réaliste, les États ne peuvent pas se faire confiance pour atteindre cette situation idéale de désarmement (qui correspond à une année de prison). En effet, si un État A décide de désarmer son territoire et que l'État B ne le fait pas, ce dernier pourrait s'emparer de l'État A sans qu'il ne puisse réellement opposer de résistance (ce qui correspond aux 25 années de prison). Le choix le plus logique et le moins risqué est donc de s'armer mutuellement afin d'éviter de perdre du territoire ou de sa souveraineté quitte à prendre le risque d'entrer en guerre (ce qui correspond aux 10 années de prison)[12].

Selon le point de vue réaliste, on en arrive à une constatation que le dilemme du prisonnier est un jeu à somme nulle : ce que l'un gagne, l'autre le perd. Ce qu'un État cherche à gagner représentera forcément une perte pour un autre. C'est une particularité de la vision des réalistes et c'est cela qui crée cette méfiance et cette compétition perpétuelle entre les États. Pour assurer sa souveraineté et sa sécurité, les États cherchent donc à se militariser, quitte à rentrer en guerre. Ainsi, d'un point de vue réaliste, une grande partie des relations internationales concerne l'armement mutuel et le conflit[13]. On peut représenter le cheminement qui amène à cette méfiance permanente entre les États en une flèche causale (figure 2).

Figure 2 : Flèche causale de la perspective réaliste



On le rappelle, la guerre n'est pas une finalité ou un objectif pour les réalistes, elle est une éventualité lorsque les moyens politiques traditionnels mis en œuvre se sont avérés insuffisants pour remplir les objectifs d'un État. En effet, comme le disait un des stratèges du temps de Napoléon, Clausewitz : « *La guerre n'est qu'un*

[12] Nau, Henry R. *Perspectives on international relations : power, institutions, and ideas*. 4th éd. Los Angeles : Sage, 2015, p. 28-29.
[13] *Ibid*, p. 29.

prolongement de la politique par d'autres moyens »[14]. La guerre serait donc un des moyens ultime de la politique, pour autant qu'elle réponde aux intérêts et aux objectifs de l'État. Sun Tzu, un des pères du réalisme et auteur de « L'art de la guerre », disait : « *On n'entreprend pas une action qui ne répond pas aux intérêts du pays* ».[15]

2.2. L'équilibre des forces (« *balance of power* »)

En se basant sur ce qui a été dit précédemment, les États vont donc avoir tendance à préférer un armement mutuel par crainte des autres États, qui sont vus comme des adversaires. Dès lors, si un État s'arme, l'autre doit s'armer pour éviter de perdre la sécurité de la souveraineté de son territoire. Ainsi, les deux États poursuivent un équilibre des forces.

Dans un système anarchique comme le conçoivent les réalistes, certains États bénéficient d'une puissance plus grande procurée par certains avantages géographiques, démographiques, stratégiques, technologiques, … Ainsi, pour avoir une chance de lutter contre ces États, d'autres forment des alliances pour éviter qu'un pays suffisamment fort ne menace leur survie. Le nombre d'États ou d'alliances, qui disposent d'une puissance significative et sont impliqués dans l'équilibre des forces, détermine la polarité du système[16]. Par exemple, durant la guerre froide, on observait deux grandes puissances, les autres États étant ralliés à l'une ou à l'autre, ce qui forme un système bipolaire. Une multitude de puissances ou d'alliances constitue un système multipolaire[17], nous y reviendrons ultérieurement.

L'équilibre des pouvoirs est à la fois une stratégie par laquelle les États cherchent à s'assurer qu'aucun autre État ne domine le système mais aussi un résultat qui fournit un équilibre approximatif entre les États. Cependant, l'équilibre des forces formé par l'alliance de plus petits États afin de lutter contre une grande puissance doit reposer sur des intentions stratégiques. En effet, dans la perspective réaliste, peu importe si une grande puissance est un ancien allié d'un État moins puissant, ce dernier doit s'aligner avec les autres contre ce pouvoir car une puissance dominante peut

[14] Clausewitz, Carl von. *De la guerre*. Tempus 127. Paris: Perrin, 2011.
[15] Tzu, Sun. *L'art de la guerre*. Paris: Flammarion, 1972.
[16] Nau, Henry R. *Perspectives on international relations : power, institutions, and ideas*. 4th éd. Los Angeles : Sage, 2015, p. 37.
[17] Leriche, Frédéric. « Chapitre 18. Le basculement du monde ? Les États-Unis et leur place dans le système mondial ». In *Les États-Unis*, p. 275-276.

changer ses affiliations ou ses valeurs (exemple du revirement d'Hitler avec le Pacte germano-soviétique)[18].

Il faut toutefois distinguer au sein du courant réaliste, deux formes possibles d'équilibre des pouvoirs : soit l'équilibre parfait, soit une puissance hégémonique qui domine toutes les autres. Les réalistes défensifs soutiennent que les États recherchent l'équilibre des forces, c'est-à-dire une puissance relativement égale qui compense le pouvoir des autres États et réduit ainsi le risque d'attaque et de guerre. Un État qui s'éloignerait de l'équilibre et qui ferait plus pencher la balance d'un côté représenterait donc un danger[19]. Pour les réalistes défensifs, la situation durant la guerre froide représentait une situation d'équilibre et donc une garantie de la sécurité.

Pour les réalistes offensifs, les États cherchent individuellement à atteindre l'hégémonie parce que gagner en puissance est toujours bénéfique. Cette hégémonie augmenterait également la stabilité et donc la paix. En effet, si une puissance domine les autres, ces dernières n'oseront pas l'attaquer car elles n'auraient aucune chance de la vaincre. Comme le décrit le politologue américain Robert Kagan, le risque survient « *lorsque la trajectoire ascendante d'une puissance montante s'approche de l'intersection de la trajectoire descendante d'une puissance déclinante* »[20]. C'est donc au moment de la transition de pouvoir entre une puissance et une autre que la guerre a le plus de chance de se produire. Selon certains réalistes, cela a été le cas au début du XXème siècle lorsque l'Allemagne a dépassé en puissance la Grande-Bretagne et cette transition se reproduira peut-être si la Chine dépasse les États-Unis en tant que puissance dominante mondiale[21].

2.3. Le dilemme de sécurité

Le dilemme de la sécurité est une formalisation courante basée sur l'équilibre des forces au sein de l'approche réaliste des relations internationales. En effet, comme expliqué précédemment, en raison de la méfiance permanente entre les États, ceux-ci recherchent un équilibre des forces, notamment en se militarisant mutuellement, afin de garantir une stabilité et la sécurité. Cependant, si un État A décide d'augmenter ses

[18] Nau, Henry R. *Perspectives on international relations : power, institutions, and ideas*. 4th éd. Los Angeles : Sage, 2015, p. 42-43.
[19] *Ibid.*
[20] *Ibid*, p. 43.
[21] *Ibid*, p. 42-43.

dépenses militaires jusqu'à surpasser en puissance celle de l'État B, ce dernier va se sentir en insécurité. Certes, il existe des moyens diplomatiques qui permettent de savoir si l'État A augmente sa puissance pour se défendre ou dans un objectif de conquête. Néanmoins, le climat de tensions et de méfiance entre les États qui est dû à la dimension anarchique du système international, force ceux-ci à douter de tous et à s'armer. Ainsi, l'État B, à cause du sentiment d'insécurité venant de l'État A, va décider de s'armer également. Cependant, si l'État A avait décidé de s'armer dans un but défensif et voit son adversaire B également augmenter ses capacités militaires, il va lui aussi se sentir dans une situation d'insécurité. C'est ainsi qu'on arrive à une boucle sans fin qui correspond à ce dilemme de sécurité. Dans une nécessité de sécurité, les États s'arment continuellement de peur des intentions de leur voisin, ce qui conduit à une course aux armements[22]. Ce modèle a permis de formaliser la course aux armements pendant la Guerre froide entre les deux grandes puissances de l'époque[23].

Ce dilemme de sécurité est une dynamique qui une fois enclenchée, ne peut plus s'arrêter à moins qu'un des deux États n'arrive plus à suivre cette course aux armements. De plus, elle peut s'enclencher de manière accidentelle puisqu'il suffit qu'un État investisse dans l'armement (par exemple suite au renouvellement de son matériel) et qu'un autre interprète cela comme une menace pour que la dynamique du dilemme de sécurité soit mise en route.

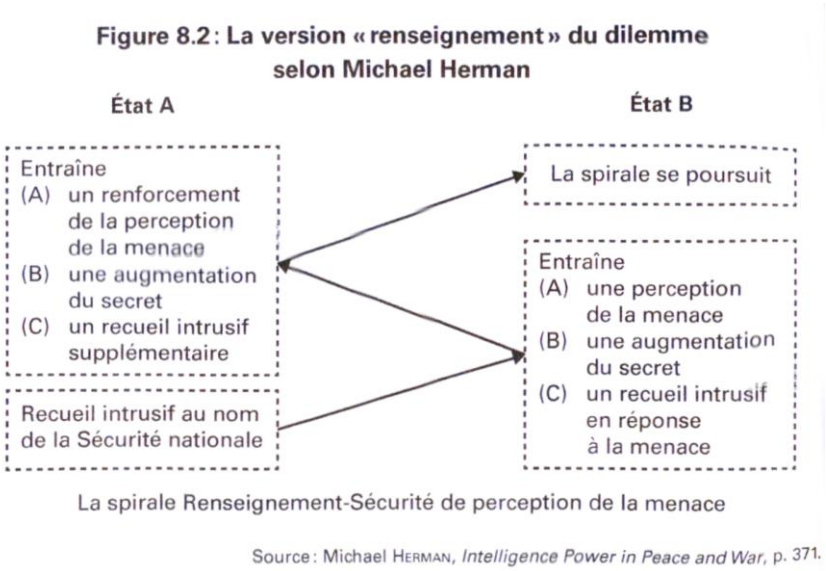
2.3.1. Le renseignement et le dilemme de sécurité

Afin d'éviter d'enclencher cette dynamique du dilemme de sécurité, les États cherchent donc à se renseigner pour évaluer les menaces potentielles, étatiques ou non-étatiques. Ainsi, les agences de renseignement mesurent le risque et permettent de réguler certaines actions qui pourraient par exemple enclencher une course aux armements. C'est ce que Raymond Aron appellera « l'intelligence de l'État personnifiée »[24]. Cependant, si le renseignement peut contribuer à éviter un dilemme de sécurité au niveau de l'armement, un même dilemme tout aussi pervers peut avoir

[22] Nau, Henry R. *Perspectives on international relations : power, institutions, and ideas*. 4th éd. Los Angeles : Sage, 2015, p. 41-42.
[23] Olivier Chopin, et Oudet Benjamin. *Renseignement et sécurité*. Cursus (Armand Colin), Armand Colin, 2016, p. 235-236.
[24] *Ibid*, p. 237.

lieu pour le renseignement lui-même. En effet, selon Michael Herman il existe une variante propre au renseignement du dilemme de sécurité, qui fait figure de paradoxe.

Figure 1: La version "renseignement" du dilemme selon Michael Herman[25]



Comme démontré sur ce schéma, il suffit qu'un État se renseigne sur un autre, notamment afin d'accroître sa sécurité en connaissant les intentions de son voisin, pour que ce dernier se sente en insécurité et veuille également se renseigner sur son voisin. A ce moment-là, la dynamique étant déjà lancée, il ne reste plus qu'au premier État à accroître ses capacités de renseignement pour que le processus se poursuive de manière infinie. Cette spirale conduit à accroître les secrets dans les rapports internationaux et collecter de l'information de façon de plus en plus intensive et intrusive[26].

Afin d'illustrer tous ces enseignements théoriques, nous allons expliquer la situation actuelle américaine et son rôle dans l'équilibre des puissances. Cette mise en contexte nous permettra d'identifier les facteurs qui ont modifiés la politique étrangère américaine.

[25] Olivier Chopin, et Oudet Benjamin. *Renseignement et sécurité*. Cursus (Armand Colin), Armand Colin, 2016, p. 238.
[26] *Ibid.*

2.4. La descente en puissance des États-Unis, ou plutôt la montée en puissance d'autres États

Après la fin de la guerre froide, les États-Unis se sont imposés comme la seule superpuissance, dominant les autres puissances à la fin du XXème siècle. Aujourd'hui se pose néanmoins la question d'un potentiel déclin de la puissance américaine. En effet, les États-Unis ne sont plus capables de régler certaines questions internationales seuls, en ignorant les positions des puissances moyennes, par exemple des États membres permanents du Conseil de Sécurité des Nations Unies. Samuel Hunthington annonçait déjà en 1999 que le monde d'aujourd'hui serait uni-multipolaire. Aujourd'hui en effet, les États-Unis restent une superpuissance mais sont confrontées à une multitude de puissances émergentes, les BRICS (Brésil, Russie, Inde, Chine et Afrique du Sud), mais aussi des puissances régionales, comme l'Allemagne ou l'Iran par exemple. Même si les États-Unis restent le seul État ayant la prééminence dans tous les domaines du pouvoir - à savoir économique, militaire, diplomatique, idéologique, technologique et culturel - avec la portée et les capacités nécessaires pour promouvoir ses intérêts dans pratiquement toutes les parties du monde, ils ne peuvent contester ou ignorer tous les autres[27]. Nous serions donc dans une phase de transition entre un monde unipolaire et un monde multipolaire, les États-Unis tentant de se maintenir au-dessus des autres et les puissances moyennes essayant de s'affirmer, au niveau régional d'abord et au niveau international ensuite[28].

Le déclin des États-Unis n'en est donc pas réellement un. On peut néanmoins opérer une distinction entre « déclin relatif » et « déclin absolu ». A ce moment, on peut qualifier la position des États-Unis dans le monde comme étant en déclin relatif par rapport aux puissances moyennes qui s'affirment de plus en plus[29].

« Les États-Unis ne sont pas actuellement dans une phase de déclin absolu. Au contraire, on peut encore raisonnablement dire que les États-Unis sauront rester plus puissants que tout autre État dans les prochaines décennies. Nous ne sommes pas dans un « monde post-Amérique », même si, il est vrai, nous ne vivons plus non plus dans « l'ère américaine » de la fin du XXe siècle. Il

---

[27] Leriche, Frédéric. « Chapitre 18. Le basculement du monde ? Les États-Unis et leur place dans le système mondial ». In *Les États-Unis*, p. 286.
[28] Huntington, Samuel P. « The Lonely Superpower ». *Foreign Affairs* 78, nº 2 (1999), p. 35-37.
[29] Leriche, Frédéric. « Chapitre 18. Le basculement du monde ? Les États-Unis et leur place dans le système mondial ». In *Les États-Unis*, p. 274.

apparaît donc raisonnable de penser que les États-Unis resteront « les premiers » mais qu'ils ne seront peut-être plus « les seuls ». » (Joseph Nye, 2013)[30]

La situation dans laquelle se trouvent les Etats-Unis étant expliquée, nous allons maintenant nous concentrer sur la puissance en elle-même ainsi que sur ses composants, en particulier le *soft power*.

3. Qu'est-ce que le « *soft power* » ?

Lorsque l'on parle de la perspective réaliste et de ses composantes, telles que l'équilibre des puissances ou le dilemme de sécurité, on parle en termes de puissance. La puissance est définie par Joseph S. Nye, grand théoricien des relations internationales et père du « *soft power* », comme ceci :

« La puissance est la capacité à développer une réelle influence sur les autres en les amenant à agir selon son propre intérêt. Elle se manifeste sous la forme du hard power qui use de méthodes radicales telles que la coercition et la corruption ou du soft power qui (…) s'emploie à convaincre par la séduction et la persuasion. » (Joseph S. Nye, 2013)[31].

Dans cette définition, on distingue deux composants de la puissance : le *hard power*, qui correspond à l'usage de moyens de coercition telle que la force armée, et le *soft power*, qui promeut l'usage de la séduction et de la persuasion. Ce pouvoir doux correspond, toujours selon Nye, à la capacité de séduire, d'attirer. Il identifie trois vecteurs majeurs du « *soft power* » : la culture, la politique étrangère et les valeurs[32].

"Soft co-optive power is just as important as hard command power. If a state can make its power seem legitimate in the eyes of others, it will encounter less resistance to its wishes. If its culture and ideology are attractive, others will more willingly follow. If it can establish international norms consistent with its society, it is less likely to have to change. If it can support institutions that make

[30] Nye, Joseph S. « L'équilibre des puissances au XXIe siècle ». *Géoéconomie* 65, nº 2 (2013), p. 24.
[31] *Ibid*, p. 19.
[32] Delcorde, Raoul. « La diplomatie d'influence ». *Revue Défense Nationale* 823, nº 8 (2019), p. 58.

other states wish to channel or limit their activities in ways the dominant state prefers, it may be spared the costly exercise of coercive or hard power" (Joseph Nye, 1990)[33].

La notion de *soft power* entre donc en opposition avec le *hard power*, à savoir le pouvoir de coercition utilisant la manière forte que ce soit des pressions politiques, économiques ou militaires. Ainsi, le *soft power* est intimement lié au pouvoir d'influencer, de modifier les comportements sans utiliser de moyens de coercition. Un État qui entretient un large panel de moyens de *soft power* est à même d'influencer les autres, sans que ces derniers ne s'en rendent compte.

Comme expliqué par Joseph Nye, mesurer le *soft power* d'un État s'assimile à mesurer l'impact de ses idées, de sa culture et de son idéologie. Le *soft power* est un pouvoir d'attraction, grâce à des ressources intangibles comme la culture, les institutions, les faiseurs d'opinion, les idées[34]. Cependant, contrairement au *hard power* qui dépend volontairement des États, le *soft power* exerce une influence sur autrui de façon partiellement indépendante de la volonté des États. Ainsi, le cinéma hollywoodien, par sa dimension culturelle, participe d'une certaine manière à l'élaboration du *soft power* américain.

« Pour comprendre le « soft power », il faut considérer les trois façons dont on peut exercer la puissance, c'est-à-dire, encore une fois, influencer autrui pour atteindre un but précis. Tout d'abord, il y a la menace par coercition, ou si l'on préfère, le « bâton ». L'alternative est l'usage de moyens financiers pour induire un changement, soit la « carotte ». Une troisième option est d'attirer et de coopter, soit le « soft power », ce que l'on appelait autrefois « gagner les esprits et les cœurs » » (Joseph Nye, 2005).[35]

En revanche, si les notions de *hard* et de *soft power* diffèrent dans leur définition, la combinaison des deux est également possible. Cette dynamique appelée *smart power*, qui naît donc d'une combinaison entre le *soft* et *hard power*, a notamment

[33] Nye, Joseph S. « Soft Power ». *Foreign Policy*, nº 80 (1990), p. 167.
[34] Delcorde, Raoul. « La diplomatie d'influence ». *Revue Défense Nationale* 823, nº 8 (2019), p. 57.
[35] Nye, Joseph. « La puissance américaine et la lutte contre le terrorisme ». *Politique américaine* 2, nº 2 (2005), p. 15.

été utilisée après la guerre d'Irak de 2003 par le gouvernement Obama[36]. A cette époque, après plusieurs échecs au Moyen-Orient et la montée en puissance d'autres États, le *soft power* américain n'était plus aussi puissant qu'il ne l'était lorsque les États-Unis étaient considérés comme l'unique superpuissance. C'est ce que nous verrons dans la prochaine section dédiée à la supposée descente en puissance des États-Unis.

3.1. La fin de la guerre froide et l'omniprésence du *soft power* américain

Comme déjà expliqué précédemment, à la sortie de la guerre froide, le monde devenait unipolaire avec à sa tête la superpuissance américaine. Les États-Unis possèdent l'armée la plus imposante au monde, capable de menacer n'importe qui, une croissance économique constante et surtout, une aura culturelle qui se diffuse dans le monde entier. Cette aura culturelle, qui représente un outil d'influence et donc de *soft power*, passe par l'utilisation majeure de l'anglais mais aussi par la diffusion de tout un mode de vie américain (Macdonalisation, Hollywood, …). A tous les niveaux, la puissance américaine est incontestée et les conséquences sont omniprésentes[37].

Les critères de puissance ont cependant évolué. Si la puissance se mesurait surtout par les ressources, notamment militaires, à la fin de la guerre froide, la puissance est à présent basée *« sur une capacité de gestion d'un environnement international à la fois complexe et interdépendant »*[38]. Ainsi, la puissance des normes a pris le dessus sur la puissance des armes.

S'il y a bien une chose à retenir du livre *« The Clash of Civilizations ?»* de Samuel Huntington, c'est qu'effectivement, la fin de la guerre froide représente la fin de la lutte des idéologies[39]. Les idées américaines ont triomphé dans la durée, contrairement aux idéaux communistes de l'URSS. Si le débat reste encore actuellement ouvert pour savoir s'il y a réellement un risque de guerre de civilisations,

[36] Olivier Chopin, et Oudet Benjamin. *Renseignement et sécurité*. Cursus (Armand Colin), Armand Colin, 2016, p. 152.
[37] Douzet, Frédérick. « États-Unis : les fragilités d'une superpuissance ». *Revue internationale et stratégique* 42, nº 2 (2001), p. 27.
[38] Tessier, Manon, et Michel Fortmann. « Les États-Unis : mutation d'une superpuissance dans l'après-guerre froide ». *Revue internationale et stratégique* 41, nº 1 (2001), p. 165.
[39] Huntington, Samuel P. « The Clash of Civilizations? » *Foreign Affairs* 72, nº 3 (1993), p. 25.

comme le prétendait Huntington, une chose est certaine c'est que l'importance de la culture et de l'influence n'ont jamais été aussi primordiales.

Avec l'émergence d'un contexte plus multipolarisé comme nous l'avons déjà expliqué, les États-Unis, dès la fin de la guerre froide, doivent créer des relations pour établir un consensus sur leur hégémonie et éviter des contestations qui pourraient aboutir à une forme d'antiaméricanisme.

> *« En raison de ce contexte multilatéralisé, il ne suffit plus de disposer de la puissance et de l'utiliser unilatéralement pour « dominer », il faut aussi disposer d'une autorité morale qui légitime ses actes et son statut. Pour une superpuissance, cela signifie donner l'exemple. Ainsi, tout acte militaire, économique ou diplomatique perçu comme illégitime risque de provoquer un ressac de la part de la communauté internationale. »*
> *(Manon Tessier et Michel Fortmann, 2001).*[40]

Comme nous allons le voir, le *soft power* que possédaient les Américains ne va pas être utilisé à bon escient et, à la suite du 11 septembre et de l'utilisation de moyens de *hard power*, un antiaméricanisme croissant va apparaître, notamment au sein de la communauté internationale.

3.2. L'échec de la guerre d'Irak et la chute du *soft power*

A la suite des attentats tragiques du 11 septembre, la menace majeure des États-Unis n'est pas un État mais un groupe terroriste. La Doctrine Bush voit alors le jour, avec pour objectif de mettre les États-Unis à la tête de la guerre contre le terrorisme. Selon cette doctrine, les États-Unis sont la seule superpuissance capable d'apporter une réponse efficace dans les crises internationales. Cette « campagne contre le terrorisme » est initiée avec la stratégie pour la sécurité nationale de 2002[41].

Suite à diverses fausses informations sur de potentielles armes de destruction massive (ADM) détenue par Saddam Hussein (*Curveball*[42]), la guerre contre l'Irak débute en 2003 avec les conséquences que l'on connaît aujourd'hui. Le but était

[40] Tessier, Manon, et Michel Fortmann. « Les États-Unis : mutation d'une superpuissance dans l'après-guerre froide ». *Revue internationale et stratégique* 41, nº 1 (2001), p. 166.
[41] Leriche, Frédéric. « Chapitre 16. La politique étrangère de Washington : de l'unilatéralisme de G. W. Bush au minilatéralisme de B. Obama ». In *Les États-Unis*, p. 248-251.
[42] Jean-Claude, Cousseran, et Hayez Philippe. *Leçons sur le renseignement*. Odile Jacob. Paris : Odile Jacob, 2017, p.

d'empêcher le commerce d'ADM entre l'Irak et Al-Qaïda et d'instaurer une démocratie en Irak afin de dissiper toute volonté terroriste. L'utilisation de moyens militaires de *hard power* est privilégiée par la Maison Blanche afin de lancer cette guerre préventive dans une optique de sécurité globale[43].

Cette guerre marque le retour à une vision unilatérale et à l'usage massif de moyens de *hard power* et tend à effacer le rôle du *soft power*[44]. Joseph Nye nous explique qu'il y a effectivement une grande tendance historique aux États-Unis à préconiser l'utilisation du *hard power* plutôt que le *soft power*, ce qui se reflète dans la culture politique américaine et dans ses institutions : *« Une culture qui fait qu'aucun politicien ne veut apparaître comme « soft », et que le Congrès préfèrera toujours augmenter le budget du Pentagone plutôt que celui du département d'État. »* (Joseph S. Nye, 2013)[45].

Il ne résultera de cette guerre qu'un échec, que ce soit en Irak où l'instauration d'une démocratie s'avère très complexe, mais aussi pour les Etats-Unis dont l'image de superpuissance est ternie au niveau régional et international. En effet, dans des pays pourtant alliés des États-Unis comme la Jordanie et le Pakistan, des sondages révèlent en effet que les d'admirateurs d'Oussama Ben Laden sont plus nombreux que ceux de George W. Bush[46]. Les États-Unis ont eu l'orgueil de croire qu'ils pouvaient gérer une affaire internationale aussi complexe, seuls, sans mettre en place une coalition internationale, ni même un consensus sur leur intervention. Leur erreur a été d'agir sans impliquer les Nations Unies dans la pacification du territoire irakien.

[43] Leriche, Frédéric. « Chapitre 16. La politique étrangère de Washington : de l'unilatéralisme de G. W. Bush au minilatéralisme de B. Obama ». In *Les États-Unis*, p. 251-253.
[44] Mattelart, Armand. « VI. Les enjeux géopolitiques de l'architecture réticulaire », Repères. Paris: La Découverte, 2009, p. 96.
[45] Nye, Joseph S. « L'équilibre des puissances au XXIe siècle ». *Géoéconomie* 65, nº 2 (2013), p. 26.
[46] Nye, Joseph. « La puissance américaine et la lutte contre le terrorisme ». *Politique américaine* 2, nº 2 (2005), p. 16.

« Les États-Unis n'ont pas su user de leur « soft power » lorsqu'ils étaient en mesure de le faire et ils n'ont pas créé le consensus international qui aurait légitimé la puissance américaine. »
(Joseph Nye, 2005)[47]

A l'échec de la Doctrine Bush s'est ajouté la crise financière de 2007-2008 (Grande Récession)[48]qui, au départ des États-Unis, va impacter le monde libéral occidental. Cette crise entache à nouveau l'image des États-Unis, non seulement auprès de leurs alliés mais également dans le monde entier. Ce n'est pas seulement l'image des États-Unis qui est touchée, c'est celle de tout le modèle économique libéral, étroitement lié à la mondialisation.

« Un des principaux problèmes concerne la redéfinition du soft power. *À l'origine, il était fondé sur l'image, les principes, les valeurs. Sur ces points, les dommages sont considérables. Dans le tiers monde, le modèle américain, le marché, la démocratie ne sont plus pris au sérieux. […] Il y a, d'autre part, une réaction plus générale contre le modèle libéral et la mondialisation... La guerre en Irak ne l'a pas créée, mais la politique de Bush l'a accélérée »*
(Fukuyama, 2007)[49].

Heureusement pour les États-Unis, les élections américaines de 2008 vont changer la donne, grâce à la mise en place d'une nouvelle stratégie par le gouvernement Obama.

3.3. La politique d'Obama et le « *smart power* »

Lorsque le président Obama entre en fonction, il décide de rassembler non seulement ses alliés au sein du parti démocrate mais également ses ennemis, comme son adversaire aux primaires démocrates Hillary Clinton qu'il nomme secrétaire d'État. Ce rassemblement, il le fera non seulement au sein de son administration mais essaiera également de l'appliquer dans sa politique étrangère. Dans ses décisions, Obama, était pleinement conscient du déclin relatif des États-Unis mais surtout de

[47] Nye, Joseph. « La puissance américaine et la lutte contre le terrorisme ». *Politique américaine* 2, nº 2 (2005), p. 17.
[48] Leriche, Frédéric. « Chapitre 18. Le basculement du monde ? Les États-Unis et leur place dans le système mondial ». In *Les États-Unis*, p. 273.
[49] Mattelart, Armand. « VI. Les enjeux géopolitiques de l'architecture réticulaire », Repères. Paris: La Découverte, 2009, p. 96.

l'opinion internationale vis-à-vis des dernières décisions en matière de politique étrangère. Ainsi, comme on va le voir, la politique Obama relève d'une approche que l'on peut qualifier de « minilatérale », mais aussi selon certains, quelque peu isolationniste[50].

« Par « minilatéralisme », on entend les coopérations engageant entre deux et une dizaine d'États, dont la logique fondamentale est de ne compter qu'un petit nombre de participants, et qui ne nécessitent pas d'institutions permanentes dédiées. » (Alice Pannier, 2015)[51]

Enlisée dans les conflits de l'Irak et de l'Afghanistan, dépassée dans le domaine de la diplomatie publique et de la promotion de son modèle démocratique au Moyen-Orient et dans le monde arabe, désorientée par la crise financière de Wall Street, l'Obama-Clinton America a été obligée de mettre en œuvre de nouvelles stratégies pour adapter son leadership et endiguer son déclin[52]. L'équipe rassemblée par Obama reconfigure la politique étrangère américaine et limite l'utilisation de moyens militaires aux seuls cas de menaces directes des intérêts américains. Cette reconfiguration du spectre de l'action extérieure américaine met fin au cycle Bush marqué par l'interventionnisme et l'unilatéralisme[53] et réduit l'utilisation d'instruments de *hard power*. Elle va également promouvoir le *soft power* grâce à l'articulation ingénieuse des deux composantes de la puissance que Joseph S. Nye appelle le « *smart power* »[54]. La nouvelle politique étrangère des États-Unis lance donc une campagne diplomatique en nouant de nouvelles relations politiques mais surtout économiques, avec l'Asie et en particulier la Chine. Le recours à la force n'est plus utilisé que pour des opérations ciblées, telles que des attaques de drones armés ou des opérations

---

[50] Leriche, Frédéric. « Chapitre 16. La politique étrangère de Washington : de l'unilatéralisme de G. W. Bush au minilatéralisme de B. Obama ». In *Les États-Unis*, U. Paris: Armand Colin, 2016, p. 254.
[51] Pannier, Alice. « Le "minilatéralisme" : une nouvelle forme de coopération de défense ». *Politique étrangère* Printemps, nº 1 (2015), p 38.
[52] Quessard, Maud. « Rebranding Soft Power: Assessing Obama's Smart Power Strategies ». *Études anglaises* 72, nº 4 (2019), p. 471.
[53] Olivier, Chopin, et Oudet Benjamin. *Renseignement et sécurité*. Cursus (Armand Colin) 0991-4498. Malakoff : Armand Colin, 2016, p. 152.
[54] *Ibid*.

spéciales, comme celle qui a tué Oussama Ben Laden en 2011[55]. On reconnaît ici clairement l'utilisation de moyens de *hard* et de *soft power* qui, en les combinant, constitue ce que Joseph Nye appelle le *smart power*.

Par son leadership en retrait (*leading from behind*) et ses attaques ciblées (*light footprint*), Obama ne désire plus seulement partager le fardeau de la sécurité collective (*burden-sharing*) mais également le transférer (*burden-shifting*)[56] dans la mesure du possible. En effet, il veut responsabiliser certaines puissances quant à leurs problèmes de sécurité régionaux et mettre en retrait les États-Unis, conscient que l'interventionnisme américain n'est plus aussi efficace qu'il ne l'a été. Z. Brzezinski, alors conseiller à la sécurité nationale, préconise de lutter contre les États hostiles par alliés interposés pour ménager les forces américaines et ne pas provoquer un engrenage dans les *proxies wars* (guerre par procuration)[57]. C'est en cela que certains qualifient Obama d'isolationniste, même si nous le considèrerons plus comme protectionniste.

Cependant, si les moyens traditionnels de *hard power* ont été diminués au profit du *soft power*, le domaine du renseignement est resté fortement sollicité en support du *hard power* surtout au Moyen-Orient, notamment pour des attaques ciblées par drones ou des actions des forces spéciales comme celle qui a permis l'élimination de l'ennemi public numéro un : Oussama Ben Laden[58]. Qu'ils soient techniques ou humains, les moyens utilisés à cette fin par le renseignement ne seront pas analysés dans ce mémoire mais restent des éléments à garder à l'esprit.

3.3.1. La dynamique d'influence à travers le domaine numérique

Selon Joseph S. Nye, *« la puissance est la capacité à développer une réelle influence sur les autres en les amenant à agir selon son propre intérêt »*. On l'a vu, afin de retrouver le *soft power* américain perdu, le président Obama a reconfiguré une nouvelle politique étrangère basée sur les relations diplomatiques et économiques,

[55] Leriche, Frédéric. « Chapitre 16. La politique étrangère de Washington : de l'unilatéralisme de G. W. Bush au minilatéralisme de B. Obama ». In *Les États-Unis*, U. Paris: Armand Colin, 2016, p. 255-256.
[56] Olivier, Chopin, et Oudet Benjamin. *Renseignement et sécurité*. Cursus (Armand Colin) 0991-4498. Malakoff : Armand Colin, 2016, p. 152-153.
[57] Ténèze, Nicolas. « La politique étrangère d'Obama : réinitialiser le leadership américain par le Smart Power ». *Revue Défense Nationale* 793, nº 8 (2016), p. 57.
[58] Bigelow, Kathryn. *Zero Dark Thirty*. Film d'espionnage. Sony Pictures Releasing, 2012.

envers de nouveaux partenaires (comme l'Asie) mais aussi envers ses alliés occidentaux. Dans cette nouvelle politique étrangère, Obama a pleinement intégré les nouveaux moyens numériques de récolte et de diffusion de l'information. Nous allons donc ici, nous focaliser sur la politique étrangère et la diplomatie comme outil de *soft power* afin de les mettre en lien avec le monde du numérique, ce qui permettra de faire un parallèle avec le monde du renseignement.

En effet, aujourd'hui la diplomatie doit faire l'apprentissage des nouveaux moyens de communication. Les outils numériques sont indispensables pour atteindre le plus grand nombre. On est passé à l'ère de l'e-diplomatie, d'autant que les jeunes diplomates aujourd'hui sont les premiers enfants de la génération Internet. Cela ne veut pas dire que les documents confidentiels doivent se retrouver sur le web mais il convient désormais de nourrir un dialogue permanent avec tous ceux qui veulent comprendre les tenants et aboutissants de la diplomatie[59].

Utiliser le numérique comme instrument de *soft power* nécessite une autre approche et d'autres méthodes. Cela demande également une implication de tous les diplomates et pas seulement celle de la dizaine de spécialistes du web rattachés au service de presse des Affaires étrangères. La diplomatie numérique est la continuation de la diplomatie classique au moyen de la technologie de l'information et conduit à une réinvention des pratiques diplomatiques. Elle correspond bien à une modalité du *smart power* en combinant les progrès sur l'Internet avec la volonté de projeter une image attirante de l'État qui l'utilise. Aujourd'hui, on perçoit bien qu'il n'y a pas de diplomatie d'influence sans révolution numérique[60].

« Dans cette ère de l'information que nous vivons actuellement, les stratégies de communication deviennent plus importantes et les objectifs sont atteints non seulement par celui qui détient la meilleure armée mais également et surtout par celui qui aura développé la meilleure stratégie de communication. » (Joseph S. Nye)[61]

---

[59] Delcorde, Raoul. « La diplomatie d'influence ». *Revue Défense Nationale* 823, nº 8 (2019), p. 59.
[60] *Ibid*, p. 59-60.
[61] Nye, Joseph S. « L'équilibre des puissances au XXIe siècle ». *Géoéconomie* 65, nº 2 (2013), p. 27.

Cependant il n'y a pas que dans la diplomatie que l'information numérisée est utilisée comme vecteur d'influence. En effet, l'économie du numérique constitue également une arme clé car aujourd'hui ce ne sont plus tellement des entreprises comme Coca-Cola, Disney, Hollywood ou McDonald's qui reflètent le *soft power* culturel américain mais plutôt les GAFA (Google, Apple, Facebook, Amazon) qui sont les relais de la culture américaine[62]. Nous reparlerons de ces entreprises et notamment le lien qu'elles ont avec certaines agences de renseignement.

Les États et les entreprises qui ont compris le rôle que représentaient les images et l'information numérique dans la dynamique d'influence, entrent aujourd'hui dans ce que l'on peut appeler une guerre de l'information. Le terme " guerre" peut paraître fort mais il est approprié face aux stratégies parfois manipulatrices qu'ont certains groupes étatiques, gouvernementaux ou civils, afin d'influencer des acteurs de la société civile qui représentent des acteurs forts dans les démocraties occidentales[63]. Nous aborderons plus loin la guerre de l'information dans le milieu du renseignement après avoir expliqué comment le cyber a révolutionné l'information. Nous verrons également à la fin de ce mémoire que cette communication d'influence peut être insidieuse et ainsi dégrader l'image d'un groupe, d'un État ou d'une entreprise, via l'utilisation d'un concept encore très récent, le « *Sharp power* » de Christopher Walker et Jessica Ludwig[64].

Mais alors, dans quelle dimension le renseignement peut-il être interprété comme un outil d'influence ? Cette question, qui reflète tout le projet de ce mémoire, permet de mettre en lien l'utilisation du renseignement, non plus comme un instrument permettant de protéger et de sécuriser l'intégralité politique et territoriale du pays, mais comme un instrument de pouvoir et d'influence au service d'un gouvernement. Pour démontrer cela, il faut tout d'abord revenir sur la définition du renseignement, de ses caractéristiques et ses utilisations potentielles.

---

[62] Delcorde, Raoul. « La diplomatie d'influence ». *Revue Défense Nationale* 823, nº 8 (2019), p. 61.
[63] Racouchot, Bruno. « Penser l'influence dans les rapports de force de la guerre économique : de la compétition aux manœuvres criminelles ». *Sécurité globale* 9, nº 1 (2017), p. 109-110.
[64] Walker, Christopher, et Jessica Ludwig. « The Meaning of Sharp Power : How Authoritarian States Project Influence ». *Foreign Affairs*, 16 novembre 2017.

4. Qu'est-ce que le renseignement ?

4.1. Une définition complexe

> *« Comme le rappelle l'expert vétéran Johnson', le renseignement répond à un besoin anthropologique: la nature humaine espère une amélioration de sa condition, mue par l'ambition, et craint simultanément le danger, soumise à un instinct de survie, ce qui provoque chez l'homme la recherche d'informations (cycle du renseignement), la protection de celles qu'il détient (contre-espionnage), la recherche d'un avantage accru (action clandestine) et la protection contre les abus du secret (accountability). »*[65]

Encore aujourd'hui, les auteurs s'accordent pour dire qu'il est extrêmement complexe de donner une définition précise du renseignement. En effet, si certains considèrent l'effort vain et superflu, d'autres s'efforcent de former un consensus sur la notion même de renseignement mais sans succès unanime pour le moment. On identifie plusieurs facteurs à l'échec de cette définition comme la diversité des phénomènes observables du renseignement, la nature secrète des services et agences, la pluralité des cultures nationales et la multiplication des destinataires et consommateurs du renseignement[66].

Ce mémoire n'a pas la prétention d'apporter une nouvelle définition, mais il a pour objectif de comprendre et d'identifier toutes les dimensions du renseignement afin de mieux l'appréhender. En effet, aborder le renseignement comme un instrument de *soft power* nous oblige à utiliser une définition, quitte à ce qu'elle ne soit pas validée par l'ensemble de la communauté scientifique. Afin de trouver une définition provisoire du renseignement, il est intéressant de s'attarder sur celle que Sherman Kent a rédigée en 1949. Cette définition impute trois dimensions au renseignement. La première est celle de la « connaissance » et s'interroge sur sa place dans l'État et les politiques de sécurité. La seconde est celle des « activités ». Cette dimension se rapporte à l'analyse du renseignement et au traitement de l'information. En d'autres termes, le renseignement se définit aussi à travers le processus par lequel l'information va être analysée, travaillée et recoupée pour devenir un renseignement à destination du

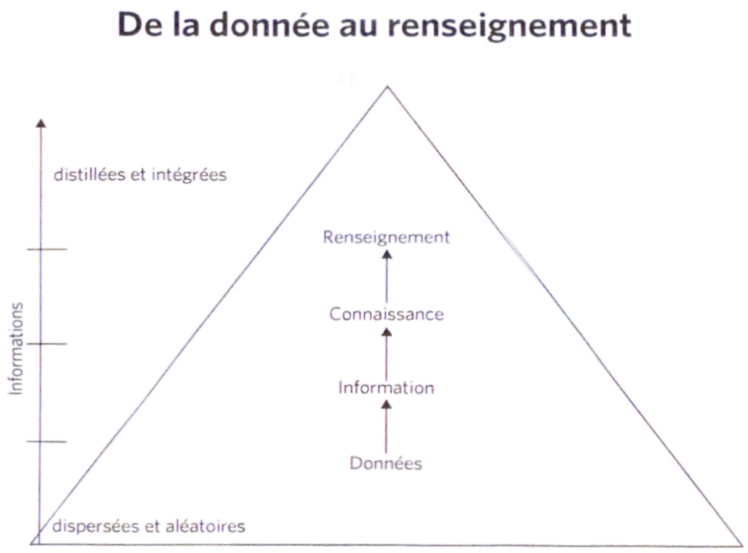
[65] Jean-Claude, Cousseran, et Hayez Philippe. *Leçons sur le renseignement*. Odile Jacob. Paris: Odile Jacob, 2017, p.
[66] Olivier Chopin, et Oudet Benjamin. *Renseignement et sécurité*. Cursus (Armand Colin), Armand Colin, 2016, p. 33.

pouvoir politique[67]. La troisième, la dimension organisationnelle, se rapporte à la manière dont est organisé le renseignement dans la bureaucratie[68].

Comme expliqué par Olivier Chopin et Benjamin Oudet, le terme « renseignement » renvoie à trois acceptions, définitions distinctes car il est à la fois une science puisqu'il produit de la connaissance (acception intellectuelle), un processus comme le montrera le cycle du renseignement dans les chapitres suivants (cfr. 4.3.) (acceptation processuelle) et une institution car le renseignement est géré par tout un système bureaucratique et administratif (acceptation institutionnelle). Ces trois définitions doivent être mises en interaction pour bien comprendre tous les aspects du renseignement.

Comme illustré sur la figure 4 qui suit, le renseignement est un système qui vise à passer du tacite à l'explicite en filtrant, précisant, qualifiant et commentant l'information. Toute information peut devenir un renseignement à condition d'être interprétée.[69]

Figure 4 : Transformation d'une donnée en renseignement[70]



Source : Singh Gill M. et Nath S., University of Ottawa.

[67] Noirhomme, Sébastien. « L'échange et l'utilisation des informations récoltées par les services de renseignement belges ». Université catholique de Louvain, 2018.
[68] Olivier Chopin, et Oudet Benjamin. *Renseignement et sécurité*. Cursus (Armand Colin), Armand Colin, 2016, p. 37.
[69] Jean-Claude, Cousseran, et Hayez Philippe. *Leçons sur le renseignement*. Odile Jacob. Paris: Odile Jacob, 2017.
[70] *Ibid*, p. 19.

A l'instar d'Olivier Chopin et Olivier Oudet dans leur livre « *Renseignement et sécurité* », nous allons nous inspirer de la définition faite par Peter Gill et Mark Phythian dans leur livre « *Intelligence in an Insecure World* ». En effet, les raisons évoquées par Chopin et Oudet pour le choix de cette définition provisoire correspondent tout à fait aux idées de cette recherche. Selon eux, le renseignement est plus que de la simple collecte d'informations puisqu'il a trait à la sécurité, notamment en fournissant une anticipation. De plus, le renseignement est nécessaire dans un environnement international compétitif (comme on l'a vu selon la perspective réaliste) et envisage l'utilisation et la planification de certaines opérations spéciales et clandestines (ce que nous détaillerons par la suite). Enfin, le renseignement a comme condition de faisabilité le secret[71].

> *« Le renseignement est un terme englobant une série d'activités – de la planification et la collecte d'information en passant par l'analyse et la dissémination – conduites en secret, dans l'objectif de maintenir ou de renforcer la sécurité relative en apportant une anticipation des menaces ou des menaces potentielles selon des modalités permettant l'introduction de stratégies ou de politiques préventives, incluant, si besoin est, des activités spéciales ou clandestines. » (Peter Gill et Mark Phythian, 2012)*[72]

4.2. Le cycle du renseignement

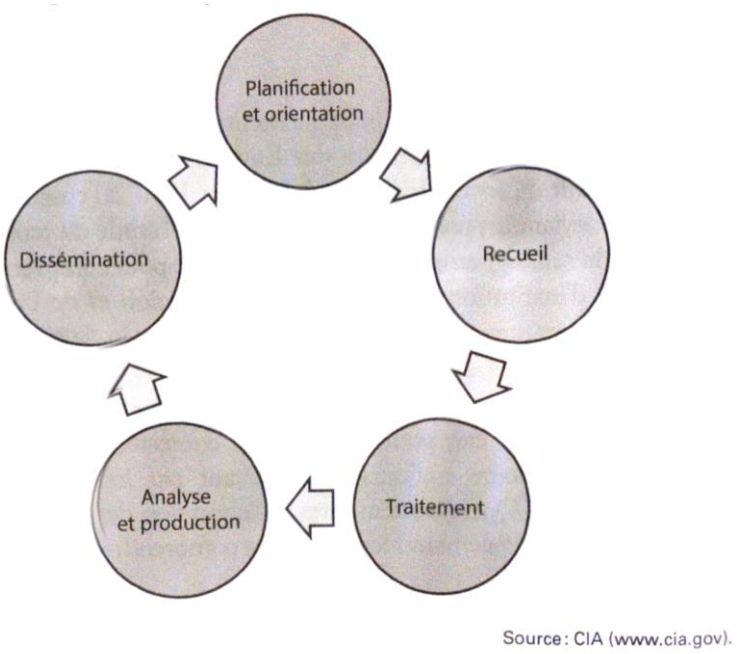
L'idée de cycle fut formulée publiquement au moment de la création du vaste dispositif de renseignement des États-Unis. Cette représentation se diffuse, à partir du foyer américain des années 1950, à l'ensemble de la littérature et devient un point de passage obligé de l'étude du renseignement. Le « cycle du renseignement » est l'outil privilégié pour comprendre le triple mécanisme d'institutionnalisation, de rationalisation et de bureaucratisation que la littérature académique et professionnelle du renseignement étudie. Le cycle du renseignement est essentiel pour comprendre le processus des machines de renseignement étatiques. En d'autres termes, ce cycle est

[71] Olivier Chopin, et Oudet Benjamin. *Renseignement et sécurité*. Cursus (Armand Colin), Armand Colin, 2016, p. 43.
[72] *Ibid*.

une définition fonctionnaliste mais aussi un modèle empirique pour rendre compte de la globalité des actions entreprises par les services de renseignement[73].

Bien qu'il existe d'innombrables variantes de ce cycle du renseignement, ici, ne sera présenté que le cycle dit « classique » élaboré en 1949 par Sherman Kent et encore utilisé aujourd'hui par la CIA pour présenter ses activités au grand public. Celui-ci se compose de cinq étapes (voir figure 5).

Figure 5 : Le cycle « classique » du renseignement[74]



Source : CIA (www.cia.gov).

Kent représente le renseignement tout d'abord comme une forme de savoir, puis comme une activité, enfin comme un type d'institution. Le renseignement est aussi conçu d'emblée comme un outil destiné au décideur afin de l'aider à prendre une décision (*provide a decision advantage*)[75].

La première phase du cycle du renseignement est celle de la « planification et de l'orientation ». Le cycle commence lorsque le décideur exprime un besoin de connaissance. Théoriquement, ce sont ces décideurs qui doivent désigner les objectifs stratégiques afin que les services de renseignement orientent leurs activités en accord

[73] Brun, Olivier. « Cycle du renseignement ». In *Dictionnaire du renseignement*, Hors collection. Paris : Éditions Perrin, 2018, p. 236-237.
[74] Olivier Chopin, et Oudet Benjamin. *Renseignement et sécurité*. Cursus (Armand Colin), Armand Colin, 2016, p. 50.
[75] *Ibid*, p. 51.

avec ces mêmes objectifs. Comme tout cycle, l'arrivée est le point de départ. Dès lors, les décideurs endossent aussi le rôle de « consommateur ». La deuxième phase est celle de la « collecte » ou du « recueil » des informations. Il s'agit d'informations venant de sources « ouvertes » et de sources « couvertes ». En ce sens, les services de renseignement utilisent tout autant les journaux, les radios, et internet, que leurs propres dispositifs, tels que les écoutes téléphoniques. La troisième phase est celle du « traitement ». Cette phase est essentielle puisqu'il s'agit de recouper les différentes informations afin de les vérifier et de les considérer comme crédibles ou non. De plus, c'est à ce moment que l'information va être classée, selon sa thématique et sa chronologie, par exemple[76].

La quatrième phase se compose de l'« analyse et de la production ». C'est l'étape de la synthèse de l'information qui va se muer en véritable renseignement. Selon la CIA, c'est lors de cette étape qu'ils déterminent comment les différentes informations sont liées les unes aux autres. Une fois l'analyse réalisée, le service de renseignement doit être capable d'expliquer ce qui se passe, pourquoi cela se déroule, ce qui peut survenir après et comment cela affecte les intérêts étatiques. C'est aussi lors de cette étape que l'analyste va attribuer certains caractères au renseignement, comme les qualités de confidentialité et d'urgence, par exemple. La cinquième et dernière étape est celle de la « dissémination ». Lorsque les informations ont bel et bien mué en de véritables renseignements, ceux-ci sont remis aux « consommateurs », c'est-à-dire les décideurs. Afin que le renseignement soit utile, il est essentiel qu'il arrive à temps à celui qui en aura l'utilité.

4.3. Critiques à l'égard du cycle du renseignement

De nombreux auteurs ont essayé d'apporter des améliorations au cycle dit "classique" et il en existe donc d'autres versions. Malheureusement, il ne semble pas y avoir de consensus général sur un cycle du renseignement. Dès lors, il apparait plus utile d'exposer les critiques faites à propos du cycle "classique". Les critiques principales peuvent se regrouper en trois thématiques : la relation décideurs-services

[76] Olivier Chopin, et Oudet Benjamin. *Renseignement et sécurité*. Cursus (Armand Colin), Armand Colin, 2016, p. 50-51.

de renseignement, les activités des services de renseignement et le principe de rétroaction[77].

Tout d'abord, il y a un désaccord entre la théorie et la pratique à propos de la relation qu'entretiennent les décideurs avec les services de renseignement. Selon la théorie, les décideurs orientent les services afin que ceux-ci réduisent les zones d'ombres qui bordent leur prise de décision. En réalité, il semblerait que *« les autorités n'orientent pas les services mais attendent de leur part des alertes, les analystes cherchent à combler leurs propres gaps de connaissance, […] [et que] les autorités n'hésitent pas à utiliser des renseignements bruts »* (Arthur Hulnick, 2006). D'autres ajoutent même que *« les responsables politiques semblent attendre du renseignement plus un soutien et une légitimation que des informations »*[78].

Ensuite, la critique porte sur l'absence de certains domaines d'activités ou de certaines relations qui sont parfois essentielles dans l'activité quotidienne d'un service de renseignement. En effet, le cycle du renseignement ne rend pas compte du contre-espionnage alors que c'est cette activité qui rend le renseignement unique. Un service de renseignement doit composer avec les adversaires que sont les autres services de renseignement, qui tentent d'induire en erreur le premier. En d'autres termes, les services de renseignement doivent développer un caractère paranoïde afin de remettre toujours en question la véracité d'une information et, se demander si celle-ci n'est pas apparue dans le cycle du renseignement dans le seul but de nuire au service. De plus, le cycle du renseignement « classique » n'aborde pas le domaine de l'action clandestine[79]. Cette action est l'œuvre d'un service de renseignement qui entreprend une mission en dehors du cadre légal sous la houlette de son gouvernement et qui nie en être l'auteur pour des raisons politiques. Bien qu'elle soit souvent la cause de nombreux fantasmes, l'action clandestine semble une activité bien réelle de certaines puissances étatiques. Néanmoins, il faut noter que ce genre d'action n'est pas une activité indispensable à l'existence d'un service de renseignement, puisque les services de renseignement belges existent tout en se passant d'un tel service.

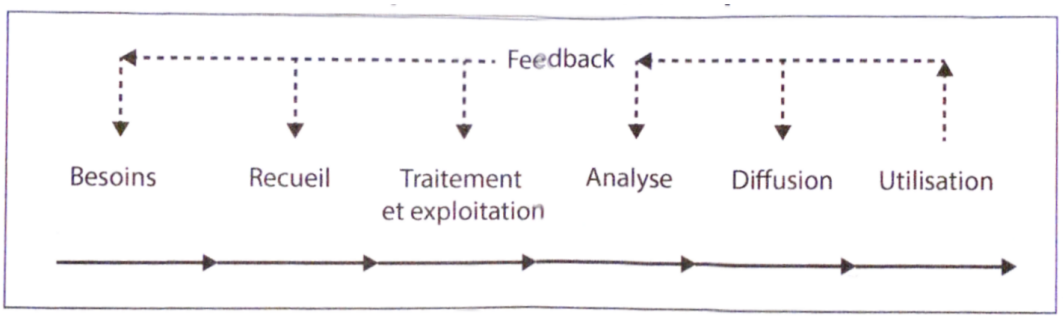
[77] Hulnick, Arthur S. « What's wrong with the Intelligence Cycle ». *Intelligence and National Security* 21, nº 6 (1 décembre 2006), p. 975.
[78] Olivier Chopin, et Oudet Benjamin. *Renseignement et sécurité*. Cursus (Armand Colin), Armand Colin, 2016, p. 59.
[79] *Ibid*.

Enfin, il est important de noter que le cycle inscrit les services de renseignement dans une relation unique avec le décideur et ne situe pas ces services dans un ensemble relationnel, marqué entre autres, par la coopération internationale. Il se pourrait qu'un service de renseignement oriente certaines de ses recherches à la demande d'un service étranger, par exemple.

La dernière critique cible l'absence de rétroaction dans le cycle du renseignement « classique ». En effet, le cycle rétroagit avec lui-même. Comme l'écrivent Olivier Chopin et Benjamin Oudet : « *[ce qu'il] manque surtout dans la notion de cycle, c'est l'idée simple que chaque étape doit pouvoir rétroagir sur les étapes antérieures pour que le système fonctionne. La représentation circulaire induit réellement en erreur sur la façon dont l'activité de renseignement fonctionne au quotidien. Il faudrait représenter le cycle a minima comme un cycle de « boucles »* ».

C'est en réponse à cette critique que la CIA, par exemple, a remplacé dans sa formation la notion de cycle par *l'intelligence process* intégrant la notion de rétroactivité de chaque étape sur les étapes antérieures. Mark Lowenthal formule ainsi un premier schéma, assez basique, basé sur *l'intelligence process* de la CIA en prenant en compte cette rétroactivité (figure 6).

Figure 6 : Représentation schématique du processus du renseignement selon Mark Lowenthal[80]

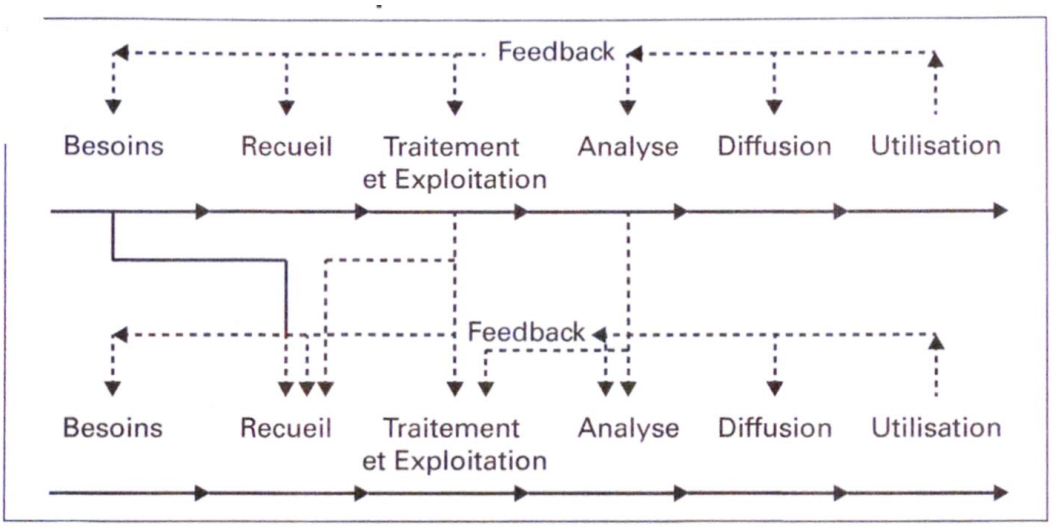


Cependant, pour démontrer ce qui se passe réellement au sein du renseignement, on ne peut s'arrêter sur un modèle si simpliste. Il faut montrer l'interconnectivité des différentes fonctions au sein du renseignement. C'est ainsi que

[80] Lowenthal, Mark. *Intelligence : From Secrets to Policy*. 5ème. Washington: CQ Press, 2011, p. 68.

Lowenthal formule un deuxième schéma plus complexe qui représente un peu mieux l'*intelligence process* de la CIA[81] (figure 7).

Figure 7 : Représentation multi-niveaux du processus du renseignement selon Mark Lowenthal[82]



Il est important de souligner que ce cycle "classique" induit l'idée que l'activité de renseignement est un travail d'équipe, contrairement à ce qui est véhiculé dans les films de fiction, où un seul homme réalise pratiquement à lui tout seul un cycle complet du renseignement. Ce cycle "classique" démontre l'importance de l'excellente réalisation de la phase antérieure afin que la phase suivante soit, elle aussi, parfaitement menée. Toutes ces phases sont les maillons d'une chaîne qui ne valent rien s'il n'y a pas d'étape précédente et suivante[83].

4.4. Les différentes méthodes de collecte de l'information

Traditionnellement, on distingue deux méthodes principales de collecte d'informations : le renseignement humain et le renseignement technique. Le renseignement humain implique principalement l'intervention des hommes (agents

[81] Olivier Chopin, et Oudet Benjamin. *Renseignement et sécurité*. Cursus (Armand Colin), Armand Colin, 2016, p. 59.
[82] Lowenthal, Mark. *Intelligence : From Secrets to Policy*. 5ème. Washington: CQ Press, 2011, p. 69.
[83] Olivier Chopin, et Oudet Benjamin. *Renseignement et sécurité*. Cursus (Armand Colin), Armand Colin, 2016, p. 54.

infiltrés, informateurs, « taupes ») et le renseignement technique désigne l'obtention d'information par la captation au moyen de technologies spécifiques[84].

Comme nous l'explique l'ex-agent de la DGSE (Direction générale de la sécurité extérieure) Olivier Mas, il n'y a pas une méthode meilleure que l'autre mais elles sont complémentaires[85]. Certes, le renseignement humain est plus risqué que le renseignement technique dans le sens où un agent doit aller sur le terrain pour récolter des informations. Cet agent peut être détecté, arrêté et, dans les cas les plus extrêmes, exécuté. Un gouvernement peut donc être impliqué dans un scandale international, car l'entrée d'un agent étranger sur un territoire est considérée comme de l'ingérence et un non-respect du droit de souveraineté de l'État sur son territoire. Cependant, cette méthode a l'avantage de coûter moins cher pour obtenir des informations et, lorsque le service a réussi à recruter une source haut placée, les informations reçues sont souvent très précieuses car très secrètes.

Pour le renseignement technique, sa plus grande faiblesse est qu'il coûte très cher. Seuls les pays les plus riches sont capables d'investir suffisamment dans des infrastructures comme des satellites, des antennes d'interception et des supercalculateurs afin de décrypter les communications. En revanche, son plus grand avantage est qu'il ne représente quasiment aucun risque puisque les agents ne doivent plus être forcément sur le terrain. De plus, certaines informations impossibles à acquérir sur le terrain peuvent être interceptées grâce au renseignement technique. C'est principalement au renseignement technique que s'intéresse ce mémoire puisque la NSA est spécialisée dans ce type de collecte de renseignement.

Selon Mark Lowenthal et Robert M. Clark dans « *The Five Disciplines of Intelligence Collection* » (2015), le renseignement technologique, excercé notamment par la NSA, comporte plusieurs ensembles comme le MASINT (*measurement and signature intelligence*) qui s'occupe de la mesure des radiations (très utile dans le domaine industriel et de l'armement) ; l'IMINT (*imagery intelligence*) dont le rôle est la photo-interprétation d'images aériennes (prises par satellites, avions ou drones) et

[84] Olivier Chopin, et Oudet Benjamin. *Renseignement et sécurité*. Cursus (Armand Colin), Armand Colin, 2016, p. 55.
[85] Mas, Olivier. Renseignement humain vs renseignement technique, 12 décembre 2019.

le SIGINT (*signal intelligence*) dont la principale préoccupation est le renseignement d'origine électro-magnétique[86].

Cette dernière dimension domine aujourd'hui la représentation que l'on a du renseignement technologique depuis les révélations concernant les techniques de collecte d'information de la NSA. Il existe trois principales subdivisions du SIGINT qui vont nous intéresser plus particulièrement. Tout d'abord, l'ELINT (*electronic intelligence*) qui capte et intercepte les ondes, le COMINT (*communications intelligence*) qui capte les communications et l'OSINT (*open source intelligence*) qui se concentre sur les sources ouvertes comme les médias, les Think-Thanks ou internet par exemple. Cependant, depuis l'apparition du « cyber » comme cinquième dimension stratégique (après l'eau, la terre, l'air et l'espace), l'OSINT connaît une subdivision : le PROTINT (*protected intelligence*), qui récolte les informations que les individus laissent dans des bases de données publiques ou privées (carte bancaire, passeport, … tout ce qui peut laisser une trace électronique)[87]. Dans le chapitre suivant, nous allons aborder cette révolution du cyber à laquelle a été confrontée la présidence d'Obama et ce qui a transformé en profondeur le renseignement et la collecte d'informations.

5. Comment le cyber a révolutionné l'information et sa collecte

Avant d'expliquer en quoi consiste la révolution de l'information pour le renseignement, il est primordial de comprendre ce que représente la surveillance de masse, notamment d'un point de vue fictif grâce au panoptique.

5.1. Le panoptique

L'image du Panopticon imprègne toutes les discussions contemporaines relatives aux questions de surveillance. Le mot et l'idée ont été inventés par le philosophe utilitaire anglais Jeremy Bentham en 1787. Repris par le philosophe français Michel Foucault dans les années 1970, le concept reste influent. Lorsqu'Oscar H. Gandy, Jr., a entrepris dans les années 1990 de discuter des implications des

[86] Olivier Chopin, et Oudet Benjamin. *Renseignement et sécurité*. Cursus (Armand Colin), Armand Colin, 2016, p. 56.
[87] *Ibid*, p. 56.

dernières technologies de l'information pour une "économie politique des informations personnelles", il a intitulé son livre The Panoptic Sort.

Le Panopticon est en fait une conception architecturale proposée par Bentham pour une prison. L'idée du Panopticon est simple. Imaginez une prison construite sous une forme circulaire. Sur le périmètre extérieur de chaque niveau se trouvent les cellules individuelles, chacune abritant un seul prisonnier et chacune entièrement isolée de l'autre pour empêcher un prisonnier de voir ou d'entendre des codétenus (voir image 1 en annexe). Chaque cellule est visible au regard de l'inspecteur, qui est logé dans un bureau central à partir duquel il peut scanner toutes les cellules au même niveau. Grâce à un système d'ouvertures et de tubes de communication trop compliqué à décrire ici (et en pratique probablement trop compliqué à construire), chaque détenu est conscient du contrôle potentiel de l'inspecteur à tout moment du jour ou de la nuit (la lumière inonde naturellement les cellules le jour et artificiellement la nuit), et les prisonniers reçoivent de temps à autre des communications verbales de l'inspecteur par le biais de ces "tubes de conversation". Ces communications verbales portent ses instructions personnalisées qui ne peuvent pas être entendues par des prisonniers auxquels elles ne sont pas destinées. Bien que le comportement des détenus soit rendu visible en permanence à l'inspecteur, les détenus ne peuvent pas réellement voir le visage et les yeux de l'inspecteur qui, encore une fois à travers un arrangement compliqué de lanternes et d'ouvertures, est rendu opaque, une silhouette qui leur rappelle sa présence continue, mais un "point totalement sombre" dont les traits ne peuvent être déchiffrés[88].

Le Panopticon est une sorte de théâtre ; ce qui est mis en scène, c'est l'illusion d'une surveillance constante. En effet, les détenus ne sont pas vraiment toujours sous surveillance, ils pensent ou s'imaginent simplement être constamment sous surveillance. Comme les détenus craignent d'être constamment surveillés et craignent d'être punis pour des transgressions, ils intériorisent donc les règles ; la punition effective sera ainsi rendue superflue. Dans un autre sens, le Panopticon tout entier est lui-même une sorte de spectacle théâtral au profit du public, dont les membres seront invités à observer. Le contrôle des prisonniers eux-mêmes est presque d'un intérêt secondaire. Le but plus large est la réforme morale de la société à travers le spectacle

[88] Whitaker, Reginald. *The end of privacy*. The new press. New York, 1999, p. 32-33.

édifiant de la discipline via la surveillance. Bentham a en outre précisé que le principe du Panopticon pouvait et devait être étendu à divers sites délimités d'activité humaine, des asiles à l'équivalent du XVIIIe siècle des institutions de protection sociale, des lieux de travail aux écoles[89].

Le design n'a jamais été réalisé, ni de son vivant, ni depuis. Pourtant, en tant que métaphore du pouvoir de la surveillance dans le monde contemporain, le concept est sans précédent. Pour Foucault, l'idée de Bentham était celle d'une "technologie politique" qui induit dans le sujet "un état de visibilité consciente et permanente qui assure le fonctionnement automatique du pouvoir." Le Panoptique imaginaire symbolise certains mécanismes, par ailleurs silencieux et invisibles, de la technique du pouvoir intériorisé, du pouvoir exercé sans la présence directe de coercition[90].

On peut donc dire que le Panoptique est un instrument d'influence, puisqu'il consiste à donner l'illusion d'une surveillance totale afin que les personnes surveillées adoptent d'elles-mêmes le comportement que l'on souhaite, sans coercition. Si le Panoptique est assez théorique, il reflète bien le principe de la surveillance de masse exercée par les États-Unis, avec l'aide d'outils numériques, et restée secrète pendant des années.

5.2. Le cyberespace

Avec l'arrivée du cyber et des outils numériques, la surveillance de masse, imprégnée par l'idée du Panoptique, a pu être réalisée pour la première fois de l'histoire. Le terme « cyber » demande toutefois à être clarifié car il existe une multitude de déclinaisons : cyberespace, cyberdéfense, cybersécurité, cyberattaque, … Ces termes très récents disposent de définitions assez floues et relatives aux perceptions de chacun. En effet, en Chine et en Russie par exemple, le cyberespace comprend tous les réseaux numériques, mais aussi la sphère politique et sociale. Ainsi, la principale menace selon eux, provient de la capacité de leurs adversaires (principalement les États-Unis et les pays occidentaux) à déstabiliser ces régimes politiques et à menacer leur contrôle sur la société[91].

---

[89] Whitaker, Reginald. *The end of privacy*. The new press. New York, 1999, p. 32-33.
[90] *Ibid*.
[91] Olivier Chopin, et Oudet Benjamin. *Renseignement et sécurité*. Cursus (Armand Colin), Armand Colin, 2016, p. 184.

En France, l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) définit le cyberespace comme *« un espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques »* et la cybersécurité comme 1' *« état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles »*[92].

Pour comprendre davantage les interactions entre le renseignement et le cyberespace, il faut distinguer trois couches dans le cyberespace.

La première couche *matérielle* ou *physique* que l'on appelle en informatique les « couches basses », sont proches de la réalité matérielle et du langage binaire des machines, et sont composées de câbles, de nœuds, de serveurs et d'ordinateurs. La deuxième couche, dite *logique* ou *logicielle* représente l'interface entre la couche basse matérielle et la couche haute sémantique qui assure la transmission des données entre deux points du réseau. Enfin, la troisième couche dite *sémantique et socio-cognitive* ou encore *informationnelle* symbolise le support du langage humain. C'est le monde des utilisateurs de la couche logique, des réseaux sociaux, des discussions et des échanges en temps réel dans le monde[93].

Ces trois couches sont indissociables et permettent ainsi leur fonctionnement mutuel. C'est ce maillage de systèmes d'informations emboîtés dans des réseaux informatiques et de télécommunications qui forme donc l'espace cyber, ou le cyberespace[94].

Ainsi, dans le Livre Blanc sur la Défense et la Sécurité Nationale publié en France en 2013 (LBDSN), l'espace numérique est considéré comme cinquième dimension stratégique. Le renseignement devient donc un outil pour lutter contre l'importance croissante des cybermenaces qui peuvent atteindre les trois couches qui constituent le cyberespace. Or, seul le renseignement, par sa flexibilité, possède les

[92] Olivier Chopin, et Oudet Benjamin. *Renseignement et sécurité*. Cursus (Armand Colin), Armand Colin, 2016, p. 183.
[93] Pech, Yannick. « Vers une intelligence cyber ? Penser le renseignement augmenté dans la noosphère ». *Prospective et stratégie* Numéro 10, nº 1 (2019), p. 76.
[94] *Ibid*.

moyens de sécuriser ces trois couches, de manière défensive mais également offensive[95].

L'administration Obama a bien compris l'importance de la cyberstratégie. En effet, les budgets alloués au domaine du cyber, autant militaire qu'économique ou politique, ont depuis lors considérablement augmentés (en 2013 il augmentait de 800 millions de dollars). La nomination en 2009 d'un *Cyber Czar*, chargé de la coordination de la cybersécurité auprès de l'administration Obama ; en 2010, le lancement opérationnel de *l'US Cybercommand* (*US Cybercom*) incorporant toutes les composantes militaires sous l'égide du directeur de la NSA et enfin en 2011, la publication de la cyberstratégie de la Maison Blanche sont d'autres éléments indicateurs qui démontrent clairement la volonté du gouvernement américain de s'imposer dans le cyberespace[96].

Cette escalade de moyens alloués au cyber est aussi une riposte à la rivalité qui s'impose peu à peu entre la Chine et les États-Unis. En effet, selon Frédérick Douzet[97], la Chine impressionne dans son avancée dans le monde du cyber. Comme expliqué précédemment, la Chine intègre non seulement tous les réseaux numériques mais aussi la sphère politique et sociale dans le cyberespace. Ainsi, elle incorpore la dimension cyber dans tous les domaines stratégiques de sa montée en puissance. La Chine a notamment démontré en 2010 sa capacité à détourner 15% du trafic des réseaux civils et militaires américains[98].

Dans une perspective réaliste, face à la perception d'une menace, les États ont en effet tendance à augmenter leur puissance pour essayer d'atteindre au minimum un équilibre des forces. Néanmoins, il est sans doute trop prématuré pour conclure à un dilemme de sécurité entre les services de renseignement chinois et américains, mais il existe déjà une course, non pas à l'armement, mais à l'information.

[95] Pech, Yannick. « Vers une intelligence cyber ? Penser le renseignement augmenté dans la noosphère ». *Prospective et stratégie* Numéro 10, nº 1 (2019), p. 77.
[96] Douzet Frédérick, « Géopolitique du cyberespace : La cyberstratégie de l'administration Obama », *Bulletin de l'association de géographes français*, 91-2 | 2014, p. 145.
[97] Douzet Frédérick. « L'art de la guerre revisité. Cyberstratégie et cybermenace chinoises ». *Hérodote* 152-153, nº 1-2 (2014), p. 166.
[98] Douzet Frédérick, « Géopolitique du cyberespace : La cyberstratégie de l'administration Obama », *Bulletin de l'association de géographes français*, 91-2 | 2014, p. 145.

5.3. Le Big data et l'Open Source Intelligence

Avec le développement d'internet, l'information ne se situe plus forcément sur le terrain comme auparavant mais elle est disponible partout, à tout moment, à la seule condition de posséder une connexion internet. Les services de renseignement recherchent le plus souvent des informations secrètes par des moyens "classifiés", c'est-à-dire des informations avec une restriction ou une limite d'accès et pour lesquels les agences doivent utiliser des moyens d'interception et d'exploitation de données plus complexes "qu'une simple recherche Google".

Cependant, les services de renseignement exploitent également les sources ouvertes et on parle alors d'OSINT (*open source intelligence*). Ce service qui a connu une expansion depuis les années 1990 est devenu indispensable à la production de l'analyse car, pour certains, les sources ouvertes contiennent les informations les plus pertinentes pour répondre aux questions posées par les décideurs[99]. En effet, c'est surtout la masse colossale du volume de données des sources ouvertes qui représente un atout pour les services de renseignement. Selon certains spécialistes, ces sources ouvertes représenteraient entre 70 et 80 % de l'approvisionnement en données du renseignement américain[100].

Cependant dans un monde où l'information est partout, les informations open source peuvent être acquises par n'importe qui : organisme étranger, étatique, civil, voire même terroriste. C'est pour cette raison que les services de renseignement diversifient leurs méthodes de collecte d'information afin de maintenir un semblant de monopole sur l'accès à ces données.

« La communauté américaine du renseignement doit trouver comment dominer cette révolution des sources ouvertes et un ensemble de technologies, plus rapidement que ses ennemis » (Amy Zegart et Michael Morell, 2019)[101]

La supériorité technologique devient dès lors la principale variable de différenciation et d'efficacité pour les services de renseignement, ce qui les poussent

[99] Olivier Chopin, et Oudet Benjamin. *Renseignement et sécurité*. Cursus (Armand Colin), Armand Colin, 2016, p. 171.
[100] *Ibid*, p. 173.
[101] *Ibid*, p. 174.

à réaliser des partenariats avec des entreprises spécialisées notamment dans l'informatique et le domaine du cyber (nous en parlerons notamment dans le chapitre consacré aux GAFA[102]). Comme le disent Olivier Chopin et Benjamin Oudet, « s*i les services de renseignement ont toujours eu à trouver l'aiguille dans la botte de foin, ce qui change désormais, c'est que celle-ci grossit de manière exponentielle* »[103].

Cette obstination à vouloir collecter le plus d'informations possibles afin de garder autant que possible le monopole de l'information peut pousser certaines agences à établir des méthodes de collecte et de surveillance de masse. Cette compétition, que ce soit entre une agence privée et étatique ou entre deux agences étatiques, mène inévitablement à une guerre de l'information.

5.4. La guerre de l'information

Le passage progressif à la société de l'information a modifié la nature des enjeux stratégiques dans l'usage offensif de l'information. Auparavant, le monde du renseignement avait deux missions essentielles : la recherche d'informations sur les puissances étrangères susceptibles de nuire aux intérêts nationaux et la sécurité du territoire.

Comme expliqué dans la première section dédiée à la perspective réaliste et au dilemme du prisonnier, on a vu que les services de renseignement pouvaient être pris dans un dilemme de sécurité, ce qui engendre une course à l'information. Cette course à l'information est en réalité une représentation de la guerre de l'information.

Les développements de l'informatique et des technologies de l'information ont conforté la pertinence du concept de la guerre de l'information. La guerre de l'information a deux dimensions : le contenant et le contenu. Les attaques portant sur le contenant visent les systèmes d'information (piratage, virus, paralysie ou destruction des communications) tandis que les attaques portant sur le contenu recouvrent les différentes formes d'usage offensif de l'information (opérations de propagande et de contre-propagande, désinformation, manipulation des connaissances de nature institutionnelle, académique, médiatique, sociétale). Ainsi, ces attaques

[102] GAFA un acronyme désignant les quatre géants américains de l'Internet fixe et mobile que sont Google, Apple, Facebook et Amazon.
[103] Olivier Chopin, et Oudet Benjamin. *Renseignement et sécurité*. Cursus (Armand Colin), Armand Colin, 2016, p. 174.

peuvent s'en prendre à toutes les couches du cyberespace décrites précédemment. Dans cet univers virtuel en constante évolution, le monde du renseignement est amené à définir son implication dans un type d'affrontement qui dépasse le cadre de ses missions traditionnelles[104].

Le monde du renseignement a dû s'adapter à ce nouveau contexte. Si la dimension du contenant (cyber) est maîtrisée, il n'en est pas de même pour les enjeux concernant le contenu. La professionnalisation du monde du renseignement dans le domaine de la guerre de l'information est acquise pour le contenant mais reste limitée aux missions ponctuelles dans le domaine du contenu. Aujourd'hui, le renseignement est donc bien capable de paralyser certaines communications mais a du mal à diffuser des informations qui seraient susceptibles d'influencer le grand public.

Cependant, certains Etats n'hésitent pas à tenter de lancer des opérations d'influence et de déstabilisation informationnelle, qui jouent parfois un rôle décisif dans la recherche de position dominante dans la structuration de l'économie mondiale[105]. C'est notamment ce que l'on appelle le « *Sharp power* »[106], un terme que l'on expliquera plus en détail à la fin de ce mémoire.

Il est temps d'examiner maintenant l'architecture du renseignement américain et le rôle que représente la NSA pour les Etats-Unis.

6. Les services de renseignement américains

Les services de renseignement sont traditionnellement distingués selon une tripartition extérieur/intérieur/militaire. Cette répartition correspond à l'histoire logique du renseignement en Europe entre le XVIIème et le XXème siècle. Si chez la plupart des services de renseignement européens, cette tripartition est respectée, comme en Allemagne ou en Finlande, dans certains États on n'observe que deux services de renseignement, comme c'est le cas en Belgique avec la Sûreté de l'État, qui dépend du Service Public Fédéral de Justice (SPFJ), et le Service Général du

[104] Harbulot, Christian. « Le monde du renseignement face à la guerre de l'information ». *Hermès, La Revue* 76, nº 3 (2016), p. 83.
[105] *Ibid*, p. 82-84.
[106] Walker, Christopher, et Jessica Ludwig. « The Meaning of Sharp Power : How Authoritarian States Project Influence ». *Foreign Affairs*, 16 novembre 2017.

Renseignement et de la Sécurité (SGRS), qui dépend directement du ministre de la Défense.

En revanche, depuis la Guerre Froide et la multiplication des disciplines de recueil de l'information, certains États comme les États-Unis ont développées d'autres formes plus complexes d'architecture du renseignement. Nous allons donc nous intéresser à l'architecture du renseignement américain afin de comprendre le rôle précis de la National Security Agency (NSA)[107].

6.1. L'« Intelligence Community » américaine

Etant donné que nous abordons le sujet du renseignement comme instrument de *soft power* avec comme objet d'étude la NSA, il est important de connaître le policy design dans lequel cette agence évolue.

L'architecture du renseignement américain appelée « *Intelligence Community* » est la plus vaste dans le monde et est devenue une référence dans le monde du renseignement. Elle est composée de seize agences spécialisées dans différents types de recueil de l'information, animant en leur sein un cycle de renseignement propre pour chaque spécialisation. L' « Intelligence Community » américaine repose sur trois niveaux : le niveau fédéral, les États fédérés et les agences locales (polices locales), et enfin les agences privées. Depuis le 11 septembre et les problèmes d'échange d'informations entre les différentes agences, cette structure est chapeautée par le Director of National Intelligence (DNI) qui a remplacé la fonction de Director of Central Intelligence (DCI) qu'occupait le directeur de la Central Intelligence Agency (CIA)[108]. Cette fonction instituée par l'Intelligence Reform and Terrorism Protection Act de 2004 vise à chapeauter les agences indépendantes (comme la CIA), les agences dépendant des départements de l'État américain (comme le FBI) ainsi que les agences militaires (dont fait partie la NSA). Le DNI est le principal conseiller du président et du National Security Council quant au renseignement relatif à la sécurité nationale, collecté par les seize agences qui participent à la réalisation du

[107] Olivier Chopin, et Oudet Benjamin. *Renseignement et sécurité*. Cursus (Armand Colin), Armand Colin, 2016, p. 80.
[108] Daninos, Franck. « La réforme perpétuelle du renseignement américain ». *Sécurité globale* 4, n° 2 (2008), p. 57.

National Intelligence Program formulé par le DNI[109]. La figure suivante représente la communauté américaine du renseignement en 2014 avec la relation entre le DNI, le National Security Council et le Community Management Staff (qui transmet les informations directement au Président) avec autour les seize agences qui la compose.

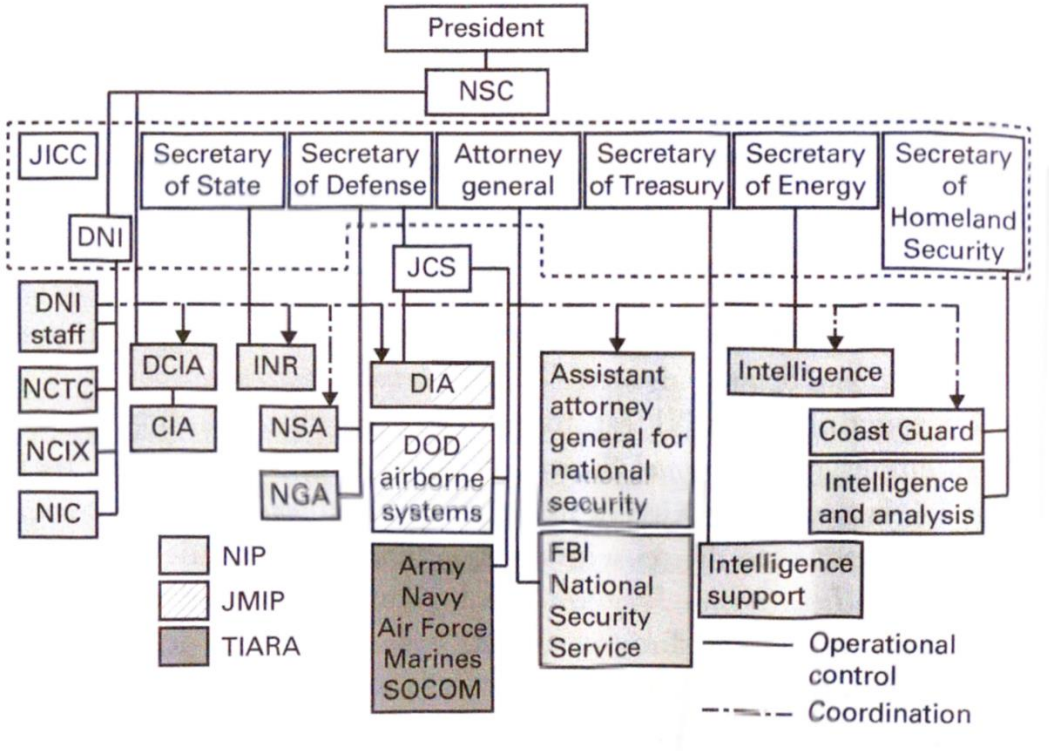
Figure 8 : La communauté américaine du renseignement en 2014[110]

Source : DNI, 2014.

La figure 9 ci-dessous est un schéma simplifié qui met en évidence les processus de contrôle opérationnel et de coordination entre les différentes agences en fonction de leur catégorie. Ainsi, même si c'est le Secrétaire à la défense qui contrôle les opérations des agences de renseignement militaire, c'est le DNI qui assure la coordination entre ces agences et toutes les autres[111].

[109] Olivier Chopin, et Oudet Benjamin. *Renseignement et sécurité*. Cursus (Armand Colin), Armand Colin, 2016, p. 81.
[110] Jean-Claude, Cousseran, et Hayez Philippe. *Leçons sur le renseignement*. Odile Jacob. Paris : Odile Jacob, 2017.
[111] Olivier Chopin, et Oudet Benjamin. *Renseignement et sécurité*. Cursus (Armand Colin), Armand Colin, 2016, p. 83.

Figure 9 : Les chaines de coordination et de contrôle dans la communauté américaine[112]



Le nombre d'agences de recueil de l'information, mais aussi la complexité de la coordination entre ces agences indiquent à quel point le renseignement est une priorité pour les Etats-Unis. L'explication de l'architecture de la communauté de renseignement des États-Unis nous permet de mieux situer le rôle de la NSA en son sein.

6.2. La National Security Agency (NSA)

La National Security Agency (NSA) a vu le jour en 1952 lors de la guerre de Corée afin de pallier les dysfonctionnements du système de renseignement américain. En effet, à l'époque, la CIA n'avait pas vu venir l'attaque militaire en 1950 de la Corée du Nord communiste sur la Corée du Sud, malgré un large réseau d'informateurs dans la région. C'est ainsi que la nouvelle agence civile et militaire spécialisée dans le renseignement d'origine électromagnétique a vu le jour.

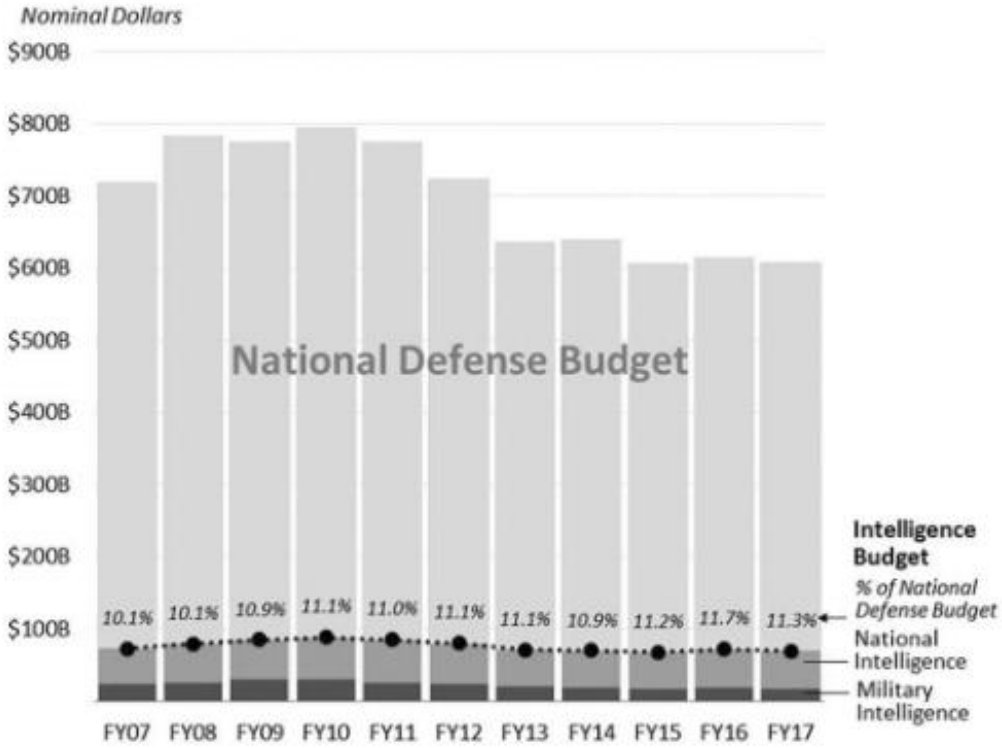
[112] Lowenthal, Mark. *Intelligence : From Secrets to Policy*. 5ème. Washington: CQ Press, 2011, p. 35.

6.2.1 Des moyens considérables

Les moyens octroyés à la NSA sont titanesques. Si le budget octroyé à *l'Intelligence Community* américaine reste globalement le même (entre 10 et 11% du budget octroyé à la défense), comme le montre la figure 10, certains services ont vu leurs moyens augmenter considérablement entre 2000 et 2014. Ainsi, le budget alloué à la NSA a été multiplié par 2,7 fois entre 2001 et 2013. Cette tendance n'est pas qu'américaine car plusieurs services de renseignement occidentaux ont vécu une augmentation similaire (principalement dû à la menace terroriste et au 11 septembre), même si leurs moyens restent inférieurs à ceux de la NSA[113]. En 2013, le budget estimé de la NSA montait à 10,8 milliards de dollars. L'agence américaine dispose également de 40 000 employés, techniciens, informaticiens ou analystes, sur les 100 000 employés qui composent l'effectif du renseignement américain[114]. Cependant, si on considère les employés de la NSA et toutes les personnes en sous-traitance, ce chiffre passe à 850 000 personnes pour l'ensemble du renseignement américain[115].

[113] Jean-Claude, Cousseran, et Hayez Philippe. *Leçons sur le renseignement*. Odile Jacob. Paris : Odile Jacob, 2017, p.
[114] Lelièvre, Arnaud. 'La Communication Web Des Services de Renseignement : Étude Sémio-Pragmatique'. UCL, 2018, p. 531.
[115] Antoine, Lefébure. *L'affaire Snowden : comment les États-Unis espionnent le monde*. Paris : La Découverte, Paris, 2014, p. 144.

Figure 10 : Budget américain du renseignement[116]



Mais ce qui représente le mieux le gigantisme de cette agence, c'est l'inauguration en 2011 de son data center dans l'Utah. Cette installation qui aura coûté 1,7 milliard de dollars dispose de 100 000 m² et consomme 65 mégawatts d'électricité (ce qui correspond à une ville de 20 000 habitants[117]). Ce data center à lui seul, pourrait stocker l'équivalent de 20 téraoctets (ce qui équivaut à la bibliothèque du Congrès) par minute selon un ancien mathématicien de la NSA[118]. Selon le journal Le Monde, le data center de l'Utah est doté de capacités de stockage inédites qui sont mesurées en yottabytes (10^{24} bits)[119]. Sachant que 1 octet équivaut à 8 bits, 1 yottabyte correspond à une capacité de stockage de 125 milliards de téraoctet. Ce data center sert donc actuellement de "bibliothèque" pour la NSA, mais il existe beaucoup d'autres centres et bases, avec chacun leurs propres fonctions.

[116] Jean-Claude, Cousseran, et Hayez Philippe. *Leçons sur le renseignement*. Odile Jacob. Paris : Odile Jacob, 2017, p.
[117] Antoine, Lefébure. *L'affaire Snowden : comment les États-Unis espionnent le monde*. Paris : La Découverte, Paris, 2014, p. 152.
[118] Carroll, Rory. « Welcome to Utah, the NSA's desert home for eavesdropping on America ». *The Guardian*. 14 juin 2013.
[119] Bernard, Philippe. « Voyage au cœur de la NSA ». *Le Monde*. 28 août 2013.

6.2.2 La surveillance de masse de la NSA

La collecte de données de masse n'est pas récente pour la NSA. En effet, dès sa création, la NSA s'intéresse à l'espionnage de ses propres citoyens via le projet Shamrock[120]. Celui-ci est initié pendant la Seconde Guerre Mondiale et consiste à collecter la plupart des télégrammes internationaux assuré directement par les réseaux de télégraphie américains (150 000 télégrammes chaque mois).

Avec le développement de la téléphonie, en 1967, les États-Unis étant en pleine guerre du Vietnam, la NSA s'intéresse également aux conversations téléphoniques afin d'établir une liste des "désordres civils" (opération Minaret). Cette liste désigne toutes les organisations luttant notamment contre la guerre du Vietnam ou pour les droits civiques pour les Afro-américains et pouvant être soutenues par des gouvernements étrangers[121].

En 1975, plusieurs commissions parlementaires mettent au jour ces pratiques, qui font un scandale aux États-Unis. À la suite de ces révélations, est adopté en 1978, le *Foreign Intelligence Surveillance Act* (FISA) qui délimite l'étendue et les prérogatives de la NSA. En conséquence, l'interception systématique des télégrammes ainsi que l'opération Minaret furent proscrites, du moins sur le sol américain. Un tribunal secret est alors créé en 1978, la Foreign Intelligence Surveillance Court qui autorise la mise sous surveillance d'un individu sous 3 conditions : si c'est un agent étranger (contre-espionnage), un espion (toujours en vertu du contre-espionnage), ou un suspect de terrorisme[122]. Ce tribunal, comme nous le verrons, deviendra beaucoup plus laxiste avec les attentats du 11 septembre et le FISA *Amendments Acts* de 2008 ainsi que *l'US Patriot Act*.

6.2.3 *US Patriot Act* et le *FISA Amendents Acts*

Après les attentats du 11 septembre, le président George W. Bush a autorisé la NSA à multiplier les opérations de surveillance grâce à *l'US Patriot Act*. L'autorisation qui a suscité le plus de polémique, suite à sa révélation par le New York Times en 2005, était celle qui visait à enregistrer les conversations téléphoniques sans avoir besoin d'un mandat délivré par la justice. Cette multiplication des opérations de

[120] Antoine, Lefébure. *L'affaire Snowden : comment les États-Unis espionnent le monde*. Paris : La Découverte, Paris, 2014, p. 86.
[121] *Ibid*, p. 85-86.
[122] *Ibid*, p. 88-89.

surveillance faisait partie du Programme de surveillance du président (PSP). Officiellement, le PSP était un « décret présidentiel » constitué d'une série d'instructions données par le président faisant force de loi pour les membres du gouvernement. Le PSP autorisait la NSA à intercepter les conversations téléphoniques et les e-mails échangés entre les États-Unis et les pays étrangers sans mandat spécial de la Cour de surveillance du renseignement étranger[123].

Suite à la révélation de ces écoutes, l'administration Bush s'était engagé à mettre fin à ce programme d'ici 2007. En réalité, le Congrès passa les deux dernières années du mandat du président Bush à voter des lois (le *Protect America Act* de 2007 et le FISA *Amendments Acts* de 2008) qui justifiaient rétroactivement le PSP et dédouanaient les entreprises de télécommunications et les fournisseurs d'accès internet impliqués. Non seulement cette législation faisait indûment croire aux Américains que leurs communications n'étaient pas visées par les écoutes téléphoniques mais en plus, elle élargissait le plan d'application du PSP à toutes les communications, à l'intérieur ou à l'extérieur du pays [124].

Grâce aux législations mises en place lors de l'administration Bush, à savoir notamment la section 215 du *Patriot Act*[125] et la section 702 du FISA *Amendments Act*[126], la NSA a pu justifier l'utilisation de ses deux principales méthodes de surveillance d'Internet : *Upsteam Collection* et le programme PRISM[127], dont nous parlerons ci-après.

Lorsque Keith Alexander prit la direction de la NSA, en 2005, sa position était très simple : « *Plutôt que de chercher une seule aiguille dans la botte de foin, son approche était la suivante : "collectons toute la botte de foin, […] collectez tout, indexez et archivez"*. » On a résumé cette philosophie par un slogan : « *Collect it all* ».

---

[123] Snowden, Edward, Etienne Menauteau, et Aurélien Blanchard. *Mémoires vives*. Seuil. Paris, 2019, p. 192-193.
[124] *Ibid*, p. 193-194.
[125] La section 215 du *Patriot Act* autorise la NSA a obtenir un ordre de la cour de surveillance du renseignement étranger des États-Unis contraignant des parties tierces à produire tout élément tangible susceptible d'être pertinent pour le renseignement extérieur et la lutte contre le terrorisme.
[126] La section 702 du FISA *Amendments Act*[126] autorise la communauté du renseignement à cibler tout étranger à l'extérieur des États-Unis dont on estime qu'il existe une probabilité suffisante pour qu'il communique « une information relevant du renseignement étranger ».
[127] Snowden, Edward, Etienne Menauteau, et Aurélien Blanchard. *Mémoires vives*. Seuil. Paris, 2019, p. 248.

« Beaucoup estiment que le problème est que nous collectons trop d'informations, et que la solution […] serait de réduire ou de filtrer les données, […] nous pensons le contraire […] la solution est de continuer à collecter le plus d'information possible tout en révolutionnant nos façons de l'indexer, de la connecter, de l'analyser, de la stocker. » (Alexander, 2003)[128]

Cette philosophie, que l'on examinera de plus près dans le chapitre consacré à la face cachée du renseignement américain, est spécifique au SIGINT. En effet, dans le renseignement d'origine électromagnétique, plus vous récoltez des informations, mieux c'est. La vision de Keith Alexander résume parfaitement la manière de penser du renseignement technologique opéré par la NSA.

6.2.4 Les révélations d'Edward Snowden

En 2013, un lanceur d'alerte nommé Edward Snowden, ancien informaticien de la CIA et consultant de la NSA en tant qu'administrateur système, dévoile l'espionnage de masse que réalise la NSA. La plupart des informations utilisées dans ce travail sont d'ailleurs extraites des documents dont il a confié la publication au journaux *The Guardian* et *Washington Post*. Ces documents ont fait l'effet d'une bombe, non seulement aux États-Unis mais dans le monde entier, car comme nous le verrons, la NSA n'était pas seulement impliquée dans l'espionnage de masse aux États-Unis mais également dans les Etats alliés. Un film est d'ailleurs dédié à ce lanceur d'alerte (Snowden)[129] et son autobiographie, « Mémoires vives »[130], fait également partie des sources de ce travail.

Grâce aux informations divulguées par Edward Snowden, un ensemble de slides PowerPoint de la NSA datant de 2011 a été révélé au grand public (certaines sont disponibles sur le site du *Guardian*[131]). Ces slides définissaient la nouvelle position de la NSA sur la surveillance : « *Sniff It All, Know It All, Collect It All, Process*

[128] Chamayou, Grégoire. « Dans la tête de la NSA. Une histoire philosophique du renseignement américain ». *Revue du Crieur* 1, nº 1 (2015), p. 27.
[129] Stone, Oliver. *Snowden*. Thriller. Open Road Films (États-Unis), Pathé Distribution (France), 2016.
[130] Snowden, Edward, Etienne Menauteau, et Aurélien Blanchard. *Mémoires vives*. Seuil. Paris, 2019.
[131] MacAskill, Ewen, et Gabriel Dance. « NSA files: decoded ». *The Guardian*. 1 novembre 2013.

It All, Exploit It All, Partner It All », autrement dit, « *tout renifler, tout connaître, tout collecter, tout traiter, tout exploiter, tout partager* »[132].

« C'était du jargon marketing, de la pure com destinée à impressionner les alliés de l'Amérique – l'Australie, le Canada, la Nouvelle-Zélande et le Royaume-Uni –, c'est-à-dire les principaux pays avec lesquels les États-Unis partagent des renseignements » (Edward Snowden, 2019).

6.2.5 Les outils de surveillance de masse : PRISM et *Usptream Collection*

Pour mieux comprendre par quels systèmes la NSA a pu secrètement intercepter autant de communications privées, il faut se pencher sur les deux outils les plus invasifs de l'agence américaine : les programmes PRISM et Upstream Collection. Ce ne sont que deux des nombreux programmes de surveillance de masse de la NSA mais ce sont les plus invasifs. Tout d'abord, le programme PRISM, sur base surtout de la section 215 du *Patriot Act*, ce qui lui permet de collecter régulièrement des données auprès de Microsoft, Yahoo!, Google, Facebook, Youtube, Skype et Apple par exemple, ou toute autre donnée susceptible d'être stockée dans le cloud, comme des e-mails, des photos, des vidéos ou des historiques de navigation. Selon Snowden, l'utilisation abusive de cette législation transformait ainsi ces entreprises en complices conscients de ce qu'il se passait[133].

Le programme Upstream Collection, quant à lui, permettait la capture régulière de données directement sur les infrastructures Internet du secteur privé tels que les interrupteurs et les routeurs qui aiguillent le trafic Internet mondial via les satellites, ou les câbles en fibre optique qui parcourent le fond des océans et permet de relier les continents entre eux. Une équipe de la NSA, la Special Sources Operations, avait installé des systèmes de mise sur écoute dans les locaux des fournisseurs d'accès à Internet un peu partout dans le monde. Ainsi, ces deux systèmes combinés

[132] Snowden, Edward, Etienne Menauteau, et Aurélien Blanchard. *Mémoires vives*. Seuil. Paris, 2019, p. 247.
[133] *Ibid*, p. 248.

garantissaient de collecter un maximum d'informations, qu'elles soient en transit ou déjà stockées[134].

Pour comprendre comment la NSA pouvait puiser directement dans vos données, il faut nous plonger dans les technologies derrière Upsteam Collection. Parmi les outils les plus invasifs de la NSA, il y a le système TURBULENCE. Concrètement, lorsqu'un URL est tapé sur un navigateur internet, l'ordinateur envoie en réalité une requête vers son serveur de destination, requête qui va être interceptée par le système TURBULENCE. Elle va être envoyée dans plusieurs serveurs installés, soit dans des salles spéciales au sein de bâtiments appartenant à des grands opérateurs télécoms privés dans des pays alliés des États-Unis, soit au sein même de certaines ambassades américaines, soit dans des bases militaires, toujours américaines. Ces serveurs sont divisés en deux parties : TURMOIL, responsable de la collecte passive de données et TURBINE, qui gère la collecte active d'informations[135].

TURMOIL va d'abord trier la requête en vérifiant ses métadonnées afin de voir si celles-ci possèdent l'un des critères définis par la NSA, lui permettant de considérer la requête comme suspecte ou non. Ces critères peuvent être des informations de particuliers comme une adresse mail par exemple, une position géographique d'origine ou de destination ou encore un mot clé comme « manif ». Ainsi, une fois le tri effectué par TURMOIL, ce dernier envoie la requête à TURBINE, mais seulement si elle est considérée comme suspecte. TURBINE va alors rediriger la requête sur les serveurs de la NSA et de là, des algorithmes décident quel malware (logiciel malveillant) va être utilisé pour infiltrer l'ordinateur qui a formulé la requête initiale. Enfin, lorsque le logiciel a été choisi, TURBINE « libère » la requête sur le réseau afin qu'elle aille à son serveur de destination mais avec le logiciel malveillant « en supplément ». Ainsi, l'information recherchée arrivera sur l'ordinateur qui a formulé l'URL en même temps que le malware implanté par la NSA. Ce dernier, installé dans un ordinateur, peut alors fouiller et avoir accès à toutes les métadonnées et données qu'il désire. Toute cette

[134] Snowden, Edward, Etienne Menauteau, et Aurélien Blanchard. *Mémoires vives*. Seuil. Paris, 2019, p. 259.
[135] *Ibid*, p. 250-251.

opération, afin qu'elle soit invisible pour n'importe quel utilisateur se passe en moins de 686 millisecondes [136].

6.3. La face cachée du renseignement américain

Ces programmes utilisés par la NSA participent en réalité à un objectif plus large de collecte et d'analyse de l'information. Nous allons désormais essayer de voir ce qui se cache derrière les justifications terroristes de ces écoutes et découvrir ainsi leur réel objectif.

6.3.1. L'espionnage entre alliés

Comme nous allons le voir dans le chapitre consacré aux relations de la NSA avec les agences étrangères, l'espionnage entre alliés est commun dans le monde du renseignement. Avant de le voir d'un point de vue pratique, nous allons nous intéresser théoriquement à son usage afin de comprendre les réels intérêts à le pratiquer et pourquoi les États-Unis ne se privent pas pour espionner leurs alliés.

Il faut tout d'abord garder en tête que selon la perspective réaliste, les services de renseignement évoluent dans un environnement de compétition et de méfiance constante, comme expliqué au début de ce mémoire. Ainsi, même s'il existe des coopérations et de la collaboration entre des services de renseignement, la méfiance que l'un a envers l'autre peut le pousser à vérifier que cette collaboration en est réellement une et n'a pas pour but d'utiliser les données transmises contre lui. Ainsi, des États alliés sont donc partenaires mais également concurrents, surtout lorsque l'on parle de renseignement économique.

La principale philosophie du renseignement est que tout ce qui peut être recueillis comme information doit être collecté. Les États-Unis l'ont bien compris et l'appliquent à la lettre. En effet, si certains États se contentent plutôt de trouver "l'aiguille dans la botte de foin" avant de la surveiller, les États-Unis préconisent d'abord le fait de collecter "la botte de foin" pour ensuite seulement analyser "l'aiguille". On comprend donc que la stratégie de Keith Alexander, directeur

[136] Snowden, Edward, Etienne Menauteau, et Aurélien Blanchard. *Mémoires vives*. Seuil. Paris, 2019, p. 250-251.

de la NSA jusqu'en 2013, du « *Collect it all* » correspond parfaitement à la philosophie du renseignement technologique.

> *« Ainsi, tant qu'il est possible de collecter, il faut collecter, pour s'assurer de n'avoir raté aucune information qui se révélerait importante à un moment ou un autre. »* [137]

6.3.2. Le renseignement économique

Si le renseignement est avant tout au service de l'État et du pouvoir exécutif en général, il peut également être utilisé non seulement pour collecter des données, mais aussi pour conseiller certaines entreprises et leur donner un avantage stratégique dans la rude concurrence du monde libéral occidental. Dans le cas des États-Unis, la pratique est connue depuis la guerre froide mais surtout depuis *l'Executive Order United States Intelligence Activities 12333* de Ronald Reagan au début des années 1980 qui permet aux services de renseignement américains d'organiser des opérations à l'étranger avec la complicité d'entreprises américaines, sans être obligé d'en informer le procureur général[138]. Si à l'époque, le but était de lutter contre l'espionnage économique, scientifique et technologique mis en place par l'URSS, la chute du mur de Berlin n'a pas freiné cette pratique, bien au contraire.

En effet, à la fin de la guerre froide, une commission du Congrès américain a examiné le renseignement économique réalisé par les agences américaines et en a conclu que ce renseignement pouvait être effectué à condition qu'il ne puisse pas bénéficier directement aux entreprises américaines[139]. Ainsi les services de renseignement, avec la fin de la guerre froide et la disparition de leur ennemi, ont trouvé un nouvel objectif : l'espionnage économique et industriel, notamment de leurs alliés[140].

---

[137] Olivier Chopin, et Oudet Benjamin. *Renseignement et sécurité*. Cursus (Armand Colin), Armand Colin, 2016, p. 208.
[138] Laïdi, Ali. « Le renseignement économique américain de Reagan à Trump. Un engagement de plus en plus ferme ». *Prospective et stratégie* Numéro 10, nº 1 (2019), p. 104.
[139] *Ibid*, p. 105.
[140] Antoine, Lefébure. *L'affaire Snowden : comment les États-Unis espionnent le monde*. Paris : La Découverte, Paris, 2014, p. 72.

L'une des raisons de mobiliser les services de renseignement dans une guerre économique n'est pas forcément de donner un avantage stratégique aux entreprises d'un pays donné. En réalité, comme l'explique Jacques Fontanel dans « *Civilisation, globalisation, guerre »* en 2003, *« Le développement du commerce international est un facteur de paix, laquelle est la situation normale de l'économie de marché »*[141]. Dans un monde sans échanges commerciaux, un État peut s'en prendre à un autre sans se soucier de potentielles pertes économiques car il n'y a aucun intérêt commercial en jeu. Dans un monde où les interactions économiques sont multiples, une analyse rationnelle coût/bénéfice permet de réduire ainsi le risque d'un potentiel conflit[142].

Cependant, les services de renseignement américain ont également effectué des opérations dans l'intérêt économique des États-Unis via un de leur système nommé ECHELON. Ce système gardé secret jusqu'en 1990 fait partie de la coopération UKUSA qui compte les États-Unis, le Royaume-Uni, l'Australie, le Canada et la Nouvelle-Zélande, dont nous reparlerons dans le chapitre suivant[143]. Ce traité, qui concerne directement la NSA puisque c'est elle qui s'occupe de l'analyse de toutes les données partagées entre les Etats, a contribué notamment aux partages d'informations économiques. Selon Ducan Campbell, qui a révélé l'existence de ce programme, Echelon *« permet d'estimer les prix à venir des produits de base, de connaître l'objectif des États lors des négociations commerciales, de surveiller le commerce international des armes, de suivre de très près l'évolution des technologies sensibles, ou encore d'évaluer la stabilité politique et la puissance économique d'un pays cible »*.[144]

Il existe une multitude d'exemples des usages du système ECHELON à des fins économiques comme l'écoute des délégués mexicains lors des négociations sur l'Accord de Libre-Echange Nord-Américain (ALENA), où des cadres de Toyota et de Nissan lors des négociations pour les droits de douanes et d'importation de voitures japonaises (Claude Delesse, 2004), où encore Airbus qui a perdu un accord de 6

[141] Lepri, Charlotte. « Les services de renseignement en quête d'identité : quel rôle dans un monde globalisé ? » *Géoéconomie* 45, nº 2 (2008), p. 41-42.
[142] *Ibid*, p. 42.
[143] Laïdi, Ali. « Le renseignement économique américain de Reagan à Trump. Un engagement de plus en plus ferme ». *Prospective et stratégie* Numéro 10, nº 1 (2019), p. 105.
[144] Antoine, Lefébure. *L'affaire Snowden : comment les États-Unis espionnent le monde*. Paris : La Découverte, Paris, 2014, p. 72.

milliards de dollars avec l'Arabie Saoudite au profit de Boeing grâce aux renseignements de la NSA[145].

Ainsi, les Américains espionnent leurs alliés au nom de la lutte contre la corruption depuis la fin de la guerre froide. Lors des révélations d'Edward Snowden, les documents révèlent que seulement 35% des ressources de la NSA sont affectées à la lutte contre les menaces terroristes, les 65% autres servent aux intérêts politiques, économiques et militaires du gouvernement américain.

Cependant, si ces écoutes concernent uniquement des domaines commerciaux ou économiques et ne démontrent pas réellement une influence exercée par les services de renseignement dans une dynamique de *soft power*, la révolution du monde numérique permet de le démontrer via les grandes entreprises américaines du monde digital, les GAFA.

6.3.3. Le réseau PRISM et les GAFA

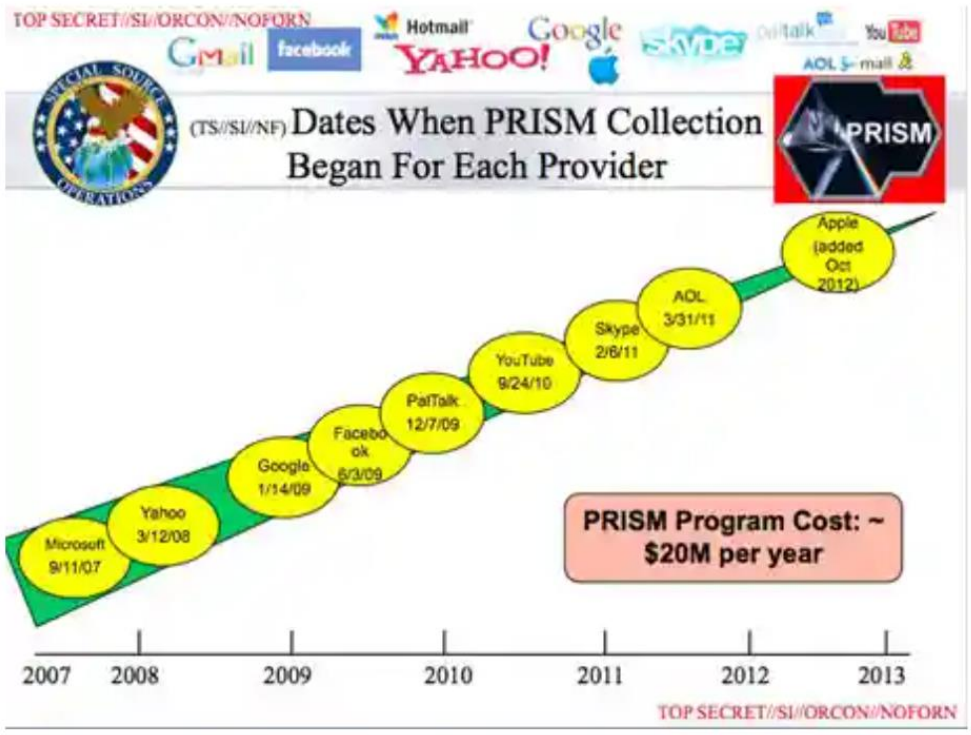
Lorsque l'on parle ici de GAFA (Google, Amazon, Facebook, Apple) on parle surtout des principales entreprises liées au domaine du numérique dans le monde occidental. Comme on l'a déjà expliqué dans ce travail, avec la révolution du monde numérique, les services de renseignement étatiques ne possèdent plus le monopole de l'information et doivent donc désormais interagir avec des entreprises privées. Ces entreprises stockent des millions de données sur leurs utilisateurs via leur boîte mail, leur smartphone, ou les réseaux sociaux par exemple. Il était donc logique pour la NSA, dans la logique de tout collecter, d'avoir un accès à ces données. Ainsi le système PRISM, mis en adéquation avec Upstream Collection, est installé en 2007 et a pour but, grâce aux mandats de la FISA, d'accéder aux banques de données de neuf géants d'internet à savoir : Microsoft, Yahoo !, Facebook, Apple, Google, Youtube, Skype, AOL et Paltalk (service de discussion vidéo)[146]. Les liens entre Amazon et la NSA sont également très étroits puisque l'entreprise américaine a créé et gère le *cloud* de la CIA, de la NSA et d'autres ministères du gouvernement

[145] Antoine, Lefébure. *L'affaire Snowden : comment les États-Unis espionnent le monde*. Paris : La Découverte, Paris, 2014, p. 73.
[146] *Ibid*, p. 122.

américain[147]. Ces entreprises n'ont pas seulement collaboré avec la NSA par le fait de la cour FISA, car l'agence américaine a payé des millions de dollars à ces entreprises pour les services rendus[148].

Le système PRISM ainsi relié aux immenses data center de ces entreprises, permet alors de recevoir toutes informations liées à l'un de ces data center, une fois la demande de la FISA autorisée (voir figure 11). Ce système, entièrement automatisé, agit littéralement comme un prisme qui diffracte la lumière en rayons de couleurs. Les analystes de la NSA n'ont plus qu'à taper dans le moteur de recherche Unified Targeting Tool (UTT) ce dont ils recherchent et ils obtiennent ce qu'ils souhaitent, comme une recherche Google[149].

Figure 11 : Slide de la NSA démontrant la connexion du réseau PRISM avec les données des différentes entreprises du net ainsi que la date de cette connexion[150]



▲ Prism Photograph: Guardian

[147] Raufer, Xavier. « Escrocs, espions, mégalos : bienvenue chez les GAFA ». *Sécurité globale* 19, nº 3 (2019), p. 80.
[148] MacAskill, Ewen. « NSA paid millions to cover Prism compliance costs for tech companies ». *The Guardian*. 23 août 2013.
[149] Antoine, Lefébure. *L'affaire Snowden : comment les États-Unis espionnent le monde*. Paris : La Découverte, Paris, 2014, p. 123.
[150] Greenwald, Glenn, et Ewen MacAskill. « NSA Prism program taps in to user data of Apple, Google and others ». *The Guardian*. 7 juin 2013.

Comme le démontre ce slide dévoilé par Snowden, on peut voir les liens entre chaque entreprise numérique et la NSA ainsi que les dates du début de leur relation. Le coût du programme PRISM est également indiqué et correspond à 20 millions de dollars chaque année.

Cependant, le fonctionnement des systèmes comme PRISM ou XKEYSCORE[151], qui sont des outils extrêmement puissants, ne sont pas ce qui nous préoccupe ici car, ce qui nous intéresse en particulier c'est plutôt le lien entre la NSA et certaines entreprises privées. En effet, comme nous avons pu l'observer, la révolution technologique a entraîné une profonde transformation dans les relations entre le secteur privé et les agences de renseignement. Si certains évoquent une « privatisation » du renseignement américain, d'autres parlent d'une « externalisation ». Les services de renseignement américains, ne sachant pas toujours suivre la cadence de l'évolution des technologies, doivent parfois faire de la sous-traitance et interagir avec les grandes entreprises liées au milieu d'internet et du numérique. Il faut en effet rappeler que « 90% du trafic mondial s'effectue grâce à un ensemble de technologies développées, possédées et/ou mises en œuvre par les autorités et les grandes entreprises américaines »[152]. Ces échanges d'informations donnent lieu à un réel « marché » de l'information où se rencontrent les agences de renseignement mais aussi les professionnels dans les technologies de pointe, que ce soit dans le domaine du big data, de l'IA ou des fournisseurs de services en traitement de l'information. Ainsi, on peut considérer que l'*Intelligence Community* américaine ne se suffit plus de ses seize agences de renseignement qui font partie de l'archétype américain[153].

Rappelons notre première hypothèse : **Grâce aux liens entre certaines grandes entreprises américaines spécialisées dans les infrastructures liées à Internet et la NSA, le gouvernement américain a pu installer une dynamique d'influence envers certains États, aujourd'hui dépendants de ces infrastructures.**

[151] Chamayou, Grégoire. « Dans la tête de la NSA. Une histoire philosophique du renseignement américain ». *Revue du Crieur* 1, nº 1 (2015), p. 27-28.
[152] Snowden, Edward, Etienne Menauteau, et Aurélien Blanchard. *Mémoires vives*. Seuil. Paris, 2019, p. 183.
[153] Olivier Chopin, et Oudet Benjamin. *Renseignement et sécurité*. Cursus (Armand Colin), Armand Colin, 2016, p. 178-179.

Cette hypothèse portant sur le lien entre la NSA et les grandes entreprises américaines spécialisées dans le domaine numérique (voir ci-dessus) est donc partiellement justifiée. En effet, comme on l'a observé, il y a un lien direct entre ces entreprises (les GAFA et d'autres) et le SIGINT américain, puisque des agences comme la NSA utilisent ces infrastructures pour récupérer leurs données, parfois à la limite de la légalité. Cependant, pour le moment, nous n'avons pas pu prouver que cette collaboration secrète entre ces entreprises et la NSA a pu réaliser une dynamique d'influence sur d'autres États. C'est désormais ce que nous allons entreprendre en examinant les liens, parfois secrets, que la NSA entretient avec d'autres agences et la façon dont elle influence ces derniers.

7. Les liens entre la NSA et les autres agences de renseignement du monde

Comme nous allons le voir dans ce chapitre, la NSA a créé un réseau tentaculaire grâce à ses nombreuses relations, notamment parmi les services de renseignement de pays alliés. C'est grâce à l'analyse de ces relations que nous pourrons déterminer s'il existe une influence de la NSA sur ces dernières et ainsi vérifier nos deux prochaines hypothèses.

7.1. Le Royaume-Uni : Government Communications Headquarters (GCHQ)

Pour comprendre le lien entre les États-Unis et le gouvernement britannique en matière de renseignement, il faut revenir à la seconde guerre mondiale et à la plus grande réussite du renseignement britannique, à savoir le déchiffrement de la machine Enigma. En effet, alors que les u-boots allemands font des ravages sur les navires britanniques et américains, la GC&CS (Governement Code and Cypher School), l'école de cryptographie britannique fondée au lendemain de la première guerre mondiale, renommée GCHQ (Government Communications Headquarters), collabore avec les Américains en matière d'écoutes et de renseignement d'origine électromagnétique dès 1941. A l'époque, le système de communication allemand était

crypté par une curieuse machine : Enigma. C'est au final, Alan Turing travaillant pour le GCHQ qui déchiffra la mystérieuse machine à écrire allemande.[154]

Par la suite, le GCHQ continua à se perfectionner dans l'invention de nouveaux moyens d'assurer le secret des télécommunications et à partager ses informations avec d'autres services, notamment ses homologues américains. Le lien entre le GCHQ et la NSA se formalisera en 1947 avec la signature du secret treaty UKUSA (pour United Kingdom/United States of America) visant à améliorer l'efficacité de leurs échanges pour l'interception des communications au sein du bloc soviétique. Outre le Royaume-Uni et les États-Unis, le traité UKUSA va créer ce qu'on appellera les « Five Eyes », c'est-à-dire un accord sur le partage de renseignements entre le Royaume-Uni, les États-Unis, le Canada, l'Australie et la Nouvelle-Zélande. Ce traité, toujours actif aujourd'hui, est resté secret jusqu'en 1976 mais ne sera connu de tous que bien après, avec le système ECHELON (p. 134)[155].

La collaboration entre les services de renseignement SIGINT américain et britannique ne s'arrête pas là. En effet, les compétences des services britanniques en matière de cryptologie sont extrêmement utiles pour la NSA, notamment pour le piratage des emails, réseaux sociaux ou téléphones portables[156]. Grâce aux documents révélés par Edward Snowden, on sait qu'entre 2009 et 2012 la NSA a financé le GCHQ a hauteur de 100 millions de livres (soit 119 millions d'euros)[157]. La coopération entre les deux agences s'est même lancée dans des opérations de cyberguerre en attaquant l'entreprise de télécommunications Belgacom en 2013 par exemple[158]/[159].

Cette relation très étroite entre les deux services répond à une nécessité pour chacun d'eux. Le GCHQ bénéficie des services de la NSA, non seulement en matière de réseaux mais également d'un point de vue financier, surtout depuis la réduction de budget de 40 millions de livres alloué à l'agence britannique. On peut y voir ainsi une

---

[154] Antoine, Lefébure. *L'affaire Snowden : comment les États-Unis espionnent le monde*. Paris : La Découverte, Paris, 2014, p. 133-134.
[155] *Ibid*, p. 134.
[156] « Pourquoi la NSA et le GCHQ ont volé des clés de chiffrement de cartes SIM ». *Le Monde*. 23 février 2015.
[157] Antoine, Lefébure. *L'affaire Snowden : comment les États-Unis espionnent le monde*. Paris : La Découverte, Paris, 2014, p. 144.
[158] Boffey, Daniel. « British spies "hacked into Belgian telecoms firm on ministers" orders' ». *The Guardian*. 21 septembre 2018.
[159] Traynor, Ian. « GCHQ: EU surveillance hearing is told of huge cyber-attack on Belgian firm ». *The Guardian*. 3 octobre 2013.

forme de sous-traitance du GCHQ pour la NSA. De son côté, l'agence américaine a également besoin des Britanniques non seulement pour leur situation géographique (90% des câbles à fibres optiques transatlantiques transitent par l'Angleterre), mais aussi pour les liens qu'ils ont encore avec les pays du Commonwealth[160].

7.2. Le secret treaty UKUSA

Le système de communications par satellite Intelsat est utilisé pour acheminer la plupart des communications téléphoniques, télécopies, télex, Internet et e-mails dans le monde. Parallèlement à ce réseau de couverture par satellites, se trouve un réseau fantôme resté très secret de postes d'écoute et de stations de suivi, organisé par des agences de renseignement occidentales qui interceptent et surveillent toutes les communications relayées par Intelsat. Il s'agit du réseau UKUSA, ainsi appelé en raison des accords encore secrets au début de la guerre froide, entre la National Security Agency des États-Unis (NSA) et le siège du gouvernement britannique (GCHQ) en tant que partenaires principaux, et la NSA clairement le partenaire principal sur la base de ressources américaines supérieures; un deuxième niveau de partenaires juniors, dont le Canada, l'Australie et la Nouvelle-Zélande; et un autre cercle extérieur de pays qui coopèrent avec l'alliance, en permettant, par exemple, l'installation de postes d'écoute sur leur territoire. Le but initial de l'UKUSA était le renseignement d'origine électromagnétique dans le contexte de la guerre froide (Claude Delesse, 2004). Chaque pied carré du bloc soviétique a été recouvert pour l'interception et le décryptage des communications militaires et politiques. Au lendemain de la « vieille guerre », il n'était pas question d'abandonner cet investissement mondial de haute technologie. Les aspirateurs stratégiquement placés dans le ciel continuent à aspirer les télécommunications du monde, malgré les appréhensions des critiques et même de certains transfuges des agences elles-mêmes. Ils exploitent même des systèmes de télécommunications terrestres, complétant ainsi la couverture quasi totale des communications mondiales[161].

Cette interception commune faite par les Five Eyes était réalisée grâce au système ECHELON (dont on peut observer quelques stations sur la figure 12), qui

[160] Antoine, Lefébure. *L'affaire Snowden : comment les États-Unis espionnent le monde*. Paris : La Découverte, Paris, 2014, p. 144-145.
[161] Whitaker, Reginald. *The end of privacy*. The new press. New York, 1999, p. 91.

constitue l'outil technologique du traité UKUSA. Ainsi, chaque membre du traité UKUSA s'est vu attribué une zone à espionner afin de pouvoir ensemble, couvrir le monde entier. Le Communications Security Establishment (CSE) au Canada intercepte les communications du nord de l'URSS et d'une partie de l'Europe, le Defense Security Directorate (DSD) en Australie ainsi que le General Communications Security Bureau (GCSB) en Nouvelle-Zélande couvrent ensemble la partie orientale de l'Océan indien, l'Asie du Sud-Est et une partie du Pacifique Sud. Comme expliqué précédemment, l'étroite collaboration entre le GCHQ et la NSA continue dans le traité UKUSA puisqu'ils se partagent le reste du monde[162].

Figure 12 : Les stations d'écoute du réseau ECHELON en 2013[163]

Lieu	Pays	Nom de code
Yakima	États-Unis	Jacknife
Sugar Grove	États-Unis	Timberline
Sabana Seca	Porto Rico	Coraline
Harrogate (Menwith Hill)	Royaume-Uni	Moonpenny
Misawa	Japon	Ladylove
Bad Aibling	Allemagne	Garlick

7.3. La France : Direction Générale de la Sécurité Extérieure (DGSE)

Si les rapports entre la Grande-Bretagne, les États-Unis et certains États du Commonwealth en matière de partage du renseignement étaient connus depuis 1976, les échanges d'informations entre les États-Unis et la France n'ont été dévoilés que récemment grâce à l'affaire Snowden. En effet, les documents transmis par Snowden mentionnent un accord de coopération connu sous le nom de « Lustre »[164] signé depuis la fin de l'année 2011. Cet accord permet à la NSA et la DGSE de se partager des données mutuellement et ce, de manière quasiment automatisée. C'est ainsi que selon

[162] Antoine, Lefébure. *L'affaire Snowden : comment les États-Unis espionnent le monde*. Paris : La Découverte, Paris, 2014, p. 139.
[163] *Ibid*, p. 117.
[164] Follorou, Jacques. « Surveillance : la DGSE a transmis des données à la NSA américaine ». *Le Monde*. 30 octobre 2013.

The Wall Street Journal, entre le 10 décembre 2012 et le 8 janvier 2013, la France a fourni 70,3 millions de données téléphoniques françaises à la NSA[165].

Si l'accord « Lustre » est le premier protocole d'échange de données entre les deux agences, la coopération entre la NSA et la DGSE existe néanmoins depuis plusieurs années. En effet, dès les années 1980, la NSA a aidé la DGSE à construire son propre système de surveillance grâce à la fourniture de puissants ordinateurs (type Cray)[166]. Ces liens étroits établis entre la NSA et la DGSE existent donc depuis des années et se sont améliorés au fil des années comme le montrent les discussions entre des hauts fonctionnaires de la DGSE et de la NSA dans les années 2006-2007, notamment sur le partage d'informations de la DGSE sur le continent africain et les questions de terrorisme[167]. Cette relation bilatérale va s'élargir au GCHQ, grand allié de la NSA, qui a également noué des liens étroits avec les renseignements français, notamment en matière de cryptage[168]. Cette relation a notamment permis au GCHQ de travailler en 2009 directement avec des agents de France-Télécom-Orange, les responsables du renseignement technique en France, en matière de déchiffrement et décryptage[169].

Les liens entre les services de renseignement français avec les agences anglo-saxonnes seraient indirectement le résultat d'une mauvaise relation interne entre les deux services français, la DGSE et la Direction Centrale de la Sécurité Intérieure (DCRI) renommée depuis 2014 Direction Générale de la Sécurité Intérieure (DGSI). En effet, suite au changement de paradigme du renseignement (révolution du cyber et nouvelles techniques de collecte de données), la DGSI est devenue dépendante techniquement de la DGSE[170]. Comme expliqué dans le journal Le Monde, la conséquence de cette rivalité est que ces deux agences ont parfois préféré privilégier des coopérations bilatérales avec la NSA ou le GCHQ plutôt que de renforcer leur

[165] Antoine, Lefébure. *L'affaire Snowden : comment les États-Unis espionnent le monde*. Paris : La Découverte, Paris, 2014, p. 65-66.
[166] Follorou, Jacques. « Espionnage de la NSA : au-delà de l'indignation, la coopération continue ». *Le Monde*. 24 juin 2015.
[167] Follorou, Jacques. « La France, précieux partenaire de l'espionnage de la NSA ». *Le Monde*. 29 novembre 2013.
[168] *Ibid*.
[169] Follorou, Jacques. « Espionnage de la NSA : au-delà de l'indignation, la coopération continue ». *Le Monde*. 24 juin 2015.
[170] Follorou, Jacques. « Pris dans leurs rivalités, les services français ont privilégié leurs liens avec la NSA et le GCHQ ». *Le Monde*. 10 décembre 2016.

collaboration. Interrogé par le même journal en 2016, l'ancien chef de la DGSI de 2007 à 2012, Bernard Squarcini disait : « *C'est regrettable mais en matière de coopération, les services français coopèrent mieux avec leurs homologues étrangers qu'entre eux. »*[171]

Cependant, malgré des relations étroites et des accords, une méfiance permanente demeure entre les services de renseignement français et étrangers. En effet, des documents divulgués par Edward Snowden datant de 2009 montrent des traces d'écoutes par les agents du GCHQ lors des négociations pour la libération de six ressortissants français à Bakassi au Nigéria[172]. Comme nous l'apprend le journal Le Monde, les ambassades françaises à N'Djamena, Niamey et Kinshasa ainsi que des grands groupes industriels français ont été mis sur écoute par les agents du GCHQ. L'Afrique ne représente pas un enjeu nouveau pour les anglo-saxons. L'accord de coopération Lustre entre la NSA et la DGSE manifestant déjà l'intérêt de la NSA notamment pour l'Afrique. Selon l'expert Fabrice Epelboin, professeur à l'institut des sciences politiques de Paris, « *Le continent Africain échappe en grande partie aux grandes oreilles Américaines (seulement 11Gb de trafic) … Mais pas aux grandes oreilles Françaises (343Gb, ou presque) …* »[173], d'où l'intérêt d'un partage d'information entre la France et les États-Unis. Il ne serait pas étonnant que les mises sur écoute par le GCHQ des ambassades et grands groupes français présents en Afrique soit en réalité orchestrées en partie par la NSA, vu la collaboration ultra privilégiée entre les deux agences anglo-saxonnes.

Le fait que trois chefs d'État français consécutifs, Jacques Chirac, Nicolas Sarkozy et François Hollande, aient été mis sous surveillance de 2006 à 2012[174], et que des ambassades et grands groupes français présents en Afrique soient mis sur écoute par la NSA et le GCHQ, ne semble pourtant pas avoir altéré la relation entre la NSA, le GCHQ et la DGSE. La réaction française lors des révélations de Snowden démontre bien l'inconfort de la position française. En effet, l'administration française se serait

[171] Follorou, Jacques. « Pris dans leurs rivalités, les services français ont privilégié leurs liens avec la NSA et le GCHQ ». *Le Monde*. 10 décembre 2016.
[172] Piel, Simon, et Joan Tilouine. « La France et ses intérêts en Afrique sous surveillance ». *Le Monde*. 8 décembre 2016.
[173] Champeau, Guillaume. « Lustre : la France aurait coopéré avec la NSA ». *Numerama*. 28 octobre 2013.
[174] Follorou, Jacques. « Espionnage de la NSA : au-delà de l'indignation, la coopération continue ». *Le Monde*. 24 juin 2015.

montrée « faussement » indignée par les écoutes de la part de son allié américain, notamment par l'existence de l'accord « Lustre », un partenariat finalement très dissymétrique[175], mais aussi par la vigilance de la France de ne pas vouloir froisser les Américains, représentant toujours actuellement la plus grande puissance au monde. C'est pour ces raisons que l'État français, pourtant le pays représentant le respect des droits fondamentaux, aurait refusé la demande d'asile d'Edward Snowden[176].

7.4. L'Allemagne : Bundesnachrichtendienst (BND)

Le Service fédéral de renseignement, nommé Bundesnachrichtendienst (BND), est le service de renseignement extérieur du gouvernement allemand, placé directement sous la tutelle de la Chancellerie. Il importe de contextualiser la situation des services de renseignement en Allemagne qui impacte leur image au sein de leur population. En effet, depuis la seconde guerre mondiale et les atrocités commises par les services de sécurité et de renseignement allemand, la Gestapo et les SS, les agences de renseignement sont toujours aujourd'hui, relativement mal perçues par la population allemande[177]. De plus, le pouvoir exécutif allemand est limité par une cour constitutionnelle extrêmement solide et leurs citoyens sont protégés par dix-sept instances régionales de défense de la vie privée, ce qui limite la pratique de l'espionnage[178].

En dépit des fortes différences avec les services de renseignement américains, le BND s'est rapproché de ceux-ci, depuis la séparation du pays opérée au début de la guerre froide. A l'époque, des bases américaines sont créées dans la partie de la République Fédérale allemande (RFA), dont certaines sont toujours en service aujourd'hui. Les Américains contribuent alors à la constitution d'un embryon de service secret allemand, qui est devenu en 1956 le BND[179]. L'Allemagne fait donc face

[175] Beckouche, Pierre. « La révolution numérique est-elle un tournant anthropologique ? » *Le Débat* 193, nº 1 (2017), p. 161.
[176] Antoine, Lefébure. *L'affaire Snowden : comment les États-Unis espionnent le monde*. Paris : La Découverte, Paris, 2014, p. 64-65.
[177] Tibère, Clément. « Allemagne ». In *Dictionnaire du renseignement*, Hors collection. Paris : Éditions Perrin, 2018, p. 45.
[178] Antoine, Lefébure. *L'affaire Snowden : comment les États-Unis espionnent le monde*. Paris : La Découverte, Paris, 2014, p. 66-69.
[179] Tibère, Clément. « Allemagne ». In *Dictionnaire du renseignement*, Hors collection. Paris : Éditions Perrin, 2018, p. 45.

à un dilemme : d'une part, la Constitution allemande limite fortement la pratique de l'espionnage, mais d'autre part, la situation de la guerre froide et à la menace que représente la Stasi, le service de renseignement de l'Allemagne de l'Est, accroissent le besoin de renseignements. On comprend dès lors le besoin des Allemands à coopérer avec les Etats-Unis, quitte à perdre une partie de leur indépendance[180]. Cette situation arrangeait bien les États-Unis étant donné la politique de *Containment* élaborée à l'époque[181].

Les documents dévoilés par Snowden en 2013 démontrent notamment qu'en décembre 2012, la NSA a enregistré les métadonnées de près de 15 millions de communications téléphoniques et 10 millions de connexions Internet par jour en Allemagne[182]. Ceci a eu l'effet d'une bombe parmi la population allemande remettant profondément en cause l'amitié américano-allemande. De plus, on y apprend que le téléphone personnel d'Angela Merkel est également sous écoute depuis 2002[183]. Comme la France, l'Allemagne est embarrassée et certains accusent la chancellerie de minimiser l'espionnage de la NSA sur le sol allemand[184].

Cette situation devient plus embarrassante encore lorsque des États européens ou partenaires de l'OTAN, tels que la France ou la Belgique, découvrent qu'ils sont également mis sur écoute par le BND, notamment grâce à l'infrastructure Deutsche Telekom. En effet, dans un accord signé en 2004 par le BND et l'entreprise de télécommunication allemande, cette dernière s'engageait à intercepter le flux massif de données de communication transitant sur son territoire, dont des données issues de France Télécom[185].

---

[180] Antoine, Lefébure. *L'affaire Snowden : comment les États-Unis espionnent le monde*. Paris : La Découverte, Paris, 2014, p. 68.
[181] Tibère, Clément. « Allemagne ». In *Dictionnaire du renseignement*, Hors collection. Paris : Éditions Perrin, 2018, p. 45.
[182] Antoine, Lefébure. *L'affaire Snowden : comment les États-Unis espionnent le monde*. Paris : La Découverte, Paris, 2014, p. 66.
[183] *Ibid*, p. 69.
[184] « Hitzige Debatte über die BND-NSA-Kooperation ». Berlin: Bundestag, 2015.
[185] Follorou, Jacques. « Deutsche Telekom a espionné la France pour le compte de la NSA ». *Le Monde*. 5 juin 2015.

« … entre 2002 et 2013 le BND a espionné pour le compte de la NSA plusieurs dirigeants européens, ainsi que des entreprises de défense, dont Airbus. »[186]

Ce transfert de données de la BND à la NSA, qui s'élevait jusqu'à 1,3 milliards de métadonnées par mois[187], se serait fait notamment via la base de Bad Aibling, qui à elle seule, aurait été responsable du transfert de 500 millions de métadonnées par mois[188]. Ancienne propriété de la NSA et considérée comme le centre d'interception le plus puissant d'Europe[189], cette base a été transférée à la BND en 2004 et sert aujourd'hui au suivi et à l'interception des données des satellites en mouvement[190]. Mais ce n'est pas la seule, car la base de l'armée de l'air américaine à Ramstein, en Allemagne, sert également au transit des données américaines, notamment pour l'usage de drone de combat américain au Moyen-Orient[191].

Au-delà de l'importance de ces révélations sur cette coopération en matière d'écoute et de transfert de métadonnées, appelée Joint Signal Activity (JSA)[192], il faut se demander si cette coopération a un réel intérêt pour l'État allemand. Selon plusieurs employés et membres du BND, cette coopération aurait été bénéfique et essentielle pour les intérêts allemands[193] : « Sans l'aide des services de renseignement, nous serions fichus »[194]. Cependant, l'énorme flux de données transmises aux États-Unis contenait essentiellement des données sur des citoyens et des entreprises allemands, ce qui laisse supposer que la BND n'a pas agi dans l'intérêt de l'État fédéral allemand mais plutôt dans celui de la NSA[195]. En effet, des entreprises comme Siemens ou EADS (*European Aeronautic Defense and Space company*, le consortium aéronautique et de défense européen) ont été visés et, ont sans doute bénéficié à

[186] Tibère, Clément. « Allemagne ». In *Dictionnaire du renseignement*, Hors collection. Paris : Éditions Perrin, 2018, p. 49.
[187] Lemaître, Frédéric. « Le scandale de la NSA continue de secouer l'Allemagne ». *Le Monde*. 24 juin 2015.
[188] « Rechtsgrundlagen der NSA-Kooperation erörtert ». Berlin : Bundestag, 2016.
[189] Follorou, Jacques. « La France espionnée avec ses propres moyens ». *Le Monde*. 30 mai 2015.
[190] « Zeuge: Daten gehen nicht ungefiltert ins Ausland ». Berlin: Bundestag, 2015.
[191] « Zeuge: Alle Daten liefen über Ramstein ». Berlin: Bundestag, 2015.
[192] Follorou, Jacques. « Les soupçons d'écoute de Fabius posent la question des dérives de l'espionnage allemand ». *Le Monde*. 13 novembre 2015.
[193] Biallas, Jörg. « Kooperation mit NSA "essentiell" ». Berlin : Bundestag, 29 avril 2016.
[194] Antoine, Lefébure. *L'affaire Snowden : comment les États-Unis espionnent le monde*. Paris : La Découverte, Paris, 2014, p. 68.
[195] « Rechtsgrundlagen der NSA-Kooperation erörtert ». Berlin : Bundestag, 2016.

d'autres entreprises concurrentes américaines[196]. Un des exemples de l'utilisation de ces données a été l'acte de cybersabotage orchestré par la NSA et l'unité 8200 de l'armée israélienne via le virus Stuxnet contre les installations nucléaires iraniennes qui utilisaient le système de contrôle de Siemens S7-300[197]. On peut donc en conclure que cet accord de coopération bilatéral (le JSA), s'il a peut-être été à un moment bénéfique pour les intérêts allemands et le BND, n'en reste pas moins un outil d'influence et d'intérêt stratégique au profit de la NSA et de la puissance américaine.

7.5. Le Japon

Avant de parler des liens de la NSA au pays du Soleil Levant, nous allons aborder la question de la présence militaire américaine au Japon. En effet, cette présence militaire américaine au Japon depuis la fin de la seconde guerre mondiale n'est un secret pour personne. A la base, cette présence avait pour but d'empêcher le Japon de constituer à nouveau une menace que ce soit pour l'Asie mais aussi pour le Pacifique et les États-Unis. C'est d'ailleurs dans ce contexte qu'en 1946, l'article 9 de la Constitution japonaise fût formulée.

« Chapitre II. Renonciation à la guerre

Article 9. Aspirant sincèrement à une paix internationale fondée sur la justice et l'ordre, le peuple japonais renonce à jamais à la guerre en tant que droit souverain de la nation, ou à la menace, ou à l'usage de la force comme moyen de règlement des conflits internationaux.

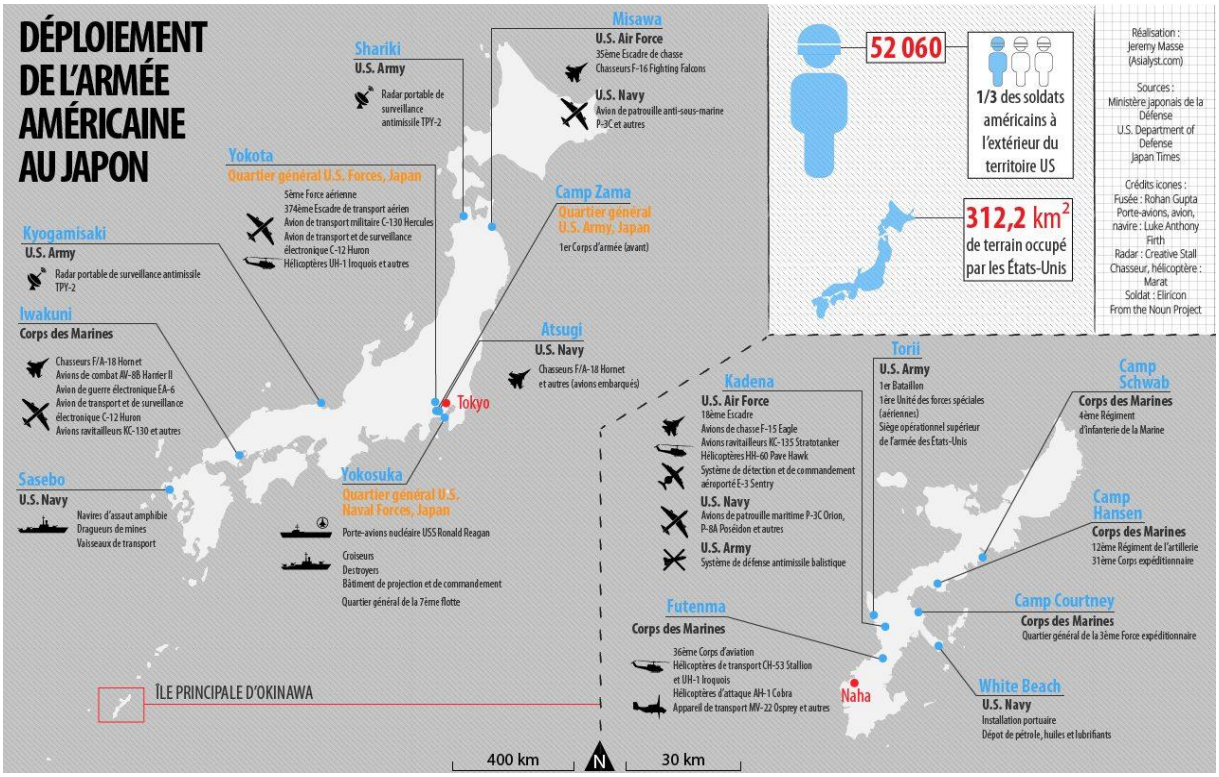
Pour atteindre le but fixé au paragraphe précédent, il ne sera jamais maintenu de forces terrestres, navales et aériennes, ou autre potentiel de guerre. Le droit de belligérance de l'État ne sera pas reconnu. »[198]

Aujourd'hui, avec la montée en puissance de la Chine et la menace que représente la Corée du Nord, le Japon, ne pouvant avoir de potentiel de guerre, a besoin

[196] Follorou, Jacques. « La France espionnée avec ses propres moyens ». *Le Monde*. 30 mai 2015.
[197] Antoine, Lefébure. *L'affaire Snowden : comment les États-Unis espionnent le monde*. Paris : La Découverte, Paris, 2014, p. 170.
[198] Constitution de l'État du Japon, § 2 (1946).

de cette présence américaine afin d'établir un équilibre des forces et ainsi, comme nous l'avons vu au début, de créer un environnement stable. La carte qui suit nous montre le déploiement impressionnant de l'armée américaine au Japon.

Figure 13 : Déploiement de l'armée américaine au Japon[199]



Source : Livre blanc de la défense du Japon de 2015.

Comme le montrent d'autres cartes en annexe (annexes 2 et 3) cette présence est associée à un plan de défense américain en cas de menace chinoise. C'est ici donc que le Japon prend toute son importance pour la NSA qui possède plusieurs stations d'écoute au Japon, dont notamment une installation dans les bases aériennes américaines de Misawa et de Yokota.

L'implication de la NSA au Japon a débuté de la même manière qu'avec l'Allemagne à savoir, l'implication de l'agence américaine dans la création d'un nouveau service de renseignement japonais, en l'occurrence ici le Chobestu. Depuis la fin de la guerre froide, son objectif est le même que celui de la NSA : *« veiller à la*

[199] Masse, Jeremy. « Le Japon, forteresse américaine en Asie-Pacifique ». *Asialyst*, 25 août 2016.

protection des réseaux de communication du gouvernement et de l'armée ainsi que fabriquer les codes et protocoles utilisés dans ces réseaux. »[200]

En 2007, la NSA a décidé de ne plus se cacher au Japon et de terminer les opérations de couverture. Ainsi, l'agence pouvait s'immiscer non seulement au sein de plusieurs bases militaires américaines mais également collaborer plus étroitement avec les services de renseignement japonais[201]. La proximité du Japon avec des puissances moyennes représentants potentiellement une menace, comme la Chine et la Russie, en fait un atout non négligeable pour les espionner. Les installations de la NSA au Japon ont également permis de mettre en œuvre la "Doctrine Alexander", « *Collect it all* ».

Ainsi, la base de Misawa collectait en 2009 plus de 8 000 signaux sur 16 satellites ciblés, la base de Yokota servait à la fabrication d'antennes de surveillance prêtes à être déployées à l'étranger et, la base d'Okinawa collectait des signaux de haute fréquence (mission STAKECLAIM) pilotée à partir du centre d'opération de la NSA à Hawaï[202]. Une partie du financement de ces infrastructures et de leur gestion était directement imputée au budget japonais.

La collaboration entre la NSA et les agences de renseignement japonaise est donc assez étroite, que ce soit pour intercepter les communications des pays voisins ou en matière de cybersécurité. Les agences américaine et japonaise se partagent ainsi des logiciels et des méthodes pour identifier les *malware*s utilisés par des pirates informatiques. De plus, en 2013, un document révélé par The Intercept dévoile que la NSA a fourni au Japon une installation de XKEYSCORE[203], le système de surveillance de masse utilisé par les *Five Eyes*.

[200] Brun, Olivier. « Japon ». In *Dictionnaire du renseignement*, Hors collection. Paris : Éditions Perrin, 2018, p. 494.
[201] Gallagher, Ryan. « JAPAN MADE SECRET DEALS WITH THE NSA THAT EXPANDED GLOBAL SURVEILLANCE ». *The Intercept*, 24 avril 2017.
[202] *Ibid.*
[203] *Ibid.*

7.6. Israël : Israeli SIGINT National Unit (ISNU)

Pour le moment, les cas étudiés révélaient que la NSA exerçait une influence sur certaines autres agences de renseignement dans le but de la collecte de données. L'analyse du lien particulier entre l'agence américaine et les services de renseignement israéliens, en particulier l'Israeli SIGINT National Unit (ISNU), plus connu sous le nom d'unité 8200[204], nous permettra de nuancer ce contrôle. En effet, dans ce cas il ne s'agit plus d'un transfert de métadonnées vers la NSA mais à l'inverse, d'un transfert de données brutes de l'agence américaine vers les analystes de l'ISNU[205]. Cet accord officieux, à nouveau révélé parmi les documents d'Edward Snowden, a été conclu en 2009[206] et concerne la protection des personnes américaines. Cependant, la coopération entre les deux services est cependant bien antérieure à cet accord.

En raison de sa situation stratégique, des pays qui lui sont limitrophes et des différences culturelles présentes dans la région, Israël a toujours investi massivement dans sa défense, militairement mais aussi au niveau du renseignement. Le Mossad est un des services de renseignement extérieur les plus performants au monde, malgré le fait qu'il ne bénéficie pas d'un budget aussi imposant que celui des Américains.

« Si « l'âme d'une nation se révèle dans ses services secrets » (John Le Carré), celle de l'État hébreu renvoie avant tout à une nation en guerre permanente pour laquelle le renseignement est une question de survie. »[207]

L'excellence israélienne dans le domaine du cyber espionnage est si importante que dans les années 1980 déjà, la NSA autorise officieusement à l'ISNU d'analyser des communications électroniques américaines à l'étranger[208]. L'accord officieux et juridiquement non contraignant de 2009 est donc une continuation de ce qui était déjà

---

[204] Ténèze, Nicolas. « Israël : la "supériorité numérique" du Moyen-Orient ». *Revue Défense Nationale* 784, nº 9 (2015), p. 60.
[205] Ferreira, Jacqueline L. (2014) "Testing the Democratic Credibility of an NSA (No Secrets Allowed) Government,"Sociological Imagination: Western's Undergraduate Sociology Student Journal: Vol. 3: Iss. 1, Article 10.
[206] Greenwald, Glenn, Laura Poitras, et Ewen MacAskill. « NSA shares raw intelligence including Americans' data with Israel ». *The Guardian*. 11 septembre 2013.
[207] Hubac, Olivier. « Israël ». In *Dictionnaire du renseignement*, Hors collection. Paris : Éditions Perrin, 2018, p. 483.
[208] Ténèze, Nicolas. « Israël : la "supériorité numérique" du Moyen-Orient ». *Revue Défense Nationale* 784, nº 9 (2015), p. 60-61.

réalisé dans les années 1980, mis à part qu'il constitue une barrière supplémentaire pour la protection des données personnelles des citoyens américains dont la durée de stockage par l'ISNU est désormais limitée à un an[209].

Cependant, si la NSA considère cette coopération comme mutuellement bénéfique[210], un rapport secret de septembre 2007 divulgué par le journal The Guardian indique que « la relation, bien que centrale dans la stratégie américaine, est devenue massivement unilatérale en faveur d'Israël. »[211] De plus, Israël n'est pas totalement considéré comme un pays allié et dénié de tout soupçon par les Américains puisque l'État hébreu est identifié comme cible potentielle pour les cyberattaques américaines au même titre que l'Iran et la Chine dans un rapport relatif à la demande de budget de la communauté du renseignement de 2013.[212] D'autres rapports, également dévoilés par The Guardian, montrent qu'un haut responsable de la NSA souligne qu'Israël, malgré l'apport bénéfique de leur relation, espionne agressivement les États-Unis et que la plus grande menace pourrait venir, non pas de services de renseignement étrangers quelconques, mais de services alliés comme Israël[213].

On peut dès lors se demander, mis à part l'excellence des services de renseignement israélien, quelles sont les raisons qui peuvent pousser la NSA à transmettre des données brutes, parfois sur ses propres citoyens, afin qu'elles soient analysées en Israël ? La question doit être analysée en profondeur, ce que nous ne ferons pas ici mais nous allons néanmoins émettre des suppositions sur base de certaines opérations que les deux services ont déjà mises au point ensemble.

Tout d'abord, l'efficience des services de renseignement israélien n'est plus à prouver et il est logique que, par l'histoire et les liens politiques et culturels qui allient les États-Unis et Israël, la NSA désire avoir le soutien de ces services plutôt que de devoir les contrer. En fournissant des données brutes à Israël, non seulement cette dernière apprécie ce geste, mais en plus elle est capable de fournir une analyse détaillée de ces données à la NSA. De plus, cet échange, même s'il est systématique, est

[209] Greenwald, Glenn, Laura Poitras, et Ewen MacAskill. « NSA shares raw intelligence including Americans' data with Israel ». *The Guardian*. 11 septembre 2013.
[210] « Ecoutes numériques : la NSA aurait transmis ses données à Israël ». *Le Monde*. 12 septembre 2013.
[211] Greenwald, Glenn, Laura Poitras, et Ewen MacAskill. « NSA shares raw intelligence including Americans' data with Israel ». *The Guardian*. 11 septembre 2013.
[212] *Ibid.*
[213] *Ibid.*

volontaire de la part de la NSA, ce qui veut dire qu'elle décide parfois ce qu'elle désire partager[214].

Ensuite, les États-Unis et Israël ont des ennemis communs comme l'Iran par exemple. Dans un contexte où certaines puissances cherchent à s'émanciper, comme l'Iran, et représentent une menace pour les États-Unis, la politique de transfert de données brutes participe à la mise en place d'une coopération permettant de donner les moyens à Israël d'attaquer l'Iran par des moyens informatiques notamment. L'exemple en 2010 du virus Stuxnet[215], créé par des ingénieurs de la NSA et implantés dans les centrifugeuses nucléaires iraniennes par l'ISNU, illustre bien les coopérations possibles afin de lutter contre des potentielles puissances émergentes. C'est ainsi qu'en 2015 par exemple, des intérimaires étrangers situés au Royaume-Uni, aux États-Unis, en Suisse, au Qatar et au Koweït ont été espionnés par l'ISNU car ils étaient chargés de négocier l'abandon du programme nucléaire iranien[216].

Ces deux raisons ne sont que des hypothèses et des suppositions, néanmoins vu les évènements et les actions faites conjointement par les deux services, il est logique de considérer ces éléments comme apportant une réponse partielle à la question de la relation NSA-ISNU et, de l'apport bénéfique que cela rapporte non seulement dans le transfert de données pour Israël mais également dans l'alliance pour la lutte régionale contre l'ennemi commun que représente l'Iran.

7.7. Que conclure des relations entre la NSA et les agences de renseignement de ces pays ?

Notre analyse a mis en évidence que la NSA partage des relations complexes avec divers services de renseignement, que ce soit via des accords (UKUSA, GCHQ, ISNU), ou via l'octroi d'installations de supercalculateurs ou de logiciels d'interception de données (DGSE, BND). Ces relations ont permis à la NSA de mettre en place un réseau permettant non seulement d'intercepter les communications sur presque tous les continents : Israël pour le Moyen-Orient, France pour l'Afrique,

[214] Greenwald, Glenn, Laura Poitras, et Ewen MacAskill. « NSA shares raw intelligence including Americans' data with Israel ». *The Guardian*. 11 septembre 2013.
[215] Antoine, Lefébure. *L'affaire Snowden : comment les États-Unis espionnent le monde*. Paris : La Découverte, Paris, 2014, p. 170.
[216] Ténèze, Nicolas. « Israël : la "supériorité numérique" du Moyen-Orient ». *Revue Défense Nationale* 784, nº 9 (2015), p. 60-61.

Allemagne pour l'Europe, Japon pour l'Asie de l'Est, le Canada pour le nord de l'Europe et les autres pays du traité UKUSA pour l'Océanie et l'Asie du Sud. Elles lui sont également utiles pour décrypter ces informations, grâce à l'expertise du GCHQ et de l'ISNU notamment. Ses immenses stockages de données, dont celui dans l'Utah par exemple, lui permettent enfin d'accéder à tout moment à ces informations. Ce réseau tentaculaire démontre la puissance que peut avoir la NSA en termes d'influence sur d'autres agences et gouvernements, qui ne sont parfois pas au courant des pratiques d'interception et de transfert de données ou de métadonnées. En effet, ce réseau est constitué le plus souvent d'accords bilatéraux totalement secrets ou partiellement cachés, ce qui en camoufle l'étendue aux yeux de tous. La NSA agit donc avec les différents services de renseignement étrangers comme s'ils faisaient entièrement partie de l'agence américaine et n'étaient qu'une extension de celle-ci, ce qui tend à confirmer la première hypothèse formulée au début de ce travail.

En fournissant divers programmes de collectes de données à certaines agences ou via divers accords de coopération de transfert de données et/ou de métadonnées, la NSA a pu accéder à toute information collectée par celles-ci, permettant au gouvernement américain de créer un lien de dépendance et d'influence vis-à-vis de ces États.

Cependant, une méfiance de la part de la NSA est toujours prise vis-à-vis de ces services, notamment de l'ISNU, car si ceux-ci sont aujourd'hui presque des alliés, certains peuvent potentiellement se retourner et représenter dans ce cas une menace.

Malgré le fait que cette dynamique d'influence a commencé il y a plusieurs dizaines d'années, on peut néanmoins faire un parallèle avec la politique de Barack Obama de *burden sharing*, c'est-à-dire : *« obtenir des autres États qu'ils fassent plus pour leur sécurité afin que les États-Unis puissent faire moins »*[217] mais également de *burden shifting*, qui consiste à transférer le fardeau de la sécurité collective plutôt que de le partager. Comme on l'a déjà dit, les États-Unis ont mis de côté le recours à la force pure de la politique Bush pour allier des éléments de *soft* et de *hard power* pour former du *smart power*. Cette dynamique implique une mise en retrait des États-Unis (*leading from behind*) et le partage du fardeau de sécurité (*burden sharing*). Les États-

[217] Struye de Swielande, Tanguy. « Asie-Pacifique : Grand Strategy de réaffirmation face à la Chine ». *Outre-Terre* 38, nº 1 (2014), p. 341.

Unis aspireraient même à transférer le fardeau de la sécurité collective et à réduire à l'avenir son implication (*burden shifting*). Cependant, tant en matière de *hard power* que de renseignement, les capacités des États à assurer leurs responsabilités sont limitées et souvent insuffisantes au vu de l'ampleur des problèmes sécuritaires dans certaines régions. Les États-Unis font face à la situation paradoxale dans laquelle « *le monde d'aujourd'hui rejette la domination américaine, mais est aussi réticent à partager le fardeau* »[218]. La stratégie appliquée par les Etats en matière de renseignement viserait donc une forme de partage de ce fardeau (*burden sharing*) mais tout en gardant un rôle de leader. Un autre argument appuyant cette analyse est l'entente de la coalition d'agences de renseignement appelé « SIGINT Seniors » qui rassemble deux divisions, une européenne (SIGINT Seniors Europe) et une du Pacifique (SIGINT Seniors Pacific), toutes deux dirigées par la National Security Agency[219]. Ensemble, cette coalition rassemble des représentants des SIGINT (pour rappel, renseignement par signaux) de 17 pays différents, dont au sein de la division européenne font partie les Five Eyes mais également la Belgique, le Danemark, la France, l'Allemagne, l'Italie, les Pays-Bas, la Norvège, l'Espagne et la Suède. Cette division "Europe" créée en 1982 possède son propre réseau de communication appelé SIGDASYS dans lequel chaque agence peut décider de partager des copies des interceptions de données qu'elle a réalisées. La division "Pacifique" quant à elle, n'a vu le jour qu'en 2005 et regroupe à nouveau les Five Eyes et la France mais aussi Singapour, la Corée du Sud, la Thaïlande et l'Inde[220]. Elle utilise un autre réseau de communication appelé CRUSHED ICE afin de partager ses renseignements[221].

Ainsi, on peut clairement voir que les États-Unis mènent une guerre de l'information et rassemblent leurs alliés, non seulement pour continuer à exercer une influence sur eux mais également, pour améliorer le renseignement contre ses adversaires, en particulier la Chine et la Russie, qui disposent d'autres infrastructures

[218] Hoop Scheffer, Alexandra de. « Chapitre 1. Obama et la guerre ». In *Le bilan d'Obama*, Académique. Paris : Presses de Sciences Po, 2012, p. 32.
[219] Gallagher, Ryan. « THE POWERFUL GLOBAL SPY ALLIANCE YOU NEVER KNEW EXISTED ». *The Intercept*, 1 mars 2018.
[220] Le Japon ne fait pas partie de cette coalition mais la NSA aimerait l'y ajouter. Cependant, les services de renseignement japonais ont refusé d'y intégrer pour le moment. Il faut dire que malgré la présence de l'armée américaine et de la NSA sur sont territoire, le Japon est parfois réticent à coopérer étroitement avec les États-Unis de peur de réactions de ses voisins.
[221] Gallagher, Ryan. « THE POWERFUL GLOBAL SPY ALLIANCE YOU NEVER KNEW EXISTED ». *The Intercept*, 1 mars 2018.

internet que celle des États-Unis. En effet, comme expliqué précédemment, l'infrastructure d'internet (câbles, satellites, serveurs, tours) est aujourd'hui contrôlée par les États-Unis, avec 90% du trafic mondial s'effectuant grâce à un ensemble de technologies développées, possédées et/ou mises en œuvre par les autorités et les grandes entreprises américaines (notamment les GAFA). Pour échapper à cette emprise, la Chine et la Russie ont développé des systèmes alternatifs tels que le Grand Firewall de Chine, les moteurs de recherche censurés d'État ou encore la constellation de satellites qui fournissent un positionnement géographique sélectif [222].

Ces systèmes alternatifs permettent d'éviter que la communication électromagnétique d'un pays ne soit entièrement dépendante d'un système issu d'un autre pays. A titre de comparaison, on peut imaginer le réseau internet comme une rivière. Si vous êtes en amont, vous pouvez contrôler le débit qui coule en aval. En revanche, si vous êtes situés en aval, vous ne pouvez bénéficier que de ce que ceux en amont vous laissent à votre disposition. Ainsi, si vos opposants sont situés en amont, ils peuvent décider de construire un barrage et ainsi couper le débit. C'est pour éviter ce scénario que la Chine et la Russie, situés en aval, essaient de créer des systèmes alternatifs. L'Iran de son côté, procède plutôt à une censure de certains sites internet et de certaines informations mais utilise tout de même les réseaux internet américains.

8. La NSA aujourd'hui

Depuis les révélations d'Edward Snowden en 2013, la NSA doit faire face à de nouvelles évolutions que nous examinons dans ce dernier chapitre, montrant certaines perspectives futures.

8.1. L'après Snowden

S'il y a bien une chose à retenir depuis l'affaire de la révélation des documents confidentiels par Edward Snowden, c'est la prise de conscience collective de la surveillance de masse opérée par la NSA et ses alliés. Nombreux sont ceux dans la société qui ont été choqués de ces révélations, en se sentant constamment observés

[222] Snowden, Edward, Etienne Menauteau, et Aurélien Blanchard. *Mémoires vives*. Seuil. Paris, 2019, p. 183.

dans leur quotidien. Aux États-Unis et ailleurs, des commissions d'enquête ont eu lieu et ont notamment abouti à un vote du Congrès américain sur *l'USA Freedom Act*, qui amende la section 215 du *Patriot Act* afin d'interdire explicitement la collecte de masse d'enregistrements téléphoniques de citoyens américains[223]. D'autres pays, comme l'Allemagne ont depuis coupé les transferts directs de données à la NSA.

Les entreprises liées de près ou de loin aux infrastructures d'internet ont également pris des mesures. Google et Apple ont ainsi opté pour un chiffrement pour leurs appareils Android et IOS. Mais c'est surtout Internet en lui-même qui est devenu plus sécurisé. En effet, l'ancienne plateforme qui hébergeait la plupart des sites internet au monde, *Hypertext Transfer Protocole* (le fameux "http" placé au-devant de chaque recherche internet) qui fût remplacé par "https", le "s" symbolisant le terme « *security* »[224].

Le Parlement européen quant à lui, a adopté en 2016 le Règlement Général sur la Protection des Données (RGPD) qui part du postulat qu'une donnée constitue aussi la propriété de la personne qu'elle représente. Ainsi, chaque donnée a droit aux mêmes protections civiles qu'une personne physique[225].

Cependant, comme le dit Edward Snowden dans sa récente biographie, adopter des règles à un niveau national ou transnational n'est pas suffisant car Internet est mondial. Aux États-Unis, même si des règles ont été mises en place pour interdire la collecte de données de masse sur des citoyens américains, la NSA peut toujours collecter celles de millions d'étrangers. Les agences qui coopéraient avec la NSA le faisaient en sachant déjà les enjeux et le choc que de telles coopérations susciteraient pour le grand public. Si dans certains États comme l'Allemagne il y a eu une limitation de la coopération, l'indignation provoquée par la révélation des documents d'Edward Snowden n'a pas empêché de nombreux autres Etats de poursuivre leur coopération avec la NSA.

[223] Snowden, Edward, Etienne Menauteau, et Aurélien Blanchard. *Mémoires vives*. Seuil. Paris, 2019, p. 366.
[224] *Ibid*, p. 366-367.
[225] *Ibid*, p. 367-368.

8.2. Le gouvernement Trump

Après avoir vu comment Barack Obama utilisait ses services de renseignement, il est intéressant d'aborder brièvement la relation entre ces derniers et le président actuellement au pouvoir, à savoir Donald Trump.

Dès la campagne de 2016 de Donald Trump, les suspicions d'ingérence russe créent une rupture entre le monde du renseignement et le président. En effet, suite aux enquêtes des services de renseignement sur Trump et son entourage, ce dernier a contesté toutes les analyses faites en s'appuyant sur deux éléments : la théorie de la politisation interne du renseignement (le monde du renseignement serait contre lui de par ses opinions) et l'incompétence des services de renseignement depuis l'invasion de l'Irak en 2003[226].

Pour la première fois de son histoire, les États-Unis ont un président qui préfère se baser sur ses propres analyses et intuitions plutôt que d'écouter les services compétents mis à sa disposition, notamment en matière de renseignement. En effet, d'une part, il ignore les résultats des analyses de ses services ; « *Gina Haspel, Directrice de la CIA, a publiquement exprimé les difficultés qu'elle rencontre à préparer les documents susceptibles de capter l'attention de son chef lors du President Daily Brief, c'est-à-dire le rapport quotidien de situation que reçoit le Président en début de journée* » (Olivier Chopin, et Benjamin Oudet, 2019), et d'autre part, Donald Trump n'hésite pas à s'opposer aux évaluations émergeant de sa propre structure de renseignement car il voit celle-ci comme une composante de son opposition politique[227].

Pour Donald Trump, quasiment toutes les crises actuelles comme en Syrie, en Corée du Nord, en Iran ou en Russie sont dues à l'incompétence de ses services de renseignement avec, comme principale justification, l'échec de la guerre en Irak de 2003, imputée injustement à ses services et non au gouvernement Bush junior.

Comme expliqué par Olivier Chopin et Benjamin Oudet, Trump exploite la thèse développée par Richard Betts à la fin des années 1970 qui consiste à dire que les échecs du renseignement sont inévitables et qu'on peut donc considérer le

[226] Olivier Chopin, et Oudet Benjamin. *Renseignement et sécurité*. Cursus (Armand Colin), Armand Colin, 2016, p. 195.
[227] *Ibid*, p. 196.

renseignement comme une simple information « parmi d'autres ». Ainsi, on observe une délégitimation du renseignement par rapport à d'autres informations. Trump ne prend donc en compte les informations et les conclusions issues du renseignement que lorsqu'elles rejoignent ses orientations politiques, tandis qu'il va plutôt les mettre de côté quand elles s'en écartent[228].

Avec Trump, on assiste à une personnalisation des relations diplomatiques : le Président fait d'avantage confiance à ses relations, sa bonne intuition et son expertise personnelle qu'à sa communauté du renseignement. Trump a sa réalité et n'arrive pas à la remettre en question. C'est pourquoi, tout ce qui est dit contre lui, ou contre ses opinions sont pour lui des « *fake news* ». Comme le souligne l'ancien directeur de la CIA Michael Hayden, depuis la première fois de leur histoire, les États-Unis ont un président pour qui la « *vérité ne compte pas* »[229].

L'imprévisibilité de Trump dans ses comportements ne rassure pas ses alliés, d'autant plus que tous ceux qui agissent contre les intérêts américains, y compris économiquement, ne sont plus considérés comme des alliés par Trump. Les nombreuses divergences d'opinion avec les pays occidentaux qui portent notamment, sur l'écologie, l'économie, le conflit syrien, ou plus récemment la gestion de la crise liée au coronavirus, conduisent les États-Unis à se replier sur eux-mêmes. Il est encore trop tôt en 2020 pour affirmer que le *soft power* américain est en train de décliner comme ce fût le cas lors de la guerre d'Irak, mais l'hypothèse est plausible. La relation que Trump entretient avec ses alliés traditionnels ne sera probablement pas sans conséquences pour les interactions entre services de renseignement, même si Trump ne peut à lui seul anéantir les relations et les accords déjà existants.

8.3. L'avenir du renseignement

Comme nous l'explique Olivier Chopin et Benjamin Oudet : « *L'environnement informationnel contemporain est parfois qualifié de quatrième révolution « industrielle », d'« âge de l'information ouverte », d'âge du «big data»*. » Avec le développement toujours croissant d'internet et d'open sources, le

[228] Olivier Chopin, et Oudet Benjamin. *Renseignement et sécurité*. Cursus (Armand Colin), Armand Colin, 2016, p. 196.
[229] *Ibid*, p. 196-197.

renseignement va évoluer de plus en plus vers le renseignement technique et la cryptologie. L'emploi d'informaticiens, d'ingénieurs réseaux va continuer de croître en délaissant plutôt la dimension humaine et social du renseignement. En l'absence de réel contrôle international sur certaines méthodes de collectes de renseignement, portant atteinte au droit du respect de la vie privée au profit de certaines directives sécuritaires, la prise de conscience collective qu'a suivi l'affaire Snowden ne modifiera pas la pratique du cyber-renseignement.

Cependant, comment recruter des analystes formés dans des domaines aussi techniques et en même temps, s'assurer qu'ils soient toujours aussi compétents dans le domaine des sciences humaines et sociales ? C'est la question posée par Olivier Chopin et Benjamin Oudet dans leur livre « *Renseignement et sécurité* ». Selon eux, le volume de données va tellement augmenter qu'il n'y aura plus d'autre choix que de faire appel à l'intelligence artificielle. Elle est déjà partiellement employée, que ce soit au sein de la NSA pour rechercher tout type de potentielle menace (le système Upstream Collection par exemple) mais également en Chine où des tests de reconnaissances faciales et de surveillance 24h/24 sont installés dans certaines villes afin d'encadrer la vie sociale de la population autour de certaines normes et de leur donner une notation sous forme de points[230]. On peut ici faire clairement un parallèle avec l'idée du Panopticon puisque le but est de "civiliser" au maximum la population, c'est-à-dire faire en sorte que la population ait l'impression d'être constamment surveillée afin que tout le monde respecte les règles, par peur de recevoir une sanction. Ce système de surveillance ainsi que son ampleur, s'il est généralisé aux villes principales que composent la Chine peuvent représenter les nouvelles composantes d'un nouveau régime politique que certains qualifient de « dictature post-moderne » (Rambures ,2018)[231].

[230] Leplâtre, Simon. « En Chine, des citoyens sous surveillance ». *Le Monde*. 15 juin 2018.
[231] Olivier Chopin, et Oudet Benjamin. *Renseignement et sécurité*. Cursus (Armand Colin), Armand Colin, 2016, p. 190-191.

9. Conclusion

Ainsi, comme le stipulait notre question de recherche[232], nous avons pu démontrer le lien entre le renseignement et son utilisation par certaines agences, en l'occurrence ici la NSA, comme facteur de puissance mais également comme instrument d'influence, ce qui correspond à la dimension de *soft power*. Non seulement, la NSA a su influencer des entreprises américaines et collecter leurs données mais en plus, elle a réussi à s'infiltrer, que ce soit par des accords secrets ou des procédures d'*hacking*, dans une grande partie des agences occidentales ou alliées des États-Unis. Cet outil de collecte et d'analyse de renseignements auquel correspond la NSA, représente l'usage de l'information comme instrument d'influence et de persuasion. Plus il y a d'informations collectées, plus il y a d'instruments d'influence.

Cela confirme donc bien deux de nos hypothèses, la première portant sur les liens entre la NSA et des entreprises privées liées au numérique[233], la deuxième portant sur le lien entre l'agence américaine et d'autres services de renseignement.[234] Cette influence est surtout portée sur des États alliés aux États-Unis depuis la fin de la seconde guerre mondiale. Une stratégie que l'on peut observer est de créer des liens avec tous ces États afin qu'ils évitent de basculer sous l'influence, voire la dominance, d'un autre État qui pourrait contester la puissance américaine (la Chine par exemple). En effet, cela fait depuis plusieurs années que le gouvernement américain et notamment le Pentagone (voir annexe 3), se méfient de cette fulgurante montée en puissance de la Chine qui pourrait faire basculer une partie de l'Asie-Pacifique dans sa sphère d'influence. Néanmoins, une analyse détaillée doit être réalisée postérieurement à ce travail afin d'identifier tous les enjeux géopolitiques derrière cette possible transition de puissance (voir chapitre 1).

---

[232] Dans quelles mesures les renseignements collectés par des collaborations établies dans le milieu du numérique et du renseignement par la National Security Agency représentent-ils des instruments de *« soft power »* au service du gouvernement des États-Unis afin d'influencer d'autres États ?

[233] Grâce aux liens entre certaines grandes entreprises américaines spécialisées dans les infrastructures liées à Internet et la NSA, le gouvernement américain a pu installer une dynamique d'influence envers certains États, aujourd'hui dépendants de ces infrastructures.

[234] En fournissant divers programmes de collectes de données à certaines agences ou via divers accords de coopération de transfert de données et/ou de métadonnées, la NSA a pu accéder à toute information collectée par celles-ci et le gouvernement américain a pu ainsi créer un lien de dépendance et d'influence vis-à-vis de ces États.

Notre troisième hypothèse, qui portait sur la création de virus ou *« malware »* et leur implantation dans certains systèmes au sein des États pour les freiner dans leur croissance[235], ne dispose pas de suffisamment d'éléments que pour être confirmée. En effet, même si la création du virus Stuxnet et son implantation dans les centrifugeuses à uranium de l'Iran[236] constitue un élément de réponse, ce seul exemple n'est pas suffisant. Néanmoins, cette cyberattaque marque pour certains le début de ce que l'on peut appeler une « cyberguerre ». Selon certains, cette guerre de l'information pourrait en effet devenir plus agressive en créant une cyberguerre, une guerre de l'ombre où les soldats seraient devenus des informaticiens et où les armes seraient des virus[237]. Cependant, à l'heure actuelle il est trop tôt que pour déclarer qu'il y a une cyberguerre ou qu'il y en aura une. En revanche, il est certain que la NSA ou d'autres agences voudront créer ou copier ce genre de virus pour lancer des cyberattaques afin d'en retirer des bénéfices. C'est déjà partiellement le cas puisque des virus utilisés par la NSA se sont ensuite retrouvés sur le « *Darknet* » et sont ensuite utilisés par des pirates de l'informatique, parfois étatiques ou même terroristes[238].

La révolution du cyber et du numérique a transformé les méthodes de collecte de l'information, la rendant accessible à tous. Cette accessibilité sans limite a poussé certaines agences à adopter des méthodes de collecte massive d'informations afin de conserver non seulement leur monopole mais également, dans le cas de la NSA, leur supériorité dans la compétition entre les différentes puissances mondiales. Plus que jamais, aujourd'hui l'information est devenue un facteur de puissance primordial pour la lutte entre les puissances. Cette information à but politique, économique ou militaire recherchée par tous se fait au prix de nombreux investissements, que ce soit dans l'amélioration des services déjà existants mais également dans des services autonomes, autrement appelés "IA", que les plus grandes puissances aimeraient mettre à profit au

[235] La NSA, en créant des virus ou des « *backdoors* » et en les implantant dans des systèmes au sein des États, parfois alliés des États-Unis, ceci leur a permis de leur donner un avantage stratégique, permettant ainsi aux États-Unis de freiner la montée en puissance de certains États de manière préventive.
[236] Antoine, Lefébure. *L'affaire Snowden : comment les États-Unis espionnent le monde*. Paris : La Découverte, Paris, 2014, p. 170.
[237] Pech, Yannick. « Vers une intelligence cyber ? Penser le renseignement augmenté dans la noosphère ». *Prospective et stratégie* Numéro 10, nº 1 (2019), p. 79.
[238] Antoine, Lefébure. *L'affaire Snowden : Comment Les États-Unis Espionnent Le Monde*. Paris : La Découverte. Cahiers Libres (La Découverte) 0526–8370. Paris, 2014, p. 173.

service de leurs agences de renseignement afin de non seulement automatiser la collecte de renseignement mais également son analyse.

La collecte massive de données ne va pas s'arrêter avec les divulgations d'Edward Snowden. En effet, avec les progrès technologiques et l'arrivée de la 5G, la plupart de nos appareils qui ne sont pas déjà connectés le seront à l'avenir, ce qui représentera encore plus de données à collecter. Or, on l'a dit, l'une des philosophies du renseignement technique est que tout ce qui peut être collecté doit l'être.

Nous avons surtout analysé le renseignement dans sa dimension de *soft power* mais il peut également être utilisé et étudié comme du *hard power*. Le renseignement, en fonction de l'information collectée, de son usage et des intérêts de l'État en question, dispose d'une flexibilité d'utilisation qui lui permet de faire agir les autres puissances dans l'intérêt de l'État, ce qui correspond à la définition même de ce qu'est la puissance. Un des usages, encore controversé mais très actuel, du renseignement comme facteur de puissance et d'influence, est son utilisation comme instrument de « *sharp power* »[239]. Cette dimension qui nécessite une future recherche, désigne la manipulation de l'information, notamment par l'usage de « *fake news* »[240]. Des services de renseignement étatiques comme en Russie ou en Chine en font aujourd'hui leur cheval de Troie afin de lutter contre le *soft power* américain, notamment par l'utilisation de théories complotistes mais toujours dans leur intérêt national. Démentir l'information en utilisation des propos populistes, en se basant sur de fausses données et l'utilisation des réseaux sociaux comme vecteur de l'information, soutient leur but de déstabiliser les régimes démocratiques en influençant une grande partie de la population, qui malheureusement, ne prend pas suffisamment le temps de vérifier ces informations. Néanmoins, ces explications ne suffisent sûrement pas et une analyse complète doit être faite dans un futur proche.

[239] Marin, Anaïs. « La dissuasion par la coopération. La Finlande, modèle de résilience face aux défis du "sharp power" russe ». *Stratégique* 121-122, nº 1-2 (2019), p. 339.
[240] Daubeauf, Benjamin. « Du "soft power" au "sharp power" : le pouvoir d'influence de la Chine ». *Courrier international*. 4 décembre 2019.

10. Bibliographie

10.1. Articles de revues scientifiques

- Angibault, Jean-Luc. « Du renseignement à l'intelligence stratégique ». *Hermès, La Revue* 76, n° 3 (2016): 93-97.
- Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, et Rob B. J. Walker. « Repenser l'impact de la surveillance après l'affaire Snowden : sécurité nationale, droits de l'homme, démocratie, subjectivité et obéissance ». *Cultures & Conflits* 98, n° 2 (2015): 133-66.
- Bausardo, Thomas. « Quel passé pour Prism et Snowden ? » *Vacarme* 66, n° 1 (2014): 142-57. https://doi.org/10.3917/vaca.066.0142.
- Beckouche, Pierre. « La révolution numérique est-elle un tournant anthropologique ? » *Le Débat* 193, n° 1 (2017): 153-66. https://doi.org/10.3917/deba.193.0153.
- Bloch, Emmanuel, et Romain Zerbib. « Le rôle du renseignement dans une stratégie globale d'influence ». *Hermès, La Revue* 76, n° 3 (2016): 131-36.
- Brun, Olivier. « Cycle du renseignement ». In *Dictionnaire du renseignement*, 236-40. Hors collection. Paris: Éditions Perrin, 2018. https://www.cairn.info/dictionnaire-du-renseignement--9782262070564-p-236.htm.
- Brun, Olivier. « Japon ». In *Dictionnaire du renseignement*, 492-95. Hors collection. Paris: Éditions Perrin, 2018. https://www.cairn.info/dictionnaire-du-renseignement--9782262070564-p-492.htm.
- Chamayou, Grégoire. « Dans la tête de la NSA. Une histoire philosophique du renseignement américain ». *Revue du Crieur* 1, n° 1 (2015): 20-39. https://doi.org/10.3917/crieu.001.0020.
- Chouet, Alain. « La coopération antiterroriste transatlantique : succès techniques et interrogations politiques ». *Sécurité globale* 4, n° 2 (2008): 21-29. https://doi.org/10.3917/secug.004.0021.
- Cogan, Charles. « Le renseignement et la démocratie. L'affaire Snowden ». Traduit par Isabelle Hausser. *Commentaire* Numéro 149, n° 1 (2015): 33-38. https://doi.org/10.3917/comm.149.0033.
- Daninos, Franck. « La réforme perpétuelle du renseignement américain ». *Sécurité globale* 4, n° 2 (2008): 51-61. https://doi.org/10.3917/secug.004.0051.

- Hoop Scheffer, Alexandra de. « Chapitre 1. Obama et la guerre ». In *Le bilan d'Obama*, 27-61. Académique. Paris: Presses de Sciences Po, 2012. https://www.cairn.info/le-bilan-d-obama--9782724611915-p-27.htm.
- Delcorde, Raoul. « La diplomatie d'influence ». *Revue Défense Nationale* 823, nº 8 (2019): 57-63.
- Denécé, Éric. « La révolution du renseignement ». *Sécurité globale* 4, nº 2 (2008): 37-49. https://doi.org/10.3917/secug.004.0037.
- Douzet, Frédérick. « États-Unis : les fragilités d'une superpuissance ». *Revue internationale et stratégique* 42, nº 2 (2001): 27-28. https://doi.org/10.3917/ris.042.0027.
- Frédérick Douzet, « Géopolitique du cyberespace : La cyberstratégie de l'administration Obama », *Bulletin de l'association de géographes français*, 91-2 | 2014, 138-149.
- Douzet, Frédérick. « L'art de la guerre revisité. Cyberstratégie et cybermenace chinoises ». *Hérodote* 152-153, nº 1-2 (2014): 161-73. https://doi.org/10.3917/her.152.0161.
- Harbulot, Christian. « Le monde du renseignement face à la guerre de l'information ». *Hermès, La Revue* 76, nº 3 (2016): 80-85.
- Hubac, Olivier. « Israël ». In *Dictionnaire du renseignement*, 483-86. Hors collection. Paris: Éditions Perrin, 2018. https://www.cairn.info/dictionnaire-du-renseignement--9782262070564-p-483.htm.
- Hulnick, Arthur S. « What's wrong with the Intelligence Cycle ». *Intelligence and National Security* 21, nº 6 (1 décembre 2006): 959-79. https://doi.org/10.1080/02684520601046291.
- Huntington, Samuel P. « The Clash of Civilizations? » *Foreign Affairs* 72, nº 3 (1993): 22-49. https://doi.org/10.2307/20045621.
- Huntington, Samuel P. « The Lonely Superpower ». *Foreign Affairs* 78, nº 2 (1999): 35-49. https://doi.org/10.2307/20049207.
- Laïdi, Ali. « Le renseignement économique américain de Reagan à Trump. Un engagement de plus en plus ferme ». *Prospective et stratégie* Numéro 10, nº 1 (2019): 103-13. https://doi.org/10.3917/pstrat.010.0103.
- Lepri, Charlotte. « Les services de renseignement en quête d'identité : quel rôle dans un monde globalisé ? » *Géoéconomie* 45, nº 2 (2008): 33-53. https://doi.org/10.3917/geoec.045.0033.

- Leriche, Frédéric. « Chapitre 16. La politique étrangère de Washington : de l'unilatéralisme de G. W. Bush au minilatéralisme de B. Obama ». In *Les États-Unis*, 245-58. U. Paris: Armand Colin, 2016. https://www.cairn.info/les-États-unis--9782200288471-p-245.htm.
- Leriche, Frédéric. « Chapitre 18. Le basculement du monde ? Les États-Unis et leur place dans le système mondial ». In *Les États-Unis*, 273-87. U. Paris: Armand Colin, 2016. https://www.cairn.info/les-États-unis--9782200288471-p-273.htm.
- Marin, Anaïs. « La dissuasion par la coopération. La Finlande, modèle de résilience face aux défis du "sharp power" russe ». *Stratégique* 121-122, nº 1-2 (2019): 329-46. https://doi.org/10.3917/strat.121.0329.
- Mattelart, Armand. « VI. Les enjeux géopolitiques de l'architecture réticulaire », 84-108. Repères. Paris: La Découverte, 2009. https://www.cairn.info/histoire-de-la-societe-de-l-information--9782707157980-p-84.htm.
- Nye, Joseph. « La puissance américaine et la lutte contre le terrorisme ». *Politique américaine* 2, nº 2 (2005): 11-20. https://doi.org/10.3917/polam.002.0011.
- Nye, Joseph S. « L'équilibre des puissances au XXIe siècle ». *Géoéconomie* 65, nº 2 (2013): 19-29. https://doi.org/10.3917/geoec.065.0019.
- Nye, Joseph S. « Soft Power ». *Foreign Policy*, nº 80 (1990): 153-71. https://doi.org/10.2307/1148580.
- Pannier, Alice. « Le "minilatéralisme" : une nouvelle forme de coopération de défense ». *Politique étrangère* Printemps, nº 1 (2015): 37-48. https://doi.org/10.3917/pe.151.0037.
- Pech, Yannick. « Vers une intelligence cyber ?Penser le renseignement augmenté dans la noosphère ». *Prospective et stratégie* Numéro 10, nº 1 (2019): 73-102. https://doi.org/10.3917/pstrat.010.0073.
- Quessard, Maud. « Rebranding Soft Power: Assessing Obama's Smart Power Strategies ». *Études anglaises* 72, nº 4 (2019): 469-85. https://doi.org/10.3917/etan.724.0469.
- Racouchot, Bruno. « Penser l'influence dans les rapports de force de la guerre économique : de la compétition aux manœuvres criminelles ». *Sécurité globale* 9, nº 1 (2017): 105-13. https://doi.org/10.3917/secug.171.0105.
- Ramos, Raphaël. « La CIA et les dividendes de la paix : l'ouverture du renseignement américain au lendemain de la guerre froide ». *Hermès, La Revue* 76, nº 3 (2016): 31-36.

- Raufer, Xavier. « Escrocs, espions, mégalos : bienvenue chez les GAFA ». *Sécurité globale* 19, nº 3 (2019): 75-88. https://doi.org/10.3917/secug.193.0075.
- Shapiro, Steven R. « Surveillance de la NSA : pourquoi le système des freins et contre-poids a été court-circuité ». Traduit par Alix Meyer. *Politique américaine* 24, nº 2 (2014): 11-27. https://doi.org/10.3917/polam.024.0011.
- Struye de Swielande, Tanguy. « Asie-Pacifique : Grand Strategy de réaffirmation face à la Chine ». *Outre-Terre* 38, nº 1 (2014): 330-41. https://doi.org/10.3917/oute1.038.0330.
- Ténèze, Nicolas. « Israël : la "supériorité numérique" du Moyen-Orient ». *Revue Défense Nationale* 784, nº 9 (2015): 58-62.
- Ténèze, Nicolas. « La politique étrangère d'Obama : réinitialiser le leadership américain par le Smart Power ». *Revue Défense Nationale* 793, nº 8 (2016): 56-62.
- Tessier, Manon, et Michel Fortmann. « Les États-Unis : mutation d'une superpuissance dans l'après-guerre froide ». *Revue internationale et stratégique* 41, nº 1 (2001): 163-70. https://doi.org/10.3917/ris.041.0163.
- Tibère, Clément. « Allemagne ». In *Dictionnaire du renseignement*, 43-50. Hors collection. Paris: Éditions Perrin, 2018. https://www.cairn.info/dictionnaire-du-renseignement--9782262070564-p-43.htm.
- Van Outrive, Lode. « Les services de renseignement et de sécurité ». *Courrier hebdomadaire du CRISP* 1660-1661, nº 35-36 (1999): 1-88. https://doi.org/10.3917/cris.1660.0001.

10.2. Monographies

- Antoine, Lefébure. *L'affaire Snowden : Comment Les États-Unis Espionnent Le Monde*. Paris : La Découverte. Cahiers Libres (La Découverte) 0526–8370. Paris, 2014.
- Jean-Claude, Cousseran, and Hayez Philippe. *Leçons Sur Le Renseignement*. Odile Jacob. Paris: Odile Jacob, 2017.
- Liégeois, Michel. *Stratégie et sécurité internationale*. Louvain-la-Neuve: Université Catholique de Louvain, 2018.
- Lowenthal, Mark. *Intelligence : From Secrets to Policy*. 5ème. Washington: CQ Press, 2011.

- Nau, Henry R. *Perspectives on international relations : power, institutions, and ideas*. 4th éd. Los Angeles: Sage, 2015.
- Olivier, Chopin, and Oudet Benjamin. *Renseignement et Sécurité*. Cursus (Armand Colin) 0991–4498. Malakoff : Armand Colin, 2016.
- Snowden, Edward, Etienne Menauteau, et Aurélien Blanchard. *Mémoires vives*. Seuil. Paris, 2019.
- Tzu, Sun. *L'art de la guerre*. Paris: Flammarion, 1972.
- Clausewitz, Carl von. *De la guerre*. Tempus 127. Paris: Perrin, 2011.
- Whitaker, Reginald. *The end of privacy*. The new press. New York, 1999.

10.3. Thèse

- Lelièvre, Arnaud. 'La Communication Web Des Services de Renseignement : Étude Sémio-Pragmatique'. UCL, 2018.
- Noirhomme, Sébastien. « L'échange et l'utilisation des informations récoltées par les services de renseignement belges ». Université catholique de Louvain, 2018.

10.4. Références cinématographiques

- Bigelow, Kathryn. *Zero Dark Thirty*. Film d'espionnage. Sony Pictures Releasing, 2012.
- Stone, Oliver. *Snowden*. Thriller. Open Road Films (États-Unis), Pathé Distribution (France), 2016.

10.5. Articles de journaux

- Bernard, Philippe. « Voyage au cœur de la NSA ». *Le Monde*. 28 août 2013. Consulté le 20 Mai 2020.
- Boffey, Daniel. « British spies "hacked into Belgian telecoms firm on ministers" orders' ». *The Guardian*. 21 septembre 2018. Consulté le 20 Mai 2020.
- Carroll, Rory. « Welcome to Utah, the NSA's desert home for eavesdropping on America ». *The Guardian*. 14 juin 2013. Consulté le 20 Mai 2020.
- Champeau, Guillaume. « Lustre : la France aurait coopéré avec la NSA ». *Numerama*. 28 octobre 2013. Consulté le 12 Mai 2020.
- Daubeauf, Benjamin. « Du "soft power" au "sharp power" : le pouvoir d'influence de la Chine ». *Courrier international*. 4 décembre 2019. Consulté le 20 Mai 2020.

- « Ecoutes numériques : la NSA aurait transmis ses données à Israël ». *Le Monde*. 12 septembre 2013.
- Follorou, Jacques. « Surveillance : la DGSE a transmis des données à la NSA américaine ». *Le Monde*. 30 octobre 2013. Consulté le 12 Mai 2020.
- Follorou, Jacques. « La France, précieux partenaire de l'espionnage de la NSA ». *Le Monde*. 29 novembre 2013. Consulté le 12 Mai 2020.
- Follorou, Jacques. « La France espionnée avec ses propres moyens ». *Le Monde*. 30 mai 2015. Consulté le 13 Mai 2020.
- Follorou, Jacques. « Deutsche Telekom a espionné la France pour le compte de la NSA ». *Le Monde*. 5 juin 2015. Consulté le 13 Mai 2020.
- Follorou, Jacques. « Espionnage de la NSA : au-delà de l'indignation, la coopération continue ». *Le Monde*. 24 juin 2015. Consulté le 12 Mai 2020.
- Follorou, Jacques. « Les soupçons d'écoute de Fabius posent la question des dérives de l'espionnage allemand ». *Le Monde*. 13 novembre 2015. Consulté le 13 Mai 2020.
- Follorou, Jacques. « Pris dans leurs rivalités, les services français ont privilégié leurs liens avec la NSA et le GCHQ ». *Le Monde*. 10 décembre 2016. Consulté le 12 Mai 2020.
- Gallagher, Ryan. « JAPAN MADE SECRET DEALS WITH THE NSA THAT EXPANDED GLOBAL SURVEILLANCE ». *The Intercept*, 24 avril 2017. Consulté le 15 Mai 2020.
- Gallagher, Ryan. « THE POWERFUL GLOBAL SPY ALLIANCE YOU NEVER KNEW EXISTED ». *The Intercept*, 1 mars 2018. Consulté le 16 Mai 2020.
- Greenwald, Glenn, et Ewen MacAskill. « NSA Prism program taps in to user data of Apple, Google and others ». *The Guardian*. 7 juin 2013. Consulté le 20 Mai 2020.
- Greenwald, Glenn, Laura Poitras, et Ewen MacAskill. « NSA shares raw intelligence including Americans' data with Israel ». *The Guardian*. 11 septembre 2013. Consulté le 15 Mai 2020.
- Lemaître, Frédéric. « Le scandale de la NSA continue de secouer l'Allemagne ». *Le Monde*. 24 juin 2015. Consulté le 13 Mai 2020.
- Leplâtre, Simon. « En Chine, des citoyens sous surveillance ». *Le Monde*. 15 juin 2018. Consulté le 16 Mai 2020.
- MacAskill, Ewen. « NSA paid millions to cover Prism compliance costs for tech companies ». *The Guardian*. 23 août 2013. Consulté le 19 Mai 2020.

- MacAskill, Ewen, et Gabriel Dance. « NSA files : decoded ». *The Guardian*. 1 novembre 2013. Consulté le 20 Mai 2020.
- Marin, Cécile. « La présence militaire américaine au Japon ». *Le Monde diplomatique*. septembre 2015. Consulté le 15 Mai 2020.
- Masse, Jeremy. « Le Japon, forteresse américaine en Asie-Pacifique ». *Asialyst*, 25 août 2016. Consulté le 15 Mai 2020.
- Piel, Simon, et Joan Tilouine. « La France et ses intérêts en Afrique sous surveillance ». *Le Monde*. 8 décembre 2016. Consulté le 12 Mai 2020.
- « Pourquoi la NSA et le GCHQ ont volé des clés de chiffrement de cartes SIM ». *Le Monde*. 23 février 2015. Consulté le 12 Mai 2020.
- Traynor, Ian. « GCHQ: EU surveillance hearing is told of huge cyber-attack on Belgian firm ». *The Guardian*. 3 octobre 2013. Consulté le 20 Mai 2020.
- Walker, Christopher, et Jessica Ludwig. « The Meaning of Sharp Power : How Authoritarian States Project Influence ». *Foreign Affairs*, 16 novembre 2017. Consulté le 31 Mai 2020.

10.6. Textes juridiques

- Bush, Georges. US Patriot Act, 107-56 § 215 (2001).
- Constitution de l'État du Japon, § 2 (1946).

10.7. Interview

- Mas, Olivier. Renseignement humain vs renseignement technique, 12 décembre 2019.

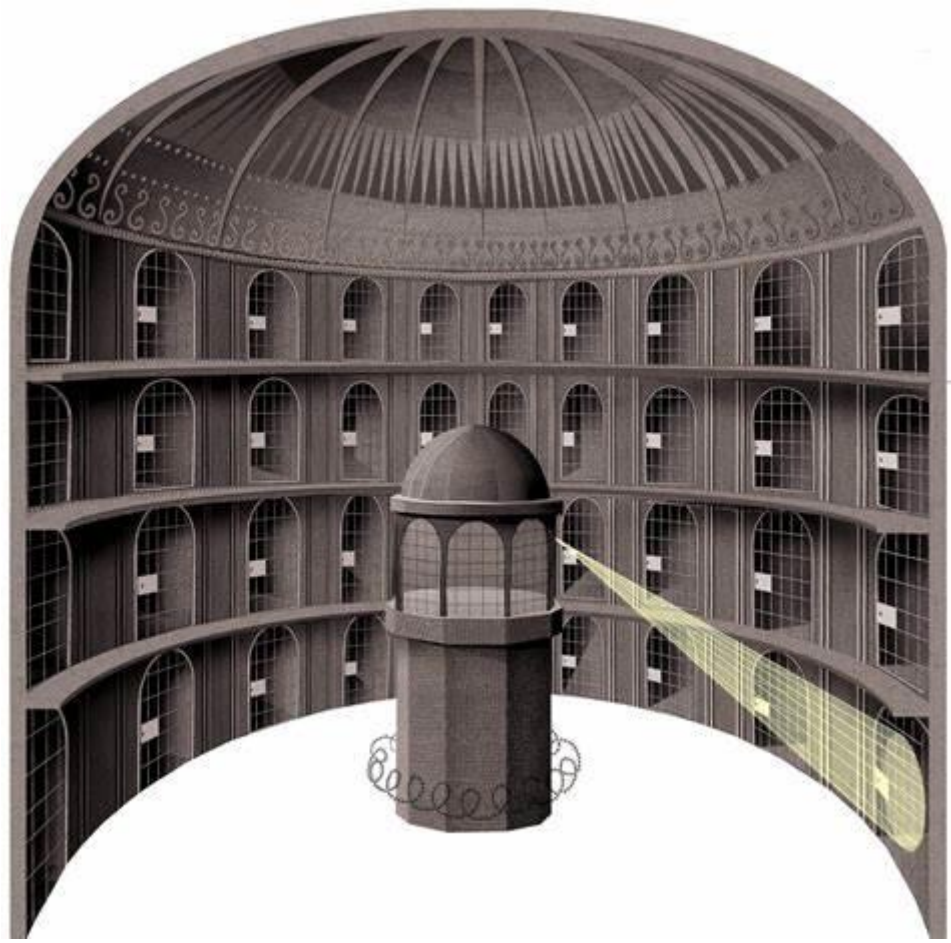
10.8. Rapports

- Assemblée de l'Union de l'Europe occidentale. « Une politique européenne de renseignement ». Paris: Assemblée de l'union de l'Europe occidentale, 1996.
- « Biallas, Jörg. « Kooperation mit NSA "essentiell" ». Berlin: Bundestag, 29 avril 2016.
- Conseil de l'Europe. « Partie 1. Les opérations de surveillance massive ». In *Surveillance de masse*, 5-62. Hors collection. Strasbourg: Conseil de l'Europe, 2016. https://www.cairn.info/surveillance-de-masse--9789287181039-p-5.htm.

- Conseil de l'Europe. « Partie 2. Le contrôle démocratique des agences de collecte de renseignements d'origine électromagnétique ». In *Surveillance de masse*, 63-109. Hors collection. Strasbourg: Conseil de l'Europe, 2016. https://www.cairn.info/surveillance-de-masse--9789287181039-p-63.htm.
- « Hitzige Debatte über die BND-NSA-Kooperation ». Berlin: Bundestag, 2015.
- Rechtsgrundlagen der NSA-Kooperation erörtert ». Berlin: Bundestag, 2016.
- *Surveillance de masse : quel contrôle démocratique ?* Conseil de l'Europe. Strasbourg, 2016.
- *Un service du renseignement de sécurité dans une société démocratique. A security intelligence service in a democratic society*. Ottawa: Ministère des approvisionnements et services Canada, s. d.
- « Zeuge: Alle Daten liefen über Ramstein ». Berlin: Bundestag, 2015.
- « Zeuge: Daten gehen nicht ungefiltert ins Ausland ». Berlin: Bundestag, 2015.

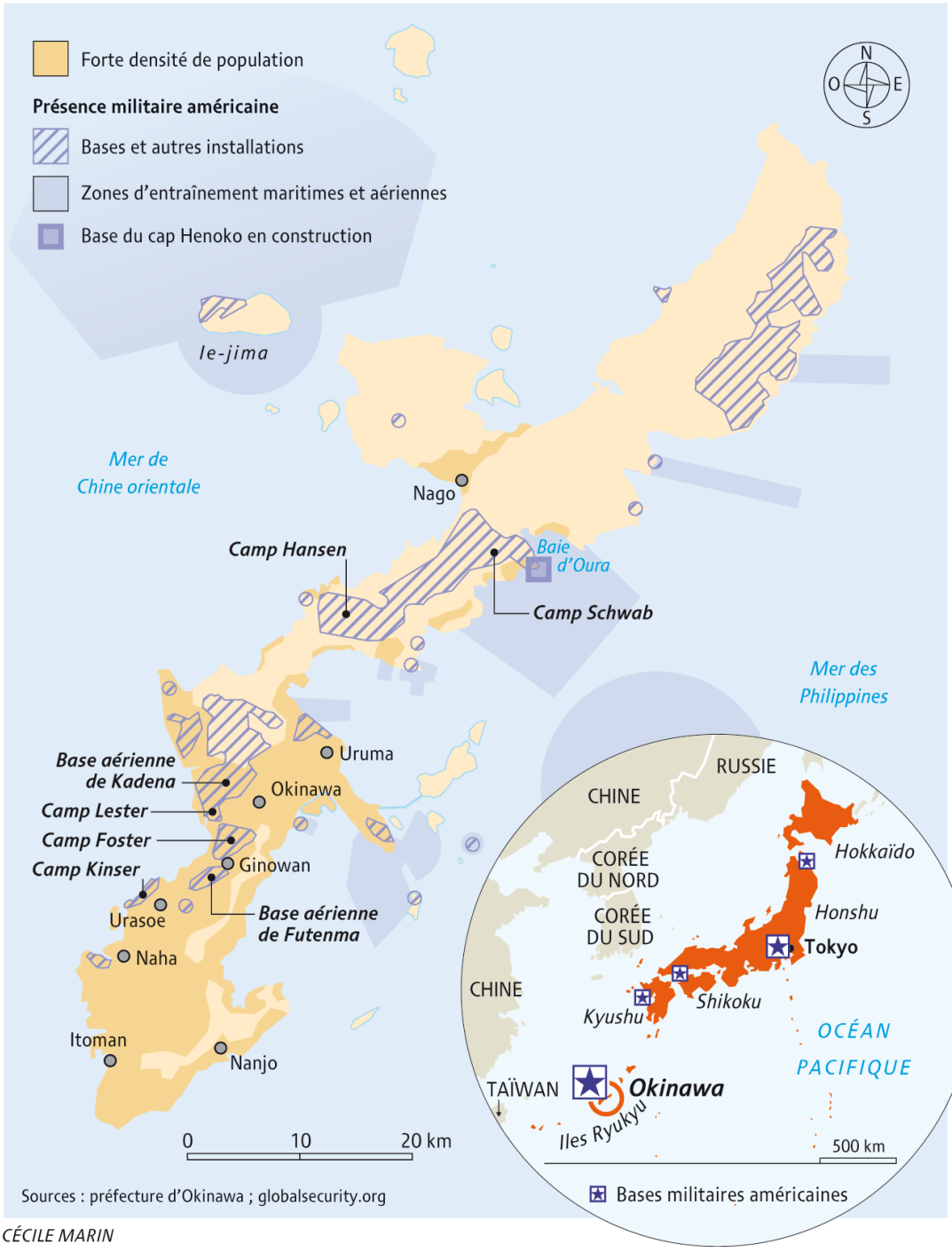
11. Annexes

11.1. Annexe 1



Source : www.partage-le.com

11.2. Annexe 2



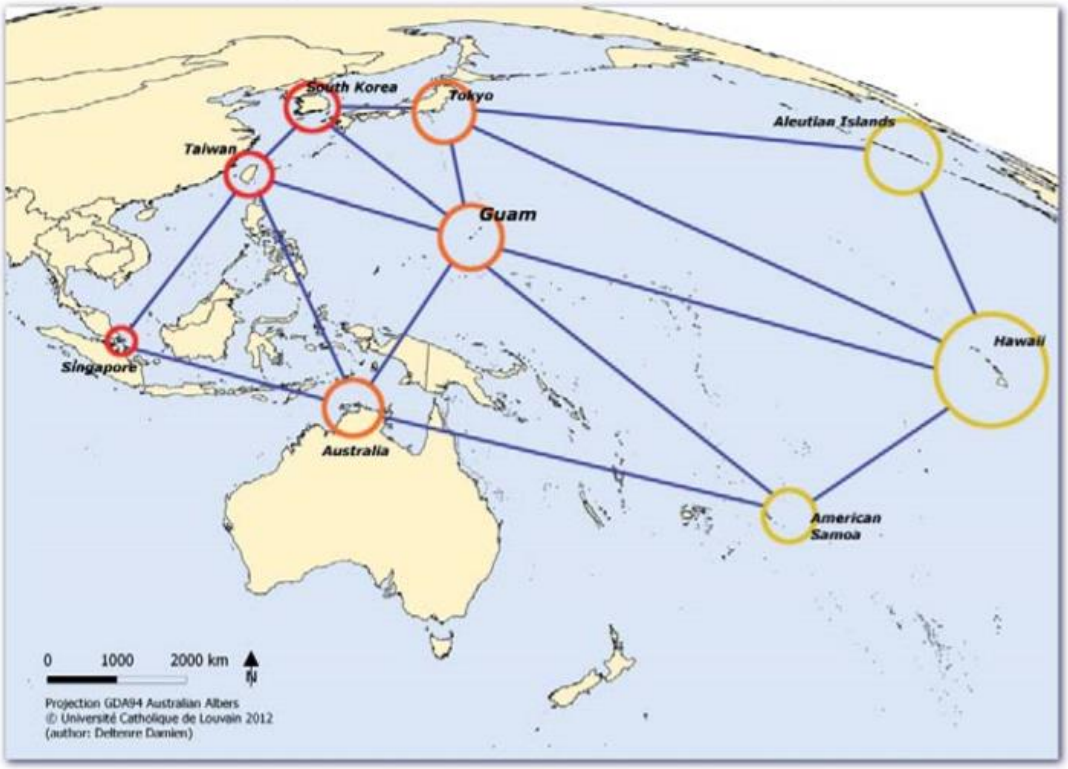
CÉCILE MARIN

241

[241] Marin, Cécile. « La présence militaire américaine au Japon ». *Le Monde diplomatique*. septembre 2015.

11.3. Annexe 3

La triple défense du Pentagone dans le Pacifique



Source : Damien Deltenre, Université catholique de Louvain, 2012 (DR)

242

[242] Struye de Swielande, Tanguy. « Asie-Pacifique : Grand Strategy de réaffirmation face à la Chine ». *Outre-Terre* 38, nº 1 (2014), p. 339.