Faculté des sciences économiques,
sociales, politiques et de communication
École des sciences politiques et sociales (PSAD)

# La cyberstratégie des Etats-Unis face aux menaces émergentes

## Analyse sous l'angle néoréaliste

Auteur : Alice AIKHENBAUM
Promoteur : Tanguy STRUYE DE SWIELANDE
Lecteur : Kimberly ORINX
Année académique : 2024-2025
Master en Sciences politiques, orientation relations internationales, à finalité diplomatie et résolution des conflits

## DECLARATION SUR L'HONNEUR – PLAGIAT

Je déclare sur l'honneur que ce travail 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.

Fait le 2 février 2025

Par Alice AIKHENBAUM

Signature

Remerciements

Je tiens à remercier toutes les personnes qui m'ont apporté leur aide lors de la rédaction de ce mémoire.

Je voudrais dans un premier temps remercier mon promoteur de mémoire, Monsieur Tanguy Struye de Swielande, pour avoir accepté d'encadrer ce mémoire et pour ses conseils.

Merci à Mathias, mon compagnon, pour les sessions d'encouragements qui m'ont permis d'arriver au bout de ce travail.

Mes sincères remerciements à mes parents, Denise et Olivier, et à mon frère Raphaël, pour leur implication intense dans la relecture et leur sens du détail.

A tous ces intervenants, je présente mes remerciements, mon respect et ma gratitude.

# Table des matières

# Introduction

« Plus de 195.4 millions de données compromises en 2024 », c'est le titre inquiétant de l'article du journal Le Monde Informatique, publié le 14 janvier 2025[1]. Cet article affiche les résultats d'une étude de l'entreprise Comparitech sur les cyberattaques par *ransomware* contre des entreprises du monde entier, avec 5 461 attaques revendiquées comme étant réussies par différents cyber gangs, et dont 1 204 ont débouché sur près de 195.4 millions de données compromises. Ces attaques, malgré leur nombre important, ne sont pourtant que la partie visible de l'iceberg. En effet, les cyberattaques possèdent un vaste arsenal permettant de menacer la sécurité de personnes du monde entier (vol de données, détournement de fond, harcèlement, chantage…) : programmes malveillants (*malware*), rançongiciel (*ransomware*), hameçonnage par e-mail ou SMS (respectivement *phishing* et *smishing*), attaques *Business E-mail Compromise* (BEC), *botnet*….

Parmi les plus touchés par ce type d'attaques, les Etats-Unis figurent en tête du classement : d'après une étude de 2022 de Statista[2], qui recense les cyberattaques visant les gouvernements et les entreprises de technologie et de défense sur la période allant de 2006 à 2020, ils auraient été la cible de 156 attaques (soit onze par an), suivi de loin par la Grande-Bretagne (47 attaques) ou encore l'Inde (23 attaques). Si les Etats-Unis apparaissent comme l'une des cibles privilégiées des cyberattaques, ce n'est pas seulement en raison de leur développement technologique avancé, mais aussi compte-tenu de leur position dominante en tant que superpuissance dans le système international. Du fait de l'anarchie des relations internationales présumée par les différents courants de la théorie réaliste, où aucun pouvoir central ne peut garantir la sécurité des Etats, ceux-ci doivent maximiser leur puissance et se protéger par leurs propres moyens. Dans ce cadre, la cyberstratégie ne peut plus être analysée uniquement sous l'angle technique ou juridique. En effet, elle s'inscrit dans une logique de compétition entre grandes puissances et devient un outil de projection de puissance et de dissuasion. Cette lecture s'inscrit donc pleinement dans la théorie du néoréalisme, développée par Kenneth Waltz, qui postule que la survie des États dans un environnement anarchique dépend de leur capacité à assurer leur sécurité par une politique de puissance.

[1] FILIPPONE Dominique, « Plus de 195 millions de données compromises en 2024 », Le Monde Informatique, 2025.
[2] GAUDIAUT Tristan, « Les pays les plus touchés par des cyberattaques massives », Statista, 2022.

Ce mémoire cherche alors à répondre à la question suivante : « Dans quelle mesure la cyberstratégie des Etats-Unis depuis les années 2000, façonnée par des cyberattaques majeures, s'inscrit-elle dans une logique néoréaliste de puissance et de sécurité ? ».
Dans ce cadre, plusieurs hypothèses seront examinées :

- Hypothèse 1 : « Les cyberattaques majeures ont conduit les Etats-Unis à adopter des innovations technologiques dans leur cyberstratégie, notamment des technologies de défense, de détection et de contre-attaque ».
- Hypothèse 2 : « En réponse aux cyberattaques de plus en plus fréquentes, les Etats-Unis ont progressivement développé une approche proactive et offensive dans le cyberespace, afin de projeter leur puissance et dissuader leurs adversaires ».
- Hypothèse 3 : « L'approche des Etats-Unis dans le domaine de la cybersécurité inclut des stratégies de renseignement avancées, comme la surveillance, les cyber-opérations clandestines, ou encore l'analyse prédictive afin d'anticiper et de neutraliser les menaces ».
- Hypothèse 4 : « La cyberstratégie des Etats-Unis reflète une militarisation croissante du cyberespace en réponse à des menaces perçues ».

Afin d'analyser ces hypothèses, ce mémoire tentera d'adopter une approche qualitative reposant sur l'étude de sources académiques, de documents stratégiques américains, ainsi que de cas emblématiques de cyberattaques ayant façonné la doctrine cybernétique des Etats-Unis. Nous mobiliserons ainsi des rapports gouvernementaux, des analyses de think tanks spécialisés, ainsi que des travaux de chercheurs en relations internationales et en stratégie militaire.

La première partie de ce mémoire sera ainsi consacrée au cadre théorique et conceptuel du néoréalisme, appliqué aux enjeux du cyberespace et à la doctrine stratégique des Etats-Unis. Par la suite, la deuxième partie analysera des études de cas de cyberattaques majeures et leur impact sur la stratégie américaine en les répartissant par thématiques stratégiques (rivalités entre puissances, vulnérabilité des infrastructures critiques, coercition et intimidation, surveillance et renseignements). Pour finir, la troisième partie examinera plus globalement la politique des Etats-Unis à ces cyberattaques à travers leurs objectifs stratégiques, leurs doctrines de dissuasion et d'intervention, ainsi que leur coopération internationale en cybersécurité.

## Objectifs du mémoire

L'objectif de ce mémoire est double : tout d'abord, il s'agit de comprendre comment des cyberattaques spécifiques ont façonné la politique des Etats-Unis, en examinant les réactions face aux différentes crises, les innovations technologiques, ainsi que les réformes législatives qui en ont découlé. D'autre part, il s'agit d'analyser cette stratégie sous l'angle de la théorie du néoréalisme, qui permettra de comprendre comment les Etats-Unis, en réponse à ces cyberattaques, ont cherché à projeter leur puissance dans le cyberespace, à dissuader leurs adversaires et à sécuriser leurs infrastructures critiques tout en maintenant leur position dominante sur la scène internationale.

Le mémoire se focalise sur la période allant des années 2000 à la fin du mandat de Joe Biden en décembre 2024. C'est effectivement au début des années 2000 que les Etats-Unis ont formalisé et mis en œuvre une véritable politique de cyberdéfense, en définissant des doctrines et des stratégies spécifiques qui se sont renforcées au fil du temps. L'arrêt de l'analyse à la fin du mandat de Joe Biden a pour but d'avoir un recul suffisant pour évaluer l'évolution et les résultats des stratégies mises en place sous cette administration. De plus, l'investiture de Donald Trump en janvier 2025 introduit aujourd'hui une nouvelle dynamique difficile à anticiper : son ancien mandat, marqué par des décisions imprévisibles et une remise en question de certaines institutions de défense et de renseignement, laisse imaginer d'éventuels changements de cap à venir. Pour autant, ceci n'étant pas encore suffisamment documenté pour faire l'objet d'une analyse, la période post-2024 sera donc l'une des limites méthodologiques de ce travail.

Concernant la délimitation dans l'espace, l'étude se concentrera principalement sur les Etats-Unis, mais inclura également leurs interactions avec d'autres acteurs majeurs dans le cyberespace, tels que la Russie, la Chine, la Corée du Nord ou encore l'Union Européenne, afin de comprendre les dynamiques de pouvoir et de sécurité qui façonnent la stratégie cybernétique américaine. Le choix des Etats-Unis comme acteur central de ce mémoire est motivé par leur pertinence historique, mais également stratégique et académique dans le domaine de la cybersécurité. En effet, ils sont reconnus comme l'une des principales puissances mondiales dans le domaine : à l'avant-garde de l'élaboration et de la mise en œuvre de stratégies complexes, ils ont fortement influencé les normes et les pratiques internationales. Grâce à cela, nous pouvons explorer comment une superpuissance développe, adapte, mais également projette ses capacités dans un domaine aussi crucial que le cyberespace. Cet Etat est également

l'illustration parfaite des dynamiques du néoréalisme, qui met l'accent sur la sécurité nationale, la compétition entre grandes puissances et l'anarchie du système international, et qui sera utilisé dans ce mémoire.

Toutefois, l'analyse de ce travail se heurte à certaines limites. D'une part, la nature même du cyberespace rend l'attribution des attaques souvent incertaine, ce qui peut compliquer l'analyse des stratégies et des réponses américaines. D'autre part, de nombreuses informations stratégiques sont toujours classifiées, et limitent donc l'accès à des sources primaires détaillant certaines cyber-opérations. Enfin, le cadre théorique du néoréalisme, bien qu'utile pour analyser la cyberstratégie américaine, soulève des débats sur sa pertinence complète face à un domaine aussi asymétrique que le cyberespace.

## État de l'art

L'état de l'art sur la cyberstratégie des Etats-Unis et son analyse sous l'angle du néoréalisme dans les relations internationales se situe à l'intersection de plusieurs champs de recherche : la cybersécurité, les relations internationales, la stratégie militaire ainsi que la théorie politique. Au départ, la cyberstratégie américaine se concentrait principalement sur la protection des infrastructures critiques et les chercheurs mettaient l'accent sur la prévention des cyberattaques, notamment sur les systèmes informatiques des structures essentielles (énergie, transports, finances)[3]. Par la suite, avec la forte augmentation des cyberattaques, des chercheurs comme Thomas Rid[4] et Kim Zetter[5] ont montré comment ces attaques ont révélé les capacités offensives des Etats-Unis et l'importance croissante des cyber-opérations clandestines. Également, les études de cas sont couramment utilisées pour illustrer comment les cyberattaques influencent la stratégie nationale. Finalement, durant la dernière décennie, la cyberstratégie américaine se militarisant de plus en plus, nous avons pu voir une augmentation des analyses sur la dissuasion cybernétique, avec une attention accrue sur la capacité à répondre aux cyberattaques et à exercer des représailles, notamment dans les travaux de Joseph Nye[6].

[3] CLARKE Richard, KNAKE Robert, « Cyber War - The Next Threat to National Security and What to Do About It », HarperCollins e-books, 2010.
[4] RID Thomas, « Active Measures. The Secret History of Disinformation and Political Warfare », Australian Journal of Defence and Strategic Studies, 2020.
[5] ZETTER Kim, « Countdown to Zero Day : Stuxnet and the Launch of the World's First Digital Weapon », Crown, 2014, 265p.
[6] NYE Joseph, « Deterrence and Dissuasion in Cyberespace », International Security, 2017.

Concernant le néoréalisme, son application au cyberespace a été explorée par plusieurs chercheurs soutenant que les États perçoivent le cyberespace dans un domaine où ils doivent projeter leur puissance pour garantir leur sécurité[7]. Pourtant, la littérature sur la cyberstratégie et le néoréalisme reste marquée par plusieurs débats, notamment sur l'efficacité à long terme des stratégies de dissuasion et la gestion de l'anarchie dans le cyberespace.

[7] NYE Joseph, « Cyberpower », Harvard Kennedy School, 2010.

# Chapitre 1 – Cadre théorique et conceptuel : néoréalisme et cyberstratégie américaine

Avant de commencer à analyser la réponse des États-Unis face aux cyberattaques majeures, il est essentiel de revenir sur les fondations théoriques de ce mémoire. Le néoréalisme, en tant que cadre analytique privilégié, nous permettra par la suite de comprendre les dynamiques de puissance, de sécurité et de survie qui structurent la stratégie américaine, tant sur la scène internationale que dans le cyberespace. Ce chapitre sera donc divisé en trois parties : tout d'abord, nous exposerons les principes fondamentaux du néoréalisme. Par la suite, nous appliquerons cette théorie aux spécificités du cyberespace, tout en prenant en compte les débats académiques qui lient ces sujets. Finalement, nous analyserons comment les Etats-Unis, en tant que superpuissance, incarnent ces principes néoréalistes dans leur stratégie cybernétique.

## I/ Principes fondamentaux du néoréalisme

Afin de comprendre l'apport du néoréalisme dans les théories des relations internationales, il est important de rappeler rapidement celle dont le néoréalisme tire ses sources, la théorie réaliste. En parallèle de la théorie libérale, la théorie réaliste a longtemps fait partie des modèles dominants pour comprendre les relations internationales et identifier leurs régularités. Comme l'indique Jean-Baptiste Jeangène Vilmer, les réalistes partagent les postulats suivants[8] :

> (1) L'anarchie du système international est un état de guerre, les intérêts des acteurs étant plus souvent en conflit qu'en harmonie. (2) Les principaux acteurs des relations internationales sont les États-nations. « Principaux » ne veut pas dire les seuls : les réalistes n'excluent pas les acteurs non étatiques, simplement ils estiment que les États sont les plus déterminants, que les acteurs non étatiques agissent souvent par l'intermédiaire des États (ce qui est particulièrement évident dans le cas des organisations internationales) et que l'efficacité des institutions internationales et du droit international dépend de leur conformité aux intérêts des grandes puissances. (3) Les États cherchent à maximiser leur intérêt national {…}. (4) La politique étrangère prime en général la politique intérieure ; la prise en compte des contraintes intérieures, notamment l'opinion publique, peut nuire à la bonne conduite diplomatique.

[8] JEANGÈNE VILMER Jean-Baptiste, « Théories des relations internationales - Chapitre II. Le réalisme », Presses Universitaires de France. Que sais-je ? 2020, p.23-42.

Ces grands principes du réalisme ont longtemps dominé la compréhension des relations internationales, mais ont également suscité de nombreuses critiques, notamment dans le contexte de la guerre du Vietnam, qui a mis en lumière certaines limites du cadre réaliste classique. Le néoréalisme, qui apparaît à la fin des années 1970, se présente comme une « rédemption scientifique »[9] du réalisme classique. Son fondateur, Kenneth Waltz, en expose les principes dans son œuvre de 1979 « Theory of International Politics »[10]. Suivi par des auteurs comme Robert Gilpin, Stephen Walt, Joseph Grieco, John Mearsheimer ou encore Jack Snyder, Waltz centre la théorie néoréaliste autour de plusieurs concepts que nous allons tenter d'analyser plus en profondeur, afin de comprendre par la suite les politiques que les États-Unis peuvent appliquer au cyberespace.

## Anarchie du système international

Dans un premier temps, reprenons une notion centrale dans les concepts réalistes et néoréalistes, l'anarchie. Dans le cadre de l'analyse des relations internationales, l'anarchie se définit comme « l'absence d'autorité centrale au-dessus des Etats »[11]. Selon Waltz, l'anarchie est structurelle, et découle non pas de la volonté humaine, mais de la structure même du système international décentralisé, dans lequel il n'existe pas d'autorité hiérarchique supérieure aux Etats pour faire respecter les règles et garantir la sécurité de tous[12]. Selon Raymond Aron, l'anarchie est même définie par « l'absence d'une instance qui détienne le monopole de la violence légitime »[13]. L'anarchie est donc « un état de guerre, qui structure constamment le comportement des Etats sur la scène internationale »[14]. C'est pourquoi les États, autonomes et indépendants, se comportent selon certaines logiques : recherche de puissance et de sécurité, méfiance vis-à-vis des intentions des autres et difficultés de coopération, logiques d'équilibres…

[9] ASHLEY, Richard K., « The Poverty of Neorealism. », International Organization, vol. 38, no. 2, 1984, pp. 225–86.
[10] WALTZ Kenneth N., « Theory of International politics », University of California, 1979.
[11] Vie publique, « Quelles sont les grandes théories en matière de relations internationales ?» Vie publique, 2024.
[12] WALTZ Kenneth N., « Theory of International politics », University of California, 1979.
[13] DUROSELLE Jean-Baptiste, « Paix et guerre entre les nations : la théorie des relations internationales selon Raymond Aron », Revue française de science politique, 12/n°4, 1962. pp. 963-979
[14] Vie publique, « Quelles sont les grandes théories en matière de relations internationales ?» Vie publique, 2024.

## Quête de sécurité et de puissance

Pour Kenneth Waltz, l'anarchie du système international amène une sélection naturelle « systémique » des Etats[15]. En effet, ceux qui n'agissent pas selon les contraintes du système risquent d'être marginalisés, d'être soumis ou de disparaître. La sécurité devient alors l'objectif premier des Etats, qui doivent alors assurer eux-mêmes leur sécurité pour survivre. Chaque Etat, ou unité selon Waltz, « doit se rendre capable de prendre soin d'elle-même car elle ne peut compter sur personne d'autre pour le faire »[16]. Cette logique d'autoconservation (self-help), également développée par John Mearsheimer, pousse donc les Etats à s'autonomiser sur le plan militaire, à acquérir ou préserver du pouvoir ainsi qu'à se méfier des intentions des autres.

Selon Mearsheimer, les Etats ne se contentent pas de suffisamment de puissance pour assurer leur sécurité : ils cherchent à maximiser leur part du pouvoir relatif[17]. De plus, l'incertitude face aux intentions des autres rend les Etats méfiants et les pousse à avoir un avantage militaire offensif. Seulement, en augmentant sa sécurité par l'acquisition d'armes, même sans intentions hostiles, un État accroît la perception de la menace, et donc l'insécurité des autres, qui vont réagir en s'armant à leur tour. Ce dilemme de sécurité, très présent dans les théories réaliste et néoréaliste, est un comportement récurrent lié aux contraintes d'un système anarchique. L'anarchie rend les Etats vulnérables ; ces derniers veulent se défendre et s'arment ; les autres perçoivent une menace et s'arment à leur tour, ce qui entraîne une spirale sécuritaire et une course aux armements. Pourtant, il est utile de noter un certain paradoxe lié à la doctrine de la dissuasion : plus les armes sont destructrices et réduisent la tentation d'attaque, plus elles stabilisent les rapports entre puissances[18]. Ces éléments créent donc une dynamique de compétition permanente, même entre Etats pacifiques ou bienveillants.

[15] WALTZ Kenneth N., « Realist thought and neorealist theory », Journal of International Affairs, 1990/44, no. 1, pp.21–37.
[16] WALTZ Kenneth N., « Theory of International politics », University of California, 1979.
[17] MEARSHEIMER John J., « The tragedy of great power politics », Norton & Co, 2001.
[18] WALTZ Kenneth N., « Theory of International politics », University of California, 1979.

## Compétition et coopération

Cette méfiance mutuelle, accompagnée d'une recherche de puissance, amène donc une logique de compétition permanente. Les grandes puissances, en particulier, sont piégées dans une « quête incessante de pouvoir »[19] afin d'atteindre une position d'hégémonie régionale qui leur accordera une sécurité presque maximale. Ces dernières adoptent alors différentes stratégies afin d'assurer leur survie. Outre les effets de la structure anarchique développés par Waltz (self-help, imitation des stratégies efficaces des puissances dominantes, course aux armements exacerbé par le dilemme de sécurité), les puissances utilisent également des stratégies de contrebalancement (balancing), de rivalité ou de guerre. Mearsheimer identifie alors plusieurs stratégies : le balancing, également développé par Stephen Walt[20] et qui vise un équilibre des puissances montantes sur la scène internationale en s'opposant à elles par des coalitions ; le buck-passing, qui vise à laisser un autre Etat affronter la menace afin d'éviter les risques et les coûts liés à l'équilibrage ; la guerre préventive, qui cherche à attaquer avant que l'ennemi ne devienne trop fort ; ou encore la dissuasion, qui veut convaincre l'ennemi que l'agression lui coûtera trop cher pour valoir le coût d'être perpétrée[21].

Dans ce contexte, la coopération internationale est perçue comme difficile, voire entravée pour les réalistes et néoréalistes. Selon Kenneth Waltz, l'inexistence d'une gouvernance mondiale implique que les affaires internationales ne peuvent pas être « gérées » comme celles d'un Etat[22]. Si les institutions peuvent effectivement, de manière temporaire, faciliter certains échanges, elles ne peuvent toutefois surmonter toutes les contraintes du système anarchique. Comme l'explique Joseph Grieco, les Etats ne sont pas seulement préoccupés par les gains absolus, à savoir ce qu'ils vont gagner quantitativement, mais surtout par les gains relatifs, donc ce qu'ils gagnent par rapport aux autres[23]. Les Etats cherchent particulièrement à ne pas laisser les autres gagner plus qu'eux, même si cela implique qu'eux-mêmes ne gagneront rien. Une coopération alors perçue comme avantageuse pour un rival sera donc souvent refusée, même si elle pourrait être bénéfique pour les deux partis. L'ordre du système anarchique naît donc de l'équilibre des puissances ainsi que de la dissuasion.

[19] MEARSHEIMER John J., « The tragedy of great power politics », Norton & Co, 2001.
[20] WALT Stephen, « The Origins of Alliances », Cornell University Press, 1987.
[21] MEARSHEIMER John J., « The tragedy of great power politics », Norton & Co, 2001.
[22] WALTZ Kenneth N., « Theory of International politics », University of California, 1979.
[23] GRIECO Joseph M., « Anarchy and the Limits of Cooperation : A Realist Critique of the Newest Liberal Institutionalism », International Organization, vol. 42, no. 3, 1988, pp. 485–507.

Selon Waltz, les organisations internationales peuvent donc jouer un rôle, notamment dans la gestion de conflits mineurs ou la codification de certaines normes, mais reflètent finalement les rapports de puissance existants, leur efficacité dépend donc du bon vouloir des grandes puissances[24].

## II/ Le néoréalisme face aux enjeux du cyberespace

Après avoir exposé les principes du néoréalisme, il est maintenant intéressant de les appliquer à l'un des sujets centraux de ce mémoire, le cyberespace. En effet, bien que celui-ci bouleverse les dynamiques classiques des relations sur la scène internationale, il reste pour autant structuré par une logique d'anarchie et de compétitivité qui le rend compatible avec une grille de lecture néoréaliste. Dans cette partie, nous allons analyser quatre éléments majeurs de cette grille de lecture : l'anarchie au sein du cyberespace, la quête de puissance et de sécurité, la compétition stratégique entre grandes puissances ainsi que les limites de coopération qui en découlent, pour finir avec les dilemmes spécifiques liés à la dissuasion et à l'attribution dans cet environnement.

### Le cyberespace, prolongement du système anarchique

Contrairement aux territoires physiques délimités par des frontières clairement identifiables, le cyberespace se caractérise par son absence de frontières, qui se joue des cadres juridiques et géographiques traditionnels[25]. Dès les années 1990, il a été associé à la dynamique de mondialisation, en facilitant notamment les flux transnationaux, qu'il s'agisse de la dématérialisation des échanges financiers, de l'accélération des communications, ou encore de la circulation massive et instantanée de l'information. Pour autant, malgré son absence de frontières, le cyberespace n'est pas un espace où les rapports de force n'existent pas. Il est au contraire marqué par une profonde anarchie, comme vue par les néoréalistes. Comme nous l'avons analysé précédemment, Kenneth Waltz définit l'anarchie non pas comme le chaos, mais comme l'absence d'une autorité centrale capable de réguler les relations entre unités souveraines[26]. Cette logique est pleinement transposable au cyberespace : il n'existe pas de « police internationale du cyberespace » ou de mécanisme centralisé de régulation, et malgré des

[24] WALTZ Kenneth N., « Theory of International politics », University of California, 1979.
[25] KEMPF Olivier, « Cyberespace et dynamique des frontières », Inflexions, 2015/3 N° 30, p.141-149.
[26] WALTZ Kenneth N., « Theory of International politics », University of California, 1979.

tentatives de coopération que nous étudierons par la suite, les États ne peuvent finalement compter que sur eux-mêmes pour se défendre et imposer leurs normes. En ce sens, le cyberespace, considéré comme un vecteur de progrès et d'ouverture, est également devenu un terrain où les Etats perdent partiellement ou totalement leur autorité et peinent à faire respecter leur souveraineté[27]. En effet, un Etat possède en pratique la capacité et la légitimité de réglementer ce qui se passe sur son territoire (activités de ses citoyens et de ses entreprises, circulation des biens ou des données…) alors que dans le cyberespace, cette capacité est largement remise en question. Comme nous le verrons par la suite, plusieurs facteurs en sont la cause : opacité des interactions numériques, anonymat des acteurs, rapidité des flux, extraterritorialité des données[28]… Comme l'indique Stéphane Taillat, la démocratisation des technologies de l'information et de la communication (TIC) permet à des acteurs non étatiques de s'approprier des capacités autrefois réservées aux grandes puissances[29]. Cela favorise donc une forme de « décentralisation du pouvoir stratégique », où le monopole de la violence n'est plus garanti par l'Etat, mais confirme l'idée néoréaliste selon laquelle les Etats évoluent dans un environnement conflictuel et incertain, où l'adaptation est cruciale pour survivre.

Dès lors, même si le cyberespace bouscule les modalités classiques de l'exercice de la souveraineté, il ne remet pas en cause la pertinence du néoréalisme mais en confirme les postulats de base, notamment la centralité de l'anarchie et l'obligation pour les États de se reposer sur eux-mêmes (self-help) pour assurer leur sécurité. Le cyberespace est ainsi un terrain où l'expression de l'anarchie structurelle de Kenneth Waltz s'intensifie[30], et dans lequel l'autorité des Etats se retrouve contestée et fragmentée, au profit de nombreux acteurs qui échappent à leur contrôle.

[27] KEMPF Olivier, « Cyberespace et dynamique des frontières », Inflexions, 2015/3 N° 30, p.141-149.
[28] Ibid.
[29] TAILLAT Stéphane, « Un mode de guerre hybride dissymétrique ? Le cyberespace », Stratégique, 2016/1 N° 111, p.89-106.
[30] WALTZ Kenneth N., « Theory of International politics », University of California, 1979.

## Quête de sécurité et de puissance dans le cyberespace

Depuis le début des années 2000, les Etats ont pris conscience que la dépendance croissante à l'égard du numérique expose leurs infrastructures critiques (énergie, transport, finance, santé, défense) à des perturbations stratégiques. Cette vulnérabilité mène à un potentiel déficit de sécurité. En effet, si ces infrastructures venaient à être paralysées, la capacité des Etats à assurer leur autonomie et donc leur survie serait mise en jeu. Par ailleurs, dans le cyberespace, la quête de sécurité ne se réduit pas au seul impératif militaire mais se décline en quatre dimensions[31] :

- Économique : protéger les intérêts des entreprises stratégiques et assurer la continuité des infrastructures nationales ;
- Judiciaire : lutter contre la cybercriminalité ;
- Stratégique : garantir la résilience nationale tout en contribuant à une coopération pour une gouvernance globale d'Internet ;
- Idéologique : promouvoir la liberté d'expression et l'ouverture du réseau, ou, pour certains acteurs, utiliser l'information en ligne pour déstabiliser des régimes adverses via des opérations d'influence.

Par ailleurs, le cyberespace ne se contente pas d'être simplement le cinquième champ de bataille de la guerre (après les espaces aérien, terrestre, maritime et spatial) : il remet en question le modèle historique de guerre régulière[32]. D'un côté, on utilise le cyber pour la guerre (opérations de sabotage, d'espionnage, frappes cinétiques offensives, défensives ou préemptives…). La détection précoce des intentions adverses étant presque impossible, les États adoptent des doctrines plus préemptives et agressives afin de se protéger des attaques potentielles. Cette dynamique, déjà à l'œuvre dans le monde physique, est accentuée dans le cyberespace par l'invisibilité et la rapidité des opérations. De l'autre, il y a également une possibilité de guerre dans le cyberespace (campagnes de désinformation, paralysie de l'économie…). Face à la montée des vulnérabilités numériques, les États appliquent alors une logique de self-help, en investissant dans la cyberdéfense nationale, en promouvant des politiques d'autonomie stratégique[33] (cloud souverain, maîtrise des chaînes

[31] HUYGHE François-Bernard, « Des armes à la stratégie », Revue internationale et stratégique, 2012/3 n° 87, p.53-64.
[32] TAILLAT Stéphane, « Un mode de guerre hybride dissymétrique ? Le cyberespace », Stratégique, 2016/1 N° 111, p.89-106.
[33] CATTARUZZA Amaël, DANET Didier, TAILLAT Stéphane, « Présentation ». In : TAILLAT, Stéphane, CATTARUZZA, Amaël et DANET, Didier, La Cyberdéfense Politique de l'espace numérique. Paris : Armand Colin. Collection U, p.124-125.

d'approvisionnement critiques…) et en constituant des unités militaires spécialisées (comme le Cyber Command américain)[34]. Le cyberespace devient ainsi un terrain d'accumulation de puissance, au même titre que les domaines terrestre, maritime, aérien ou spatial[35].

Selon Joseph Nye, l'émergence du cyberespace signifie une diffusion de la puissance, et sa transition vers des acteurs non étatiques : le domaine numérique autoriserait les actions asymétriques, mais aussi une contestation voire un contournement de la puissance[36]. Pour autant, le cyberespace serait plus en faveur des puissances traditionnelles, qui peuvent mobiliser et exploiter les ressources nécessaires au domaine numérique afin de renforcer leur puissance. Il faut cependant noter que le risque d'escalade dans le cyberespace reste important. En effet, une escalade peut très rapidement survenir suite au mauvais calcul d'un agresseur quant aux enjeux de sa cible[37], comme nous pourrons le voir par la suite avec l'exemple de l'attaque sur SonyPictures.

## Compétition stratégique et coopération

Ces dynamiques de puissance et de quête de sécurité dans le cyberespace ne sont pas sans effets. Comme décrit par les néoréalistes, le dilemme de sécurité s'applique également sur le terrain numérique. En effet, les mesures prises par un Etat pour accroître sa propre sécurité, que ce soit pour développer des cyberarmes offensives ou en renforçant la surveillance numérique, sont perçues par les autres comme autant de menaces potentielles. Ces derniers réagissent donc en renforçant à leur tour leurs capacités, ce qui crée une spirale d'armement cybernétique et une compétition sécuritaire accrue. Dans cet environnement où l'opacité et l'anonymat sont de mise, les intentions stratégiques sont particulièrement difficiles à interpréter, ce qui renforce la méfiance mutuelle et rend la coopération internationale encore plus fragile[38].

[34] U.S. Cyber Command, « Our History », U.S. Cyber Command.
[35] KELLO Lucas, Traduit de l'anglais par RICHARD Thomas, « Les cyberarmes : dilemmes et futurs possibles », Politique étrangère, 2014/4 Hiver, p.139-150.
[36] Ibid.
[37] Ibid.
[38] NYE Joseph, GOLDSMITH Jack Landman, "The Future of Power." Bulletin of the American Academy of Arts and Sciences 64, no. 3 (2011): 45–52.

Pour autant, nous pouvons observer une double approche d'Internet dans l'attitude des Etats. D'un côté, nous pouvons voir une logique de compétition stratégique dans laquelle les puissances cherchent à imposer leur propre vision du cyberespace à travers des normes techniques, juridiques et politiques[39]. Ce phénomène est particulièrement visible dans les débats autour de la gouvernance de l'Internet, entre les partisans d'une approche multilatérale dominée par les États (notamment la Russie et la Chine) et ceux défendant un modèle multi-acteurs, plus ouvert, soutenu notamment par les États-Unis et leurs alliés[40]. À titre d'exemple, la Chine et la Russie promeuvent à l'ONU un modèle de souveraineté qui renforcerait le contrôle étatique sur Internet, tandis que les États-Unis, historiquement favorables à une gouvernance multi-acteurs via l'ICANN, tentent de préserver leur influence sur les architectures techniques et normatives du réseau mondial[41]. De l'autre côté, les Etats affichent également une rhétorique de coopération intergouvernementale[42]. Sur le plan national, les Etats revendiquent un pouvoir de contrôle souverain sur leurs infrastructures numériques, tandis que sur le plan international, ils plaident pour une coopération entre Etats afin de fixer ensemble les règles du jeu.

## Défis de l'attribution et de la dissuasion dans le cyberespace

Dans ce contexte de compétition intense, où la méfiance mutuelle et la difficulté de coopération sont décisives, la question de la dissuasion dans le cyberespace devient centrale. Pour autant, si la dissuasion est un pilier de la stabilité entre grandes puissances dans le néoréalisme, son efficacité est affaiblie dans ce nouvel espace. L'opacité des interactions numériques, l'anonymat des acteurs et la rapidité des flux compliquent considérablement l'identification des responsables et la mise en œuvre de régulations efficaces. Il faut donc analyser la manière dont les doctrines de dissuasion sont adaptées, transformées ou remises en cause dans l'environnement numérique.

---

[39] CATTARUZZA Amaël, DANET Didier, TAILLAT Stéphane, « Présentation ». In : TAILLAT, Stéphane, CATTARUZZA, Amaël et DANET, Didier, La Cyberdéfense Politique de l'espace numérique. Paris : Armand Colin. Collection U, p.124-125.

[40] NOCETTI Julien, « Internet et sa gouvernance : crispations internationales et nouveaux enjeux » In : TAILLAT, Stéphane, CATTARUZZA, Amaël et DANET, Didier, La Cyberdéfense Politique de l'espace numérique. Paris : Armand Colin. Collection U, 2018, p.130-135.

[41] Ibid.

[42] NOCETTI Julien, « Internet et sa gouvernance : crispations internationales et nouveaux enjeux » In : TAILLAT, Stéphane, CATTARUZZA, Amaël et DANET, Didier, La Cyberdéfense Politique de l'espace numérique. Paris : Armand Colin. Collection U, 2018, p.130-135.

La doctrine de la dissuasion, formulée au lendemain de la Seconde Guerre mondiale et développée pendant la guerre froide, postule que « s'il n'y a pas eu d'agression soviétique contre l'Europe occidentale, ce n'est pas parce que les intentions agressives seraient inexistantes en URSS, mais grâce à l'effet dissuasif des capacités militaires occidentales »[43]. En ce sens, la stratégie de dissuasion vise à inciter l'ennemi à ne pas attaquer sa cible en lui faisant croire que les coûts et bénéfices d'une agression potentielle ne seront pas à son avantage[44]. Cette logique, alors largement appliquée dans le contexte nucléaire, est aujourd'hui examinée à l'ère des cyberattaques, où la difficulté d'attribution et la diversité des acteurs créent de nouveaux défis.

Comme nous l'avons évoqué précédemment, la dissuasion repose sur la capacité d'infliger des représailles crédibles à un adversaire afin de l'inciter à renoncer à une attaque[45]. A l'ère du cyberespace, cette théorie est reprise sous le terme de « dissuasion par la punition »[46], qui vise à menacer de sévères représailles (sanctions économiques, contre-attaques cybernétiques, représailles militaires...) en cas de cyberattaque. Pour illustrer ce type de dissuasion, on peut citer les sanctions économiques prises par Barack Obama en 2014 face aux attaques présumées de la Corée du Nord contre l'entreprise SonyPictures[47] que nous reprendrons par la suite dans une étude de cas. Cependant, dans le cyberespace, cette approche est mise à l'épreuve en raison de la difficulté d'attribution des attaques et de la diversité des acteurs impliqués (hacktivistes, groupes inspirés par des États, terroristes...)[48]. Pour adapter cette théorie, Joseph Nye[49] a alors mis en avant le concept de « deterrence by interdiction », qui consiste à rendre les attaques inefficaces en renforçant la résilience des infrastructures numériques plutôt que de s'appuyer sur la menace de représailles. Il est notamment soutenu par d'autres chercheurs pour qui « l'adoption de normes de cybersécurité plus strictes réduit l'efficacité des attaques et renforce la dissuasion »[50]. Un dernier type de dissuasion est proposé par les chercheurs : la dissuasion par le déni. Celle-ci, en augmentant la complexité des

[43] CARTIGNY Claude, « Le concept de dissuasion et ses conséquences sur les doctrines stratégiques », Recherches Internationales, n°21, 1986, pp.77-84.
[44] IASIELLO Emilio, « La cyberdissuasion est-elle une stratégie illusoire ? », Air University, ASPJ Afrique et Francophonie, 2018.
[45] MORGAN, Patrick M., « Deterrence Now », Cambridge University Press, 2003.
[46] LIBICKI Martin C., « Cyberdeterrence and Cyberwar », Rand Corporation, 2009.
[47] LEHU Jean-Marc, « Cyberattaque : la gestion du risque est-elle encore possible ? Analyse et enseignements du cas Sony Pictures », La Revue des Sciences de Gestion, 2018/3 N° 291-292, p.41-50.
[48] RID Thomas, BUCHANAN Ben, « Attributing Cyber Attacks », Journal of Strategic Studies, 2015, 4-37.
[49] NYE Joseph, « Deterrence and Dissuasion in Cyberespace », International Security, 2017.
[50] TIKK Eneken, KERTTUNEN Mika, « Routledge handbook of international Cybersecurity », Routledge, 2020.

défenses, vise à décourager les attaquants en réduisant leurs chances de succès, en rendant l'attaque trop coûteuse ou inefficace[51].

Cependant, bien que ces concepts soient bien établis, leur application au cyberespace est sujette à débat : l'absence de frontières physiques et la rapidité des cyberattaques rendent la mise en œuvre de la dissuasion complexe. De plus, comme indiqué précédemment, l'attribution étant un élément essentiel des stratégies de dissuasion, il peut être difficile de les appliquer au cyberespace, où les techniques de brouillage, les anonymiseurs ou les proxys empêchent parfois une attribution claire et précise[52]. Aussi, la montée en puissance des acteurs non étatiques (groupes terroristes, hacktivistes, pirates informatiques...) modifie cette vision réaliste de la concurrence entre États pour leurs intérêts nationaux. En effet, les cyberattaques menées par des groupes criminels ou des hacktivistes ne répondent pas toujours à une logique rationnelle d'intérêts étatiques, ce qui complique grandement leur dissuasion[53].

La proportionnalité des représailles est également au cœur du débat. Une réponse excessive à une cyberattaque (attribuée ou non) pourrait conduire à une escalade non souhaitée, tandis qu'à l'inverse, une réponse insuffisante pourrait conduire à une nouvelle escalade[54]. Comme le souligne Jack Beard, « les commandants qui emploient des cybercapacités dans des attaques peuvent être contraints de faire des calculs difficiles. Les dommages attendus pour la population civile liés aux « effets directs » de l'attaque sont clairement inclus dans leurs évaluations de la proportionnalité »[55]. Pour illustrer cela, on peut citer en exemple l'affirmation des Etats-Unis selon laquelle ils pourraient considérer une attaque informatique d'une certaine ampleur comme un acte de guerre, dès lors qu'elle causerait des dommages civils ou compromettrait leurs intérêts de souveraineté[56].

[51] BENDIEK Annegret, METZGER Tobias, « Deterrence theory in the cyber-century : Lessons from a state-of-the-art literature review », German Institute for International and Security Affairs, 2015.
[52] IASIELLO Emilio, « La cyberdissuasion est-elle une stratégie illusoire ? », Air University, ASPJ Afrique et Francophonie, 2018.
[53] Ibid.
[54] TIKK Eneken, KERTTUNEN Mika, « Routledge handbook of international Cybersecurity », Routledge, 2020.
[55] BEARD Jack, « The Principle of Proportionality in an Era of High technology », Oxford University Press, 2018.
[56] HUYGHE François-Bernard, « Des armes à la stratégie », Revue internationale et stratégique, 2012/3 n° 87, p.53-64.

Enfin, la dimension asymétrique du cyberespace complique la réponse dissuasive. Contrairement à la puissance militaire, qui est facilement quantifiable, de petits États ou des groupes non gouvernementaux peuvent infliger des dommages importants aux grandes puissances par le biais d'attaques sophistiquées. Cela modifie l'équilibre des forces, qui ne peut être évalué dans le cyberespace, et favorise l'effet de surprise recherché par l'ennemi[57].

Pour conclure, si le cyberespace introduit de nouveaux défis stratégiques et techniques, il reste en grande partie structuré par les dynamiques fondamentales mises en lumière par le néoréalisme : anarchie, incertitude, quête de sécurité, et compétition entre grandes puissances. Toutefois, certains aspects, comme la difficulté d'attribution ou les limites de la dissuasion, montrent que cette grille d'analyse nécessite d'être adaptée, voire complétée, pour appréhender pleinement les réalités du cyberespace.

## III/ Les Etats-Unis comme illustration du néoréalisme dans le cyberespace

Maintenant que les aspects théoriques de ce mémoire ont été abordés, nous pouvons les décliner aux Etats-Unis. Par leur antériorité technologique sur le cyberespace et sur l'architecture d'Internet, qui leur a permis de mettre en place les premières normes et des moyens de contrôle, les Etats-Unis dominent largement le cyberespace. Dans cette dernière partie, nous analyserons donc la domination des Etats-Unis sur le cyberespace, qui fait pourtant l'objet de nombreuses critiques parmi les puissances émergentes. Par la suite, nous étudierons l'évolution des doctrines américaines en cybersécurité depuis le début des années 2000 jusqu'à la fin du mandat de Joe Biden, entre posture défensive, dissuasion active et projection de puissance.

### Domination sur le cyberespace

Internet, comme nous le connaissons aujourd'hui, provient d'un développement technologique initié puis largement dirigé par les Etats-Unis. Tiré des origines d'un projet militaire dans le contexte de rivalité stratégique avec l'URSS pendant la Guerre froide, les autorités américaines lancent l'Advanced Research Projects Agency (ARPA) en 1958[58]. Leur

[57] KEMPF Olivier, « Cyber et surprise stratégique », Stratégique, 2014/2 N° 106, p.111-123.
[58] CERUZZI Paul E., « Aux origines américaines de l'Internet : projets militaires, intérêts commerciaux, désirs de communauté », Le Temps des médias, 2012/1 n° 18, p.15-28.

objectif est d'assurer la supériorité technologique des Etats-Unis au niveau de la défense. Cette agence donnera par la suite naissance à l'ARPANET, premier réseau de communication par paquet[59]. Ce dernier vise à garantir la résilience des communications militaires en cas de guerre nucléaire, en connectant différents centres de calculs à travers le territoire américain. A partir de ce réseau, l'agence lance plusieurs innovations techniques majeures, notamment les protocoles TCP/IP qui deviendront la base universelle d'Internet à partir de 1983[60]. Toujours utilisés aujourd'hui, ces protocoles montrent déjà la capacité des Etats-Unis à imposer leurs normes au niveau international dans le cyberespace.

A travers cette infrastructure, les Etats-Unis imposent progressivement leurs normes techniques, leur architecture du réseau et leur propre logique de gouvernance. En 1983, ARPANET est scindé en deux : la première partie reste sous le contrôle du Department of Defense, tandis que l'autre est confiée à la National Science Foundation (NSF)[61]. Cette dernière ouvrira l'accès du réseau aux institutions universitaires et aux fournisseurs commerciaux, ce qui amènera dans les années 1990 l'explosion du trafic commercial à travers le web, toujours sous contrôle indirect du gouvernement américain par le biais du Department of Commerce, qui assurera jusqu'en 2005 la gestion des noms de domaine et des adresses IP via l'Internet Corporation for Assigned Names and Numbers (ICANN)[62].

Ce contrôle administratif et technique montre une forme de souveraineté numérique, dans laquelle le gouvernement américain conserve la capacité de gérer, voire d'interrompre les extensions nationales (.fr, .be…) en cas de nécessité[63]. La quasi-totalité des serveurs et des capacités technologiques étant situés sur le territoire américain, tout comme l'hégémonie des noms de domaines alors dominants (.com, .gov, .us) reflète une infrastructure façonnée selon les intérêts stratégiques des Américains. Maintenant très contesté par de nombreuses puissances émergentes, comme la Chine, la Russie et certains pas du Moyen-Orient[64], ce

[59] CERUZZI Paul E., « Aux origines américaines de l'Internet : projets militaires, intérêts commerciaux, désirs de communauté », Le Temps des médias, 2012/1 n° 18, p.15-28.
[60] Ibid.
[61] Ibid.
[62] NOCETTI Julien, « Internet et sa gouvernance : crispations internationales et nouveaux enjeux » In : TAILLAT, Stéphane, CATTARUZZA, Amaël et DANET, Didier, La Cyberdéfense Politique de l'espace numérique. Paris : Armand Colin. Collection U, 2018, p.130-135.
[63] Ibid.
[64] NOCETTI Julien, « Internet et sa gouvernance : crispations internationales et nouveaux enjeux » In : TAILLAT, Stéphane, CATTARUZZA, Amaël et DANET, Didier, La Cyberdéfense Politique de l'espace numérique. Paris : Armand Colin. Collection U, 2018, p.130-135.

monopole montre la capacité d'un Etat à façonner les normes globales par le simple fait de la création d'une technologie.

Par ailleurs, cette domination s'appuie sur la puissance des géants technologiques américains : les GAFAM (Google, Apple, Facebook, Amazon et Microsoft), se sont développés jusqu'à arriver à renforcer à leur tour l'influence systémique des Etats-Unis sur le fonctionnement quotidien du cyberespace[65]. Leurs services, presque omniprésents, permettent de structurer tant l'économie mondiale que de concentrer données, standards et capacités d'innovation sur le territoire américain avant de les imposer au monde entier. Comme le souligne Louis Wiart, ces entreprises majeures exercent une « influence déterminante sur les perspectives de développement d'Internet »[66] : leur position dominante leur permet d'accroître la dépendance des sociétés contemporaines vis-à-vis des technologies américaines, ce qui donne aux Etats-Unis un avantage compétitif, ainsi qu'un levier stratégique sans équivalent dans le cyberespace.

Cette hégémonie des Etats-Unis sur le cyberespace, qui amène un système largement asymétrique par rapport aux autres puissances, ne manque pas de susciter des frustrations croissantes chez ces dernières. Dès les années 2000, d'autres Etats comme la Chine, la Russie, l'Inde ou certains pays du Moyen-Orient dénoncent cette domination américaine sur les ressources critiques du cyberespace (protocoles, DNS, normes, infrastructures…). Cette contestation en devient d'autant plus politique, que ces Etats contestataires appellent à une gouvernance multilatérale et à une répartition plus équitable des responsabilités dans la gestion d'Internet[67]. Ces tensions seront approfondies dans le dernier chapitre de ce mémoire, mais illustrent déjà à ce stade la portée stratégique de la domination américaine dans un espace, nouveau, global, et non régulé.

[65] WIART Louis, « Les stratégies des GAFAM », Nectart, 2023/32.
[66] Ibid.
[67] NOCETTI Julien, « Internet et sa gouvernance : La rivalité entre États-Unis et grands émergents ». In : DE MONTBRIAL, Thierry et MOREAU DEFARGES, Philippe, Ramses 2015 Le défi des émergents. Paris : Institut français des relations internationales. Ramses, p.206-209.

## Autonomie, quête de sécurité et compétition

L'analyse de la domination structurelle et normative des Etats-Unis dans le cyberespace met déjà en lumière un fait central : leur posture ne repose pas uniquement sur des avantages techniques ou économiques, mais bien sur une volonté d'imposer et de préserver une position hégémonique dans un nouvel espace, le cyberespace, considéré comme instable, conflictuel et anarchique. Comme nous l'avons vu précédemment, c'est précisément ce que décrit le néoréalisme : dans un environnement sans autorité supérieure qui impose les règles du jeu, les Etats agissent pour maximiser leur autonomie, préserver leur sécurité et garantir leur survie, même au prix d'une compétition permanente.

Face à l'anarchie du cyberespace, les Etats-Unis mettent donc en œuvre une logique de self-help tout en se méfiant des autres acteurs. Ils façonnent eux-mêmes les règles, les standards techniques, ainsi que l'écosystème normatif mondial. En conservant jusqu'en 2016 la supervision de l'ICANN, en structurant l'espace numérique autour des GAFAM et en maintenant sur leur territoire une part importante des infrastructures vitales d'Internet[68], Washington applique donc une stratégie typique d'une puissance vue par les néoréalistes : préserver l'asymétrie technologique et normative afin de contenir la montée en puissance des rivaux. Cette dynamique répond également à un impératif fondamental du néoréalisme, la quête de sécurité, qui devient ici indissociable de la maîtrise du cyberespace.

Les États-Unis ont développé des stratégies de dissuasion hybrides, mêlant durcissement défensif (infrastructures résiliantes, doctrines de cybersécurité) et capacités offensives (préemption, infiltration, perturbation des réseaux adverses)[69] que nous analyserons par la suite. Comme l'a montré l'évolution doctrinale américaine à partir de 2018 (voir chapitre 3), cette stratégie repose sur une anticipation permanente des menaces, y compris en zone grise, ce qui montre un refus croissant de subir l'initiative adverse[70]. Mais cette recherche de sécurité n'est pas sans effet. Plus les États-Unis développent leurs capacités cyber, souvent dans le secret, via les agences de renseignement ou des opérations non revendiquées, plus les puissances concurrentes perçoivent ces actions comme des menaces directes[71]. Cela déclenche

[68] NOCETTI Julien, « Internet et sa gouvernance : crispations internationales et nouveaux enjeux » In : TAILLAT, Stéphane, CATTARUZZA, Amaël et DANET, Didier, La Cyberdéfense Politique de l'espace numérique. Paris : Armand Colin. Collection U, 2018, p.130-135.
[69] VALERIANO Brandon, JENSEN Benjamin et MANESS Ryan C., « Cyber Strategy: The Evolving Character of Power and Coercion ». Oxford : Oxford University Press, 2021.
[70] Ibid.
[71] NOCETTI Julien, « Internet et sa gouvernance : crispations internationales et nouveaux enjeux » In : TAILLAT, Stéphane, CATTARUZZA, Amaël et DANET, Didier, La Cyberdéfense Politique de l'espace numérique. Paris : Armand Colin. Collection U, 2018, p.130-135.

des mécanismes d'équilibrage défensif, voire offensif, parfaitement décrits dans le dilemme de sécurité : chaque renforcement d'un État, même défensif, est perçu comme un danger par les autres, qui s'arment à leur tour, ce qui amène à une spirale compétitive.

Enfin, les États-Unis montrent une nette réticence à abandonner une part de leur autonomie stratégique au profit d'une gouvernance internationale, qui peut être amenée à être contraignante. Bien qu'ils participent à des forums multilatéraux (comme le Groupe d'experts gouvernementaux à l'ONU ou les discussions au sein du G7), leur engagement dans ces enceintes reste largement instrumentalisé. Il vise avant tout à préserver leurs marges de manœuvre plutôt qu'à établir un cadre contraignant dont la sécurité profitera à tous. Ce comportement rejoint l'analyse de Kenneth Waltz selon laquelle, dans un système anarchique, les institutions reflètent l'équilibre des forces existant, mais ne peuvent pas les corriger durablement[72]. La coopération, dans ce cadre, n'est pas écartée en soi, mais n'est envisagée que lorsqu'elle renforce les intérêts stratégiques d'un État ou lui permet d'en limiter les coûts.

Pour finir, la posture américaine dans le cyberespace constitue un exemple très cohérent de la théorie néoréaliste. En cherchant à préserver leur suprématie dans un domaine pas encore régulé, en refusant toute gouvernance contraignante, en adaptant leurs doctrines aux logiques de confrontation asymétrique et en contestant toute remise en cause de leur domination, les États-Unis adoptent une stratégie de puissance classique, simplement transposée à un nouvel espace. Le cyber devient ainsi un champ d'application contemporain des dynamiques anciennes du système international, avec ses tensions, ses rivalités et ses jeux d'influence.

[72] WALTZ Kenneth N., « Theory of International politics », University of California, 1979.

# Chapitre 2 – Cyberattaques majeures et impact sur la stratégie américaine

Alors que le chapitre précédent visait à poser les fondations théoriques de ce mémoire, ce second chapitre cherche désormais à analyser comment certaines cyberattaques majeures ont influencé, accéléré ou infléchi la posture sécuritaire des Etats-Unis. En effet, nombre de ces attaques ont montré des vulnérabilités structurelles et déclenché des réponses politiques ou doctrinales fortes qui ont contribué à définir les lignes directrices de la cyberstratégie américaine. A travers nos quatre hypothèses initiales correspondant au prisme de la cybersécurité américaine (défense, attaque, renseignement et militarisation du cyberespace), l'objectif sera de montrer par différentes études de cas les rivalités entre puissance, la vulnérabilité des infrastructures critiques, la cybercoercition et les enjeux liés à la surveillance.

## I/ Cyberattaques et rivalités entre puissances

### Stuxnet

L'opération Stuxnet est l'un des premiers exemples emblématiques d'arme numérique utilisée dans un objectif stratégique de rivalité entre puissances. Cette attaque a été lancée dans le cadre de l'opération secrète *Olympic Games*, une campagne de sabotage à distance des infrastructures du programme nucléaire iranien de Natanz, qui visait à contraindre son arrêt, ralentir le fonctionnement de la centrale de Bouchehr et éviter une intervention israélienne contre l'Iran[73]. Initiée par l'administration Bush en 2006 puis intensifiée sous l'administration Obama, cette opération était restée secrète devant la nécessité de garantir l'effet de surprise, d'éviter tout information préjudiciable à la conception et à la réalisation de l'opération et de masquer l'identité des responsables en cas d'erreurs ou de dommages collatéraux[74].
Développé conjointement par la *National Security Agency* américaine (NSA) et l'unité 8200 du Mossad, Stuxnet a été découvert par le grand public en juin 2012 par un article du New York Times : David E. Sanger, son rédacteur, s'est en effet appuyé sur des sources officielles disant que le virus avait été orchestré par les Etats-Unis et Israël[75]. Ce ver informatique ultra-

[73] DOUZET Frédérick et TAILLAT Stéphane, « Chapitre 6. Les enjeux de politique internationale L'affirmation du leadership américain ». In : TAILLAT, Stéphane, CATTARUZZA Amaël et DANET Didier, La Cyberdéfense Politique de l'espace numérique. Paris : Armand Colin. Collection U, 2018, p.111-122.
[74] VENTRE Daniel, « Le point de vue des SHS sur les opérations secrètes dans le cyberespace. Revue de littérature », Études françaises de renseignement et de cyber, 2024/2 n° 3, p.139-153.
[75] LOUIS-SIDNEY Barbara, « La dimension juridique du cyberespace ». Revue internationale et stratégique, 2012/3 n° 87, p.73-82. DOI : 10.3917/ris.087.0073.

sophistiqué, spécialement conçu pour infiltrer les systèmes de contrôle industriel et perturber le fonctionnement des centrifugeuses IR-1 sans déclencher d'alerte immédiate, est la première cyberattaque connue à avoir causé des dégâts physiques concrets à une infrastructure industrielle[76], sans destruction visible ni perte humaine directe[77]. Le développement de Stuxnet a nécessité plusieurs années de recherche, de simulations et de tests, notamment sur des centrifugeuses IR-1 obtenues via le démantèlement du programme nucléaire libyen, et que Kadhafi aurait remises en gage de son renoncement à l'arme nucléaire[78]. Il ne s'agit pas d'un *malware* diffusé de manière opportuniste : le virus a été conçu comme une arme numérique ciblée, afin de mettre en place une stratégie de sabotage camouflée[79]. Cette précision chirurgicale s'explique aussi par la volonté de limiter les dommages collatéraux. Selon Richard Clarke, le virus « avait tout l'air d'avoir été rédigé ou validé par une équipe d'avocats de Washington », du fait des nombreuses précautions prises pour garantir sa sécurité[80]. Cela est confirmé dans l'article de David Sanger, qui confirme le fait que les investigateurs du virus auraient consacré une partie non négligeable de leur temps à s'assurer que Stuxnet « ne violait pas le droit des conflits armées »[81]. Ce souci du droit montre bien la tension entre innovation technologique offensive et besoin de légitimation dans l'espace international. Même clandestinement, une cyberopérations de cette ampleur se doit de respecter les contraintes du droit international.

Pour autant, bien que camouflée, l'opération comporte aussi une dimension psychologique. Comme le souligne Olivier Kempf, la révélation de l'opération par la presse n'a rien d'anodin. En laissant fuiter certaines informations, sans les confirmer officiellement ni les démentir, l'administration usait d'une stratégie de subversion. En effet, l'enjeu était également de révéler l'action pour impressionner l'ennemi : ce qui comptait le plus n'était pas tant l'action cyber contre Natanz, mais bien la fuite d'informations organisée pour révéler la plus vaste opération qu'était « *Olympic Games* » dans le but de crédibiliser les Etats-Unis sur leurs discours de cyberdissuasion et leur détention d'armes offensives[82]. En effet, la crédibilité,

[76] AMIR-ASLANI Ardavan, « Stuxnet vs Shamoon : la cyberguerre au Moyen-Orient », Sécurité globale, 2013/2 N° 24, p.9-14.
[77] Ibid.
[78] GERGORIN Jean-Louis, « La stratégie furtive de Barack Obama : une novation majeure », Commentaire, 2012/3 Numéro 139, p.719-724.
[79] TAILLAT Stéphane, « Un mode de guerre hybride dissymétrique ? Le cyberespace », Stratégique, 2016/1 N° 111, p.89-106.
[80] RID Thomas, BUCHANAN Ben, « Attributing Cyber Attacks », Journal of Strategic Studies, 2015, 4-37.
[81] LOUIS-SIDNEY Barbara, « La dimension juridique du cyberespace ». Revue internationale et stratégique, 2012/3 n° 87, p.73-82. DOI : 10.3917/ris.087.0073.
[82] KEMPF Olivier, « Cyber et surprise stratégique », Stratégique, 2014/2 N° 106, p.111-123.

c'est la démonstration des capacités[83]. Du point de vue de l'attribution, les Etats-Unis faisaient parti des rares suspects possibles : le niveau de test sur les centrifugeuses était très avancé, très coûteux, et les machines de test presque impossibles à obtenir. Cela rendait donc l'opération pratiquement inexécutable pour des acteurs non étatiques, et seuls quelques gouvernements dans le monde disposaient des capacités techniques et industrielles nécessaires permettant de concevoir, tester et déployer un tel virus[84]. La précision du code, la connaissance technique des systèmes iraniens et l'effort de ciblage excluent en effet la piste d'un groupe indépendant, car ce niveau d'ingénierie implique un accès au renseignement industriel et une logistique complexe qui est typique des services de renseignement étatiques. Comme avec la première attaque nucléaire contre le Japon, les Etats-Unis ont donc lancé Stuxnet comme une « cyber frappe » préventive, première cyberattaque de l'Histoire[85]. Cette attaque entraîne plusieurs conclusions : tout d'abord, « les cyberattaques visant les infrastructures majeures sont une menace militaire majeure à laquelle il convient de faire face par la défense et par la dissuasion »[86]. De plus, elle montre que les Etats peuvent utiliser le cyberespace pour mener des opérations de sabotage à distance, à des fins de dissuasion, de prévention ou de coercition, grâce au recours d'armes qui permettent une action rapide, potentiellement non attribuable et qui brouille les lignes de la guerre classique. Le précédent de Stuxnet est alors devenu un cas d'école dans les doctrines de cybersécurité, et a durablement influencé les doctrines offensives américaines, notamment celles de *Defend Forward* et de *Persistent Engagement*, qui seront développées par la suite dans ce mémoire.

Finalement, ce cas montre aussi une dynamique néoréaliste claire. En effet, face à l'impossibilité de réguler collectivement le cyberespace et à l'émergence des menaces asymétriques, les Etats-Unis ont cherché à privilégier une stratégie préventive unilatérale et clandestine dans le but de préserver leur supériorité. Egalement, l'absence de cadre contraignant international, typique de l'environnement anarchique que nous avons pu analyser dans le chapitre précédent, justifie l'usage de la puissance offensive pour moduler les rapports de force. Cette logique de *self-help* que l'on retrouve régulièrement dans la stratégie américaine renforce l'idée que dans le cyberespace, comme dans les arènes classiques, la sécurité dépend de nous-même et des moyens à notre disposition.

[83] Ibid.
[84] RID Thomas, BUCHANAN Ben, « Attributing Cyber Attacks », Journal of Strategic Studies, 2015, 4-37.
[85] GERGORIN Jean-Louis, « La stratégie furtive de Barack Obama : une novation majeure », Commentaire, 2012/3 Numéro 139, p.719-724.
[86] Ibid.

## L'ingérence russe dans les élections de 2016

Bien qu'ils se trouvent parmi les principaux instigateurs de nombreuses offensives et de surveillance à l'échelle mondiale, les Etats-Unis n'en sont pas moins vulnérables et sont régulièrement visés par des attaques. Ils deviennent même en 2016 la cible d'une cyber offensive sans précédent : une ingérence stratégique et politique orchestrée soigneusement par la Russie dans le but de perturber l'élection présidentielle américaine qui se déroulait, et affaiblir les fondements démocratiques du pays.

L'ingérence est d'abord détectée par les services de renseignement américains, notamment le FBI, puis documentée dans le rapport de l'enquête dirigée par le procureur spécial Robert Mueller[87]. Cette enquête, ouverte en mai 2017 dans un fort contexte de tensions liées aux différentes accusations de soutien russe dans la victoire de Donald Trump, établit en 2019 que « le gouvernement russe a interféré dans l'élection présidentielle de 2016 de façon généralisée et systématique »[88] et débouche sur l'inculpation de six officiers des services de renseignement militaires russes[89]. L'implication du GRU (Direction principale du renseignement russe) dans cette campagne montre pour la première fois un Etat adversaire accusé publiquement d'avoir mené une offensive informationnelle d'une telle ampleur contre les processus électoraux américains[90].

L'opération d'influence de la campagne d'ingérence russe a deux axes principaux : tout d'abord, elle met en place des attaques techniques ciblant les infrastructures électorales, avec des tentatives d'intrusion dans les systèmes d'enregistrement des électeurs dans les cinquante Etats américains[91]. De l'autre côté, c'est un travail massif de manipulation informationnelle qui est orchestrée par l'Internet Research Agency (IRA), une société financée par l'oligarque russe Evgueni Prigozhin : officiellement privée mais en réalité au service du Kremlin, cette entreprise met en place dès 2014 une cellule consacrée uniquement à la politique américaine, avec pour objectif de « mener une guerre informationnelle » contre les Etats-Unis, en « répandant la menace envers les candidats et le système politique en général »[92].

---

[87] MASTOR Wanda, « Les États-Unis et le culte du secret. L'exemple du privilège de l'exécutif », Titre VII, 2023/1 N° 10, p.80-87.
[88] BORNSTEIN Roman, « Ingérence numérique, mode d'emploi », Le Débat, 2020/1 n° 208, p.42-55.
[89] CHAUVANCY François, « La guerre du futur : façonner l'environnement informationnel », Diplomatie, 2020.
[90] Ibid.
[91] BORNSTEIN Roman, « Ingérence numérique, mode d'emploi », Le Débat, 2020/1 n° 208, p.42-55.
[92] Ibid.

La stratégie de l'IRA a pour but d'utiliser contre elles la transparence des démocraties et de leurs débats, afin de créer une indignation généralisée et une spirale de haine dans la société américaine en exploitant la polarisation de la population déjà marquée. La cellule de l'IRA essaie de toucher trois catégories de population : la communauté afro-américaine, les jeunes progressistes, et les électeurs blancs conservateurs[93]. A chaque groupe sont destinés des messages contradictoires, extrêmes, via des armées de trolls, de bots, de faux profils et de publicités ciblées sur les réseaux sociaux. Dans les documents internes de l'IRA qui ont servi aux enquêtes, on peut y retrouver l'ordre de « créer de l'intensité politique en soutenant les groupes radicaux, les citoyens insatisfaits de leur situation socio-économique et les mouvements sociaux d'opposition »[94]. Par exemple, la violence policière est alternativement décrite comme un génocide contre les Noirs, ou comme une légitime défense contre la sauvagerie des gangs ; tandis que l'immigration est présentée comme un droit humain inaliénable puis comme une invasion justifiant une intervention militaire[95]. Ce procédé vise à convaincre chaque camp que l'adversaire est radicalisé, et rend donc impossible tout consensus ou débat. L'objectif final n'est donc pas spécialement d'élire un candidat, mas plutôt de rendre le pays ingouvernable.

Comme le note Julien Nocetti, les réseaux sociaux se prêtent particulièrement à cette manipulation : ils ne vérifient pas et ne hiérarchisent pas les informations qu'ils diffusent, les contenus les plus partagés n'étant pas les plus vérifiés mais les plus émotionnels[96]. Cela favorise donc la circulation rapide de rumeurs, de désinformation et de documents volés (comme les mails du Parti démocrate, rendus publiques pour créer un scandale médiatique et déstabiliser)[97]. La guerre ne se joue donc plus sur les champs de bataille traditionnels, mais dans les flux d'information qui structurent la perception collective de la réalité.

Les chiffres donnent une idée de l'ampleur de l'opération, bien que toutes les données ne soient pas toujours disponibles. En 2020, les plateformes reconnaissent avoir identifié plus de 10.4 millions de publications issues de 3 841 comptes Twitter (à présent X), 116 000 messages diffusés par 133 comptes Instagram, 8 000 publications de 470 comptes Facebook et

[93] Ibid.
[94] Ibid.
[95] Ibid.
[96] NOCETTI Julien, « La menace dans le champ cyber - Une menace multiforme et diffuse ». In : DE MONTBRIAL, Thierry et DAVID, Dominique, Ramses 2019 Les chocs du futur. Paris : Institut français des relations internationales. Ramses, 2019, p.296-299.
[97] BORNSTEIN Roman, « Ingérence numérique, mode d'emploi », Le Débat, 2020/1 n° 208, p.42-55.

1 100 vidéos par 17 chaînes Youtube[98]. L'audience estimée : 126 millions d'utilisateurs sur Facebook, 20 millions sur Instagram, 14 millions sur Twitter, et 309 000 sur Youtube[99]. Évidemment, si aucune étude ne permet de conclure que ces campagnes ont directement fait basculer le vote, elles ont tout de même incontestablement amplifié les dynamiques de polarisation, de méfiance institutionnelle et de fragmentation sociale.
Dans ce contexte, la réaction américaine montre une forte prudence stratégique. Plutôt que d'attribuer formellement l'ingérence dès 2016, l'administration Obama a opté pour des fuites contrôlées dans la presse pour signaler à Moscou que l'opération avait été détectée, sans pour autant franchir le seuil de la riposte et ainsi éviter une escalade incontrôlée[100].

Plus largement, cette ingérence montre les vulnérabilités systématiques des démocraties face à leurs adversaires et aux guerres d'influence. En effet, les Etats autoritaires peuvent exploiter la transparence des régimes libéraux ainsi que la structure ouverte du débat public pour déstabiliser la société[101]. L'attaque ne cible donc pas une infrastructure physique, mais bien un système de représentation et de légitimité : c'est une guerre cognitive, dans laquelle les citoyens deviennent involontairement les vecteurs de la menace en relayant les messages de l'adversaire[102]. La campagne russe démontre ainsi qu'une cyberattaque peut générer des fractures durables dans l'espace politique, sans pour autant laisser de traces.

[98] Ibid.
[99] Ibid.
[100] NOCETTI Julien, « Internet et sa gouvernance : La rivalité entre États-Unis et grands émergents ». In : DE MONTBRIAL, Thierry et MOREAU DEFARGES, Philippe, Ramses 2015 Le défi des émergents. Paris : Institut français des relations internationales. Ramses, 2015, p.206-209.
[101] NOCETTI Julien, « Information, désinformation : les leçons du Covid De Wuhan aux présidentielles américaines ». In : DE MONTBRIAL, Thierry et DAVID, Dominique, Ramses 2022 Au-delà du Covid. Paris : Institut français des relations internationales. Ramses, p.102-107.
[102] CHAUVANCY François, « La guerre du futur : façonner l'environnement informationnel », Diplomatie, 2020.

## II/ Cyberattaques et vulnérabilités des infrastructures critiques

Parmi les cyberattaques qui ont profondément influencé les stratégies américaines, nous pouvons en distinguer certaines par leur caractère incontrôlé et leur diffusion massive. Il s'agit d'attaques plus chaotiques, imprévisibles, souvent sans cible précise ni revendications claires, et sans logique stratégique immédiatement apparente. Lâchées dans le cyberespace, certaines de ces opérations échappent rapidement au contrôle de leurs auteurs et finissent par affecter des milliers d'acteurs publics et privés dans le monde entier, y compris ceux qui n'étaient pas du tout visés. Les cas des attaques WannaCry et NotPetya en 2017 en sont de parfaits exemples.

### WannaCry

Le 12 mai 2017, le *ransomware* WannaCry déclenche une attaque qui frappe plus de 300 000 ordinateurs dans 150 pays[103] : après pénétration dans une machine, son virus s'active et « prend en otage » les données de l'ordinateur en les chiffrant avec une clé cryptée, ce qui les rend inaccessibles[104]. L'utilisateur voit alors seulement un message porteur d'une demande de rançon, à envoyer à une adresse de paiement en monnaie virtuelle afin de garantir l'invisibilité de la transaction[105]. Ce qui rend l'attaque redoutable est sa capacité à se répliquer automatiquement d'un système à l'autre, sans intervention humaine, seulement en utilisant une faille *zero-day*[106] de Microsoft Windows. La faille avait été identifiée en secret par la NSA, qui avait développé un « exploit »[107] nommé EternalBlue afin de s'en servir pour le renseignement. Cet exploit est pourtant dérobé et publié par un groupe de hackers activistes, les Shadow Brokers, qui fusionne EternalBlue avec un ver informatique auto-répliquant afin de transformer une arme de renseignement en outil de destruction massive accessible à tous sur Internet[108].

Les conséquences de l'attaque sont quasi immédiates. La Russie est le pays le plus touché, suivi de l'Ukraine, de l'Inde et de Taïwan[109]. En Europe, c'est le système de santé

---

[103] NOCETTI Julien, « Géopolitique de la cyber-conflictualité ». Politique étrangère, 2018/2 Été, p.15-27.
[104] AMINOT Jean-Luc, « WannaCry, une frayeur à l'échelle planétaire », Annales des Mines - Responsabilité & environnement, 2020/2 N° 98, p.53-56.
[105] Ibid.
[106] Faille zero-day : faille informatique n'ayant aucune antériorité, ce qui rend très difficile la création d'une contremesure (Aminot).
[107] Exploit : élément de programmation informatique servant à exploiter une faille de sécurité dans un système (Aminot).
[108] GÉRY Aude, « La lutte contre la prolifération des armes cyber : un défi pour la stratégie française de cyberdéfense ». Les Champs de Mars, 2018/1 N° 30 + Supplément, p.307-316.
[109] AMINOT Jean-Luc, « WannaCry, une frayeur à l'échelle planétaire », Annales des Mines - Responsabilité & environnement, 2020/2 N° 98, p.53-56

britannique (NHS) qui est le plus particulièrement touché : l'infrastructure informatique de nombreux hôpitaux est paralysée, les consultations annulées et les opérations reportées, le tout avec une perte temporaire des dossiers médicaux. L'ensemble aura coûté près de 92 millions de livres sterling à la Grande-Bretagne[110].

Dès mai 2017, des chercheurs en cybersécurité informatique notaient des similarités entre le code de WannaCry et celui de Contopee, utilisé en février 2016 pour détourner des fonds de la banque centrale du Bangladesh, et attribué au groupe Lazarus, qui semblerait lié à la Corée du Nord[111]. Comme l'indique Aude Géry, ces similitudes ont par la suite été confirmées par les services de renseignement américains, bien que Pyongyang ait nié ces accusations quelques jours plus tard[112]. Si l'attribution directe à la Corée du Nord reste débattue, la logique de signature dans le code laisse tout de même planer le doute sur une opération hybride entre action étatique couverte et groupe affilié.

WannaCry illustre ainsi un phénomène de « prolifération étatique indirecte »[113] : les outils numériques offensifs conçus par des Etats sont réappropriés, modifiés puis déployés par des groupes étatiques ou non dans des objectifs de sabotage, de rançonnage ou de démonstration de force. Egalement, elle montre aussi qu'un acteur non étatique, ne disposant que de faibles ressources, peut faire peser un risque encore plus sérieux que des acteurs étatiques puissants. En effet, selon Julien Nocetti, il manque souvent à ces acteurs privés les compétences pour développer les codes sophistiqués qui permettraient de maîtriser les codes de leur *malware*[114]. Cela explique pourquoi les effets de WannaCry ont sûrement dépassé leurs intentions initiales, car sans système de contrôle des dégâts ni ciblage sélectif, l'attaque s'est propagée en touchant des secteurs critiques de manière aveugle. Finalement, cette dissémination non contrôlée de *malwares* puissants, rendus accessibles par simple téléchargement, augmente de manière considérable le risque d'escalade et d'instabilité. Elle démontre que le cyberespace est devenu un champ de confrontation où les armes numériques peuvent muter, circuler, et s'échapper du contrôle de leurs concepteurs. Pour les Etats-Unis, cette attaque est le signal qu'une arme issue de leur propre arsenal, utilisée contre eux et leurs alliés, oblige à repenser les mécanismes de sécurité, de gestion des vulnérabilités et de prévention de la prolifération.

---

[110] Ibid.
[111] GÉRY Aude, « La lutte contre la prolifération des armes cyber : un défi pour la stratégie française de cyberdéfense ». Les Champs de Mars, 2018/1 N° 30 + Supplément, p.307-316.
[112] Ibid.
[113] Ibid.
[114] NOCETTI Julien, « Géopolitique de la cyber-conflictualité ». Politique étrangère, 2018/2 Été, p.15-27.

## NotPetya

Quelques semaines seulement après WannaCry, une nouvelle attaque massive frappe l'Ukraine le 27 juin 2017. Utilisant la même faille de sécurité que le virus précédent, sa propagation et son utilisation sont pourtant différentes : en effet, NotPetya est un logiciel de type wiper, qui détruit les données des machines infectées de manière irréversible[115], dans un objectif cette fois non pas de gain financier, mais de sabotage. Les attaquants ont pris le contrôle des serveurs d'une société concevant un logiciel pour 80 % des entreprises ukrainiennes, dans le but d'y insérer un logiciel caché, plus de deux mois avant l'attaque[116]. Ce logiciel a permis de contaminer simultanément les entreprises ukrainiennes, parmi lesquelles des infrastructures critiques (banques, aéroports, énergie et télécommunications), mais également des sociétés privées internationales opérant sur le territoire, et de paralyser complètement leur activité[117]. Là encore, plusieurs entreprises mondiales s'en trouvent affectées : par la suite, l'impact économique de l'attaque sera estimé à plus de 10 milliards de dollars par la Maison Blanche[118].

Dans un contexte de tensions géopolitiques avec la Russie, l'opération est vite perçue comme une attaque spécialement ciblée contre l'Ukraine. En février 2018, les pays de l'alliance des Five Eyes (Etats-Unis, Canada, Australie, Royaume-Uni, Nouvelle-Zélande) attribuent publiquement l'attaque à la Russie[119]. Cette attribution sera lourde de sens, et permet d'inscrire NotPetya dans une stratégie de dissuasion bien plus vaste que face à une simple cybercriminalité. Elle ouvre la voie à une nouvelle doctrine, où la reconnaissance publique d'une attaque étatique sert autant à mobiliser les alliés qu'à tenter de renforcer la crédibilité des capacités de riposte.

NotPetya illustre une nouvelle dynamique : celle d'un cyberespace qui se voit comme un prolongement du champ de bataille géopolitique, où des attaques peuvent viser un Etat spécifique tout en engendrant des effets, contrôlés ou non, à l'échelle mondiale[120]. Comme le souligne Julien Nocetti, cette logique touche de plus en plus les infrastructures critiques, qui deviennent des cibles privilégiées de la guerre cyber (secteurs de l'énergie,

---

[115] PARSOIRE Didier et HÉON Sébastien, « Le prix du risque cyber ». Revue d'économie financière, 2019/1 N° 133, p.155-170.
[116] NOCETTI Julien, « La menace dans le champ cyber - Une menace multiforme et diffuse ». In : DE MONTBRIAL, Thierry et DAVID, Dominique, Ramses 2019 Les chocs du futur. Paris : Institut français des relations internationales. Ramses, 2019, p.296-299.
[117] Ibid.
[118] Ibid.
[119] NOCETTI Julien, « Géopolitique de la cyber-conflictualité ». Politique étrangère, 2018/2 Été, p.15-27.
[120] Ibid.

télécommunications, systèmes financiers, voire médias)[121]. D'autres attaques, comme le sabotage de la compagnie pétrolière saoudienne Aramco, la mise hors service du réseau ukrainien en 2015, ou encore l'attaque de TV5 Monde en 2015 également montrent une seule et même réalité : les cyberattaques ne se contentent plus de dérober l'information pour espionner, elles cherchent aussi à perturber, désorganiser, voire même détruire[122].

Cela s'inscrit dans l'évolution même des outils numériques : comme l'explique Pierre Parsoire, nous sommes passés d'un modèle de *ransomware* générique, lancé à l'aveugle dans une logique de « pêche au chalut », à des *malwares* beaucoup plus ciblés qui infectent en profondeur une victime ou un système pour atteindre les sauvegardes, perturber durablement les opérations, ou tout simplement effacer des données[123]. Cette attaque marque donc également un changement de paradigme, où la logique financière laisse place à une logique de puissance. La capacité de nuisance devient alors une arme géopolitique à part entière. Pour les Etats-Unis, cette nouvelle génération d'attaques appelle donc à renforcer les capacités de résilience des infrastructures critiques et à adapter les doctrines de réponses, non plus seulement face à des groupes criminels, mais contre des Etats utilisant le numérique comme un outil stratégique d'agression.

## III/ Cyberattaques comme outils de coercition et d'intimidation

### Attaque contre SonyPictures

L'affaire Sony Pictures en 2014 montre une autre facette de la cyberconflictualité auquel les Etats-Unis ont dû faire face : celle d'un outil d'intimidation politique, employé cette fois-ci non pas pour désorganiser un État, mais pour influencer directement une décision culturelle et médiatique et déstabiliser une entreprise privée.

[121] Ibid.
[122] NOCETTI Julien, « Géopolitique de la cyber-conflictualité ». Politique étrangère, 2018/2 Été, p.15-27.
[123] PARSOIRE Didier et HÉON Sébastien, « Le prix du risque cyber ». Revue d'économie financière, 2019/1 N° 133, p.155-170.

En novembre 2014, Sony Pictures Entertainment, un des plus grands studios de production cinématographique américain, est victime d'une cyberattaque d'une ampleur inégalée par sa violence, et par les conséquences sur la désorganisation fonctionnelle de l'entreprise, par un groupe auto-nommé Guardians of Peace (GOP)[124]. Cette attaque a lieu quelques semaines avant la sortie du film The Interview, une comédie qui mettait en scène un complot de la CIA visant à assassiner Kim Jong-Un. Dès la sortie de la bande-annonce du film le 25 juin 2014, la Corée du Nord dénonce le film comme étant une révocation, et menace de représailles s'il venait à être diffusé[125].

Les événements s'enchaînent très rapidement : fin novembre 2014, des cadres dirigeants de l'entreprise reçoivent un message de menace et de demande de rançon. Le 24 novembre, le groupe GOP lance une attaque destructrice : un *malware* efface les données et paralyse l'ensemble du système informatique du studio[126]. Des dizaines de fichiers confidentiels sont exfiltrés puis diffusés à la presse, comme des scénarios non finalisés, les salaires des stars, des correspondances internes, ou encore des numéros de sécurité sociale et de téléphone. GOP envoie des messages menaçants aux employés et aux salles de cinéma, présageant des attaques de représailles similaires aux attentats du 11 septembre 2001[127]. Après un début d'enquête, le FBI cite la Corée du Nord comme suspect potentiel. Jusqu'à mi-décembre, le groupe fera fuiter des milliers de mails internes et de documents de l'entreprise. Sous la pression, Sony annule temporairement la sortie du film. Barack Obama critique publiquement cette décision, qu'il considère comme étant un recul dangereux face à la censure et une atteinte à la liberté d'expression, et accuse directement à la télévision la Corée du Nord, bien qu'aucune preuve réelle n'ait été fournie[128]. Le film sera tout de même projeté dans quelques salles indépendantes.

Le 22 décembre, une étrange panne généralisée a lieu sur le réseau nord-coréen pendant dix heures, et se poursuit de manière récurrente les jours suivants[129]. Bien que non revendiquée par les Etats-Unis, plusieurs chercheurs pensent que cette panne était une opération de représailles, certes discrète, mais symbolique. Dès le 2 janvier 2015, Obama annonce une série de sanctions punitives contre la Corée du Nord, ce qui peut confirmer cette tentative de

[124] LEHU Jean-Marc, « Cyberattaque : la gestion du risque est-elle encore possible ? Analyse et enseignements du cas Sony Pictures », La Revue des Sciences de Gestion, 2018/3 N° 291-292, p.41-50.
[125] Ibid.
[126] LEHU Jean-Marc, « Cyberattaque : la gestion du risque est-elle encore possible ? Analyse et enseignements du cas Sony Pictures », La Revue des Sciences de Gestion, 2018/3 N° 291-292, p.41-50.
[127] Ibid.
[128] Ibid.
[129] Ibid.

représailles[130]. Dans ce cas, la riposte américaine mêle pression publique, signal stratégique et flou opérationnel qui souligne la gestion pragmatique d'une attribution incertaine, mais politiquement assumée.

Cette affaire marque un tournant dans la cyberstratégie américaine : tout d'abord à cause de la violence de l'attaque, qui aura dévoilé un total de 775 813 documents de l'entreprise[131], mais aussi par son objectif politique et symbolique, celui de faire pression sur une entreprise privée pour censurer un contenu culturel. Cette attaque révèle donc un usage du cyber comme outil d'intimidation, de propagande, voire de diplomatie parallèle, où l'information devient une arme[132]. Elle brouille également les lignes traditionnelles entre sphères publique et privée, car c'est une entreprise privée qui est visée, mais c'est l'Etat qui doit réagir, qui doit assumer l'attribution et qui doit riposter.

Pour Jean-Marc Lehu, cette attaque peut être interprétée à plusieurs niveaux : vandalisme politique, chantage idéologique, ou démonstration de force numérique[133]. Quelles que soient ses motivations profondes, elle soulève plusieurs enjeux fondamentaux, tels que la capacité à attribuer une attaque avec certitude, la responsabilité juridique transnationale, la réaction appropriée d'un Etat quand une de ses entreprises privées est visée et plus largement, la liberté d'expression face à la coercition étrangère. Le fait que le code du *malware* contienne des éléments en coréen laisse penser à une opération au moins partiellement nord-coréenne, mais aucune preuve irréfutable n'a jamais été établie[134]. Le FBI, tout en désignant la Corée du Nord, a reconnu le manque de certitudes absolues, ce qui soulève une nouvelle fois la question cruciale de la crédibilité de l'attribution et de la légitimité d'une riposte étatique.

Finalement, cette attaque souligne une ambiguïté propre à la nature même de la guerre cyber : les Etats démocratiques doivent répondre à des menaces asymétriques qui visent tant leurs valeurs que leurs entreprises, le tout sans déclencher d'escalade incontrôlée[135]. Dans ce cas précis, la Maison Blanche a choisi une riposte risquée par une attribution publique et des sanctions économiques, tout en laissant le doute sur les capacités de représailles réelles des

[130] NOCETTI Julien, « Introduction », Politique étrangère, 2018/2 Été, p.10-13.
[131] LEHU Jean-Marc, « Cyberattaque : la gestion du risque est-elle encore possible ? Analyse et enseignements du cas Sony Pictures », La Revue des Sciences de Gestion, 2018/3 N° 291-292, p.41-50.
[132] NOCETTI Julien, « Introduction », Politique étrangère, 2018/2 Été, p.10-13.
[133] LEHU Jean-Marc, « Cyberattaque : la gestion du risque est-elle encore possible ? Analyse et enseignements du cas Sony Pictures », La Revue des Sciences de Gestion, 2018/3 N° 291-292, p.41-50.
[134] NOCETTI Julien, « Introduction », Politique étrangère, 2018/2 Été, p.10-13.
[135] Ibid.

Etats-Unis. Elle incarne un exemple parfait de « red line » symbolique franchie non pas par une armée, mais par une action informationnelle visant à imposer une censure extraterritoriale. Ce cas souligne donc à quel point le cyberespace est devenu un terrain de confrontation stratégique, même autour d'enjeux qui relèvent, en apparence, du divertissement.

## IV/ Surveillance et renseignements dans la cybersécurité : l'affaire Edward Snowden

L'affaire Edward Snowden occupe une place à part dans les cyberstratégies américaines. Contrairement aux attaques précédentes, qu'elles soient menées par des acteurs étatiques ou non, cette affaire provient de l'intérieur même du système de sécurité américain. En 2013, en dévoilant l'ampleur des programmes de surveillance de la NSA, Snowden ne révèle pas seulement des outils informatiques, il expose au grand jour la mécanique stratégique du cyber espionnage américain et soulève une question cruciale : que faire lorsque la menace vient de l'intérieur du système, par un agent légitimé par l'Etat qui choisit de le défier au nom de l'éthique ?

Les documents rendus publics font notamment état du programme PRISM, un système de surveillance massive qui s'appuie sur des accords secrets entre la NSA et les GAFAM[136]. Grâce à ce programme et l'accès direct aux données des géants américains du numérique, les agences américaines interceptent en toute opacité des millions de communications, y compris celles d'acteurs gouvernementaux et de responsables politiques étrangers[137]. Cette surveillance visait à la fois des institutions internationales, des ministères, des ONG, et même des dirigeants alliés, comme la chancelière allemande Angela Merkel, dont le téléphone privé était mis sur écoute, ou la présidente brésilienne Dilma Rousseff[138]. Cette stratégie, selon plusieurs chercheurs, correspond à une logique de sécurité anticipatrice, où la connaissance totale du cyberespace devient un impératif stratégique afin de dominer les autres. Certains évoquent un basculement vers une logique de domination technologique totale par les Etats-Unis, où la NSA s'affranchit des limites territoriales, juridiques et politiques au nom de la prévention des menaces. Le programme PRISM marque donc une rupture, car il expose la contradiction du

[136] PÉTINIAUD Louis, « Cartographie de l'affaire Snowden ». Hérodote, 2014/1 n° 152-153, p.35-42.
[137] Ibid.
[138] KEMPF Olivier, « Cyberespace et dynamique des frontières », Inflexions, 2015/3 N° 30, p.141-149.

discours américain. D'un côté, il y a la promotion d'un « Internet libre » ; de l'autre, une réalité de surveillance globale panoptique[139]. Ce paradoxe fragilise la position américaine dans les forums internationaux, en particulier lorsque Washington tente de défendre une gouvernance multipartite d'Internet fondée sur la transparence, alors même que ses propres pratiques montrent une captation totale et unilatérale des flux d'informations.

Les réactions internationales sont immédiates. Snowden se voit attribuer l'asile politique dans plusieurs pays, dont la Russie, ce qui constitue un revers diplomatique majeur pour Washington[140]. La Chine laisse faire, tandis que le Brésil décide d'annuler une visite d'Etat de Dilma Rousseff à Washington et demande une réforme de la gouvernance d'Internet pour limiter la domination américaine. Du côté européen, 21 Etats de l'Union européenne rejettent sa demande du fait de leur dépendance stratégique vis-à-vis des Etats-Unis[141].

L'affaire a également un effet paralysant sur les discours internationaux sur la cybersécurité. En effet, plusieurs négociations avec la Chine sur un éventuel accord sont suspendues, et la crédibilité des Etats-Unis en tant que partenaire est sérieusement mise à mal[142]. La majorité des pays veulent d'ailleurs retirer l'ICANN de la supervision américaine, et veulent revoir le système de gouvernance d'Internet[143]. L'administration Obama ne s'excusera pas, prétextant que « cela s'est toujours fait »[144] et que « l'espionnage pour des raisons de sécurité nationale est légitime, mais pas l'espionnage économique »[145]. Ce double discours fragilise donc les relations avec la Chine et la Russie, qui sans être surprises de la stratégie américaine, vont à leur tour renforcer leurs volontés de souveraineté étatique dans le cyberespace[146]. En d'autres termes, cette crise renforcera les logiques de fragmentation du cyberespace : plusieurs puissances, comme la Chine ou la Russie, vont utiliser l'affaire Snowden pour justifier le développement de leurs ordres infrastructures numériques nationales, imposer des règles de localisation des données, et légitimer un contrôle accru des flux

[139] KEMPF Olivier, « Cyber et surprise stratégique », Stratégique, 2014/2 N° 106, p.111-123.
[140] NOCETTI Julien, « Internet et sa gouvernance : La rivalité entre États-Unis et grands émergents ». In : DE MONTBRIAL, Thierry et MOREAU DEFARGES, Philippe, Ramses 2015 Le défi des émergents. Paris : Institut français des relations internationales. Ramses, 2015, p.206-209.
[141] Ibid.
[142] LEWIS James A., « Étude préliminaire sur les analyses en cybersécurité : l'affaire Snowden comme étude de cas ». Hérodote, 2014/1 n° 152-153, p.26-34.
[143] DOUZET Frédérick et TAILLAT Stéphane, « Chapitre 6. Les enjeux de politique internationale L'affirmation du leadership américain ». In : TAILLAT, Stéphane, CATTARUZZA Amaël et DANET Didier, La Cyberdéfense Politique de l'espace numérique. Paris : Armand Colin. Collection U, 2018, p.111-122.
[144] KEMPF Olivier, « Cyberespace et dynamique des frontières », Inflexions, 2015/3 N° 30, p.141-149.
[145] Ibid.
[146] PÉTINIAUD Louis, « Cartographie de l'affaire Snowden ». Hérodote, 2014/1 n° 152-153, p.35-42.

d'information. Elle contribue également à alimenter la rhétorique d'un « Internet souverain », face à un Internet mondialisé mais contrôlé par des acteurs américains.

Plus profondément encore, l'affaire Snowden interroge sur la relation entre sécurité et liberté dans les régimes démocratiques. A quel moment la collecte préventive de données franchit-elle le seuil de la surveillance de masse ? Peut-on garantir la sécurité nationale sans aliéner les droits fondamentaux ? Finalement, comment réagir quand l'auteur d'une fuite est perçu, selon les camps, soit comme un traître, soit comme un lanceur d'alerte ?
Au sein même des Etats-Unis, certains voient Snowden comme étant un criminel ayant mis en danger la sécurité nationale, tandis que d'autres le voient comme un héros qui a révélé des pratiques en contradiction avec les valeurs démocratiques[147]. Cette polarisation montre également une fracture plus large dans les sociétés démocratiques contemporaines, où les enjeux de transparence, de contrôle citoyen et de sécurité deviennent de moins en moins réconciliables, en plus de celle d'une crise du consentement démocratique autour de l'usage des technologies de surveillance dont les modalités sont souvent décidées sans aucun débat public.

Cette affaire révèle également l'existence d'un écosystème mondial du renseignement : si les Etats-Unis sont au centre de cette toile, c'est aussi parce qu'ils contrôlent une part écrasante de l'infrastructure d'Internet, ce qui leur confère à la fois un pouvoir unique et une responsabilité qui dépasse le cadre strictement national. Mais cette centralité technique est maintenant perçue comme une vulnérabilité politique : les Etats-Unis sont obligés d'assumer la transparence, ainsi que la responsabilité qu'implique leur position de « gardien » des réseaux. Ce cas illustre par ailleurs un des paradoxes néoréalistes : pour pouvoir garantir leur sécurité sur la scène internationale, les Etats cherchent à adopter des stratégies agressives même envers leurs alliés. La surveillance globale mise en place dans ce cas d'étude montre une volonté réelle de contrôler l'environnement informationnel mondial pour dominer sur le domaine technique, mais aussi prévenir les menaces. Comme le structure la pensée néoréaliste, la méfiance est de mise, même entre partenaires, car elle est inhérente à l'anarchie du système où chaque acteur doit anticiper les risques de trahison et cherche à maximiser ses propres capacités.

[147] LEWIS James A., « Étude préliminaire sur les analyses en cybersécurité : l'affaire Snowden comme étude de cas ». Hérodote, 2014/1 n° 152-153, p.26-34.

L’analyse de l’ensemble de ces études de cas montre qu’elles ont joué un rôle important dans la stratégie américaine. En effet, chacune de ces attaques a révélé des vulnérabilités stratégiques qui ont permis aux Etats-Unis d’adapter leur réponse pour renforcer leurs capacités techniques, réorganiser leurs institutions et adopter une posture plus offensive dans le cyberespace. Toutes ces réponses montrent une logique de *self-help*, de compétition ainsi que de dissuasion, face à l’anarchie du cyberespace afin de garantir les intérêts nationaux. Egalement, les Etats-Unis ont choisi de sécuriser leur position grâce à l’accumulation de leur puissance face à l’impossibilité de se reposer sur des garanties collectives.

# Chapitre 3 – La cyberstratégie américaine : objectifs et transformation

Depuis les années 2000, le cyberespace est devenu un champ stratégique qui oppose tant les opportunités technologiques que des confrontations entre Etats. Face à la multiplication des cyberattaques, à l'intrusion incessante d'acteurs étatiques et non étatiques dans ses réseaux ainsi qu'à la dépendance accrue de ses infrastructures critiques aux nouvelles technologies, les Etats-Unis ont progressivement intégré la dimension cyber dans leur stratégie de sécurité nationale. Le cyber devient donc non seulement un outil de protection, mais aussi un outil offensif qui appuie la projection de sa puissance. La cyberstratégie américaine s'articule donc autour de deux axes : la défense, centrée sur la résilience, la prévention et la sécurisation des systèmes et infrastructures critiques ; et l'offensive dans le but de dissuader, perturber, voire neutraliser les capacités adverses. En mobilisant l'ensemble de ses agences (NSA, CISA, US Cyber Command) et en développant des doctrines spécifiques, les Etats-Unis montrent une volonté de maintenir une supériorité stratégique dans un espace où les frontières comme les règles ne sont pas clairement établies.

Dans ce dernier chapitre, nous analyserons tout d'abord la notion même d'infrastructures critiques, en définissant celles considérées comme propres aux Etats-Unis. Par la suite, nous étudierons l'évolution des différentes doctrines sous les administrations Bush (2001-2009), Obama (2009-2016), Trump (2016-2020) et Biden (2020-2024). Finalement, nous observerons la posture des Etats-Unis dans leurs alliances et dans les forums multilatéraux concernant le cyberespace.

## I/ Protection et résilience des infrastructures : un enjeu de sécurité nationale

### Définition de la notion d'infrastructure critique

La notion « d'infrastructure critique » est une notion largement développée dans les pays occidentaux, et tout particulièrement aux Etats-Unis. Pour autant, ce concept reste relativement vague, tant il tend à englober une grande variété d'éléments sans définition précise.

Aux Etats-Unis, l'expression « *critical national infrastructure* » apparaît pour la première fois dans les années 1990, à la suite d'une série d'attentats ayant marqué fortement la conscience sécuritaire du pays : l'attentat contre le World Trade Center en 1993, celui d'Oklahoma City en 1995 ainsi que l'attaque au gaz sarin dans le métro de Tokyo la même année[148]. C'est dans une *Presidential Decision Directive* que le terme est introduit, dans le but d'organiser et de structurer les politiques nationales de lutte contre le terrorisme sur le sol américain. Si la directive n'en fournit pas une définition claire et exhaustive, elle fait tout de même référence à plusieurs secteurs (aéroports, gares, routes, autoroutes, lieux de circulation de masse, installations nucléaires, et réseaux de distribution de l'énergie)[149]. C'est en 1996 que cette réflexion se structure, avec la création par le Président Bill Clinton de la *President's Commission on Critical Infrastructure Protection* (PCCIP). Cette commission part du principe que certaines infrastructures sont si vitales que « leur incapacité ou leur destruction affaiblirait considérablement la défense ou la sécurité économique des Etats-Unis »[150]. L'*Executive Order 13010*, qui officialise la mise en place de cette Commission, propose une première liste d'infrastructures critiques qu'il est nécessaire de protéger : les télécommunications, les systèmes de génération d'électricité, les systèmes de stockage et de transport du gaz et du pétrole, le secteur bancaire et financier, les transports de personnes, l'approvisionnement et distribution de l'eau, les services d'urgences (médicaux, policiers, pompiers), ainsi que les structures assurant la continuité du gouvernement[151].

Le rapport de la commission souligne également un élément fondamental : la majorité de ces infrastructures appartiennent au secteur privé. Cette réalité impose donc une collaboration étroite entre autorités publiques et acteurs privés, afin d'élaborer une stratégie nationale cohérente en faveur de la protection de ces infrastructures[152]. Le premier rapport de la PCCIP inclut donc la création d'un centre de coordination au sein du FBI, le *National Infrastructure Protection Center*, mais continue de confier aux agences et aux différents départements ministériels le soin de réaliser les études de vulnérabilité selon leurs secteurs. La collaboration entre le secteur public et le secteur privé est également encouragé par la Maison Blanche et sera approfondi dans le *Cybersecurity Information Sharing Act*, introduit en 2014 et promulgué en 2015 dans le cadre d'une volonté de renforcer la résilience et la défense en

[148] GALLAND Jean-Pierre, « Critique de la notion d'infrastructure critique », Flux, 2010/3 n° 81, p.6-18.
[149] Ibid.
[150] Ibid.
[151] Ibid.
[152] Ibid.

profondeur, en facilitant le partage d'informations entre le secteur privé et les agences gouvernementales[153]. Par ailleurs, le *Cyber Threat and Intelligence Integration Center* permet également une identification des opportunités technologiques dans le secteur privé ainsi qu'une coopération pour renforcer les capacités et la cohérence des institutions et des politiques en offrant une analyse stratégique de la menace aux décideurs politiques[154].

A la suite des attentats du 11 septembre 2001, la liste des infrastructures critiques est élargie. Elle inclut désormais les sites nucléaires, le secteur agricole ainsi que l'organisation de manifestations exceptionnelles, comme par exemple les Jeux Olympiques, considérés comme des cibles potentielles à forte visibilité[155]. En 2003, la Maison Blanche instaure une nouvelle *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, qui affine une nouvelle fois la définition des infrastructures à protéger. Ce document distingue, en plus des infrastructures critiques, les « biens clés », des sites ou objets ayant une valeur historique, culturelle, symbolique ou économique particulière. Cela comprend donc certains monuments nationaux, des sites industriels stratégiques, ainsi que les stades sportifs, considérés comme étant des lieux pouvant provoquer un fort impact psychologique en cas d'attaque.

Pour autant, il est important de noter que les réponses légales pouvant être données par le gouvernement américain en cas d'attaque touchant ses infrastructures critiques ne sont pas claires. Plusieurs chercheurs indiquent en effet que le gouvernement devrait s'appuyer sur les conséquences des actions d'acteurs non étatiques pour mener ses opérations, et dresser par la suite un cadre légal plus contraignant pour empêcher les opérations illégales sur son cyberespace[156]. Également, une zone grise persiste dans le champ juridique, particulièrement en ce qui concerne les activités menées par les services de renseignement et les agences chargées des opérations spéciales. Sous couvert de « raison d'État », qu'il s'agisse de lutte contre le terrorisme, de protection de la sécurité intérieure ou d'activités de contre-espionnage, certaines actions dans le cyberespace échappent à un cadre légal pleinement défini[157]. Cette

[153] TAILLAT Stéphane, « Cyber opérations offensives et réaffirmation de l'hégémonie américaine : une analyse critique de la doctrine de Persistent Engagement », Hérodote, 2020/2 N° 177-178, p.313-328.
[154] GUIFFARD Jonathan, « Sur les rives du Potomac, le centre du système de renseignement et de cyberdéfense des États-Unis », Études françaises de renseignement et de cyber, 2024/1 N° 2, p.43-57.
[155] Ibid.
[156] DELORS Quentin, une review de l'ouvrage « US National Cybersecurity. International Politics, Concepts and Organisation » de VAN PUYVELDE Damien et BRANTLY Aaron F., Routledge, 2017, 238p., dans Etudes Internationales, 2018, pp.435-437.
[157] MASTOR Wanda, « Les États-Unis et le culte du secret. L'exemple du privilège de l'exécutif », Titre VII, 2023/1 N° 10, p.80-87.

ambiguïté permet le recours à des opérations clandestines, parfois justifiées a posteriori par la gravité des menaces ou la nécessité d'une réponse rapide. Dans ce contexte, le cyberespace devient un terrain d'action privilégié pour des interventions à faible visibilité, difficilement attribuables, et qui brouillent les frontières entre la guerre, le renseignement et la sécurité intérieure.

## Création et renforcement des institutions liées à la cybersécurité

La prise de conscience progressive de la vulnérabilité des infrastructures critiques a ainsi amené les autorités américaines à élargir leur périmètre de protection. Mais à mesure que les menaces se sont déplacées vers le cyberespace, notamment avec l'essor d'Internet et la multiplication des cyberattaques, il est rapidement apparu que la protection physique seule ne suffisait plus. La sécurisation des systèmes numériques, devenus les véritables nerfs vitaux de ces infrastructures, est maintenant devenu une priorité stratégique. Cette évolution a entraîné la création de nouvelles institutions spécialisées et le renforcement progressif de l'architecture déjà existante des politiques nationales de cybersécurité, dans un but d'assurer à la fois la résilience et la défense active des systèmes critiques.

Le système américain de cybersécurité repose sur une pluralité d'agences, réparties entre les sphères civile et militaire, avec une forte composante relevant du renseignement. Plusieurs acteurs sont en première ligne : le *Department of Homeland Security* (DHS), la *Cybersecurity and Infrastructure Agency* (CISA), mais surtout les agences de renseignement qui vont jouer un rôle central dans l'identification, l'attribution et la neutralisation des cybermenaces. Parmi celles-ci, nous pouvons citer la *Central Intelligence Agency* (CIA). Bien qu'historiquement centrée sur le renseignement humain, la CIA a développé de nombreuses capacités en matière de cyberespionnage offensive, notamment via son *Directorate of Digital Innovation* créé en 2015[158]. Même si la CIA a un rôle dans le cyberespace moins central, elle reste tout de même plus autonome que d'autres agences sur le sujet et offre de nombreuses capacités d'innovation dans le domaine numérique, notamment pour soutenir ses missions de collecte et d'exploitation du renseignement à l'étranger, mais aussi mener des opérations clandestines par des moyens cyber[159]. Néanmoins, comme l'indique Stéphane Taillat,

[158] GUIFFARD Jonathan, « Sur les rives du Potomac, le centre du système de renseignement et de cyberdéfense des États-Unis », Études françaises de renseignement et de cyber, 2024/1 N° 2, p.43-57.
[159] Ibid.

« prévenir, gérer et répondre aux menaces de l'espace numérique est le domaine de toute l'administration américaine, mais particulièrement le *Department of Defense* (DoD) »[160]. En effet, la moitié des dépenses dans le secteur cyber sont assurées par le DoD pour les années les 2017, 2018 et 2019, ce qui représente environ 8.5 milliards de dollars sur une totalité de 15 milliards de dollars[161]. L'année suivante, la part des dépenses du DoD dans le secteur cyber correspondaient à 9.6 milliards de dollars sur 17 milliards de dollars[162].

La *National Security Agency* (NSA), créée en 1952, a longtemps été l'acteur central de la cybersécurité offensive et défensive aux Etats-Unis. Jusqu'à la montée en puissance de structures spécialisées, comme l'*US Cyber Command* (USCYBERCOM) à partir de 2010, elle a joué un rôle prédominant au sein du DoD, notamment grâce à ses moyens humains et financiers considérables, ainsi qu'à son influence dans l'élaboration des doctrines cyber américaines[163]. Sa mission s'articule autour de plusieurs fonctions[164] : fournir du renseignement pour anticiper les menaces cyber et éclairer les décisions politiques du gouvernement fédéral ; identifier les vulnérabilités des systèmes sensibles (notamment ceux liés au commandement nucléaire) ; développer des solutions cryptographiques à haut niveau de sécurité ; concevoir des produits intégrés d'évaluation, de protection et d'atténuation à destination du DoD et d'autres agences fédérales. Elle mène également des opérations défensives, dans le prolongement de la mission du *Computer Security* qu'elle détient depuis la fin des années 1960, et offensives, dont l'interception de signaux électromagnétiques (comme l'interception passive de flux de données et une collecte active de renseignement sur les systèmes d'information adverses), en coordination avec d'autres partenaires gouvernementaux[165].

[160] TAILLAT Stéphane, « La cyberdéfense américaine à l'âge de Donald Trump », Questions internationales, 2019/3 n°98, p.88-96.
[161] Ibid.
[162] Ibid.
[163] Ibid.
[164] National Security Agency, « NSA Cybersecurity », National Security Agency.
[165] GUIFFARD Jonathan, « Sur les rives du Potomac, le centre du système de renseignement et de cyberdéfense des États-Unis », Études françaises de renseignement et de cyber, 2024/1 N° 2, p.43-57.

A partir de 2010, le gouvernement veut sortir les capacités militaires d'attaque et de défense du cyberespace américain hors de la seule sphère du renseignement[166]. Le *US Cyber Command* (USCYBERCOM) est donc créé afin de fusionner l'ensemble des entités de cyberdéfense du DoD. La NSA n'est pas intégrée à cette nouvelle unité, en raison de son rôle historique et de son importance bureaucratique : l'officier général chargé de l'USCYBERCOM est donc également le directeur de la NSA[167]. Pour autant, l'USCYBERCOM a pour mission de défendre les réseaux du DoD et de mener des opérations dans le cyberespace, notamment en soutien à des opérations militaires conventionnelles ou en contribuant à la défense des infrastructures critiques américaines[168].

Élevé au statut de commandement autonome en 2018, l'USCYBERCOM est la pièce maîtresse du DoD sous l'administration Trump, dans la logique de cette dernière de rompre avec les hésitations des administrations précédentes et en adéquation avec les documents de stratégie nationale et de défense sortis la même année. Le but de cette stratégie est de revenir à une compétition entre grandes puissances, tout en réaffirmant la puissance américaine[169]. Dans un document programmatique de 2018, l'USCYBERCOM préconise des actions constantes pour maintenir la supériorité des Etats-Unis en toutes circonstances[170]. Dans un autre document, appelé « Atteindre et maintenir la supériorité dans le cyberespace », l'entité montre que les Etats-Unis ont perdu l'initiative face à leurs adversaires car ils refusaient d'aborder la conflictualité numérique comme un engagement persistant. L'agence conclut son rapport en disant qu'elle doit « reprendre l'initiative pour atteindre une supériorité opérationnelle (une liberté d'action) et une « persistance » (sa capacité d'anticipation des menaces) »[171]. L'USCYBERCOM est donc l'instrument de cette posture offensive des Etats-Unis et de cette notion de combat permanent pour conserver l'avantage, que nous observerons par la suite dans les différentes doctrines mises en place.

---

[166] Ibid.
[167] TAILLAT Stéphane, « Cyber opérations offensives et réaffirmation de l'hégémonie américaine : une analyse critique de la doctrine de Persistent Engagement », Hérodote, 2020/2 N° 177-178, p.313-328.
[168] TAILLAT Stéphane, « La cyberdéfense américaine à l'âge de Donald Trump », Questions internationales, 2019/3 n°98, p.88-96.
[169] Ibid
[170] DOUZET Frédérick et TAILLAT Stéphane, « Chapitre 6. Les enjeux de politique internationale L'affirmation du leadership américain ». In : TAILLAT, Stéphane, CATTARUZZA Amaël et DANET Didier, La Cyberdéfense Politique de l'espace numérique. Paris : Armand Colin. Collection U, p.111-122.
[171] TAILLAT Stéphane, « Cyber opérations offensives et réaffirmation de l'hégémonie américaine : une analyse critique de la doctrine de Persistent Engagement », Hérodote, 2020/2 N° 177-178, p.313-328.

Par ailleurs, la réponse américaine aux cybermenaces se heurte à d'importantes difficultés de coordination. Malgré la multiplication des agences impliquées, la fragmentation des compétences entre les entités civiles, militaires et de renseignement génère souvent des doublons, des rivalités institutionnelles et des lenteurs bureaucratiques[172]. Cette dispersion des initiatives empêche une efficacité globale du dispositif, d'autant que les risques d'empiètement entre agences sont fréquents (en particulier dans les domaines sensibles comme l'attribution des attaques ou la conduite des réponses offensives). Ces challenges structurels soulignent ainsi la nécessité, régulièrement rappelée par les experts et les responsables politiques, d'une gouvernance plus intégrée et d'une articulation plus cohérente entre les différents échelons de la cyberstratégie américaine[173].

## II/ Évolution des doctrines de 2001 à 2024 : la militarisation du cyberespace

Afin de comprendre l'évolution de la politique de sécurité nationale des Etats-Unis, en particulier en ce qui concerne leur approche au niveau du cyberespace, il est utile de revenir à une typologie proposée par l'ancien secrétaire adjoint à la Défense américaine Lawrence J. Korb[174]. Il identifie en effet trois écoles de pensée qui structurent les débats sur la sécurité nationale aux Etats-Unis.

### Administration Bush : de 2001 à 2009

La première école, souvent associée aux néoconservateurs, met l'accent sur le renforcement de l'hégémonie américaine. Elle préconise l'usage de la force pour lutter contre les menaces, y compris de manière préventive, notamment dans le cadre de la guerre contre le terrorisme, les Etats « voyous » et les armes de destruction massive[175]. Par ailleurs, elle considère aussi que les Etats-Unis doivent assumer ce rôle de puissance dominante, et qu'ils doivent diffuser leur modèle politique, et ce par la force si nécessaire. Un parfait exemple de

[172] JACKSON Michael J., LIEBER Paul, « Countering Disinformation : Are We Our Worst Enemy ? », The Cyber Defense Review, 2020/5.
[173] TAILLAT Stéphane, « Cyber opérations offensives et réaffirmation de l'hégémonie américaine : une analyse critique de la doctrine de Persistent Engagement », Hérodote, 2020/2 N° 177-178, p.313-328.
[174] KORB Lawrence J., traduit de l'anglais par DE POORTÈRE Aurélie, « La stratégie de sécurité nationale du président Obama ou la fin de l'ère Bush », Politique américaine, 2010/2 N° 17, p.13-26.
[175] Ibid.

cette école peut se trouver dans l'administration Bush (2001-2009). En effet, au lendemain des attentats du 11 septembre 2001, l'administration Bush élabore une doctrine de sécurité fondée sur la primauté militaire, la prévention stratégique ainsi que sur l'affirmation d'un *leadership* unilatéral, sans nécessairement recourir à l'approbation d'alliés ou d'organisations internationales[176]. Comme le témoignent la création de l'Office de la Sécurité intérieure de la Maison Blanche quelques jours après les attentats, dans un but de « coordonner les efforts pour protéger les Etats-Unis et ses infrastructures critiques des conséquences des attaques terroristes », et la création du *Department of Homeland Security* (DHS) dont une des priorités est alors l' « analyse des informations et la protection des infrastructures », nous pouvons voir que la vulnérabilité des infrastructures critique est peu à peu érigée en concept incontournable pour l'appréhension des catastrophes, qu'elles soient d'ordre naturel ou technologique[177].

Dans ce contexte, bien que les doctrines spécifiques sur le cyberespace restent très limitées, il y a une prise de conscience de cet espace comme étant un espace de conflictualité potentielle. L'administration Bush intègre donc l'idée d'un ennemi déterritorialisé, insaisissable, qui va détourner les technologies de la mondialisation pour désinformer, saboter et mobiliser. Comme l'exprime alors Bush lui-même, la « nouvelle guerre mondiale » serait longue et multiforme, et utiliserait à la fois des drones, des missiles de précision, mais aussi des moyens invisibles ou non conventionnels[178]. Cette vision se reflète dans les premiers documents stratégiques de l'ère post-11 septembre, comme la *National Security Strategy* de 2002 ou les premières réflexions sur la cybersécurité nationale à partir de 2003-2004. En 2003, l'administration Bush commence à formaliser les contours d'une politique cyber en publiant le *National Strategy to Secure Cyberspace*, qui identifie déjà les infrastructures critiques comme des cibles vulnérables[179]. Ces essais restent toutefois largement secondaires par rapport à la doctrine de guerre contre le terrorisme[180], dans laquelle le cyberespace est envisagé comme un nouvel espace de compétition et de conflits.

[176] MILLIÈRE Guy, « Ce que veut Bush : recomposer le monde », Outre-Terre, 2003/4 no 5, p.17-25.
[177] GALLAND Jean-Pierre, « Critique de la notion d'infrastructure critique », Flux, 2010/3 n° 81, p.6-18.
[178] Ibid.
[179] The White House, « National Strategy to Secure Cyberspace », 2003, Department of Energy.
[180] SPYROPOULOS Georgios., « L'influence de Thucydide et de Démosthène Sur La Politique Étrangère Des USA », Diplomatie, 2010/43, 74–84.

En parallèle, les doctrines militaires s'adaptent : le DoD adopte dès 1998 la doctrine interarmées *Information Operations*, par la suite régulièrement révisée (en 2006, 2012 et 2014 notamment), qui insiste sur l'intégration des champs électromagnétique, électrique et psychologique, soit les couches physiques, informationnelles et cognitives du conflit, dans les politiques de défense et de sécurité nationale[181]. Ce cadre montre une militarisation croissante du cyberespace qui s'accélèrera dès les années 2000 et anticipera des pratiques qui se systématiseront par la suite : espionnage numérique, sabotage d'infrastructures, ou encore opérations d'influence, tant par des acteurs étatiques que non-étatiques[182].

Par la suite, des pratiques telles que le piratage à des fins d'extraction de données (*collection*) et pour faciliter les opérations futures (*enabling operations*) seront assimilées à des actes d'espionnage entre Etats[183]. Cela permettra aux Etats-Unis de développer une base doctrinale pour étendre leurs activités d'augmentation de collecte et de surveillance par le biais de la NSA et la CIA. Bien que l'espionnage en temps de paix ne soit pas explicitement prohibé par le droit international, il soulève néanmoins des ambiguïtés juridiques et stratégiques. En effet, certaines opérations de renseignement peuvent facilement être interprétées comme des actes de perturbation, voire de destruction, brouillant ainsi la frontière entre espionnage et attaque[184]. Les opérations seront tant « clandestines », cherchant à dissimuler les tactiques de l'intervention, que « couvertes » (*covert actions*). La distinction, comme le soulignera le DoD, ne tient plus qu'à la dissimulation de l'intention ou de l'auteur, ce qui introduit une zone grise permanente dans les opérations cyber[185].

[181] DOUZET Frédérick et TAILLAT Stéphane, « Chapitre 6. Les enjeux de politique internationale L'affirmation du leadership américain ». In : TAILLAT, Stéphane, CATTARUZZA Amaël et DANET Didier, La Cyberdéfense Politique de l'espace numérique. Paris : Armand Colin. Collection U, p.111-122.
[182] Ibid.
[183] Ibid.
[184] Ibid.
[185] VENTRE Daniel, « Le point de vue des SHS sur les opérations secrètes dans le cyberespace. Revue de littérature », Études françaises de renseignement et de cyber, 2024/2 n° 3, p.139-153.

## Administration Obama : de 2009 à 2016

La présidence Obama (2009-2016) va s'inscrire dans ce que Korb identifie comme étant la deuxième école de pensée. Celle-ci cherche à œuvrer à la stabilité du monde, en utilisant la supériorité militaire comme moyen de dissuasion et d'endiguement. Elle considère également, comme la première école, que le terrorisme, les Etats « voyous » et les armes de destruction massives sont les menaces les plus sérieuses pour les Etats-Unis[186]. Pour autant, il est dit que ces menaces ne peuvent pas être gérées sur tous les fronts, ni à tout moment, par la force militaire : il faut alors recourir à un mélange entre hard et soft power avec l'appui de la communauté internationale. Le but est de permettre sur du long terme de contenir et de dissuader les menaces avant d'envisager le recours à la force militaire, tout en installant une paix stable et durable grâce à la coopération internationale[187].

Le gouvernement Obama internationalise le réseau Internet. En effet, dès 2010, les codes des noms de domaines internationaux peuvent dès lors être écrits en alphabets arabe, cyrillique et chinois[188]. D'autre part, l'administration renforce progressivement la structuration institutionnelle de la cyberstratégie américaine, avec pour objectif de développer une posture dite de « défense active » (*Active Defense*). Celle-ci vise à défendre en interne les infrastructures du DoD tout en soutenant les opérations extérieures dans le cyberespace[189]. Cette orientation se formalise avec tout d'abord la *Presidential Policy Directive 21* (PPD-21) et le *National Infrastructure Protection Plan*, qui élèvent la protection des infrastructures critiques au plus haut rang de priorité stratégique nationale[190]. La PPD-21 réorganise également la coordination entre différents niveaux d'acteurs, qu'ils soient fédéraux, fédérés, locaux, publics et privés, en plaçant le DHS au centre du dispositif de gestion des risques[191]. Par ailleurs, en 2011, la publication de la *International Strategy for Cyberspace* reflète la volonté des Etats-Unis de promouvoir un cyberespace qui soit à la fois sûr, ouvert et interopérable, tout en affirmant leur intention de le défendre activement par des moyens dissuasifs, y compris le recours à des capacités offensives si nécessaire. Le processus décisionnel implique également

[186] KORB Lawrence J., traduit de l'anglais par DE POORTÈRE Aurélie, « La stratégie de sécurité nationale du président Obama ou la fin de l'ère Bush », Politique américaine, 2010/2 N° 17, p.13-26.
[187] KORB Lawrence J., traduit de l'anglais par DE POORTÈRE Aurélie, « La stratégie de sécurité nationale du président Obama ou la fin de l'ère Bush », Politique américaine, 2010/2 N° 17, p.13-26.
[188] DOUZET Frédérick et TAILLAT Stéphane, « Chapitre 6. Les enjeux de politique internationale L'affirmation du leadership américain ». In : TAILLAT, Stéphane, CATTARUZZA Amaël et DANET Didier, La Cyberdéfense Politique de l'espace numérique. Paris : Armand Colin. Collection U, p.111-122.
[189] TAILLAT Stéphane, « Cyber opérations offensives et réaffirmation de l'hégémonie américaine : une analyse critique de la doctrine de Persistent Engagement », Hérodote, 2020/2 N° 177-178, p.313-328.
[190] Ibid.
[191] Ibid.

un dialogue inter-agences et inter-ministériel, afin de minimiser les risques induits par les opérations numériques (dommages collatéraux, interférences avec les opérations de renseignement…)[192].

On observe alors un double mouvement dans la posture américaine vis-à-vis du cyberespace. D'un côté, l'administration Obama soutient la coopération internationale à travers la mise en œuvre de conditions structurelles favorables, comme la promotion de l'innovation numérique, le dialogue entre acteurs publics et privés, ainsi que la collaboration entre les différentes grandes plateformes numériques[193]. Plutôt que d'imposer un contrôle direct, perçu comme intrusif et très sensible d'un point de vue politique, le but est également de privilégier des mécanismes de régulation souple ainsi qu'une prévention des conflits par des cadres structurels collectifs[194]. D'un autre côté, le développement des capacités offensives se poursuit. Comme le montrent les révélations d'Edward Snowden en 2013 que nous avons pu évoquer précédemment sur les pratiques de la NSA (surveillance massive et exploitation de failles), la puissance américaine repose aussi sur une maîtrise totale et opaque du cyberespace afin de pleinement conserver l'avantage stratégique par un accès privilégié et discret aux flux numériques mondiaux. Obama institutionnalise également la cyberdissuasion : en 2015, l'*Executive Order 13694* ouvre la voie à des sanctions ciblées contre des acteurs du cyberespace hostiles, qu'ils soient étatiques ou non[195]. Cette stratégie de punition fait du cyber un outil à la fois diplomatique et stratégique, intégré à la politique de puissance. Comme nous l'avons précédemment analysé avec l'attaque contre SonyPictures en 2014, l'administration utilise également les outils juridiques, économiques et symboliques comme instruments de dissuasion. Le Pentagone recommande par ailleurs d'adopter une posture dissuasive à l'égard des adversaires numériques, combinant interdictions claires et menaces de représailles[196]. Depuis 2014, les Etats-Unis ont ainsi pris une série de mesures pour affirmer leur volonté de faire cesser les cyberattaques hostiles : inculpation de hackers affiliés à des États ; sanctions ciblées contre des individus ou des entités ; campagnes d'attributions publiques d'attaques ou encore évocations explicites de potentielles réponses militaires[197].

---

[192] TAILLAT Stéphane, « La cyberdéfense américaine à l'âge de Donald Trump », Questions internationales, 2019/3 n°98, p.88-96.
[193] DOUZET Frédérick et TAILLAT Stéphane, « Chapitre 6. Les enjeux de politique internationale L'affirmation du leadership américain ». In : TAILLAT, Stéphane, CATTARUZZA Amaël et DANET Didier, La Cyberdéfense Politique de l'espace numérique. Paris : Armand Colin. Collection U, p.111-122.
[194] Ibid.
[195] Ibid.
[196] Ibid.
[197] Ibid.

## Administration Trump : de 2016 à 2020

Sous la première administration Trump, la stratégie au sein du cyberespace change d'échelle. Alors que les doctrines précédentes restaient relativement prudentes et opéraient une politique de dissuasion classique, l'approche adoptée par l'administration Trump s'inscrit dans une logique offensive plus assumée et compétitive, qui vise un retour à la compétition entre grandes puissances, à une hégémonie absolue des Etats-Unis, et une domination stratégique. Ce changement est formalisé par la publication de la *National Cyber Strategy* de 2018, qui vise à rompre avec la modération des administrations précédentes. Comme l'indique Mike Pence, alors vice-Président sous Donald Trump : « Loin sont les jours où les Etats-Unis laissaient leurs adversaires s'en prendre à eux en toute impunité », avant d'ajouter que « la sécurité américaine dominera tout autant dans le domaine numérique que dans le domaine physique »[198]. Cette approche proactive des Etats-Unis, où la stratégie de persévérance et de confrontation continue, doit permettre de contrer les menaces à leur source et d'augmenter la sécurité du pays tout en confortant leur position stratégique. Pour l'administration Trump, il ne s'agit plus de regarder l'ascension des compétiteurs (la Chine et la Russie), ni de se laisser faire par les perturbateurs (l'Iran et la Corée du Nord)[199]. Il faut donc reprendre l'initiative perdue par les « faiblesses supposées de l'administration Obama » et répondre dès maintenant aux adversaires concernant les risques qu'ils font peser sur l'équilibre stratégique[200]. La société internationale est également perçue comme un jeu à somme nulle entre grandes puissances, et dans lequel les Etats-Unis devraient profiter de leur position au sommet de la hiérarchie[201].

Cette approche se caractérise donc par deux doctrines, mises en place à partir de 2018 : la doctrine du *Defend Forward* et du *Persistent Engagement*. Ces nouvelles stratégies sont ancrées dans le besoin « d'agir dans le cyberespace dans une compétition quotidienne afin de préserver les avantages militaires des États-Unis et de défendre les intérêts américains »[202]. Il ne s'agit donc plus de réagir ou de dissuader, mais bien de contester l'adversaire en continu pour conserver une initiative stratégique.

---

[198] TAILLAT Stéphane, « Cyber opérations offensives et réaffirmation de l'hégémonie américaine : une analyse critique de la doctrine de Persistent Engagement », Hérodote, 2020/2 N° 177-178, p.313-328.
[199] Ibid.
[200] Ibid.
[201] DOUZET Frédérick et TAILLAT Stéphane, « Chapitre 6. Les enjeux de politique internationale L'affirmation du leadership américain ». In : TAILLAT, Stéphane, CATTARUZZA Amaël et DANET Didier, La Cyberdéfense Politique de l'espace numérique. Paris : Armand Colin. Collection U, p.111-122.
[202] CORN Gary P., RENALS Peter, « Scenarios for Defend Forward ». IN : GOLDSMITH Jack, The United States' Defend Forward Cyber Strategy : A Comprehensive Legal Assessment. Oxford University Press, 2022, 357p., pp.24- 31.

1. La doctrine de *Persistent Engagement*

La doctrine de *Persistent Engagement* est officiellement formulée pour la première fois dans un rapport de l'USCYBERCOM en 2018[203], qui affirme que la « supériorité par la persistance s'obtient en saisissant et en conservant l'initiative dans le cyberespace, en engageant et en contestant continuellement les adversaires et en leur causant de l'incertitude, où qu'ils manoeuvrent »[204]. Cette doctrine repose sur la nécessité de répondre de manière proactive aux menaces cyber en menant des opérations offensives continues, afin de perturber l'adversaire en amont et d'empêcher sa liberté d'action[205].

Sous l'administration Trump, cette doctrine incarne une « théorie de la victoire » et une restructuration de la cyberstratégie américaine[206]. Déjà amorcée par l'administration Obama, la doctrine est infléchie sous Trump avec une intensification et une systématisation des réponses aux attaques numériques subies par les Etats-Unis. Cela se traduit notamment par une politique d'exposition et de punition des auteurs supposés d'activités malveillantes[207]. En 2019, l'administration Trump a ainsi procédé à sept mises en accusation d'individus et d'entités associés à la Russie, la Chine, l'Iran, et la Corée du Nord. Depuis 2017, une dizaine d'annonces de sanctions ont été annoncées sur la même période contre des hackers coréens supposés, dans la lutte contre les Gardiens de la révolutions iraniens et pour l'interférence russe dans les élections de 2016[208].

La Chine, bien que régulièrement accusée d'activités de cyberespionnage, n'a toutefois pas fait l'objet de sanctions économiques directes, en raison des risques de représailles sur les entreprises occidentales entretenant des relations contractuelles avec des sociétés chinoises[209]. Pour autant, dès 2015, un décret présidentiel d'Obama (13694) induisait que les sanctions seraient « contre des auteurs d'activités malveillantes (…) susceptibles de constituer une menace pour la sécurité nationale ». Après l'ingérence de la Russie en 2016, ce décret est complété par le décret présidentiel 13757, qui y ajoute des clauses contre les entraves et sabotages dans le cadre des processus électoraux[210].

---

[203] Ibid.
[204] Ibid.
[205] CORN Gary P., RENALS Peter, « Scenarios for Defend Forward ». IN : GOLDSMITH Jack, The United States' Defend Forward Cyber Strategy : A Comprehensive Legal Assessment. Oxford University Press, 2022, 357p., pp.24- 31.
[206] TAILLAT Stéphane, « Cyber opérations offensives et réaffirmation de l'hégémonie américaine : une analyse critique de la doctrine de Persistent Engagement », Hérodote, 2020/2 N° 177-178, p.313-328.
[207] Ibid.
[208] Ibid.
[209] Ibid.
[210] Ibid.

Malgré ce durcissement doctrinal, comme la majorité des attaques sont sous le seul de l'agression, elles déjouent les stratégies visant à les prévenir et à y répondre. La dissuasion est donc considérée comme insuffisante pour les prévenir[211]. Dans ce contexte, la doctrine de *Persistent Engagement* s'affirme comme une alternative aux deux logiques traditionnelles : l'usage ponctuel de la force militaire d'un côté, et la dissuasion nucléaire de l'autre. Elle vise à multiplier les effets coercitifs des menaces militaires, des avertissements diplomatiques et des sanctions économiques, ce qui converge avec la logique stratégique de rétablissement de la supériorité américaine. Elle contraste également avec les stratégies de 2011 et de 2015 sous l'administration Obama, qui souhaitaient respectivement une « option de réponse crédible » pour dissuader, basée sur des menaces de représailles une fois les limites dépassées, et cherchaient une stratégie de cyberdissuasion pour empêcher les autres Etats et acteurs non étatiques de promulguer des cyberattaques contre les intérêts des Etats-Unis[212], en réaffirmant haut et fort que les Etats-Unis reprenaient la main sans passer à l'agression armée[213].

Cependant, cette doctrine présente plusieurs limites : l'ambiguïté de ses objectifs et l'absence de précédents clairs rendent son efficacité difficile à évaluer. Elle peut également servir de justification à d'autres Etats ou groupes sponsorisés, dont les capacités à infliger des dommages semblent augmenter. En outre, la doctrine implique le développement de procédures de ciblage numérique sophistiquées et le recours à des arsenaux de *malware* ou de failles zero-*day*, qui, en cas de prolifération ou de perte de contrôle, pourraient alimenter une escalade incontrôlée. Ce risque est d'autant plus préoccupant que les dommages collatéraux sont difficilement prévisibles dans un espace aussi interconnecté et instable que le cyberespace.

### *2.* La doctrine du *Defend Forward*

En parallèle de la doctrine de *Persistent Engagement*, la stratégie américaine s'est aussi dotée d'un autre pilier conceptuel majeur : la doctrine du *Defend Forward*. Formulée pour la première fois en 2018 dans le même rapport de l'USCYBERCOM qui présente la doctrine précédente[214], cette approche vise à « augmenter la résilience, défendre en avant et contester

[211] Ibid.
[212] CORN Gary P., RENALS Peter, « Scenarios for Defend Forward ». IN : GOLDSMITH Jack, The United States' Defend Forward Cyber Strategy : A Comprehensive Legal Assessment. Oxford University Press, 2022, 357p., pp.24- 31.
[213] TAILLAT Stéphane, « La cyberdéfense américaine à l'âge de Donald Trump », Questions internationales, 2019/3 n°98, p.88-96.
[214] CORN Gary P., RENALS Peter, « Scenarios for Defend Forward ». IN : GOLDSMITH Jack, The United States' Defend Forward Cyber Strategy : A Comprehensive Legal Assessment. Oxford University Press, 2022, 357p., pp.24- 31.

les adversaires »[215]. Cette fois-ci, la doctrine s'appuie la nécessité de confronter les menaces cyber directement à leur source, avant qu'elles n'atteignent les réseaux ou les infrastructures critiques américaines. Comme le définit explicitement le rapport annuel de l'USCYBERCOM de 2018, il s'agit de « perturber ou stopper une activité cyber malveillante à sa source, y compris lorsqu'elle demeure en dessous du seuil de conflit armé »[216].

La doctrine de *Defend Forward* s'inscrit donc dans une posture intermédiaire, adaptée aux conflits de « zone grise », où les activités hostiles sont calibrées pour rester sous le seuil juridique et politique de l'agression armée. Elle permet à l'armée américaine et aux agences de renseignement de mener des opérations de perturbation ciblée, de dégrader les capacités adverses et de faire une collecte de renseignement anticipée, notamment par l'infiltration discrète des réseaux étrangers[217]. Ces activités consistent à « préparer le champ de bataille » numérique, parfois de manière préemptive, en accédant à des infrastructures étrangères avant même l'éclatement d'un conflit, dans une logique de surveillance et de préparation stratégique[218]. Concrètement, *Defend Forward* a été mis en œuvre dans des opérations précises : par exemple, dès 2018, des équipes de l'USCYBERCOM ont été déployées en Ukraine, en Estonie et au Monténégro pour identifier les modes opératoires des cyberacteurs russes, anticiper leurs actions et renforcer la résilience des systèmes locaux[219]. Ces *hunt forward missions* (missions de chasse en avant) permettent une interaction directe avec les cybermenaces dans des espaces tiers, avant qu'elles ne puissent être redirigées contre les intérêts américains.

Sous l'administration Trump, ces doctrines constituent un « tournant dans l'approche du Département de la Défense vis-à-vis de la compétition stratégique et des menaces cyber, élargissant leur attention au-delà de la planification traditionnelle en temps de guerre pour inclure la réalité de campagnes hostiles permanentes dans le cyberespace »[220]. Ce changement doctrinal correspond donc à la reconnaissance de la nature continue et diffuse des cyberconflits modernes, dans lesquels les Etats-Unis sont engagés quotidiennement sans déclaration officielle de guerre.

---

[215] Ibid.
[216] Ibid.
[217] VALERIANO Brandon, JENSEN Benjamin et MANESS Ryan C., « Cyber Strategy: The Evolving Character of Power and Coercion ». Oxford : Oxford University Press, 2021.
[218] HEALEY Jason, « The Implications of Persistent (and Permanent) Engagement in Cyberspace ». Atlantic Council, 2020.
[219] LIN Herb, ZEGART Amy B. (dir.), « Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations ». Washington, D.C. : Brookings Institution Press.
[220] BORGHARD Erica D., SCHNEIDER Jacquelyn G., « Defending Forward: The 2018 Cyber Strategy is a Step in the Right Direction », War on the Rocks. 2018.

Cette posture, bien que défensive dans ses justifications, s'apparente souvent à une stratégie offensive préventive, ce qui soulève plusieurs interrogations éthiques et juridiques. Comme l'analysent Michael Fischerkeller et Richard Harknett, deux architectes intellectuels de la doctrine, cette approche repose sur une forme de compétition continue, où le contrôle du temps et de l'initiative stratégique devient plus important que l'usage ponctuel de la force. Elle incarne une volonté de rétablir une supériorité stratégique permanente en perturbant systématiquement les capacités adverses[221].

Cependant, comme pour *Persistent Engagement*, des critiques émergent concernant l'ambiguïté des objectifs, la difficulté d'évaluer l'efficacité de ces stratégies, et le risque de prolifération incontrôlée des outils numériques utilisés (*malwares*, failles *zero-day*). L'extension des opérations à des réseaux tiers ou non belligérants pose aussi des problèmes de souveraineté numérique, de transparence et de proportionnalité. Enfin, le fait que ces doctrines soient menées en grande partie par des agences militaires et de renseignement, sans véritable supervision parlementaire ou débat public, soulève des enjeux démocratiques majeurs.

Pour autant, l'élévation de l'USCYBERCOM au rang de commandement, le renforcement des capacités de la NSA et l'affirmation du recours systématiques aux opérations offensives montrent que l'administration Trump cherche à entrer dans le cyberespace de manière offensive, dissuasive et autonome. Le cyberespace devient donc un levier central de la politique de puissance américaine : les Etats-Unis ne sont plus là pour stabiliser l'ordre international, mais pour préserver leur prééminence dans un système anarchique où toute perte d'initiative peut montrer un signe d'affaiblissement.

## Administration Biden : de 2020 à 2024

Sous l'administration Biden, la stratégie cybernétique américaine a poursuivi l'approche proactive initiée sous Trump, tout en cherchant à l'encadrer par une coopération internationale renforcée. La doctrine du *Defend Forward* a été maintenue et intégrée dans la stratégie nationale de cybersécurité de 2023, et souligne également la nécessité de perturber les activités hostiles et malveillantes à leur source tout en restant en dessous du seuil du conflit armé[222].

[221] FISCHERKELLER Michael P., GOLDMAN, Emily O., HARKNETT, Richard J., « Cyber Persistence Theory : Redefining National Security in Cyberspace ». Oxford : Oxford University Press, 2022.
[222] LOSTRI Eugenia, PELL Stephanie, « The Biden Administration's Implementation Plan for the National Cybersecurity Strategy », The Lawfare Institute, 2023.

Parallèlement, l'administration a mis l'accent sur la résilience des infrastructures critiques, en promouvant des partenariats public-privé pour sécuriser les secteurs essentiels de l'énergie, de la santé et des transports[223]. Notamment, la loi sur le signalement des incidents cybernétiques pour les infrastructures de 2022 (CIRCIA) oblige les agences concernées à signaler les incidents ainsi que les paiements de rançon à la CISA, ce qui permet une réponse plus rapide et une meilleure analyse des menaces. Elle renforce également les normes de cybersécurité pour les fournisseurs de logiciels et des services de *cloud*, en imposant notamment des preuves de conformité et des sanctions contre des acteurs étatiques dont les attaques auraient été attribuées et qui auraient été reconnus comme étant responsables[224].
Dès 2020, l'administration Biden met également en place le *Cybersecurity Collaboration Center,* qui vise à devenir un lieu de partage de renseignement, ainsi qu'un réseau de bonnes pratiques et d'alertes sur les menaces cyber quotidiennes avec les entreprises et les agences gouvernementales. Par la suite, ce réseau sera aussi développé comme un réseau académique, avec un programme d'excellence concernant 403 institutions américaines dans le domaine de la recherche scientifique et de la formation de futurs chercheurs en cybersécurité[225].

La cyberstratégie américaine illustre une transformation profonde de la manière dont les États-Unis envisagent leur sécurité nationale et leur position dans l'ordre stratégique mondial. Face à la montée en puissance des cybermenaces, à la multiplication des attaques visant les infrastructures critiques, et à l'utilisation croissante du cyberespace par des acteurs étatiques et non étatiques, Washington a progressivement façonné une réponse à la fois défensive et offensive, qui repose sur un large éventail d'instruments, d'agences, de doctrines et de partenariats.

Sur le plan défensif, les États-Unis ont construit un cadre institutionnel qui s'est structuré autour de la protection des infrastructures critiques : cette défense repose tant sur la sécurisation physique des secteurs critiques, mais aussi sur la résilience des systèmes numériques qui sont interconnectés. Nous pouvons voir la volonté de défendre les intérêts nationaux avec l'implication du secteur privé, la création d'agences (comme la CISA ou l'USCYBERCOM) et le développement d'un écosystème de partage d'informations. Toutefois, cette approche reste confrontée à des limites : fragmentation institutionnelle,

[223] CISA, « Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) », Cybersecurity and Infrastructure Security Agency (CISA).
[224] Ibid.
[225] GUIFFARD Jonathan, « Sur les rives du Potomac, le centre du système de renseignement et de cyberdéfense des États-Unis », Études françaises de renseignement et de cyber, 2024/1 N° 2, p.43-57.

complexité bureaucratique, et flou juridique autour des actions dans la zone grise, notamment celles menées par les agences de renseignement. Sur le plan offensif, les États-Unis ont franchi un seuil doctrinal important à partir de 2018, avec les doctrines de *Persistent Engagement* et de *Defend Forward* qui montrent un changement de paradigme stratégique : elles rejettent l'idée que le cyberespace peut être stabilisé par la dissuasion seule, et lui substituent une logique d'action continue, de confrontation permanente et de préemption. En opérant directement dans les réseaux adverses, en perturbant leurs capacités en amont, et en affichant leur volonté de réagir de manière ciblée, les États-Unis entendent non seulement défendre leurs intérêts, mais aussi réaffirmer leur suprématie technologique et stratégique.

Cependant, cette stratégie offensive n'est pas sans zones d'ombre. Elle repose sur une intensification des opérations clandestines, un usage étendu d'outils offensifs à haut potentiel de dissémination, et une posture juridico-stratégique ambiguë. Elle pose également des défis majeurs en matière de contrôle démocratique, de souveraineté numérique et de stabilité globale du cyberespace. En définitive, les États-Unis utilisent le cyber à la fois comme un bouclier et une épée : un moyen de protéger leur territoire numérique contre les intrusions, mais aussi une arme de projection de puissance dans un espace stratégique sans frontières. Cette double logique, qui associe résilience défensive et pression offensive constante, montre que le cyber n'est plus un simple outil secondaire de soutien, mais bien un pilier central de la stratégie de puissance américaine dans le XXIe siècle.

## III/ Alliances et coopération internationale : une réponse collective aux cybermenaces

Face à l'anarchie du cyberespace, les Etats-Unis ne peuvent plus compter uniquement sur leurs capacités nationales pour garantir leur sécurité. La complexité du monde numérique, la rapidité des attaques et l'interconnexion mondiale des réseaux nécessitent en effet une coopération étroite avec d'autres acteurs, tant pour assurer une défense collective que pour promouvoir des normes, communes à tous et non contestées. Pour autant, la stratégie américaine oscille entre des alliances avec des partenaires « *like-minded* » et la défense de son autonomie stratégique, le tout dans un environnement où la gouvernance d'Internet se trouve de plus en plus contestée par les puissances émergentes.

## Coopération avec les alliés : les *Five Eyes* et l'OTAN

L'un des piliers historiques de la coopération sécuritaire du cyberespace et de l'information repose sur le réseau des *Five Eyes* : fondée dès la fin de la Seconde Guerre mondiale, cette alliance est par la suite devenue un levier majeur dans l'enjeu de l'hégémonie informationnelle des Etats-Unis. Conçu dans un premier temps dans un contexte de Guerre froide, dans le plus grand secret dans le but d'intercepter les communications des soviétiques puis dans celui de continuer l'espionnage de communications planétaires, le réseau des *Five Eyes* (Etats-Unis, Canada, Australie, Nouvelle-Zélande et Royaume-Uni) est fondé par l'accord UKUSA de 1946[226]. Ce dernier met en place une collaboration étroite entre les services de renseignement de ces cinq pays, notamment dans le domaine du renseignement électromagnétique (SIGINT) et à commencer par l'échange de données issues d'interceptions radio, satellites et de communications numériques. La NSA et ses homologues des autres pays se répartissent ainsi des zones de surveillance globales et partagent des données brutes, des analyses et des méthodes d'interception[227].

Par la suite, le partenariat des *Five Eyes* est renforcé par la création du système ECHELON, capable de capter des via satellites et câbles sous-marins. Selon certains chercheurs, ce système rend l'alliance des *Five Eyes* comme « l'alliance de surveillance la plus puissante jamais conçue ». Le réseau peut en effet enregistrer jusqu'à deux millions de conversations à la minute, et a pour mission principale d' « espionner les gouvernements (amis ou ennemis), les partis politiques, les syndicats, les mouvements sociaux et les entreprises »[228]. Le fonctionnement du réseau repose alors sur une confiance très forte entre ses membres et est fondé sur des procédures communes de collecte, des équipements interopérables, et un partage réciproque de données classifiées[229]. Aujourd'hui, cette alliance joue toujours un rôle central dans la coopération au sein du cyberespace, notamment en ce qui concerne l'attribution des cyberattaques, la coordination des réponses ou le partage de renseignements sur les menaces. Toutefois, elle est également fortement critiquée pour son caractère exclusif et asymétrique, qui renforce tant la domination technologique des Etats-Unis que celle du Royaume-Unis, ce qui va renforcer les contestations internationales. En effet, au sein de l'OTAN par exemple, certains partenaires européens ont souvent exprimé des réserves face à cette logique de cercle

[226] RAMONET Ignacio, « Chapitre II. Les « cinq yeux » et le reseau Échelon ». In : L'empire de la surveillance Suivi de deux entretiens avec Julian Assange et Noam Chomsky. Paris : Gallimard. Folio Actuel, 2024, p.43-53.
[227] Ibid.
[228] RAMONET Ignacio, « Chapitre II. Les « cinq yeux » et le reseau Échelon ». In : L'empire de la surveillance Suivi de deux entretiens avec Julian Assange et Noam Chomsky. Paris : Gallimard. Folio Actuel, 2024, p.43-53.
[229] Ibid.

fermé qui rend difficile la mise en place de véritables mécanismes multilatéraux de réponse ou d'attribution coordonnée dans le cyberespace[230].

Au-delà du cercle restreint des *Five Eyes* (*Tier A*, ou *Second Party)*, la NSA a progressivement élargi ses partenariats à d'autres Etats avec une coopération différenciée : un deuxième niveau, le *Third Party*, regroupe des pays qui collaborent ponctuellement avec les Etats-Unis dans des programmes spécifiques, encadrés par des accords bilatéraux, et qui s'appuient souvent sur des contreparties matérielles (financement, transferts de technologies, ou encore accès à des capacités avancées d'interception)[231]. Parmi eux, une vingtaine de pays sont rassemblés sous l'appellation *Computer Network Operations*, et participent à une « coopération ciblée » avec la NSA, selon leurs expertises ou leur positionnement géostratégique. Un troisième cercle inclut des États jugés « neutres » ou « amicaux », comme le Brésil, le Mexique, l'Argentine, l'Indonésie, le Kenya ou encore l'Afrique du Sud. Avec ces derniers, Washington entretient des « coopérations exceptionnelles » à géométrie variable, dans un cadre plus opportuniste et moins institutionnalisé. Enfin, un dernier groupe de pays est explicitement identifié comme cible par la NSA : la Chine, la Russie, l'Iran, le Venezuela ou la Syrie font l'objet d'activités offensives de renseignement, dans une logique de confrontation stratégique persistante[232].

Concernant les coopérations au sein de l'espace euro-atlantique, l'OTAN joue un rôle croissant dans l'organisation du partage de renseignement et de capacités cyber : le *NATO Advisory Committee on Special Intelligence* (NACSI) est la principale plateforme de discussion sur les enjeux SIGINT, et qui regroupe les membres des *Five Eyes* ainsi que plusieurs autres pays européens clés (Allemagne, Belgique, Danemark, Espagne, France, Italie, Pays-Bas, Norvège, Suède), qui forment ensemble l'alliance élargie des *14-Eyes*. Ces États échangent régulièrement des données sensibles dans le domaine militaire, notamment dans le cadre de la lutte contre le terrorisme ou de la surveillance de zones de conflit[233]. Une initiative équivalente existe pour la région Asie-Pacifique, autour d'un groupe dit des *10-Eyes*, qui inclut notamment Singapour, la Corée du sUd et la Thaïlande aux côtés des *Five Eyes*[234]. Par ailleurs, depuis

[230] TAILLAT Stéphane, « Cyber opérations offensives et réaffirmation de l'hégémonie américaine : une analyse critique de la doctrine de Persistent Engagement », Hérodote, 2020/2 N° 177-178, p.313-328.
[231] DELESSE Claude, « Chapitre premier. Les coopérations étrangères ». In : NSA National Security Agency L'histoire de la plus secrète des agences de renseignement. Paris : Tallandier. Hors collection, 2022, p.291-293.
[232] DELESSE Claude, « Chapitre premier. Les coopérations étrangères ». In : NSA National Security Agency L'histoire de la plus secrète des agences de renseignement. Paris : Tallandier. Hors collection, 2022, p.291-293.
[233] Ibid.
[234] Ibid.

l'adoption de sa première politique de cyberdéfense en 2008, l'OTAN a aussi renforcé sa posture collective face aux menaces numériques. Le Cyber Defence Pledge, adopté en 2016, engage les États membres à investir davantage dans leurs moyens de protection numérique, et à améliorer l'interopérabilité de leurs dispositifs[235]. Pour autant, de fortes divergences persistent entre alliés, en particulier sur la question de l'attribution des attaques et des modalités de réponse. Si certains États, comme les États-Unis ou le Royaume-Uni, privilégient une approche plus coercitive incluant des sanctions ciblées ou des campagnes d'exposition publique des auteurs présumés (*naming and shaming*), d'autres partenaires européens se montrent plus prudents car ils redoutent fortement les effets d'escalade ou l'instrumentalisation politique de ces pratiques[236].

## Contestation de la gouvernance d'Internet

Bien qu'une coopération avec certains alliés soient mise en place par les Etats-Unis concernant le partage de renseignements et de certaines capacités cyber, d'autres puissances mondiales comme la Chine ou la Russie sont peu enclines à fixer avec les Etats-Unis des normes contraignantes communes en matière de sécurité de l'Internet[237]. En effet, les contestations concernant la gouvernance d'Internet et l'hégémonie américaine sont majoritairement portées par les grands pays émergents, qui réclament une meilleure représentation dans les instances mondiales de technologie, et craignent pour leur souveraineté numérique[238].

Dès 2005, lors du Sommet mondial sur la société de l'information à Tunis, une tentative de réforme de la toile et de son système de gouvernance s'est soldée par un échec : malgré la création d'une nouvelle institution, le Forum pour la Gouvernance d'Internet (FGI), après des négociations les ayant opposés frontalement à la Chine, à l'Iran et au Brésil, les Etats-Unis ont gardé la mainmise sur l'organisme chargé du système de gestion et d'administration de domaine, l'ICANN (voir chapitre 1)[239]. Ces prérogatives inquiètent fortement les contestataires, qui pensent que les Etats-Unis pourraient « couper » un pays du reste d'Internet

[235] Organisation du traité de l'Atlantique Nord (OTAN), « Cyber Défense Pledge », OTAN, 2016.
[236] TAILLAT Stéphane, « Cyber opérations offensives et réaffirmation de l'hégémonie américaine : une analyse critique de la doctrine de Persistent Engagement », Hérodote, 2020/2 N° 177-178, p.313-328.
[237] DELORS Quentin, une review de l'ouvrage « US National Cybersecurity. International Politics, Concepts and Organisation » de VAN PUYVELDE Damien et BRANTLY Aaron F., Routledge, 2017, 238p., dans Etudes Internationales, 2018, pp.435-437.
[238] NOCETTI Julien, « Internet et sa gouvernance : La rivalité entre États-Unis et grands émergents ». In : DE MONTBRIAL, Thierry et MOREAU DEFARGES, Philippe, Ramses 2015 Le défi des émergents. Paris : Institut français des relations internationales. Ramses, p.206-209.
[239] FOUCART Stéphane, « Les Etats-Unis maintiennent leur hégémonie sur Internet », Le Monde, 2005.

en invalidant son extension nationale (« .fr », « .be » …). Pour autant, le FGI ne reste alors qu'un organe consultatif, mais est considéré à l'époque comme le « premier outil de coopération internationale autour des questions d'intérêt public liés aux usages de l'Internet : lutte contre l'utilisation du réseau à des fins de terrorisme, contre les flux financiers illicites ou encore contre le spam »[240]. Également, bien que l'administration américaine en place en 2005 refuse d'abandonner son rôle « historique », le texte adopté mentionne que chacun reconnaît que « tous les gouvernements devraient avoir un rôle et des responsabilités équivalents dans la gouvernance internationale d'Internet, dans le maintien de sa stabilité, de sa sécurité et de sa continuité »[241].

Par la suite, plusieurs propositions ont été faites lors d'instances et de forums multilatéraux : pour certains, la gouvernance d'Internet doit respecter le libre jeu du marché ; pour d'autres, elle doit rester dans le cadre d'une autorégulation se faisant par la communauté technologique. Enfin, certains ont proposé l'adoption d'une Constitution ou d'un traité de l'Internet, qui élèverait sa gouvernance au niveau d'une gouvernance mondiale[242]. Ce qui est sûr, c'est que les Etats-Unis sont régulièrement critiqués à cause de leur prééminence sur les infrastructures numériques mondiale, leur influence normative, et la domination de leur industrie sur le net.

En effet, comme l'explique Julien Nocetti, beaucoup d'Etats ont pris conscience depuis les Printemps arabes du pouvoir subversif de l'accès aux technologies numériques : Internet est à la fois le « produit ambivalent de la culture politique des Etats-Unis et l'expression de leur tradition impériale »[243]. Cela conduit également la diplomatie américaine à faire du positionnement d'Internet un facteur clé de différenciation par rapport aux puissances émergentes autoritaires, tout en cherchant par ailleurs à défendre les intérêts économiques des grands acteurs américains de l'Internet[244]. D'autres craignent également un Internet dominé par les Etats-Unis, qui chercheraient à l'utiliser pour déstabiliser, ou s'ingérer dans les affaires

[240] Ibid.
[241] Ibid.
[242] NOCETTI Julien, « Internet et sa gouvernance : La rivalité entre États-Unis et grands émergents ». In : DE MONTBRIAL, Thierry et MOREAU DEFARGES, Philippe, Ramses 2015 Le défi des émergents. Paris : Institut français des relations internationales. Ramses, p.206-209.
[243] Ibid.
[244] Ibid.

d'Etats souverains[245]. L'affaire Snowden en 2013 n'a fait que confirmer ces soupçons et accélérer les démarches vers une déconnexion progressive des réseaux américains[246].

Cette confrontation reflète donc des visions opposées de la souveraineté numérique. En réponse à l'hégémonie américaine, la Chine et la Russie ont par exemple proposé de développer leurs propres espaces numériques nationaux pour pouvoir être souverains et imposer une localisation physique des données des usagers sur leur territoire[247]. Rejoints par l'Iran, l'Arabie Saoudite ou encore la Corée du Nord, l'ensemble de ces Etats font « la promotion d'un contrôle de l'Internet par les Etats au sein de l'Union internationale des télécommunications (UIT) »[248]. Les Etats-Unis ont alors menacé du risque d'une « balkanisation du cyberespace », c'est-à-dire sa fragmentation en zones d'influences fermées, et qui annoncerait donc la fin d'un Internet libre, ouvert et sûr[249]. Comme l'indique Frédérick Douzet, les négociations internationales flanchent régulièrement sur deux points cruciaux que les Etats occidentaux mettent en avant : le respect des droits de l'Homme (liberté d'expression, accès à l'information, respect de la vie privée) et l'implication d'acteurs non étatiques dans un modèle de gouvernance multipartite[250].

D'autre part, plusieurs autres motifs de désaccord ont lieu. Tout d'abord, le fait que près de 70 % des échanges de données numériques dans le monde transitent par les Etats-Unis, contre 5 % par la Chine, ont amené les BRICS (Brésil, Russie, Inde, Chine, Afrique du Sud), en partenariat avec une vingtaine d'Etats africains, à lancer leur propre projet de câble sous-marin de 32 000 km[251]. De plus, un argument démographique est avancé : Internet s'internationalise de plus en plus, et perd donc ses caractéristiques occidentales. En 2012, déjà 66 % des internautes vivaient en dehors du monde occidental[252].

---

[245] DOUZET Frédérick et TAILLAT Stéphane, « Chapitre 6. Les enjeux de politique internationale L'affirmation du leadership américain ». In : TAILLAT, Stéphane, CATTARUZZA Amaël et DANET Didier, La Cyberdéfense Politique de l'espace numérique. Paris : Armand Colin. Collection U, 2018, p.111-122.

[246] NOCETTI Julien, « Internet et sa gouvernance : La rivalité entre États-Unis et grands émergents ». In : DE MONTBRIAL, Thierry et MOREAU DEFARGES, Philippe, Ramses 2015 Le défi des émergents. Paris : Institut français des relations internationales. Ramses, p.206-209.

[247] DOUZET Frédérick et TAILLAT Stéphane, « Chapitre 6. Les enjeux de politique internationale L'affirmation du leadership américain ». In : TAILLAT, Stéphane, CATTARUZZA Amaël et DANET Didier, La Cyberdéfense Politique de l'espace numérique. Paris : Armand Colin. Collection U, 2018, p.111-122.

[248] DOUZET Frédérick, « La géopolitique pour comprendre le cyberespace », Hérodote, 2014/1 n° 152-153, p.3-21.

[249] DOUZET Frédérick et TAILLAT Stéphane, « Chapitre 6. Les enjeux de politique internationale L'affirmation du leadership américain ». In : TAILLAT, Stéphane, CATTARUZZA Amaël et DANET Didier, La Cyberdéfense Politique de l'espace numérique. Paris : Armand Colin. Collection U, 2018, p.111-122.

[250] DOUZET Frédérick, « La géopolitique pour comprendre le cyberespace », Hérodote, 2014/1 n° 152-153, p.3-21.

[251] Ibid.

[252] NOCETTI Julien, « Internet et sa gouvernance : La rivalité entre États-Unis et grands émergents ». In : DE MONTBRIAL, Thierry et MOREAU DEFARGES, Philippe, Ramses 2015 Le défi des émergents. Paris : Institut français des relations internationales. Ramses, p.206-209.

Pour autant, les grands émergents ne forment pas un bloc monolithique, mais les négociations ont montré que cet ensemble d'Etats veut de plus en plus faire valoir sa vision des choses. L'UIT a donc constitué une tribune pour remettre en cause la prééminence des Etats-Unis, et tente de replacer les discussions dans un cadre étatique classique[253]. Mais Washington, malgré le souhait de structurer sa participation aux débats internationaux sur les normes numériques comme le montre la création en 2022 du Bureau of Cyberspace and Digital Policy[254], montre surtout la volonté de réaffirmer sa position dans les enceintes multilatérales.

Dans ce contexte de tensions, la diplomatie cyber américaine s'appuie surtout sur des discussions bilatérales à travers des coalitions restreintes d'Etats *like-minded*. L'objectif est de mettre en place des normes se basant sur des valeurs communes de cybersécurité, d'ouverture et de coopération technique. Washington fait donc un rappel des normes en 2015 : interdiction de mener ou de soutenir une opération numérique causant des dommages intentionnels à des infrastructures vitales, interdiction de cibler des centres de réponse d'urgence, interdiction de laisser se développer des actions numériques malveillantes sur leur territoire[255]… Par ailleurs, d'autres normes sont encouragées, comme le renforcement de protection des infrastructures critiques respectives, le partage des informations, l'assistance mutuelle en cas d'attaque, ou la coopération à la stabilité et la sécurité du cyberespace[256]. Mais cette stratégie à ses limites : comme le souligne Guillaume Delors, les Etats-Unis ne peuvent pas, à eux seuls, réguler les comportements malveillants dans le cyberespace[257]. La prolifération d'outils offensifs, leur possible réutilisation par des groupes non étatiques, et l'absence d'un cadre légal contraignant sur les responsabilités étatiques compliquent toute tentative de régulation globale. Pour les Etats-Unis, l'objectif est pour l'instant de contenir l'escalade stratégique. Mais en l'absence d'un consensus mondial, ils renforcent aussi la fragmentation de l'Internet : ils misent sur la coopération entre puissances démocratiques pour fixer des standards communs, tout en refusant une gouvernance contraignante qui limiterait leur souveraineté et leur autonomie.

---

[253] Ibid.
[254] GUIFFARD Jonathan, « Sur les rives du Potomac, le centre du système de renseignement et de cyberdéfense des États-Unis », Études françaises de renseignement et de cyber, 2024/1 N° 2, p.43-57.
[255] DOUZET Frédérick et TAILLAT Stéphane, « Chapitre 6. Les enjeux de politique internationale L'affirmation du leadership américain ». In : TAILLAT, Stéphane, CATTARUZZA Amaël et DANET Didier, La Cyberdéfense Politique de l'espace numérique. Paris : Armand Colin. Collection U, 2018, p.111-122.
[256] Ibid.
[257] DELORS Quentin, une review de l'ouvrage « US National Cybersecurity. International Politics, Concepts and Organisation » de VAN PUYVELDE Damien et BRANTLY Aaron F., Routledge, 2017, 238p., dans Etudes Internationales, 2018, pp.435-437.

L’étude de la cyberstratégie des Etats-Unis nous confirme leur posture néoréaliste au sein du cyberespace. En effet, face à des menaces croissantes, Washington privilégie le renforcement de se capacités internes via l’adoption de doctrines de dissuasion, de projection de puissance, et de militarisation progressive du cyberespace. La stratégie américaine montre bien une logique de puissance et d’autonomie stratégique dans un environnement anarchique, dans un but de maximiser leurs intérêts et leur hégémonie, et ce peu importe les moyens pour y arriver (surveillance globale, développement d’outils offensifs…). L’Etat reste donc l’acteur central, dont la puissance est synonyme de sécurité, et la coopération n’est acceptée que lorsqu’elle ne compromet pas l’autonomie stratégique.

# Conclusion

Dans ce mémoire de synthèse, nous avions pour objectif d'étudier l'évolution de la stratégie américaine dans le cyberespace à travers une analyse néoréaliste, face à l'intensification des menaces du cyberespace depuis le début des années 2000. Pour structurer cette réflexion, nos avons formulé quatre hypothèses, que notre analyse a permis d'évaluer grâce aux doctrines successives et aux outils mobilisés par les Etats-Unis.

Premièrement, l'hypothèse selon laquelle les cyberattaques majeures ont conduit les Etats-Unis à adopter des innovations technologiques dans leur stratégie se confirme. En effet, les cas de *Stuxnet*, de *NotPetya* ainsi que l'ingérence russe de 2016 nous ont permis de montrer la vulnérabilité des infrastructures critiques américaines. En réponse, les Etats-Unis ont donc développé des capacités techniques de plus en plus sophistiquées (structuration de nouvelles agences spécialisées, renforcement des infrastructures, programmes de contre-attaque numériques…) dans une logique de *self-help,* où la technologie permet d'assurer sa puissance et sa sécurité dans le système international anarchique.

Deuxièmement, les Etats-Unis ont effectivement adopté une posture proactive et offensive dans le cyberespace. Depuis la doctrine Bush, fondée sur la prévention et la domination, jusqu'aux doctrines *Defend Forward* et *Persistent Engagement* sous Trump et continué sous Biden, nous pouvons observer un basculement vers des stratégies préemptives qui visent tant à prévenir les attaques, qu'à projeter la puissance américaine.

Troisièmement, l'hypothèse selon laquelle les stratégies de cybersécurité américaines intègrent une dimension de renseignement avancé se confirme : le cas de l'affaire Snowden en 2013 montre l'ampleur des dispositifs de surveillance et de collecte de données opérées par la NSA, qui, combinées aux opérations clandestines, induisent une approche qui se base sur la maîtrise de l'information comme outil stratégique à la fois pur anticiper les menaces et dissuader les adversaires.

Finalement, la quatrième hypothèse sur la militarisation croissante du cyberespace est également validée. En effet, le rattachement du cyberespace à la doctrine militaire américaine et à sa reconnaissance comme étant un domaine d'opération de la guerre (aux côtés de la terre, de la mer, de l'air et de l'espace) et la montée en puissance de l'USCYBERCOM montrent que les Etats-Unis voient désormais le cyberespace comme une scène stratégique à part entière. Le

cyberespace est donc devenu un champ de rivalité à portée géopolitique, où la suprématie technologique peut devenir un enjeu de sécurité nationale.

La stratégie américaine dans le cyberespace correspond donc aux dynamiques du néoréalisme (compétition, méfiance, dissuasion et renforcement des capacités dans une logique de *self-help* pour atteindre la puissance et la sécurité) qui visent à préserver leur puissance hégémonique ainsi que leur sécurité. Notre analyse a pu montrer que, face à des cyberattaques majeures, les Etats-Unis ont pu adopter des stratégies centrées sur l'autonomie, la projection de puissance, la surveillance globale et la dissuasion offensive. Cela nous permet de confirmer le postulat néoréaliste selon lequel les Etats restent les acteurs principaux du système international et agissent selon leurs intérêts nationaux, sans accepter de coopération sauf si cette dernière ne remet pas en cause leur souveraineté et leur avantage relatif dans le jeu international.

Certes, même si le discours américain parle de coopération et de gouvernance partagée, la réalité des politiques menées montre une logique de hiérarchie où l'objectif reste le même : maintenir l'hégémonie américaine par la conservation de la mainmise sur les architectures stratégiques du cyberespace et par la modélisation des normes en fonction des intérêts de Washington. Ce paradoxe illustre parfaitement la vision néoréaliste de Waltz, où les institutions internationales ne permettent pas de modifier les rapports de force, mais permettent de les refléter.

Pour autant, ce travail met aussi en évidence les limites du néoréalisme lorsque les spécificités du cyberespace entrent en jeu. En effet, l'anonymat des acteurs, l'asymétrie des capacités, la difficulté d'attribution ainsi que le besoin de coopération entre secteurs public et privé montrent que, bien que le néoréalisme soit efficace pour expliquer les comportements étatiques dominants, il serait utile de le compléter par des approches qui permettrait d'appréhender la conflictualité hybride et les dynamiques de l'ensemble des acteurs au sein du cyberespace.

# Bibliographie

## Livres et ouvrages


BEARD Jack, « The Principle of Proportionality in an Era of High technology », Oxford University Press, 2018. URL : https://papes.ssrn.com/sol3/papers.cfm?abstract_id=3119384

BENDIEK Annegret, METZGER Tobias, « Deterrence theory in the cyber-century : Lessons from a state-of-the-art literature review », German Institute for International and Security Affairs, 2015. URL : https://www.swp-berlin.org/publications/products/arbeitspapiere/Bendiek-Metzger_WP-Cyberdeterrence.pdf

BORGHARD Erica D., SCHNEIDER Jacquelyn G., « Defending Forward: The 2018 Cyber Strategy is a Step in the Right Direction », War on the Rocks. 2018. URL : https://warontherocks.com/2018/09/defending-forward-the-2018-cyber-strategy-is-a-step-in-the-right-direction

CLARKE Richard, KNAKE Robert, « Cyber War - The Next Threat to National Security and What to Do About It », *HarperCollins e-books*, 2010, https://www.jstor.org/stable/26270542?seq=1

FISCHERKELLER Michael P., GOLDMAN, Emily O., HARKNETT, Richard J., « Cyber Persistence Theory : Redefining National Security in Cyberspace ». *Oxford : Oxford University Press*, 2022. URL : https://global.oup.com/academic/product/cyber-persistence-theory-9780197550880

LIBICKI Martin C., « Cyberdeterrence and Cyberwar », *Rand Corporation*, 2009. URL : https://www.rand.org/pubs/monographs/MG877.html

LIN Herb, ZEGART Amy B. (dir.), « Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations ». *Washington, D.C. : Brookings Institution Press*. URL : https://www.brookings.edu/book/bytes-bombs-and-spies

LOSTRI Eugenia, PELL Stephanie, « The Biden Administration's Implementation Plan for the National Cybersecurity Strategy », *The Lawfare Institute*, 2023. URL : https://www.lawfaremedia.org/article/the-biden-administration-s-implementation-plan-for-the-national-cybersecurity-strategy?utm

MEARSHEIMER John J., « The tragedy of great power politics », *Norton & Co*, 2001. https://samuelbhfaure.com/wp-content/uploads/2015/10/s2-mearsheimer-2001.pdf

MORGAN, Patrick M., « Deterrence Now », *Cambridge University Press*, 2003. URL : https://ir11.co.uk/wp-content/uploads/2018/11/morgan-deterrence-now-compressed.pdf

NYE Joseph, « Cyberpower », *Harvard Kennedy School*, 2010. https://www.belfercenter.org/publication/cyber-power

NYE Joseph, « Deterrence and Dissuasion in Cyberespace », *International Security*, 2017. https://direct.mit.edu/isec/article/41/3/44/12147/Deterrence-and-Dissuasion-in-Cyberspace

RID Thomas, « Active Measures. The Secret History of Disinformation and Political Warfare », *Australian Journal of Defence and Strategic Studies*, 2020.

TIKK Eneken, KERTTUNEN Mika, « Routledge handbook of international Cybersecurity », *Routledge*, 2020. URL : https://www.taylorfrancis.com/books/edit/10.4324/9781351038904/routledge-handbook-international-cybersecurity-eneken-tikk-mika-kerttunen

VALERIANO Brandon, JENSEN Benjamin et MANESS Ryan C., « Cyber Strategy : The Evolving Character of Power and Coercion ». *Oxford* : *Oxford University Press*, 2021. URL : https://global.oup.com/academic/product/cyber-strategy-9780197681065

WALT Stephen, « The Origins of Alliances », *Cornell University Press*, 1987, https://web.stanford.edu/class/ips198/docs/Walt.pdf

WALTZ Kenneth N., « Theory of International politics », *University of California*, 1979, https://dl1.cuni.cz/pluginfile.php/486328/mod_resource/content/0/Kenneth%20N.%20Waltz%20Theory%20of%20International%20Politics%20Addison-Wesley%20series%20in%20political%20science%20%20%20%201979.pdf

WALTZ Kenneth N., « Realist thought and neorealist theory », *Journal of International Affairs*, 1990/44, no. 1, pp.21–37. URL : http://www.jstor.org/stable/24357222

ZETTER Kim, « Countdown to Zero Day : Stuxnet and the Launch of the World's First Digital Weapon », *Crown*, 2014, 265p. https://www.docdroid.net/JhkoIKe/kim-zetter-countdown-to-zero-day-stuxnet-and-the-launch-of-the-worlds-first-digital-weapon-crown-publishers-2014-pdf

## Chapitres d'ouvrages

CATTARUZZA Amaël, DANET Didier, TAILLAT Stéphane, « Présentation ». In : TAILLAT, Stéphane, CATTARUZZA, Amaël et DANET, Didier, *La Cyberdéfense Politique de l'espace numérique*. Paris : Armand Colin. Collection U, p.124-125. DOI : 10.3917/arco.taill.2023.01.0124. URL : https://shs.cairn.info/la-cyberdefense--9782200634223-page-124?lang=fr

CORN Gary P., RENALS Peter, « Scenarios for Defend Forward ». IN : GOLDSMITH Jack, *The United States' Defend Forward Cyber Strategy : A Comprehensive Legal Assessment. Oxford University Press*, 2022, 357p., pp.24- 31. URL : https://books.google.be/books?hl=fr&lr=&id=nHhXEAAAQBAJ&oi=fnd&pg=PP1&dq=cyber+operations+clandestines+usa&ots=hv_sk8iydq&sig=jAa6-VjhUMTHQIx421aPFDX1z5M&redir_esc=y#v=onepage&q&f=false

DELESSE Claude, « Chapitre premier. Les coopérations étrangères ». In : *NSA National Security Agency L'histoire de la plus secrète des agences de renseignement. Paris : Tallandier. Hors collection*, 2022, p.291-293. URL : https://shs.cairn.info/nsa-national-security-agency--9791021008632-page-291?lang=fr

DOUZET Frédérick et TAILLAT Stéphane, « Chapitre 6. Les enjeux de politique internationale L'affirmation du leadership américain ». In : TAILLAT, Stéphane, CATTARUZZA Amaël et DANET Didier, *La Cyberdéfense Politique de l'espace numérique. Paris : Armand Colin. Collection U*, 2018, p.111-122. DOI : 10.3917/arco.danet.2018.01.0111. URL : https://shs.cairn.info/cyberdefense-politique-de-l-espace-numerique--9782200621292-page-111?lang=fr.

NOCETTI Julien, « Internet et sa gouvernance : La rivalité entre États-Unis et grands émergents ». In : DE MONTBRIAL, Thierry et MOREAU DEFARGES, Philippe, Ramses 2015 *Le défi des émergents. Paris : Institut français des relations internationales. Ramses, 2015*, p.206-209. DOI : 10.3917/ifri.demon.2014.01.0206. URL : https://shs.cairn.info/le-defi-des-emergents--9782100717330-page-206?lang=fr

NOCETTI Julien, « Internet et sa gouvernance : crispations internationales et nouveaux enjeux » In : TAILLAT, Stéphane, CATTARUZZA, Amaël et DANET, Didier, La *Cyberdéfense Politique de l'espace numérique. Paris : Armand Colin. Collection U*, 2018, p.130-135. DOI : 10.3917/arco.danet.2018.01.0130. URL : https://shs.cairn.info/cyberdefense-politique-de-l-espace-numerique--9782200621292-page-130?lang=fr

NOCETTI Julien, « La menace dans le champ cyber - Une menace multiforme et diffuse ». In : DE MONTBRIAL, Thierry et DAVID, Dominique, *Ramses 2019 Les chocs du futur. Paris : Institut français des relations internationales.* Ramses, 2019, p.296-299. DOI : 10.3917/ifri.demon.2018.01.0296. URL : https://shs.cairn.info/les-chocs-du-futur--9782100779413-page-296?lang=fr

NOCETTI Julien, « Information, désinformation : les leçons du Covid De Wuhan aux présidentielles américaines ». In : DE MONTBRIAL, Thierry et DAVID, Dominique, Ramses 2022 *Au-delà du Covid. Paris : Institut français des relations internationales*. Ramses, p.102-107. DOI : 10.3917/dunod.colle.2022.01.0102. URL : https://shs.cairn.info/ramses-2022--9782100822102-page-102?lang=fr

PELOPIDAS Benoît, « Chapitre 2. L'irrésistible technologique à l'épreuve. Quand le déterminisme capacitaire nie le choix politique ». IN : *Repenser les choix nucléaires La séduction de l'impossible. Paris : Presses de Sciences Po. Académique,* p.59-97. URL : https://shs.cairn.info/repenser-les-choix-nucleaires--9782724627404-page-59?lang=fr

RAMONET Ignacio, « Chapitre II. Les « cinq yeux » et le réseau Échelon ». IN : *L'empire de la surveillance Suivi de deux entretiens avec Julian Assange et Noam Chomsky. Paris : Gallimard. Folio Actuel*, 2024, p.43-53. URL : https://shs.cairn.info/l-empire-de-la-surveillance-suivi-de-deux-entretiens-avec-julian-assange-et-noam-chomsky--9782073039545-page-43?lang=fr

## Articles de revues scientifiques

AMINOT Jean-Luc, « WannaCry, une frayeur à l'échelle planétaire », Annales des Mines - Responsabilité & environnement, 2020/2 N° 98, p.53-56. DOI : 10.3917/re1.098.0053. URL : https://stm.cairn.info/revue-responsabilite-et-environnement-2020-2-page-53?lang=fr

AMIR-ASLANI Ardavan, « Stuxnet vs Shamoon : la cyberguerre au Moyen-Orient », Sécurité globale, 2013/2 N° 24, p.9-14. DOI : 10.3917/secug.024.0007. URL : https://shs.cairn.info/revue-securite-globale-2013-2-page-9?lang=fr

ASHLEY, Richard K., « The Poverty of Neorealism. », International Organization, vol. 38, no. 2, 1984, pp. 225–86. JSTOR, http://www.jstor.org/stable/2706440

BORNSTEIN Roman, « Ingérence numérique, mode d'emploi », Le Débat, 2020/1 n° 208, p.42-55. DOI : 10.3917/deba.208.0042. URL : https://shs.cairn.info/revue-le-debat-2020-1-page-42?lang=fr

CARTIGNY Claude, « Le concept de dissuasion et ses conséquences sur les doctrines stratégiques », Recherches Internationales, n°21, 1986, pp.77-84. DOI : https://doi.org/10.3406/rint.1986.2777. URL : https://www.persee.fr/doc/rint_0294-3069_1986_num_21_1_2777

CERUZZI Paul E., « Aux origines américaines de l'Internet : projets militaires, intérêts commerciaux, désirs de communauté », *Le Temps des médias*, 2012/1 n° 18, p.15-28. DOI : 10.3917/tdm.018.0015. URL : https://shs.cairn.info/revue-le-temps-des-medias-2012-1-page-15?lang=fr

CHAUVANCY François, « La guerre du futur : façonner l'environnement informationnel », *Diplomatie*, 2020. URL : https://moodle.uclouvain.be/pluginfile.php/336000/mod_folder/content/0/2020_La%20guerre%20du%20futur%2C%20façonner%20l'environnement%20informationnel.pdf?forcedownload=1

DELORS Quentin, une review de l'ouvrage « US National Cybersecurity. International Politics, Concepts and Organisation » de VAN PUYVELDE Damien et BRANTLY Aaron F., Routledge, 2017, 238p., dans *Etudes Internationales*, 2018, pp.435-437. URL : us National Cybersecurity. International Politics… – Études internationales – Érudit

DOUZET Frédérick, « La géopolitique pour comprendre le cyberespace », *Hérodote*, 2014/1 n° 152-153, p.3-21. DOI : 10.3917/her.152.0003. URL : https://shs.cairn.info/revue-herodote-2014-1-page-3?lang=fr

DUROSELLE Jean-Baptiste, « Paix et guerre entre les nations : la théorie des relations internationales selon Raymond Aron », *Revue française de science politique*, 12/n°4, 1962. pp. 963-979. DOI : https://doi.org/10.3406/rfsp.1962.403400 URL : www.persee.fr/doc/rfsp_0035-2950_1962_num_12_4_403400

GALLAND Jean-Pierre, « Critique de la notion d'infrastructure critique », *Flux*, 2010/3 n° 81, p.6-18. DOI : 10.3917/flux.081.0006. URL : https://shs.cairn.info/revue-flux1-2010-3-page-6?lang=fr

GÉRY Aude, « La lutte contre la prolifération des armes cyber : un défi pour la stratégie française de cyberdéfense ». *Les Champs de Mars*, 2018/1 N° 30 + Supplément, p.307-316. DOI : 10.3917/lcdm.030.0307. URL : https://shs.cairn.info/revue-les-champs-de-mars-2018-1-page-307?lang=fr

GERGORIN Jean-Louis, « La stratégie furtive de Barack Obama : une novation majeure », *Commentaire*, 2012/3 Numéro 139, p.719-724. DOI : 10.3917/comm.139.0719. URL : https://shs.cairn.info/revue-commentaire-2012-3-page-719?lang=fr

GRIECO Joseph M., « Anarchy and the Limits of Cooperation : A Realist Critique of the Newest Liberal Institutionalism », *International Organization*, vol. 42, no. 3, 1988, pp. 485–507., http://www.jstor.org/stable/2706787.

GUIFFARD Jonathan, « Sur les rives du Potomac, le centre du système de renseignement et de cyberdéfense des États-Unis », *Études françaises de renseignement et de cyber*, 2024/1 N° 2, p.43-57. DOI : 10.3917/efrc.232.0043. URL : https://shs.cairn.info/revue-etudes-francaises-de-renseignement-et-de-cyber-2024-1-page-43?lang=fr

HUYGHE François-Bernard, « Des armes à la stratégie », *Revue internationale et stratégique*, 2012/3 n° 87, p.53-64. DOI : 10.3917/ris.087.0053. URL : https://shs.cairn.info/revue-internationale-et-strategique-2012-3-page-53?lang=fr

IASIELLO Emilio, « La cyberdissuasion est-elle une stratégie illusoire ? », *Air University, ASPJ Afrique et Francophonie*, 2018, https://www.airuniversity.af.edu/Portals/10/ASPJ_French/journals_F/Volume-09_Issue-1/iasiello_f.pdf

JACKSON Michael J., LIEBER Paul, « Countering Disinformation : Are We Our Worst Enemy ? », *The Cyber Defense Review*, 2020/5. URL : https://moodle.uclouvain.be/pluginfile.php/336000/mod_folder/content/0/2020_Cyber%20Defense%20Review%20IOIW%20special%20ed.pdf?forcedownload=1

JEANGÈNE VILMER Jean-Baptiste, « Pour un réalisme libéral en relations internationales », *Commentaire*, 2013/1 Numéro 141, p.13-20. DOI : 10.3917/comm.141.0013. URL : https://shs.cairn.info/revue-commentaire-2013-1-page-13?lang=fr

JEANGÈNE VILMER Jean-Baptiste, « Théories des relations internationales - Chapitre II. Le réalisme », *Presses Universitaires de France. Que sais-je ?* 2020, p.23-42. URL : https://shs.cairn.info/theories-des-relations-internationales--9782130785644-page-23?lang=fr

KELLO Lucas, Traduit de l'anglais par RICHARD Thomas, « Les cyberarmes : dilemmes et futurs possibles », *Politique étrangère*, 2014/4 Hiver, p.139-150. DOI : 10.3917/pe.144.0139. URL : https://shs.cairn.info/revue-politique-etrangere-2014-4-page-139?lang=fr

KEMPF Olivier, « Cyber et surprise stratégique », *Stratégique*, 2014/2 N° 106, p.111-123, DOI : 10.3917/strat.106.0111, URL : https://shs.cairn.info/revue-strategique-2014-2-page-111?lang=fr

KEMPF Olivier, « Cyberespace et dynamique des frontières », *Inflexions*, 2015/3 N° 30, p.141-149. DOI : 10.3917/infle.030.0141. URL : https://shs.cairn.info/revue-inflexions-2015-3-page-141?lang=fr

KORB Lawrence J., traduit de l'anglais par DE POORTÈRE Aurélie, « La stratégie de sécurité nationale du président Obama ou la fin de l'ère Bush », *Politique américaine*, 2010/2 N° 17, p.13-26. DOI : 10.3917/polam.017.0013. URL : https://shs.cairn.info/revue-politique-americaine-2010-2-page-13?lang=fr

LEHU Jean-Marc, « Cyberattaque : la gestion du risque est-elle encore possible ? Analyse et enseignements du cas Sony Pictures », *La Revue des Sciences de Gestion*, 2018/3 N° 291-292, p.41-50. DOI : 10.3917/rsg.291.0041. URL : https://shs.cairn.info/revue-des-sciences-de-gestion-2018-3-page-41?lang=fr

LEWIS James A., « Étude préliminaire sur les analyses en cybersécurité : l'affaire Snowden comme étude de cas ». *Hérodote*, 2014/1 n° 152-153, p.26-34. DOI : 10.3917/her.152.0026. URL : https://shs.cairn.info/revue-herodote-2014-1-page-26?lang=fr

LOUIS-SIDNEY Barbara, « La dimension juridique du cyberespace ». *Revue internationale et stratégique*, 2012/3 n° 87, p.73-82. DOI : 10.3917/ris.087.0073. URL : https://shs.cairn.info/revue-internationale-et-strategique-2012-3-page-73?lang=fr

MASTOR Wanda, « Les États-Unis et le culte du secret. L'exemple du privilège de l'exécutif », *Titre VII*, 2023/1 N° 10, p.80-87. DOI : 10.3917/tvii.010.0080. URL : https://droit.cairn.info/revue-titre-vii-2023-1-page-80?lang=fr

MILLIÈRE Guy, « Ce que veut Bush : recomposer le monde », *Outre-Terre*, 2003/4 no 5, p.17-25. DOI : 10.3917/oute.005.0017. URL : https://shs.cairn.info/revue-outre-terre1-2003-4-page-17?lang=f

NOCETTI Julien, « Géopolitique de la cyber-conflictualité ». *Politique étrangère*, 2018/2 Été, p.15-27. DOI : 10.3917/pe.182.0015. URL : https://shs.cairn.info/revue-politique-etrangere-2018-2-page-15?lang=fr

NOCETTI Julien, « Introduction », *Politique étrangère*, 2018/2 Été, p.10-13. DOI : 10.3917/pe.182.0010. URL : https://shs.cairn.info/revue-politique-etrangere-2018-2-page-10?lang=f

NYE Joseph, GOLDSMITH Jack Landman, « The Future of Power. », *Bulletin of the American Academy of Arts and Sciences* 64, no. 3 (2011) : 45–52. http://www.jstor.org/stable/41149419

PARSOIRE Didier et HÉON Sébastien, « Le prix du risque cyber ». *Revue d'économie financière*, 2019/1 N° 133, p.155-170. DOI : 10.3917/ecofi.133.0155. URL : https://shs.cairn.info/revue-d-economie-financiere-2019-1-page-155?lang=fr

PÉTINIAUD Louis, « Cartographie de l'affaire Snowden ». *Hérodote*, 2014/1 n° 152-153, p.35-42. DOI : 10.3917/her.152.0035. URL : https://shs.cairn.info/revue-herodote-2014-1-page-35?lang=fr

RID Thomas, BUCHANAN Ben, « Attributing Cyber Attacks », Journal of Strategic Studies, 2015, 4-37, DOI: 10.1080/01402390.2014.977382. URL : Attributing_Cyber_Attacks.pdf

SPYROPOULOS Georgios., « L'influence de Thucydide et de Démosthène Sur La Politique Étrangère Des USA », *Diplomatie*, 2010/43, 74–84. URL : https://www.jstor.org/stable/26981425.

TAILLAT Stéphane, « Un mode de guerre hybride dissymétrique ? Le cyberespace », *Stratégique*, 2016/1 N° 111, p.89-106. DOI : 10.3917/strat.111.0089. URL : https://shs.cairn.info/revue-strategique-2016-1-page-89?lang=fr

TAILLAT Stéphane, « La cyberdéfense américaine à l'âge de Donald Trump », *Questions internationales*, 2019/3 n°98, p.88-96. DOI : 10.3917/quin.098.0088. URL : https://shs.cairn.info/magazine-questions-internationales-2019-3-page-88?lang=fr

TAILLAT Stéphane, « Cyber opérations offensives et réaffirmation de l'hégémonie américaine : une analyse critique de la doctrine de Persistent Engagement », *Hérodote*, 2020/2 N° 177-178, p.313-328. DOI : 10.3917/her.177.0313. URL : https://shs.cairn.info/revue-herodote-2020-2-page-313?lang=fr

VAN PUYVELDE Damien, « L'analyse du renseignement aux Etats-Unis : entre art et science », Sécurité et stratégie, 2015/3 20, p.25-31. DOI : 10.3917/sestr.020.0025. URL : https://shs.cairn.info/revue-securite-et-strategie-2015-3-page-25?lang=fr

VENTRE Daniel, « Le point de vue des SHS sur les opérations secrètes dans le cyberespace. Revue de littérature », *Études françaises de renseignement et de cyber*, 2024/2 n° 3, p.139-153. DOI : 10.3917/efrc.242.0139. URL : https://shs.cairn.info/revue-etudes-francaises-de-renseignement-et-de-cyber-2024-2-page-139?lang=fr

WIART Louis, « Les stratégies des GAFAM », *Nectart*, 2023/32. URL : Les stratégies des GAFAM | Cairn.info

## Articles journalistiques

FILIPPONE Dominique, « Plus de 195 millions de données compromises en 2024 », *Le Monde Informatique*, 2025. URL : lire-plus-de-195-millions-de-donnees-compromises-en-2024-95729.html

FOUCART Stéphane, « Les Etats-Unis maintiennent leur hégémonie sur Internet », *Le Monde*, 2005. URL : https://www.lemonde.fr/afrique/article/2005/11/17/les-etats-unis-maintiennent-leur-hegemonie-sur-internet_711179_3212.html

## Sites Internet et pages de sites

CISA, « Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) », *Cybersecurity and Infrastructure Security Agency* (CISA), https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia?utm

GAUDIAUT Tristan, « Les pays les plus touchés par des cyberattaques massives », *Statista*, 2022, Graphique: Les pays les plus touchés par des cyberattaques massives | Statista

HEALEY Jason, « The Implications of Persistent (and Permanent) Engagement in Cyberspace ». *Atlantic Council*, 2020. URL : https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/the-implications-of-persistent-and-permanent-engagement-in-cyberspace

National Security Agency, « NSA Cybersecurity », *National Security Agency*. URL : National Security Agency/Central Security Service > Cybersecurity > Overview

Organisation du traité de l'Atlantique Nord (OTAN), « Cyber Défense Pledge », *OTAN*, 2016. URL : official_texts_133177.htm

The White House, « National Strategy to Secure Cyberspace », 2003, *Department of Energy*. https://www.energy.gov/sites/prod/files/National%20Strategy%20to%20Secure%20Cyberspace.pdf

U.S. Cyber Command, « Our mission and vision », *U.S. Cyber Command*. Mission and Vision

U.S. Cyber Command, « Our History », *U.S. Cyber Command.* Command History

Vie publique, « Quelles sont les grandes théories en matière de relations internationales ?» *Vie publique*. URL : https://www.vie-publique.fr/fiches/269844-theories-relations-internationales-realiste-liberale-constructiviste#:~:text=Le%20néo%2Dréalisme%2C%20apparu%20à,États%20(concept%20de%20polarité)

Ce mémoire propose une lecture néoréaliste de la stratégie des États-Unis dans le cyberespace depuis les années 2000. Il montre comment les cyberattaques majeures ont entraîné le développement de technologies défensives, de doctrines offensives et d'une militarisation progressive du cyberespace. À travers l'analyse des politiques américaines sous Bush, Obama, Trump et Biden, il met en lumière une logique de puissance fondée sur la dissuasion, le renseignement et l'autonomie stratégique.
Malgré une rhétorique de coopération, la posture américaine reste dominée par la quête de sécurité et la préservation de l'hégémonie dans un système international structuré par l'anarchie.

Cyberespace
Néoréalisme
Etats-Unis
Cybersécurité
Dissuasion

**UNIVERSITÉ CATHOLIQUE DE LOUVAIN**
**Faculté des sciences économiques, sociales, politiques et de communication**
**École des sciences politiques et sociales (PSAD)**
Place Montesquieu, 1 bte L2.08.05, 1348 Louvain-la-Neuve, Belgique | **www.uclouvain.be/psad**