Centre d'étude des crises
et conflits internationaux

Cybersécurité :

Analyse des documents stratégiques de Washington

Raphaël Delbrouck

Octobre 2020
Note d'analyse no. 74

Cybersécurité :
Analyse des documents stratégiques de Washington

Raphaël Delbrouck

Direction: Tanguy Struye de Swielande

Centre d'étude des crises et conflits internationaux
Université catholique de Louvain
Place Montesquieu 1, bte L2.08.07
1348 Louvain-la-Neuve
Belgique
www.cecrilouvain.be

A propos de l'auteur

Raphael Delbrouck est chercheur, diplômé d'un master à l'UCL en relations internationales, finalité spécialisée en diplomatie et résolution des conflits. Ses recherches portent sur les aspects sécuritaires, de défense et économiques des rapports entre grandes puissances géopolitiques.

TABLE DES MATIERES

INTRODUCTION

Dans un environnement de concurrence stratégique réémergée, la Chine et la Russie sont les deux principales puissances rivales, dites révisionnistes, des Etats-Unis. Au-delà de la compétition, l'Administration Trump se montre particulièrement encline à entrer en confrontation avec ces acteurs dont les dangers sont systématiquement réitérés, à côté de la Corée du Nord et de l'Iran, qualifiés quant eux d'Etats-paria. A cet égard, la dernière *National Security Strategy* (NSS) de 2017 se recoupe étroitement avec la *National Defense Strategy* (NDS) de 2018.

La Chine s'impose depuis le début des années 2010 comme acteur prédominant sur la scène internationale. La NSS soutient que c'est par une stratégie de long terme qu'elle poursuit son ascension, affirme son influence et sa puissance. Elle intimide ses voisins en procédant à une militarisation accrue en Mer de Chine méridionale et orientale. Le texte attire d'ailleurs l'attention sur ses stratagèmes de dépendance économique par le financement intensif de projets d'infrastructures au sein de pays insolvables d'Asie-Pacifique[1], d'Amérique du Sud et d'Afrique[2]. Washington dénonce régulièrement les dévaluations démesurées de sa monnaie et la concurrence faussée sur ses marchés. La Chine cherche à devenir *leader* dans les technologies de pointe, tant convoitées par les Etats-Unis. Elle n'en tire pas uniquement profit pour brider la liberté de sa population, mais également à des fins économiques et militaires[3]. C'est bien là que la situation prend encore une autre tournure. Pékin est accusé de miner l'économie américaine depuis des années par ses cyber activités. A l'époque, en 2017, Washington déclarait que ses moyens sophistiqués lui permettaient déjà de rivaliser à l'échelle d'une « guerre économique »[4]. Ses politiques de distorsion commerciale s'avèrent liées au transfert forcé de technologies et au vol récurrent de la propriété intellectuelle américaine. Sa progression technologique serait corrélative à une hausse de rapports d'espionnage sur le sol américain sous forme d'opérations d'exfiltration de données. Le contrôle de l'information et la pression exercée sur les entreprises américaines établies en Chine et aux Etats-Unis servent les politiques industrielles chinoises. Si elles ciblent le transfert de savoir-faire, le danger devient imminent en ce que ces manœuvres ont une incidence sur la sécurité civile et militaire aux Etats-Unis, sous-jacente à la dimension économique.

Quant à la Russie, elle est accusée de soutenir des régimes dictatoriaux et d'ébranler les structures de l'OTAN. Elle mènerait des opérations de guerre de l'information pour influencer l'opinion publique des Etats de la communauté internationale[5]. De ce fait, Moscou exploite les technologies émergentes pour discréditer les régimes démocratiques

[1] *National Security Strategy*, Washington : US Department of State, U.S. GPO, décembre 2017, p. 46
[2] Ibid., pp. 51-52
[3] Ibid., p. 25
[4] Ibid., p. 21
[5] Ibid., p. pp. 25-26, p. 35

pas uniquement dans les pays occidentaux, mais également en Géorgie, en Crimée et dans la partie orientale de l'Ukraine[6]. L'invasion de la Géorgie et de l'Ukraine démontre sa détermination à violer sans détour la souveraineté des Etats aux portes de l'Europe[7]. La modernisation de ses moyens militaires dans le domaine du cyber, du nucléaire et des missiles balistiques demeure une menace bien réelle.

En dépit des sanctions imposées par les Nations Unies, la Corée du Nord persiste à adopter une rhétorique belliciste. Son comportement irresponsable se manifeste par une démonstration de la puissance récurrente, jusqu'à multiplier le nombre de ses essais balistiques de plus en plus inquiétants. Mise à part une population muselée depuis 75 ans, le régime autoritaire et isolé compte bien se prémunir des menaces extérieures par la force violente. La Corée du Nord augmente son arsenal nucléaire, ses armes biologiques, chimiques, conventionnelles afin de contraindre la Corée du Sud et les Etats-Unis. De surcroit, à l'exemple des acteurs révisionnistes, Pyongyang défie ouvertement le *leadership* américain en menant des cyber activités malveillantes[8].

L'Etat d'Iran est dirigé par un régime oppresseur semant la terreur au sein d'une société civile asservie. La stabilité régionale est le défi principal du Moyen-Orient, mais le gouvernement provoque ouvertement ses voisins en créant un arc d'influence et de déséquilibre. Son dessein est d'imposer une domination régionale par la violence. Le régime est accusé d'avoir réamorcé son programme nucléaire en dépit du *Joint Comprehensive Plan of Action* (JCPoA) signé en 2015. L'Iran développe en parallèle un programme de missiles balistiques de grande envergure. Les dirigeants soutiennent des groupements terroristes afin d'atteindre ces objectifs[9]. En réponse, l'armée américaine mène des opérations de contreterrorisme et de cybersécurité sur le territoire iranien[10].

Si les enjeux de la cyberesécurité figurent dans la NSS et la NDS (cf. *supra*), ils ne sont rien moins que l'objet de la *National Cyber Strategy* (NCS) et de la *Department of Defense Cyber Strategy* (DCS). D'autres types de documents officiels s'y consacrent. La *Cloud strategy* répond au besoin d'une transition technologique, en l'occurrence numérique, tandis que les Budgets présidentiels de l'*Office of Management and Budget* (OMB) et les bilans budgétaires du Département de la Défense se focalisent sur la réduction des coûts de la cybersécurité. L'actuelle Administration affiche clairement la volonté de répondre aux objectifs de sécurité par des moyens de la force. Les documents officiels accentuent la coopération militaire avec les alliés et partenaires, cependant sans faire l'impasse sur une stratégie d'influence, à tout le moins de persuasion.

[6] *National Defense Strategy*, Washington : US Department of Defense, U.S. GPO, janvier 2018, p. 2- 3
[7] *National Security Strategy*, op. cit., p. 47
[8] *National Defense Strategy*, op. cit., p. 2-3 ; *National security strategy*, op. cit., p. 46
[9] *National Defense Strategy*, op. cit., p. 2-3
[10] *National Security Strategy*, op. cit., p. 47, p. 49

La présente analyse a pour ambition de rendre compte de leur consistance. Elle se divise en deux parties. La première présente les enjeux généraux des technologies de nouvelle génération, avant d'aborder les budgets dédiés. La seconde partie propose une lecture plus approfondie des documents de Washington sous l'angle de quatre grandes priorités : le peuple, la nation et *l'American way of life* (2.1.), la prospérité économique (2.2.), la paix par la force (2.3.) et l'image du *leadership* américain (2.4.). La conclusion retraduit les éléments de l'analyse en trois caractéristiques, par analogie au rôle international que les Etats-Unis endossent traditionnellement : « l'auto-préservation » ou la préservation des intérêts nationaux, la « conquête » par le *leadership* techno-économique, « sauver » en garantissant la stabilité internationale. De cette perspective, nous évoquerons quelques écueils liés à un risque de déséquilibre entre les objectifs fondamentaux et les moyens pratiques, voire techniques que les documents renferment.

1. Enjeux technologiques

La NCS de 2018 publiée par la Maison Blanche affirme que le cyberespace est devenu inséparable de la vie socio-politique et économique de la nation[11]. Les institutions publiques, l'armée, les entreprises et les citoyens dépendent au quotidien des nouvelles technologies de l'information et de la communication (NTIC). Les Etats-Unis intègrent désormais le cyberespace en tant que secteur clé, indissociable des autres dimensions de la puissance nationale[12]. En soutien à la NCS, la DCS du Département de la Défense est plus axée sur le rôle pratique de l'armée. Pour protéger le *homeland*, le Département a la ferme intention d'accroitre ses activités dans ce domaine[13]. Le cyberespace et le spatial, en pleine évolution, sont convoités par toute une gamme d'acteurs internationaux : investisseurs, consommateurs, scientifiques, spécialistes de la défense, législateurs, compétiteurs stratégiques[14]. Les menaces des puissances révisionnistes et des régimes hors-la-loi croitront dans les années à venir en raison de leurs progressions rapides en matière de technologies de nouvelle génération, telle que l'intelligence artificielle (IA), le *Machine Learning* (ML) et les technologies mobiles[15]. Le but est de préparer les Etats-Unis à toute guerre ouverte dont les tenants et aboutissants dépendront de la maitrise de ces nouveaux environnements stratégiques, d'où l'importance d'un investissement soutenu.

1.1. IA, 5G, *Space Force*

La NSS rappelle que l'information est cruciale à la sécurité nationale, la diplomatie et une économie mondiale à croissance durable. Les rivaux des Etats-Unis l'instrumentalisent pour nuire aux valeurs et aux institutions occidentales. Les failles des systèmes gouvernementaux et des entreprises leur permettent de se doter de données exfiltrées de sources personnelles et commerciales. Ils effectueraient en effet des opérations marketing de masse sur base de critères d'activités, d'intérêts, d'opinions individuelles afin de disséminer leur propagande. Les risques sécuritaires se multiplieront à mesure qu'ils acquièrent une connaissance des publics cibles[16]. Par conséquent, les Etats-Unis entendent conserver leur prédominance technologique et dans le monde de la recherche en vue de perpétuer leurs avantages compétitifs[17]. Le gouvernement américain confirme effectivement l'importance de l'innovation en promouvant des institutions et des programmes destinés à dynamiser la compétitivité des Etats-Unis. Si l'Administration se donne pour objectif d'enrayer les

[11] *National Cyber Strategy*, Washington: The White House, U.S. GPO, 2018, p. 1
[12] Ibid., p. 20
[13] *Department of Defense Cyber Strategy*, Washington: US Department of Defense, U.S. GPO, 2018, p. 1- 2, p. 7
[14] *Artificial Intelligence and National Security,* Washington : CRS Reports, Library of Congress, août 2020, p. 1
[15] L'IA et le ML *(Machine Learning)*, couvrent l'arsenal nucléaire et de missiles balistiques dans le domaine militaire, à côté de la diplomatie, le renseignement, l'économie et la finance.
[16] *National Security Strategy*, op. cit., p. 34
[17] *National Cyber Strategy,* op. cit., p. 9, p. 16

pratiques commerciales prédatrices de la Chine – fusions et acquisitions déloyales, vol de propriété intellectuelle –, elle mise sur l'informatique quantique (ISQ), l'IA et les technologies mobiles de cinquième génération (5G).

La 5G a la capacité d'accroître le transfert de données à une vitesse exponentielle – 10 à 100 fois plus vite que la 4G –, et d'élargir la bande passante avec une latence ultra faible – de 50 millisecondes pour la 4G, à 1 ou 2 millisecondes pour la 5G. Elle permettrait d'exploiter le potentiel entier des services numériques à cet effet[18] et de desservir les applications IA futures du secteur commercial (p. ex. véhicules autonomes, solutions *smart cities*) et de soutenir l'autonomie de dispositifs interconnectés (p. ex. *smart homes*, systèmes de précision dans l'agriculture, machinerie industrielle, robotique de pointe). Le gouvernement américain entend faire profiter autant les consommateurs que les industries des avantages de cette technologie (p. ex. aide aux personnes handicapées, télémédecine, automatisation, efficacité des opérations). Enfin, la 5G devrait générer des retombées économiques bénéfiques (p. ex. productivité augmentée, emplois, salaires, pouvoir d'achat, croissance)[19]. Il a été démontré nombre de fois par le passé que les entreprises pionnières sur les marchés des technologies sont celles qui captent l'essentiel des recettes. De ce fait, partout dans le monde des entreprises se lancent dans une course à la 5G. D'autre part, le gain économique considérable à la clé ne passe pas inaperçu auprès des Etats. Ceux-ci voient aussi tout l'intérêt de se frayer une place sur ce marché rentable. Ainsi, le gouvernement américain soutient son déploiement par la mise à disposition des fréquences de bande passante et la rationalisation des processus d'implémentation de petites cellules 5G[20].

Le Etats-Unis se donnent aussi pour objectif de pérenniser leur *leadership* dans le domaine spatial. La NSS ne peut être plus clair à ce sujet. Le *homeland* n'est plus un sanctuaire inébranlable. Des terroristes s'en prennent aux citoyens américains. Des cyber activités sont lancées contre les infrastructures privées et publiques. Comme mentionné, d'autres sont conçues pour subvertir les informations et les politiques nationales. Tandis que l'extension mondiale de la connectivité numérique est un des facteurs corrélatifs de ces vulnérabilités, de nouvelles menaces résultent de l'exploitation commerciale et militaire de l'espace. Les communications et réseaux financiers, les systèmes de renseignement *(*cfr. *infra)* dépendent

[18] La 5G a été développée en réponse à la demande croissante du consommateur en données mobiles : plus d'utilisateurs commerciaux et industriels utilisent des données en fonction de l'augmentation et de la diversification de la production de dispositifs, répondant à cette demande.

[19] Une étude *Accenture* en 2017 prévoyait que les fournisseurs en télécommunications investiront dans les années à venir plus de 275 milliards de dollars en infrastructures 5G, générant 3 millions d'emplois et une augmentation de 500 milliards de dollars en PIB. in *Fifth-Generation (5G) Telecommunications Technologies - Issues for Congress*, Washington : CRS Reports, Library of Congress, janvier 2019, p. 7

[20] Ibid, pp. 6-7 ; *National Security Implications of Fifth Generation (5G) Mobile Technologies*, Washington : CRS Reports, Library of Congress, octobre 2020, p. 1

de la liberté d'action dans l'espace. Cette dépendance aux Etats-Unis s'est fortement accrue ces dernières décennies. D'autres acteurs étatiques et non-étatiques, autrefois contraints par des obstacles insurmontables, ont acquis les compétences pour s'approprier les systèmes spatiaux et les informations qui en proviennent[21]. Les éventuelles menaces issues de ce changement de rapport de force doivent impérativement être anticipées en monopolisant l'espace. C'est ce qui a motivé la création de l'*United States Space Force* (USSF) fin 2019. L'*US Space Force* constitue désormais la 6ème branche des Forces Armées des Etats-Unis. Elle a été créée parmi le Département de l'*Air Force* (DAF) avec l'adoption de la *National Defense Authorization Act* de 2020 (NDAA FY2020)[22]. Le Commandement des Opérations Spatiales (*Space Operation Command*) est centralisé au niveau de la *United States Space Command*. Ce service a existé entre 1985 et 2002 avant d'être rétabli en août 2019. Le Congrès autorisa le 20 décembre 2019 la création de l'USSF, en remplacement de l'*Air Force Space Command*[23].

1.2. Le *Cloud* de la Défense

Aujourd'hui l'IA n'est plus une notion innovante en soi, mais cette technologie a évolué à un stade sans précédent. L'adaptation du processus d'acquisition des moyens de défense est jugée vitale pour en faire une exploitation optimale. Le *Cloud*, aussi appelé nuage informatisé, répond au problème auquel fait face le Département de la Défense en matière de gestion de l'information. L'architecture numérique sur laquelle reposait l'IA a pendant longtemps été fragmentée, découplée, dans un contexte où il n'est désormais plus possible de reporter la transition technologique. Le Département dispose de multiples systèmes d'informations dans le monde qui encore en 2018 reliaient les infrastructures nationales de façon incohérente. Le travail du Département, a pendant longtemps, été mis à mal par la limitation de ressources matérielles et humaines, l'acquisition inadéquate de compétences et des passations de contrats laborieux. Jusqu'à récemment, beaucoup d'effectifs étaient confrontés à des difficultés dans l'accomplissement de leurs tâches, parfois au point de ne plus être en mesure de traiter les données de la Défense efficacement. Ces lacunes affectent inévitablement les missions des décideurs et des militaires[24]. Il est indéniable que la *Joint force* perdra sa supériorité si les systèmes hérités du passé tardent à être modernisés[25]. Depuis, la transition est en route, mais elle ne se déroule pas de manière homogène.

[21] *National Security Strategy*, op. cit., p. 31
[22] *Defense Primer: The US Space Force*, Washington : CRS Reports, Library of Congress, avril 2020, p. 1
[23] Ibidem.
[24] *DoD Cloud Strategy,* Washington : US Department of Defense, U.S. GPO, décembre 2018, p. 1
[25] *National Defense Strategy,* op. cit., p. 1

Pour y remédier, la stratégie *Cloud* comporte quatre grands principes. Premièrement, son architecture unifiée suppose une offre de service d'infrastructure et d'un service de plateforme distincts (IaaS et PaaS). Deuxièmement, le *Cloud* doit être capable de gérer en parallèle des environnements virtuels séparés, à tous niveaux de classification. Troisièmement, cette technologie favorise autant une informatique centralisée, qu'une informatique tactique conçue pour les militaires sur le terrain. Enfin, son implémentation est censée faciliter l'émergence de technologies, telles que l'IA[26]. Afin de maximiser l'utilité du nuage, les données sont gérées par divers outils de soutien – lacs de données et *hubs* de données[27] –, à leur tour accélérés et amplifiés par la technologie *Cloud*[28]. En résumé, le *Cloud* est une solution flexible qui garantit la transparence de l'information en partage. Son architecture accroit la sécurité des technologies de l'information (IT), tout comme la rapidité de calcul et de traitement de données, ce à quoi la 5G contribue en aval.

1.3. Les budgets

Suivant la même logique, l'*Office of Management and Budget* confirme que la cybersécurité est essentielle à la modernisation des TI[29]. Comme abordé ci-dessus, l'usage de plateformes numériques en ligne est inséparable de l'activité quotidienne des agences fédérales. L'OMB constatait en 2018 que les systèmes mis à leur disposition depuis plus d'une décennie étaient devenus trop coûteux. Leur obsolescence occasionne un manque d'opportunités, freine la collaboration et la créativité[30]. Des agences ayant adopté des solutions *Cloud* quelques années auparavant avaient fait des économies considérables, s'élevant de 500.000 dollars jusqu'à 10 millions de dollars par an[31]. Depuis, le gouvernement fédéral encourage l'ensemble des agences fédérales et civiles de migrer vers ces outils. Selon les perspectives budgétaires, les économies générées stimuleront la productivité des services[32]. Le financement de la Défense en matière de IA avait d'ailleurs nettement augmenté en 2018. Le budget incluait 1,75 milliards de dollars répartis sur 6 ans, à côté d'un investissement de 6 milliards de dollars dans 20 programmes de la *Defense Advanced Research Projects Agency's* (DARPA). Certains experts étaient d'avis qu'un financement fédéral

[26] *DoD Cloud Strategy,* op. cit., p. A-2
[27] Ces deux concepts sont étroitement liés à la gestion du *Big Data.* Les lacs de données permettent de stocker d'immenses volumes de données structurées, semi-, ou non-structurées à l'état brut pour une durée indéterminée. Un *hub* de données est une plateforme de stockage virtuelle qui permet de les analyser et de les partager de façon sécurisée au sein d'une architecture unifiée. En outre, les données communiquent entre elles « (…)dans toutes les directions ». in LE BIG DATA.FR, *Data Lake : définition, avantages et inconvénients pour l'entreprise* [en html], https://www.lebigdata.fr/data-lake-definition (19/10/2020) ; LE BIG DATA.FR, *Data Hub définition : tout savoir sur les hubs de données* [en html], https://www.lebigdata.fr/data-hub-definition (19/10/2020)
[28] *DoD Cloud Strategy,* op. cit., p. 5
[29] *An American Budget – Analytical Perspectives (Budget of the US Government), Fiscal Year 2019,* Washington : Office of Management and Budget (OMB), US GPO, 2018, p. 273
[30] Ibid., p. 225
[31] Ibidem.
[32] Ibid., p. 273

supplémentaire était nécessaire pour concurrencer les rivaux stratégiques des Etats-Unis et éviter un « déficit de l'innovation » de la technologie militaire. Des voix opposées à une augmentation soutiennent l'idée que l'armée doit mettre à profit l'expertise, la recherche et le développement (R&D) menés dans le secteur commercial[33].

Plus généralement, le budget des Etats-Unis pour la sécurité s'élevait à 686,1 milliards de dollars pour l'année 2019 (5% de plus qu'en 2018)[34], contre 740,5 milliards de dollars pour le budget de 2021 (hausse de 7,93%), dont 705,4 milliards de dollars seront affectés au Département de la Défense[35]. Concernant la cybersécurité, le budget a été estimé à près de 15 milliards de dollars, ce qui représente une augmentation de 583,4 millions de dollars (4,1%) par rapport à 2018. Le Département de la Défense, plus gros contributeur, avait déclaré un apport de fond à hauteur de 8,5 milliards de dollars, soit, une augmentation de 340 millions de dollars (4,2 %) par rapport à 2018[36]. Le Budget de 2021 accorde plus que jamais la priorité aux Industries du Future (IotF) : l'IA, la science informatique quantique (QIS), la 5G et autres systèmes de communications avancés, la biotechnologie, la production manufacturière de pointe[37]. Les financements de la Défense pour le cyber, l'IA et le spatial sont en nette hausse également. Sa proposition de budget annonce un apport de 9,8 milliards de dollars (15,29% de plus qu'en 2019) destinés au cyberespace, dont 5,4 milliards pour la cybersécurité, 3,8 milliards aux opérations cyber et 556 millions de dollars dans les sciences et technologies. En addition, 841 millions de dollars seront consacrés à l'IA. Le Département investit 789 millions pour le *Cloud* et 1,5 milliards dans le secteur des microélectroniques, dont la 5G. D'autre part, 18 milliards de dollars sont dédiés au domaine spatial. Ce montant inclut 15,4 milliards de dollars pour l'*US Space Force*, dont 1,6 milliards pour trois lancements spatiaux EELV, 1,8 milliards pour GPS III et d'autres projets divers, 2,5 milliards pour SBIRS (*Space Based Infrared Systems*) et OPIR (*Overhead Persistent Infrared)*, 249 millions de dollars pour l'*US Space Command*, et enfin, 337 millions de dollars pour l'Agence de Développement Spatial[38].

---

[33] *Artificial Intelligence and National Security*, op. cit., p. 6

[34] Toujours est-il qu'en 2019 le ratio dépenses/PIB de 3,1% restait bien inférieur aux décennies antérieures. in *Defense Budget Overview, FY 2019,* Washington: United States Department of Defense, février 2018, p. 1-1, p. 1-3

[35] DEFENSE.GOV, *DOD Releases Fiscal Year 2021 Budget Proposal* [en html], https://www.defense.gov/Newsroom/Releases/Release/Article/2079489/dod-releases-fiscal-year-2021-budget-proposal/ (19/10/2020)

[36] *An American Budget – Analytical Perspectives – FY 2019,* op. cit., p. 273

[37] *A Budget for America's Future, analytical perspectives – FY 2021*, Washington : Office of Management and Budget (OMB), US GPO, 2020, p. 233

[38] *DOD Releases Fiscal Year 2021 Budget Proposal,* op. cit.

2. Objectifs et moyens stratégiques : quatre priorités

La prochaine section analyse désormais les objectifs et les moyens mis en œuvre pour répondre aux enjeux de la cybersécurité sous l'angle des quatre priorités évoquées précédemment. Elles s'alignent avec les quatre piliers de la NCS et de la NSS, à quelques exceptions près.

2.1. Peuple et nation : *l'American way of life*

La nation, le peuple et le *homeland* américains sont inséparables de *l'American way of life,* mode de vie sous forme de morale nationale déjà consacrée par les principes de la Déclaration d'indépendance de 1776[39]. La première priorité de la NCS est leur préservation. Le texte indique d'emblée que cette priorité doit être réalisée en renforçant la cybersécurité. Pour ce faire, une meilleure collaboration interinstitutionnelle est préconisée, non seulement entre les départements et les agences fédérales, mais également entre l'Etat fédéral et les gouvernements fédérés/locaux. Dans cette intention, l'administration Trump annonce également la centralisation d'organes de pouvoir au sein du gouvernement[40]. Une meilleure communication doit être établie entre les fonctionnaires à tous les échelons pour la bonne marche des institutions démocratiques : il est impérieux de protéger les processus électoraux[41]. Les budgets des Etats fédérés alloués à la cybersécurité - entre 0% à 2% de la totalité des budgets IT-, rendent compte la raison pour laquelle les défis attendus n'auraient pas été relevés en 2018. Les gouvernements témoignaient d'une trop grande dépendance par rapport aux programmes gouvernementaux afin de financer leurs activités : 49% des Etats cherchaient des sources alternatives, notamment auprès d'organismes fédéraux. 47% dépendaient de programmes du *Department of Homeland Security* (DHS). 82% percevaient la cybersécurité comme une priorité nationale, mais seulement 13% se déclaraient suffisamment compétents, déclin de 3% comparé à l'année 2012[42].

Par ailleurs, la NCS attire l'attention sur la coopération étroite entre les instances gouvernementales, les localités et la société civile, l'industrie privée en particulier [43], afin de protéger les réseaux publics/privés[44]. D'ailleurs, dans son second pilier, la NSS entend perfectionner les infrastructures nationales et numériques en les dotant des nouvelles technologies décrites ci-dessus. Cela comprend la modernisation des aéroports, des ports maritimes, des voies navigables, des routes, des systèmes de transit et des

[39] *« We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness », «(…)to them shall seem most likely to effect their safety and happiness ».* in ARCHIVE.GOV, *Declaration of Independence: A Transcription* [en html] : https://www.archives.gov/founding-docs/declaration-transcript (19/10/2020)

[40] *National Cyber Strategy*, Washington: The White House, U.S. GPO, 2018, p. 6

[41] Ibid., p. 9

[42] *An American Budget – Analytical Perspectives – FY 2019,* op. cit., p. 275

[43] En référence à la population, au monde académique et scientifique, et à l'industrie privée en particulier.

[44] *Department of Defense Cyber Strategy,* op. cit., p.1, p. 3, p. 5

télécommunications[45]. La libre circulation des biens, le transit du pétrole et du gaz naturel dépend de la sécurité des lignes de communication nationales[46]. A ce même titre, le troisième pilier de la NSS et le premier pilier de la NCS insistent sur le libre accès à l'environnement spatial. La connaissance, le savoir-faire scientifique et les systèmes spatiaux de la nation américaine en dépendent[47]. Les chaines logistiques et les services de la nation doivent être confortés à cet effet. L'étude des tendances et risques liés aux progrès technologiques – IA, QIS, 5G – répond au besoin d'adopter des pratiques sûres (NSS, 2ème pilier)[48]. A cette fin, le gouvernement continuera d'élaborer des normes avec l'appui de la *National Institute of Standards and Technology* (NIST)[49]. Dans le même esprit, le *Joint Artificial Intelligence Center* (JAIC) de la Défense rappelle que la coopération devra s'établir à travers un système d'informations uniformisé, à distance en *Cloud*, basé sur un modèle managérial d'entreprise[50]. Des fournisseurs IT, en sous-traitance avec le Département de la Défense, ont pour mission de sécuriser les informations sensibles de l'industrie militaire[51]. Ils ont ainsi acquis avec les décennies un rôle indispensable dans la planification des cyber activités et des opérations militaires[52]. Ce procédé implique une responsabilité partagée de commandement et de contrôle (C2)[53].

2.2. Prospérité, sécurité économique

La prospérité et la sécurité économique sont au cœur de la seconde priorité. La NCS souligne qu'une économie stable permet d'exceller dans la recherche, le développement, de perpétuer l'innovation. Réciproquement, l'économie mondiale est de plus en plus dépendante des IT[54]. Si les Etats-Unis revendiquent le *leadership* dans « (…)l'écosystème des technologies émergentes »[55], le cyberespace est vecteur de croissance et catalyseur de la concurrence. C'est ce qui explique pourquoi l'Administration veut mettre en place un marché technologique fiable. L'objectif est de susciter une demande et une offre adéquate dopant le développement[56]. Pour ce faire, le Département de la Défense préconise une approche de performance et de compétition axée sur le financement soutenu des ressources[57]. L'*International Data Corporation* prévoit un accroissement des dépenses non-fédérales dans le domaine de la cybersécurité, bien davantage que dans le domaine des TI

[45] *National Security Strategy*, op. cit., p. 19
[46] *National Cyber Strategy,* op. cit., pp. 9-10
[47] *National Security Strategy*, op. cit., p. 31 ; *National Cyber Strategy,* op. cit., pp. 9-10
[48] *National Security Strategy*, op. cit., p. 20
[49] *National Cyber Strategy,* op. cit., p. 8
[50] *DoD Cloud Strategy,* op. cit., p. 2, p. 4
[51] *National Cyber Strategy,* op. cit., p. 9
[52] *Department of Defense Cyber Strategy,* op. cit., p. 5
[53] *DoD Cloud Strategy,* op. cit., p. 5
[54] *National Cyber Strategy,* op. cit., p. 14
[55] Ibid., pp. 15-16
[56] Ibid., pp. 14-16
[57] *National Defense Strategy*, pp. 4-5 ; *Department of Defense Cyber Strategy*, p. 4, p. 7

en général. Elles avoisineront 101,6 milliards de dollars en 2020[58]. A l'instar de la première priorité, le gouvernement plaide pour un système de coordination efficace avec les Etats fédérés, les agences fédérales[59] et l'industrie pour déjouer les barrières technologiques, telles que l'anonymisation et les techniques de cryptage[60].

Le budget de 2021 met l'accent sur l'établissement de lignes directrices de développement et d'utilisation de l'IA dans les secteurs économiques. La promotion d'un environnement international, en soutien au R&D, doit faciliter l'ouverture des marchés à l'égard les industries américaines. Avec l'aide fédérale, les entreprises optimisent l'IA dans les secteurs de la sécurité financière et alimentaire. La SEC (*Securities and Exchange Commission*) applique des algorithmes ML pour contrôler et détecter les erreurs sur les marchés des placements. En outre, en septembre 2019, la CFPB (*Consumer Financial Protection Bureau*) avait adopté de nouvelles politiques permettant une exploitation extensive des données et algorithmes ML dans les services et produits financiers. Par conséquent, la stimulation de la concurrence baisse les prix et fournit aux consommateurs de meilleurs produits et services. Le Département de l'Agriculture (USDA) conduit des recherches sur le développement et l'utilisation ML et IA, afin de créer des modèles de rendements de culture, basés sur des analyses météorologiques. Ces efforts doivent encourager la prospérité des régions agricoles[61].

Pour finir, le gouvernement voit l'intérêt d'investir l'espace par sa commercialisation. En décembre 2017, le Président Trump signa la Première Directive de politique spatiale (SPD 1), appelant les Etats-Unis à prendre la tête d'une nouvelle course, celle du (…)retour des humains sur la lune pour une exploration et exploitation de long terme »[62]. En mars 2019, Mike Pence, le Vice-Président, avait réitéré l'importance d'envoyer des astronautes américains sur la lune endéans les 5 ans. Le budget de 2021 souligne les efforts R&D en vue d'accomplir cet objectif à commencer par la surface lunaire - objectif de la *Lunar Surface Innovation Initiative* - , tout en scrutant les possibilités d'aller sur Mars :

> *(…)Technologies are prioritized that enable a sustainable presence on the lunar surface that also feed forward directly to Mars including in-situ resource utilization, cryogenic fuel storage and management, surface excavation, manufacturing and construction, and advanced space power(…)*[63].

L'expansion de la sphère d'influence économique des Etats-Unis dans l'orbite terrestre basse, sur la lune et au-delà repose sur la compétitivité du secteur commercial spatial[64].

---

[58] *An American Budget – Analytical Perspectives - FY 2019*, op. cit., p. 275

[59] Les agences fédérales devraient encourager ce mécanisme. Bon nombre d'entre elles (76) évaluées par l'OMB en 2018 auraient une gestion responsable de leurs informations. Plusieurs avaient d'ailleurs des dépenses dans des missions plus étendues que la protection de leurs réseaux. in, *An American Budget – Analytical Perspectives - FY 2019*, op. cit., p. 273

[60] *National Cyber Strategy,* op. cit., p. 10

[61] *A Budget for America's Future, analytical perspectives – FY 2021*, op. cit., p. 225

[62] Ibid., pp. 236

[63] Ibid., pp. 236-237

[64] Ibidem.

2.3. La paix, par la force

La troisième priorité de la NCS est la préservation de la paix par la force. La dissuasion et l'identification des comportements contraires aux intérêts nationaux sont inhérentes à une bonne gestion de l'information, en ce qu'elle concourt au « (…)caractère létal de la *Joint Force* »[65]. La qualité des services du Département de la Défense repose sur la faculté de stocker et de diffuser des données au cours d'opérations militaires sur des champs de bataille toujours plus modernes[66]. Les rapides évolutions technologiques – IA, ML, 5G –, ainsi que la nature changeante de la guerre affectent l'environnement sécuritaire[67] , devenu plus vaste, moins palpables, semé de nouveaux défis, sans oublier l'avènement de nouveaux protagonistes. Cette tendance bouscule inévitablement les rapports de puissance traditionnels.

Le Département de la Défense est à nouveau au diapason avec l'Administration quant aux engagements internationaux. La puissance américaine dépend d'une coopération effective avec les alliés/partenaires, reposant sur l'établissement des mesures de confiance et des règles communes du cyberespace. La NCS de la Maison Blanche soutient que les normes de responsabilité en matière de droit international issues des travaux du *Groupe d'experts gouvernementaux des Nations Unies* (UNGGE) doivent continuer d'encadrer le comportement des Etats[68]. En outre, un objectif connexe est l'anticipation des menaces. Il s'agit d'identifier les programmes de recherche, les tactiques et les opérations d'acteurs malintentionnés[69] par une collecte conjointe de l'information. Au niveau opérationnel, la DCS de la Défense est plus pratique. Le texte est spécifiquement axé sur la protection des infrastructures de défense, l'interopérabilité, l'expérience opérationnelle de l'armée. Ici aussi, l'accent n'est donc pas seulement mis sur la dissuasion, mais également sur la prévention des menaces, avant leur éradication. Pour y parvenir, de concert avec la NCS, la DCS de la Défense préconise une mobilisation de tous les « (…)instruments de la puissance nationale »[70]. Mais le texte du Département insiste davantage sur le développement des moyens adéquats, non seulement afin de se parer des tentatives d'exfiltration de données militaires, mais d'être en mesure de « (…)livrer des guerres futures et d'en sortir victorieux »[71]. De fait, il sera essentiel de déployer les moyens cyber en soutien aux forces aériennes, navales, terrestres et spatiales de l'armée américaine[72]. La *Joint Force* dépend donc autant de « (…)l'agilité par l'innovation »[73] que de la « (…)résilience des systèmes et

[65] *Department of Defense Cyber Strategy*, op. cit., p. 4 ; *Cloud strategy*, op. cit., p. 10
[66] Ibid. (*Cloud strategy,* avant-propos)
[67] *National Defense Strategy*, op. cit., p. 3
[68] *Department of Defense Cyber Strategy*, op. cit., p. 5 ; *National Cyber Strategy,* op. cit., p. 20
[69] « *(…)malign influence and information operations such as information campaigns and non-state propaganda and disinformation. »,* in ibidem.
[70] *"(…)diplomatic, information, military (both kinetic and cyber), financial, intelligence, public attribution, and law enforcement capabilities.",* in ibidem. ; *Department of Defense Cyber Strategy,* op. cit., p. 4
[71] Ibid., p. 2 ; *National Defense Strategy*, op. cit., p. 3
[72] *Department of Defense Cyber Strategy,* op. cit., p. 1
[73] Ibid., p. 4

réseaux »[74]. C'est ici que le *big data*, la robotique, les biotechnologies, la 5G et surtout l'IA, domaines clés, prennent un sens concret : une meilleure automatisation et analyse de données doit faciliter l'identification et l'éradication immédiate des activités hostiles sur le terrain par la force[75].

La *Cloud strategy,* plus technique, répond spécifiquement aux besoins « (…)d'adaptation par l'innovation »[76] en soutenant par exemple les C4ISR[77]. Au cours des opérations de terrain, le *Cloud* de la Défense permettrait un approvisionnement spontané des ressources. Les effectifs de la *Joint Force* disposeront automatiquement de données fiables à tout moment, en tout lieu[78]. Les informations sont aussi cruciales quant à la prise des décisions politico-militaires, que ce soit en temps de guerre ou en temps de paix. L'intelligibilité de leur transmission dépend d'algorithmes dont les données sont organisées, visibles dans l'espace virtuel sécurisé, le cas échéant en commun avec les forces de coalition. De cette manière, l'exploitation souple de l'IA et du ML par l'intermédiaire du *Cloud* facilite la communication tout au long de la chaine de commandement dans les moments les plus décisifs[79]. Ces atouts améliorent par la même occasion les liens diplomatiques et les capacités de négociation : *« Reinforcing America's traditional tools of diplomacy, the Department provides military options to ensure the President and our diplomats negotiate from a position of strength. »*[80].

Actuellement, des applications concrètes démontrent toute l'utilité de l'IA dans les systèmes ISR. La première phase de *Projet Maven* est axée sur le traitement automatisé des renseignements en soutien aux opérations de contre-espionnage dans la lutte contre l'Etat islamique. Des algorithmes ML incorporés dans des ensembles de renseignements recueillis permettent de passer au peigne fin des séries d'images et séquences vidéo enregistrées par des drones et d'identifier automatiquement des activités potentiellement hostiles. Déchargés de ces tâches, les analystes tirent des conclusions plus efficacement. Par ailleurs, la CIA conduit une centaine de projets ou l'IA est sollicitée dans des tâches de reconnaissance d'images et d'analyses prédictives. L'*Intelligence Advanced Research Projects Activity* (IARPA) parraine plusieurs projets IA destinés à produire d'autres outils analytiques. Citons le développement d'algorithmes pour une reconnaissance et traduction vocale multilingue dans des lieux bruyants, la géolocalisation d'images dissociée de métadonnées, la fusion d'images 2-D pour créer des modèles 3-D[81]. La NCS et la NDS priorisent par ailleurs les investissements pour renforcer la résilience de la cybersécurité au

[74] *Department of Defense Cyber Strategy,* op. cit., p. 1
[75] Ibid., p. 4
[76] *DoD Cloud Strategy,* op. cit., p. 3, pp. 8-9
[77] *Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance*
[78] *DoD Cloud Strategy,* op. cit., pp. 3-4
[79] Ibid., pp. 5-6
[80] *National Defense Strategy*, op. cit., p. 1
[81] *Artificial Intelligence and National Security* op. cit., pp. 8-10

cours des opérations spatiales[82]. Citons les implications pour le positionnement, la navigation et la datation (PNT), les communications satellites et la surveillance météorologique[83]. Puis, le budget spatial pour 2021 entend stimuler le financement QIS R&D, cumulant les investissements des agences fédérales à hauteur de 50% en plus par rapport à 2020. Ce budget est en voie de doubler pour l'année 2022. L'investissement de la *National Science Foundation* (NSF) doublera avec un apport additionnel de 120 millions de dollars dédié à la *National Quantum Initiative*. Le Département de l'Energie (DOE) stimulera les efforts en information quantique des laboratoires nationaux et académique et des industries grâce à une augmentation de 75 millions de dollars. Un financement est prévu afin que la NASA étudie les conditions de faisabilité d'une expérience sur le phénomène d'intrication quantique appliqué à Internet dans l'espace. En 2021, le DoD investira plus de 59 milliards de dollars dans la recherche, l'ingénierie et les activités de prototypage pour favoriser les capacités militaires de pointe dans l'espace dans un avenir proche. Citons les armements défensifs et offensifs hypersoniques, la résilience des systèmes spatiaux de la sécurité nationale et les capacités de dissuasion nucléaires stratégiques et non-stratégiques flexibles[84].

2.4. Image du *leadership*

En ce qui concerne la quatrième priorité, la démarche propose un rapprochement avec des éléments du premier, second et troisième piliers du texte officiel de la NCS.

Ce serait une erreur de croire que le gouvernement américain se limite à l'unique démonstration de la puissance militaire ou de la force de police. Pour cette dernière priorité, les Etats-Unis tentent de légitimer leur image, leur statut d'hégémon bienveillant sur la scène internationale. L'objectif est de pérenniser l'influence américaine. L'Administration tente de légitimer leurs initiatives par le bienfondé des lois et du droit international. Elle s'attache à ce que les nations adhérant aux mêmes valeurs idéologiques adoptent des règles édictées. La NCS prône ouvertement que les intérêts américains sont indissociables des biens communs. Son troisième pilier précise que la dissuasion et l'enrayement du cybercrime ne seront payants que si leurs auteurs comprennent les conséquences de leurs actes. Ceux-ci doivent être convaincus de l'effectivité des moyens conçus pour les poursuivre, les traduire en justice et leur imposer des coûts[85]. Il s'agit non seulement de faciliter la poursuite de criminels à l'étranger, mais aussi de mettre hors d'état de nuire les infrastructures du crime organisé, indique le premier pilier[86]. Il faut à ce titre moderniser le droit de la criminalité informatique pour le recueil légal des informations. Le

[82] *National Defense Strategy*, op. cit., p. 6 ; *National Cyber Strategy, op. cit.,* p. 10
[83] Ibidem.
[84] *A Budget for America's Future, analytical perspectives – FY 2021*, op. cit., pp. 236-237
[85] *National Cyber Strategy,* op. cit., p. 21
[86] Ibid. p. 11

troisième pilier de la NCS indique également que les organismes fédéraux doivent disposés des compétences légales pour agir en conséquence[87].

En outre, les droits de l'homme sont trop souvent érodés par la censure numérique. Les régimes répressifs prennent illégitimement le contrôle d'Internet sous des prétextes de souveraineté[88]. La liberté dépend de la libre circulation de l'information. Son accès est propice au commerce international, à l'émergence de marchés techno-économiques. Autrement dit, Internet contribue à la prospérité, à l'innovation et à la démocratie. Dans ce cadre, les Etats-Unis, veulent promouvoir à travers la *Freedom Online Coalition* une architecture ouverte de ce médium[89]. Le soutien du gouvernement américain au développement des technologies et des formations en sécurité numérique prend ici tout son sens. Si l'innovation économique est un facteur de la puissance matérielle, la santé économique des Etats-Unis dépend de l'acquisition de brevets scientifiques. Dans ce cadre, la NCS, en phase avec le second pilier de la NSS, souligne l'importance d'une main-d'œuvre dans le domaine de la cybersécurité en stimulant l'éducation et l'emploi. L'Administration insiste sur l'essor d'un réservoir de talents nationaux et internationaux[90]. D'un point de vue idéologique, cette approche exprime la nécessité de diffuser la culture américaine.

La NCS envisage également de soutenir les alliés et partenaires, aussi bien dans leur interopérabilité que dans l'élaboration des leurs propre politiques nationales[91]. Le Département de la Défense s'efforce de consolider leur savoir-faire en vue de réduire les coûts collectifs de la sécurité[92]. Dans ce contexte, la future *Cyber Deterrence Initiative* repose sur la notion de *burden sharing,* puisqu'elle devra être composée de membres capables de se défendre et de soutenir l'Amérique. Mise à part cela, Washington attend de leur part qu'ils augmentent par eux-mêmes leurs capacités[93]. Le premier pilier de la NCS souligne que l'accroissement du consensus international par le biais d'instruments multilatéraux tels que l'*UN Convention Against Transnational Organized Crime,* le *G7 24/7 Network Points of Contact*, et la *Convention on Cybercrime of the Council of Europe* est indispensable à la réalisation de ces objectifs[94].

[87] *National Cyber Strategy,* op. cit., p. 21
[88] Ibidem.
[89] Ibid., p. 24-25
[90] Ibid., p. 17 ; *Department of Defense Cyber Strategy,* op. cit., p. 6
[91] *National Cyber Strategy,* op. cit., p. 26
[92] *Department of Defense Cyber Strategy,* op. cit., p. 6
[93] *National Cyber Strategy,* op. cit., p. 26
[94] Ibid., p. 11

CONCLUSION

En conclusion, les documents stratégiques de Washington en matière de cybersécurité soumis à l'étude croisée font preuve d'une relative consistance. Deux brèves remarques s'imposent toutefois au sujet de la NCS et de la NSS. Leurs piliers se recoupent, sauf à quelques détails près, et ne se superposent pas complètement aux priorités de notre analyse. Effectivement, des éléments clés des second et troisième piliers de la *National Security Strategy* s'appliquent spécifiquement au premier pilier de la NCS, donc à notre première priorité[95]. Similairement, quelques passages des premier, second et troisième piliers de la *National Cyber Strategy* semblent concorder davantage avec son quatrième pilier, en référence à la dernière priorité de l'analyse[96].

Les enjeux, les objectifs et les moyens dont les textes font état peuvent se résumer en trois points. Le premier point a trait à la préservation nationale par une meilleure gestion institutionnelle. Cette gestion implique deux types de relations de confiance et de responsabilités. Rappelons que la première priorité - la nation, le peuple -, souligne le renforcement de la cybersécurité. Premièrement, ce renforcement serait réalisable par le mécanisme de coordination nécessitant le cas échéant une centralisation d'instances fédérales. A l'échelle des Etats fédérés, ceux-ci sont enjoints de consolider leur collaboration et de moins dépendre du budget fédéral, selon les injonctions de l'OMB. Deuxièmement, la nécessité d'une collaboration public/privé régie par une responsabilité de commandement et de contrôle a été mise en lumière. Les acteurs du secteur commercial ont un rôle de première importance dans l'intention d'atténuer les risques de menaces. Ces deux types de relations exigent un partage sécurisé de l'information en faveur du traitement efficace de données sensibles, notamment grâce au *Cloud*. La transition technologique va de pair avec l'adoption d'un modèle de management d'entreprise. Ce modèle s'incarne par une centralisation des ressources au sein d'un espace virtuel normé, transparent entre acteurs. Ce premier point ne reflète pas moins la mise en œuvre d'une stratégie de nature néo-mercantiliste[97]. Sans qu'il y ait pour autant question d'hermétisme, les Etats-Unis adoptent une position d'auto-préservation. L'Administration procède à un repli institutionnel sur la base nationale. En résultat, une forte imbrication structurelle s'observe entre le domaine public et le secteur privé.

[95] cf. p. 9 à 10

[96] cf. p. 14 à 15

[97] Pour plus de détails sur les stratégies géoéconomiques néo-mercantilistes, hégémoniques et libéral-institutionnels théorisées par Mikael Wigell, voir R. DELBROUCK, *La relation sino-américaine : analyse de la politique étrangère américaine depuis 2017* - Note d'analyse n° 71, Louvain-la-Neuve : CECRI, septembre 2020, pp. 26-32 ; R. DELBROUCK, *Etat de la relation transatlantique : la politique étrangère américaine en perspective* - Note d'analyse n° 69, août 2020, pp. 24-31.

Le deuxième point renvoie à la conquête par l'innovation techno-économique. A côté d'une stratégie néo-mercantiliste, des éléments d'une stratégie hégémonique se dénotent. La seconde et la troisième priorité s'alignent, vu que prospérité et sécurité économique sont inhérentes aux avantages technologiques d'une armée victorieuse. Par rapport à la seconde priorité, nous avions vu que la prospérité permet d'être dominant dans le secteur des TI. Citons l'importance de stimuler l'offre et la demande sur les marchés concurrentiels, nationaux et internationaux. En d'autres termes, une position de force sur les marchés permet de développer les avantages stratégiques civilo-militaires dans le but de dominer dans tous domaines confondus - aérien, naval, terrestre, spatial, en l'occurrence le cyberespace. Inversement, la troisième priorité met l'accent sur la paix par la force, dont la puissance militaire. L'agilité de la *Joint Force* par l'adaptation et l'innovation doit permettre d'anticiper, d'identifier, d'éradiquer la menace. La résilience des infrastructures, des réseaux et l'interopérabilité de l'armée en dépendent. Ces atouts requièrent une transition vers le *Cloud*, concomitant à une mainmise sur la 5G, l'IA, le ML, si essentiels aux C4ISR, les PNT et la QIS. Par conséquent, l'innovation technologique reste garante de la sécurité économique.

Le dernier point est moins de l'ordre de la force tel quel, que de la force de persuasion et de l'influence pour sauvegarder la stabilité internationale. Ici, les Etats-Unis revêtent principalement un rôle hégémonique. Deux réflexions s'imposent.

(1) D'abord, nous déduisons que la troisième et la quatrième priorité se combinent. Si la troisième priorité est la préservation de la paix par la force, la quatrième entend promouvoir l'influence américaine. Un des objectifs communs de ces deux priorités est la « dissuasion » de la menace et des comportements contraires aux intérêts américains et ceux des alliés/partenaires. A ce stade, les notions de force et d'influence devraient donc être relativisées : là où les moyens matériels et légaux revêtent une force de persuasion sur la pertinence de leurs effets, l'influence, au sens étroit du terme, à vocation à mettre en lumière le bienfondé des lois et du droit par leur adhésion. Rappelons que les règles et normes, les mesures de confiance œuvrent à édifier l'environnement mondial du cyberespace.

(2) Ensuite, la quatrième priorité, dans son sens le plus strict, met en avant la volonté des Etats-Unis de prodiguer des biens collectifs. La mission de les préserver est à réaliser avec des alliés/partenaires capables, témoignant de la volonté de perpétuer les valeurs libérales en interdépendance par un partage des coûts. Dans ce dernier cas de figure, une posture hégémonique se conjugue à une posture libéral-institutionnelle. A ce titre, Internet est garant des démocraties et de leur prospérité. Rappelons aussi le rôle normatif des instruments multilatéraux pour l'affranchir de toute censure. Enfin, concernant la protection des idées américaines, la formation et l'emploi sont censés générer en continu une réserve de main-d'œuvre qualifiée propice à l'économie et à la sécurité technologique. La culture économique et politique des Etats-Unis doit attirer le génie, au même titre que le capital

d'investissement venant de tout horizon. En termes de *soft power* et d'influence, l'attractivité des valeurs américaines conforte la compétitivité de l'économie nationale.

Dès lors, quelques réflexions s'imposent sur d'éventuels obstacles auxquels l'Administration pourrait faire face. Il n'est pas exclu que la centralisation institutionnelle envisagée vienne entraver les relations de confiance entre les secteurs privé, public et militaire, ni la coopération entre les Etats fédérés, ni leurs efforts vers plus d'autonomie budgétaire. En d'autres mots, un déséquilibre entre ces objectifs serait susceptible de biaiser les responsabilités entre acteurs. La circulation et le traitement des données en serait affectés, générant un surcoût de la cybersécurité. Notons aussi que la réticence avérée de l'*America First* pour le multilatéralisme tranche avec la coopération préconisée avec les alliés/partenaires : *« With key countries in the region, we will bring together bilateral and multilateral security relationships to preserve the free and open international system.* »[98] ; *« We will bolster existing bilateral and multilateral partnerships and develop new relationships to address significant terrorist threats.* »[99] *; « (…)building new cybersecurity approaches that use emerging technologies, improving information-sharing and risk management related to cross-sector interdependencies(…)* »[100] ; *« We will push other nations to expedite their assistance in investigations and to comply with any bilateral or multilateral agreements or obligations.* »[101] ; *« The United States will encourage other nations to publicly affirm these principles (adherence to cyber norms) and views through enhanced outreach and engagement in multilateral fora.* »[102] ; *« The United States Government will defend the open, interoperable nature of the Internet in multilateral and international fora(…)* »[103]*.* Dans le même ordre d'idées, surtout sur fond de la guerre économique avec la Chine, les intérêts des industries américaines se heurtent au protectionnisme de l'administration Trump. Sa posture néo-mercantiliste serait susceptible de porter préjudice au mécanisme de coopération promu entre les domaines public et privé. Il en va de même en général en matière d'emplois pour la constitution d'une réserve de talents. Ces deux contradictions accentueraient la perte d'influence et par extension le déclin relatif du *leadership* des Etats-Unis.

Mis à part cela, les documents de sécurité font un usage intensif des vocables « compétition » et « dissuasion ». Quatre sens se distinguent dans leur articulation. Premièrement, il est question de dissuader, d'éviter les menaces, les conflits, au pire la guerre. Il faut pour cela être capable d'entrer en 'compétition', en 'concurrence', 'rivaliser' : « *(…)deter cyber actors(…)* »[104] *;* « *(…)future bad behavior(…)* »[105] *; « (…)deter conflict*

[98] *National Defense Strategy*, op. cit., p. 9
[99] Ibid., p. 10
[100] Ibid., p. 9
[101] Ibid., p. 11
[102] Ibid., p. 20
[103] Ibid., p. 25
[104] Ibid., p. 8, *National Security Strategy*, op. cit., p. 13

through(…) »[106] *;* « *(…)deterring war and maintaining the rules(…)* »[107] *;* « *(…)deter aggression(…)* »[108]. Deuxièmement, la capacité d'entrer en 'compétition', en 'concurrence', peut revêtir une connotation purement économique, sans lien avec une apparente confrontation ou agression directe : « *(…)strengthening United States industry's competitive position(…)* »[109] *;* « *(…)recruit and retain critical cybersecurity talent in light of the competitive private sector environment(…)* »[110] *;* « *(…)strengthening US industry's competitive position in the global digital economy(…)* »[111]*.* Troisièmement, les documents font souvent état de la nécessité non seulement de 'dissuader', mais aussi de 'contrer', de 'défaire' les menaces et agissements des concurrents, ce en dehors de tout conflit armé : « *(…)deter and counter(…)* »[112] *;* « *Deterring or defeating(…)* »[113] *;* « *(…)below the level of armed conflict(…)* »[114]. Quatrièmement, 'prévenir', 'dissuader', 'préserver la paix', implique la préparation à entrer en guerre et d'en sortir victorieux. D'où l'importance d'une concurrence stratégique, sans exclure la dimension économique, pour sauvegarder les avantages compétitifs des Etats-Unis : « *(…)compete, deter, and win in the cyberspace domain(…)* »[115] *;* « *(…)to prevent war is to be prepared to win one(…)* »[116] *;* « *(…)Prioritize preparedness for war(…)* »[117] *;* « *(…)Achieving peace through strength requires the Joint Force to deter conflict through preparedness for war(…)* »[118]*.* Il n'est pas improbable que de cette profusion polysémique surgisse une incertitude quant à l'adoption d'une stratégie viable, comme en a déjà attesté la complaisance de Donald Trump pour les autocrates et les discours extrêmement rigoristes à leur égard, tout comme à l'égard de ses alliés. Ces quatre dernières années, le contraste frappant entre la logique de confrontation du Président américain, sa déférence envers ses rivaux et la proclamation d'une résolution pacifique des problèmes - en Asie et en Afrique par exemple - reflète ce déséquilibre. L'ambiguïté qui en résulte se traduirait par une difficulté à définir des objectifs de court à long terme, ainsi que des moyens adéquats pour les réaliser, à savoir que leur cohérence conditionne le décodage de l'environnement international, du rapport à autrui et de leur rôle identitaire vis-à-vis du monde.

---

[105] *National Cyber Strategy*, op. cit., p. 21
[106] *National Defense Strategy*, op. cit., p. 6
[107] Ibid., p. 8
[108] Ibid., p. 3
[109] *National Cyber Strategy*, op. cit., p. 25
[110] Ibid., p. 17
[111] Ibid., p. 25
[112] *National Defense Strategy*, op. cit., p. 4
[113] Ibid., p. 5
[114] Ibid., p. 7
[115] *Department of Defense Cyber Strategy*, op. cit., p. 7
[116] *National Defense Strategy*, op. cit., p. 5
[117] Ibid., p. 6
[118] Ibidem.

BIBLIOGRAPHIE

Documents officiels

Department of Defense Cyber Strategy, Washington: US Department of Defense, U.S. GPO, septembre 2018, 7 pp. [Disponible en ligne : https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF - consulté le 19/10/2020]

DoD Cloud Strategy, Washington : US Department of Defense, U.S. GPO, décembre 2018, 17 pp., [Disponible en ligne : https://media.defense.gov/2019/Feb/04/2002085866/-1/-1/1/DOD-CLOUD-STRATEGY.PDF - consulté le 19/10/2020]

National Cyber Strategy, Washington: The White House, U.S. GPO, septembre 2018, 29 pp. [Disponible en ligne : https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf - consulté le 19/10/2020]

National Defense Strategy, Washington: US Department of Defense, U.S. GPO, janvier 2018, 11 pp. [Disponible en ligne : https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf - consulté le 19/10/2020]

National Security Strategy, Washington : US Department of State, U.S. GPO, décembre 2017, 56 pp. [Disponible en ligne : https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf - 17/09/2020 - consulté le 19/10/2020]

A Budget for America's Future, analytical perspectives - FY 2021, Washington : Office of Management and Budget (OMB), US GPO, 2020, 307 pp. [Disponible en ligne : https://www.govinfo.gov/content/pkg/BUDGET-2021-PER/pdf/BUDGET-2021-PER.pdf - consulté le 19/10/2020]

An American Budget – Analytical Perspectives (Budget of the US Government FY 2019), Washington : Office of Management and Budget (OMB), US GPO, 2018, 323 pp. [Disponible en ligne : https://www.govinfo.gov/content/pkg/BUDGET-2019-PER/pdf/BUDGET-2019-PER.pdf - consulté le 19/10/2020]

Defense Budget Overview, FY 2019, Washington: US Department of Defense, février 2018, 110 pp. [Disponible en ligne : https://dod.defense.gov/Portals/1/Documents/pubs/FY2019-Budget-Request-Overview-Book.pdf - consulté le 19/10/2020]

Publications en ligne

ARCHIVE.GOV, *Declaration of Independence: A Transcription* [en html] : https://www.archives.gov/founding-docs/declaration-transcript (consulté le 19/10/2020)

DEFENSE.GOV, *DOD Releases Fiscal Year 2021 Budget Proposal* [en html], https://www.defense.gov/Newsroom/Releases/Release/Article/2079489/dod-releases-fiscal-year-2021-budget-proposal/ (consulté le 19/10/2020)

LE BIG DATA.FR, *Data Hub définition : tout savoir sur les hubs de données* [en html], https://www.lebigdata.fr/data-hub-definition (consulté le 19/10/2020)

LE BIG DATA.FR, *Data Lake : définition, avantages et inconvénients pour l'entreprise* [en html], https://www.lebigdata.fr/data-lake-definition (consulté le 19/10/2020)

Rapport de recherche, *fact sheets*

Artificial Intelligence and National Security, Washington : CRS Reports, Library of Congress, août 2020, 39 pp. [Disponible en ligne : https://fas.org/sgp/crs/natsec/R45178.pdf - consulté le 19/10/2020]

Defense Primer: The United States Space Force, Washington : CRS Reports, Library of Congress, avril 2020, 3 pp. [Disponible en ligne : https://fas.org/sgp/crs/natsec/IF11495.pdf - consulté le 19/10/2020]

Fifth-Generation (5G) Telecommunications Technologies - Issues for Congress, Washington : CRS Reports, Library of Congress, janvier 2019, 32 pp. [Disponible en ligne : https://fas.org/sgp/crs/misc/R45485.pdf - consulté le 19/10/2020]

National Security Implications of Fifth Generation (5G) Mobile Technologies, Washington : CRS Reports, Library of Congress, octobre 2020, 2 pp. [Disponible en ligne : https://fas.org/sgp/crs/natsec/IF11251.pdf - consulté le 19/10/2020]

Les recherches du CECRI sont menées au sein de l'Institut de science politique Louvain-Europe (ISPOLE) de l'Université catholique de Louvain. Elles portent sur la géopolitique, la politique étrangère et l'étude des modes de prévention ou de résolution des crises et des conflits.

L'analyse des éléments déclencheurs des conflits et des instruments de leur gestion - sanctions et incitants économiques comme moyens de politique étrangère; crises et interventions humanitaires; rôle de la mémoire dans un processus de réconciliation, par exemple - est combinée à l'étude empirique de différends internationaux et de processus de paix spécifiques.

UCL
Université
catholique
de Louvain