CÉRIUM

CAHIERS
WORKING PAPER

Les enjeux géopolitiques et géoéconomiques liés au cyberespace

Adrien Savolle

No. 29
2023 - 05

Québec

CENTRE D'ÉTUDES
ET DE RECHERCHES
INTERNATIONALES

CÉRIUM

Université de Montréal

Les enjeux géopolitiques et géoéconomiques liés au cyberespace

Adrien Savolle[1]

Résumé

Les enjeux de sécurités nationales liés aux technologies numériques sont de plus en plus couverts par les médias. Ce traitement découle d'un accroissement en nombre des cyberattaques répertoriés, corrélé à des prises de conscience étatiques de plus en plus aigües des opportunités et des menaces nouvelles qui accompagnent le développement du cyberspace. Ce *Cahier du Cérium* cherche à dresser le contexte global entourant ces phénomènes en traitant des divers mécanismes de territorialisation du cyberspace, tout en soulignant les formes de compétition technico-économique mises en place par les États en son sein.

Abstract

National security issues related to digital technologies are increasingly covered by the media. This is due to an increase in the number of cyberattacks, correlated to a growing awareness of the new opportunities and threats that accompany the development of cyberspace. This *Cahier du Cérium* seeks to draw up the global context surrounding these phenomena by dealing with the various mechanisms of territorialization of cyberspace, while underlining the forms of techno-economic competition set up by the States within it.

Citation
Adrien Savolle. (2023). Les enjeux géopolitiques et géoéconomiques liés au cyberespace. *Cahier du CÉRIUM Working Paper No 29*. Centre d'études et de recherches internationales de l'Université de Montréal.

[1] Candidat au doctorat en anthropologie à l'Université Laval et chargé de cours à l'Université de Montréal. Boursier CRSH et membre du GRITH (ULaval), il est également chargé de recherche sur l'Asie pour le CÉTASE (UdeM), le CÉRIUM (UdeM) et le Centre de recherche sur le futur des villes (uOttawa).

Introduction

« En tant que réseau sociotechnique (Eveno, 2004), Internet est administré, contrôlé, et donc façonné par des groupes humains en fonction de différents enjeux et contraintes, notamment géopolitiques, et il influe en retour sur la manière dont les relations de pouvoir se structurent et s'équilibrent. Ainsi, dans le cadre d'une analyse géopolitique, cet aspect sociotechnique façonne également les conflits territoriaux et les rivalités de pouvoir sur des territoires, *a fortiori* en cas de conflit ouvert » (Pétiniaud, 2022 : 114).

Le mot cyberspace apparaît pour la première fois dans les œuvres d'art de la Danoise Susanne Ussing entre 1968 et 1970, puis gagne en popularité avec la parution des fictions littéraires *Burning Chrome* (1982) et *Neuromancien* (1984) de William Gibson. Étudié en géographie à partir des années 1990[2], le cyberespace est mobilisé comme concept « dès la fin des années 2000 dans les stratégies et les doctrines de nombreux États comme un espace de menace à la sécurité nationale, un 'territoire' à maîtriser et une priorité stratégique » (Douzet, 2020 : 5). Cet espace est intimement lié aux algorithmes qui le créent, et repose donc sur un ancrage physique (*datacenter*, câbles, satellites) qui est modelé par des acteurs économiques le plus souvent privés, dont les responsabilités sont réelles, comme l'a montré l'invasion du Costa Rica par le Nicaragua en 2010, qui était basée sur des données de Google Maps. La question de l'accès aux données par la puissance publique pour des raisons de sécurité médiatisée par les révélations d'Edward Snowden en 2013 « est en pleine évolution au niveau mondial, à la fois à cause des contraintes politiques, mais également à cause de l'évolution extrêmement rapide des technologies et des systèmes » (Bergé et Grumbach, 2016), ce qui explique que « la territorialisation du cyberespace se retrouve dans la stratégie des États qui cherchent à se le réapproprier et mieux le maîtriser, depuis les infrastructures physiques jusqu'à l'information qui y circule » (Douzet, 2020 : 6).

[2] Voir Cattaruzza (2019 : 12) pour les premiers travaux en langue française et Ash et *al.* (2018) pour ceux en anglais.

Dans ce contexte, la géopolitique classique, celle qui s'intéresse essentiellement aux États en tant qu'acteurs souverains qui ont pour horizon la guerre, et dont les enjeux sont des territoires et des ressources, reste pertinente, mais limitée pour comprendre les mécanismes interétatiques à l'œuvre au sein du cyberspace. La géoéconomie, qui prend comme objet d'étude la compétition technico-économique en tant qu'objectif étatique (Moreau Defarges, 2023), sera donc également mobilisée.

La géopolitique/géoéconomie du cyberspace demande l'analyse de multiples facteurs (a minima des facteurs institutionnels, géographiques, techniques, politiques et militaires, sans compter les relations spécifiques de chaque État avec les multinationales incontournables du secteur), que la présente étude ne peut couvrir exhaustivement. Comme la régulation du cyberspace reste en construction, tant au niveau des États que des institutions internationales, un bref état des lieux des évolutions réglementaires et des alliances interétatiques sera réalisé dans la première partie. La partie suivante s'intéressera plus précisément aux politiques mises en place par les États-Unis, la Chine et la Russie vis-à-vis du cyberspace, ce choix résultant de la place prépondérante qu'occupent ces pays dans le monde numérique. La dernière partie décrira les différentes modalités ou types d'opérations dans le cadre de cyberguerres en s'appuyant sur des cas concrets choisis et bien documentés. La conclusion reprendra l'ensemble des points analysés et soulignera les autres sujets d'étude à mener pour avoir une vision globale de la géopolitique du cyberspace.

1- Prise de conscience des cyber-menaces et cadres nationaux et internationaux existants

« Cyber diplomacy is both a response to and a factor in the continuing battle for influence in and over cyberspace » (Barrinha et Renard, 2020 : 764).

La cybersécurité est de plus en plus souvent au cœur de l'actualité, notamment par la multiplication des vols de données et la quasi-banalisation des « rançongiciels » qui touchent autant les entreprises privées que les administrations locales, nationales et parfois supra-étatiques. Elle fait également l'objet de discussions dans toute une série de forums internationaux, et notamment dans différents forums de l'Organisation des Nations unies (ONU).

En 1998, une proposition de la Russie aboutit à un traité des Nations unies visant à interdire les armes électroniques et informatiques, et à la formation, en 2004, d'un groupe d'experts gouvernementaux de l'ONU sur les développements dans le domaine des technologies de l'information et de la communication dans le contexte de la coopération internationale. Ce groupe a reconnu dès 2013[3] l'applicabilité du droit international au cyberspace et a proposé en 2015 aux États de s'engager volontairement à respecter des « bonnes conduites ». On retrouve dans ces « bonnes conduites » la transparence des politiques mises en place et la coopération avec les pays victimes de cyberattaques. Il faut toutefois souligner que le dernier cycle de négociations dans lequel a été avancé l'interdiction de cyber-contre-attaquer (*hack back*) en mobilisant des prestataires privés[4], ou encore l'imposition

[3] Pour une vision des activités onusiennes spécifiquement dévolues à la cybersecurité avant 2013, voir Maurer (2011) et Nye (2013).

[4] Les compagnies privées ou groupes de hackers connectés aux services de sécurités étatiques (qui dans les deux cas sont un type nouveau de mercenaires) ne seront pas traités dans ce papier, de par la multitude des configurations existantes et le nombre de faits répertoriés. Lorsque ce type d'acteur est grandement suspecté, c'est le pays commanditaire qui sera cité. Ce texte ne traitera pas non plus des cyberattaques provenant de groupes non affiliés à des États, quels que soient leurs objectifs.
Notons aussi que ces groupes jouent sur leur indépendance supposée, ce qui affranchit l'État commanditaire des alliances et soutiens officiels, comme le montre la tentative d'attaque partant

de contrôles des exportations pour des outils cyber-malveillants, s'est conclue par un échec découlant des divergences dans les intérêts des États membres. L'emploi même du vocable choisi depuis lors dans les discussions[5] est révélateur de conflits géopolitiques plus larges (Danet et Desforges, 2020), ce qui amène des chercheurs à souligner l'éclosion d'une nouvelle configuration géopolitique nommée « *'Cyber Westphalian' world* » (Demchak et Spidallieri, 2022 : 15) caractérisée parfois par une balkanisation du Web (Colon, 2021 : 362 ; Gao et al., 2019 : 1953)[6]. Les écrits non-académiques sur le sujet évoquent de leur côté l'émergence d'une « *Technological economic Cold War* » (Cheng et Shunsuke, 2022 ; Woo, 2020).

Dans ce contexte, le Groupe de haut niveau sur la coopération numérique créé par le secrétariat général de l'ONU recommandait en juin 2019 « que le Secrétaire général des Nations unies promeuve, de toute urgence, un processus de consultation souple et ouvert afin de mettre au point des mécanismes modernes de coopération numérique mondiale » (ONU, 2019). Dans la même veine, on peut lire sur la page Internet du Bureau de l'Envoyé du Secrétaire général pour les technologies les propos suivants : « la coopération numérique mondiale présente d'importantes lacunes et les questions relatives aux technologies numériques sont trop souvent reléguées en arrière-plan dans les programmes politiques. Même lorsqu'il y a coopération, celle-ci est souvent parcellaire et n'aboutit pas à des résultats concrets ou à des processus de suivi solides » (ONU, 2023).

---

vraisemblablement de mercenaires liés à la Chine pour capter des données de sécurité critiques dans des instituts militaires russes en mars 2022 (The New York Times, 2022).

Pour commencer une étude sur le sujet, le livre de Maurer (2018) est sans doute la référence incontournable. Il est également à noter que la nationalité des chercheurs influence souvent leur intérêt dans ce domaine. Pour les groupes supposément basés au Pakistan, voir Bommakanti, 2022 et Patel et Chudasama, 2021. Pour ceux basés en Corée du Nord, voir Youn et al., 2022, etc.

Les entreprises de cybersécurité privées comme Dragos (2023) sont une autre source de renseignement utile.

[5] En particulier l'emploi de « souveraineté numérique » ou d' « autonomie stratégique numérique ».

[6] Pour un historique des diverses approches et analyses entourant le cyberspace dans la littérature de langue anglaise, voir Mueller, 2020.

Notons également l'« Appel de Paris pour la confiance et la sécurité dans le cyberespace » fait par le président français le 12 novembre 2018 à l'occasion de la réunion à l'UNESCO du Forum de gouvernance de l'Internet, qui contient neuf principes fondamentaux sur base volontaire des États, mais aussi des entreprises, des collectivités locales et des associations. Cet appel a dû attendre novembre 2021 pour recevoir la signature des États-Unis, et, en l'absence de la signature de la Chine et de la Russie, ne constitue pas un cadre international efficace. Ajoutons également la « Déclaration commune sur la promotion d'un comportement responsable des États dans le cyberespace » proposée par les États-Unis, qui n'est à ce jour signée que par 29 pays[7], et qui n'est lui non plus aucunement contraignant (voir U.S. Department of State, 2019). L'« Appel de Paris » comme la « Déclaration commune » semblent cristalliser davantage les différences majeures dans la façon d'appréhender les relations étatiques dans le cyberspace qu'apporter une quelconque base de discussion entre les États. Les pays signataires de ces textes font partie de ceux qui prônent (jusqu'à un certain point dans les faits) une transparence de leurs positionnements et actions dans le cyberspace.

Au niveau des États justement, les cyber-ambassadeurs se multiplient avec la création de ce poste par l'Australie en 2016, par la France en 2017, par l'Estonie et les Pays-Bas en 2018, et par le Royaume-Uni en 2019 (CyberTechAccord, 2021), mais les disparités sont grandes comme le démontrent les nombreuses divergences de politiques nationales et de lobbying des multinationales exercées sur eux[8], ou encore le fait que près de la moitié des pays de la zone Asie-Pacifique n'ont même pas de stratégie définie en ce qui concerne la cybersécurité (Ang, 2022 : 94). Reste

[7] Allemagne, Australie, Belgique, Canada, Colombie, Danemark, Espagne, Estonie, États-Unis, Finlande, France, Hongrie, Islande, Italie, Japon, Lettonie, Lituanie, Norvège, Nouvelle-Zélande, Pays-Bas, Pologne, République de Corée, République tchèque, Roumanie, Royaume-Uni, Slovaquie, Slovénie et Suède.

[8] Au mois d'août 2017, le Danemark a par exemple nommé un diplomate en Californie chargé des « relations diplomatiques » avec les GAFAM. Casper Klynge, premier nommé à ce poste, est débauché en mars 2020 par Microsoft et devient lobbyiste en chef de l'Europe pour cette compagnie.

alors les tentatives d'alliances régionales, mais celles-ci donnent pour le moment des résultats des plus mitigés, sauf dans le cas de l'Union européenne[9].

En ce qui concerne l'Amérique du Sud, l'absence d'accord formel additionnée au pouvoir excessif des agences de renseignement dans ces pays présente un danger pour la maîtrise des cyber-opérations d'après plusieurs chercheurs (Alvarez-Valenzuela et Vera-Hott, 2022 : 164 ; Delerue, 2020 : 34). Le sujet a bien été effleuré par plusieurs institutions régionales (Union des nations sud-américaines, Organisation des États américains, Comité interaméricain contre le terrorisme), mais la création du « Groupe de travail sur la coopération et les mesures de confiance dans le cyberespace », qui vise depuis 2017 le renforcement régional de la confiance entre les pays de la région, et le développement d'activités de renforcement des capacités, n'a pour le moment pas donné de résultats probants (Alvarez-Valenzuela et Vera-Hott, 2022).

Même constat concernant les pays du Golfe, où l'engagement de s'aider mutuellement et de développer des systèmes et des politiques relatives à la cybersécurité pris lors du Sommet de Camp David en 2015 est jusqu'à présent resté lettre morte (Alshabib et Martins, 2022).

L'Association des nations de l'Asie du Sud-est (ANASE), pour sa part, a bien des comités travaillant sur la cybersécurité, mais l'organisation est assez diserte sur ses activités réelles (Asean, 2023), et les politiques nationales au sein de l'association peuvent faire penser que le chantier n'est pas véritablement fonctionnel[10].

[9] Le 30 juillet 2020, le Conseil de l'Union européenne a jugé responsables six individus (de nationalités russe et chinoise) et trois entités (des sociétés commerciales chinoises et le service de renseignement des armées russes), de tentative d'intrusion contre le siège de l'Organisation pour l'interdiction des armes chimiques à La Haye en avril 2018, et d'être à l'origine des campagnes de rançonnage « WannaCry » et « NotPetya ». Le Conseil a également prononcé des mesures restrictives à leur encontre (Official Journal of the European Union, 2020).

[10] En effet, seuls quatre pays de l'ANASE ont spécifiquement défini des agences responsables de la cybersécurité : Singapour (Cyber Security Agency of Singapour), la Malaisie (CyberSecurity Malaysia), les Philippines (Department of Information and Communications de l'information et des

L'Union africaine a également des mécanismes qui encouragent les coopérations entre ses États membres. Ils sont compris dans l'article 28 de la « Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel » adoptée en 2014, mais ils n'ont aucun effet contraignant et reposent sur la bonne volonté des pays concernés, avec des résultats des plus mitigés.

L'Europe s'est pour sa part dotée le 19 juin 2017 d'une boîte à outils cyberdiplomatique qui suggère un mécanisme de riposte en cas de besoin : « la réponse diplomatique de l'UE aux actes de cybermalveillance fera pleinement usage des mesures relevant de la politique étrangère et de sécurité commune, y compris, si nécessaire, des mesures restrictives. Une réponse conjointe de l'UE face aux actes de cybermalveillance serait proportionnée à la portée, l'échelle, la durée, l'intensité, la complexité, la sophistication et l'incidence de la cyberactivité » (Conseil de l'UE, 2017). Cette posture est d'ailleurs appliquée suite aux actes de cybermalveillance[11] commis par la Fédération de Russie à l'encontre de l'Ukraine quelques heures avant le début de l'invasion, avec l'octroi d'une aide à un pays non-membre de l'Union pour assurer la stabilité du cyberspace au sein même de l'Union : « le risque existe que les cyberattaques visant l'Ukraine, y compris contre des infrastructures critiques, se propagent à d'autres pays et aient des effets systémiques mettant en péril la sécurité des citoyens européens. L'Union européenne, en étroite collaboration avec ses partenaires, envisage de nouvelles mesures pour prévenir, décourager et dissuader de tels comportements malveillants dans le cyberespace, ainsi que pour y faire face. L'Union européenne continuera d'apporter un soutien politique, financier et matériel coordonné à l'Ukraine pour en renforcer la cyber-résilience » (Conseil de l'UE, 2022). L'UE semble donc être l'alliance régionale la plus aboutie sur la question.

---

communications), et l'Indonésie (Badan Siber dan Sandi Negara, le Cyber Body et l'Agence nationale de cryptage) (Ang, 2022 : 94).

[11] Attaque du réseau satellitaire KA-SAT dont Viasat (compagnie américaine spécialisée dans les télécommunications par satellite) est propriétaire.

Il reste enfin les alliances militaires et les alliances sur le renseignement qui englobent elles aussi des dispositions comme le montrent les deux cas emblématiques suivants. Dans le cas de l'Organisation du Traité de sécurité collective fondée en 1992 sous l'impulsion de la Russie, elle n'a été véritablement mobilisée que depuis la première invasion de l'Ukraine en 2014 (Teurtrie, 2017), et semble dans un piteux état depuis la seconde invasion, le 24 février 2022 (Samaran, 2023). En ce qui concerne le cyberspace, la mention dans la « Stratégie de sécurité collective pour la période allant jusqu'en 2025 » de l'« Agence de sécurité collective de l'Organisation du Traité de sécurité collective responsable des armes, équipements militaires et spéciaux, technologies, techniques, logiciels, moyens linguistiques, juridiques et organisationnels; y compris les canaux d'information et de télécommunication utilisés pour assurer la sécurité collective » mérite tout de même d'être noté, même si les informations à son sujet sont des plus minces.

De son côté, l'Organisation du Traité de l'Atlantique Nord (OTAN) a adopté dès 2008 une politique de défense du monde numérique avant de spécifier en 2014 que les cyberattaques pouvaient justifier une riposte de l'ensemble des membres, précision réaffirmée en 2016, moment où le cyberespace a été défini comme un nouveau domaine opérationnel dans lequel l'OTAN doit se défendre aussi efficacement que dans les airs, sur terre et en mer (Brent, 2019). Cette conceptualisation est réitérée et explicitée le 14 juin 2021 par les propos suivants : « les Alliés sont conscients que, dans certaines circonstances, les incidences d'actes de cybermalveillance majeurs aux effets cumulés sont telles que ces actes peuvent être considérés comme équivalant à une attaque armée » (OTAN, 2021).

L'ensemble de ces données démontrent que de très nombreux pays ont identifié le cyberspace comme un espace en soi, présentant des opportunités et des menaces. Les institutions internationales comme les alliances régionales et les alliances militaires se sont adaptées à cette nouvelle réalité, mais les tentatives pour généraliser une réglementation appropriée se sont pour le moment conclues par

des échecs, « Appels » et « Déclarations » compris. Les politiques de partage d'informations et de processus coordonnés en la matière ne semblent donc pour le moment efficients qu'au sein del'UE, et d'après Henrikson (2019), de l'Organisation de coopération de Shanghai (OCS)[12] alors que les cyberattaques entre États se multiplient.

2- Menaces de plus en plus prégnantes et description des forces étatiques en présence

« In Crimea and Donbass, Russian authorities and separatist forces were able to attract digital traffic into their respective networks and modify BGP routes in order to divert the local Internet traffic from continental Ukraine, drawing a kind of 'digital frontline' consistent with the military one » (Douzet, Salamatian et al., 2020: 179).

Cette multiplication des cyberattaques a amené les États à organiser des services de cyberdéfense, et les investissements pour la sécurisation du cyberspace ne cessent de croître d'une année budgétaire à l'autre. Le National Cyber Power Index 2022 est comme tout classement discutable, notamment quant aux caractéristiques choisies, mais reste très pertinent pour donner une idée des forces en présence. Ainsi, les dix premiers États en termes de puissance générale dans le cyberspace sont, en ordre décroissant : les États-Unis, la Chine, la Russie, le Royaume-Uni, l'Australie, les Pays-Bas, la Corée du Sud, le Vietnam, la France et l'Iran.

Mais le classement se modifie suivant le critère considéré. Ainsi, si l'on considère les capacités de renseignement ou, plus prosaïquement, d'espionnage, le classement est : États-Unis, Chine, Royaume-Uni, Australie, Pays-Bas, Israël, Corée du Sud, Canada, France et Russie. Notons également la seconde place de l'Ukraine dans les

[12] «Sur les questions numériques, plutôt qu'en organisation régionale à vocation intégratrice, l'OCS joue une partition essentiellement défensive. Plateforme de mise à l'ordre du jour et d'élaboration de normes, elle se réunit pour établir un langage commun sur les normes de souveraineté de l'information et apporter des arguments juridiques contre ce que ses membres perçoivent comme des 'interventions étrangères' (Ibragimova 2013) » (Nocetti, 2020 : 273).

capacités de défense du cyberspace et les trois premières postions en ce qui concerne les capacités d'attaque, lesquelles sont occupées par les États-Unis, la Chine et la Russie (Voo et *al.*, 2022).

Avec un tel classement, il est clair que la géopolitique du cyberspace est intimement liée à la géopolitique en général, et qu'elle en est devenue l'un de ses éléments centraux lors de la dernière décennie[13]. Il devient alors pertinent de s'intéresser aux politiques spécifiques adoptées par les acteurs les plus importants : les États-Unis, la Chine et la Russie.

a) Les États-Unis

Le *Patriot Act*, formulé au lendemain des attentats du 11 septembre 2001, impose aux entreprises américaines du numérique de collaborer avec l'administration américaine et de transmettre les données qu'elles hébergent dans le cadre d'affaires touchant à la sécurité nationale. La communauté américaine du renseignement s'est donc largement appuyée sur le secteur privé en ce qui concerne ses capacités dans le cyberspace. Il ne faut pas sous-estimer non plus l'apport d'organisations telles que l'Intelligence Advanced Research Project Activities (IRPA), la Defense Advanced Research Project Agency (DARPA) et l'incubateur de technologie de la CIA, In-Q-Tel (Van Puyvelde, 2019, cité par Renault et al., 2022 : 26). Le pays adopte publiquement en 2011 une politique spécifique au cyberspace qui prend en compte les aspects diplomatiques et défensifs (Barrinha et Renard, 2017).

Avec la *National Cyber Strategy* adoptée en 2018, les États-Unis affirment qu'ils travailleront avec des États partageant les mêmes idées afin de coordonner et de soutenir les réponses des uns et des autres à des cyberincidents malveillants importants, notamment par le partage de renseignements, des déclarations

[13] Voir sur cette question Barrinha et Renard (2017), Housen-Couriel (2017), Renard (2018) et Riordan (2019).

publiques de soutien aux mesures de riposte adoptées, et l'imposition conjointe de conséquences pour les acteurs malveillants.

L'année 2018 est également un tournant dans l'approche américaine des cyber-opérations avec l'adoption d'une approche proactive qui rejoint la volonté politique de réaffirmer unilatéralement l'hégémonie américaine (Taillat, 2020), et qui se traduit en 2019 par la « Loi d'autorisation de la défense nationale », laquelle permet à l'armée d'utiliser tous les moyens nécessaires (attaques préventives comprises) pour assurer la sécurité des États-Unis dans le cyberspace (Gold, 2020). Ajoutons que le pays a pris l'habitude d'imposer des sanctions contre pays et individus soupçonnés (car non jugés) d'avoir commis des cyberattaques (Ford, 2022)[14].

b) La Chine

La Chine a pour sa part boycotté le Comité consultatif des gouvernements de l'*Internet Corporation for Assigned Names and Numbers* (ICANN) entre 2001 et 2009, en raison du statut politique accordé à Taiwan et de la structure multipartite de l'institution (Creemers, 2020 : 303).

La Chine réfléchit à son positionnement stratégique dans le cyberspace depuis le début des années 2010, tant au niveau sécuritaire (contre-terrorisme) qu'au niveau des alliances régionales et internationales (Segal, 2017). Comme l'a décrit le président Xi Jinping lors de la conférence mondiale sur l'Internet de 2015 à Wuzhen, la cybersouveraineté signifie « respecter le droit de chaque pays de choisir sa propre voie de développement de l'Internet, son propre modèle de gestion de l'Internet, [et] ses propres politiques publiques sur l'Internet » (Segal, 2017). Le premier principe indiqué dans la cyberstratégie chinoise de 2016 est d'ailleurs de respecter

[14] L'administration Obama a entamé des poursuites aboutissant à la mise en examen de cinq officiers de l'armée chinoise en mai 2014 (Douzet, 2018 : 90). Les poursuites de personnes soupçonnées d'être rattachées à des services de pays étrangers continue depuis lors (voir Zagaris, 2022).

et de protéger la souveraineté des États dans le cyberspace (Xinhua, 2016). Mais, constatant la militarisation rapide du cyberspace tant par la Russie que par les États-Unis, l'objectif de paix y supplante rapidement celui de la souveraineté numérique dans l'*International Strategy of Cooperation on Cyberspace* rédigée conjointement par le ministère des Affaires étrangères et l'Administration du cyberspace chinois (TSCIOPRC, 2017). La conflictualité observée explique aussi la création d'une force stratégique de soutien en réunissant les anciens départements APL3 (espionnage numérique) et APL4 (guerre électronique et informationnelle) en 2015 (Creemers, 2020 : 301). Lors du 20e congrès national du Parti communiste chinois (PCC) se déroulant en octobre 2022, le fait d'arrimer l'intelligence artificielle aux forces armées a été explicité, soulignant une fois de plus l'importance que le PCC accorde aux cybercapacités de son armée (Gao, 2022).

De plus, la détérioration de sa relation avec les États-Unis et l'intensification de la concurrence internationale pour le leadership technologique[15] influencent grandement ses politiques actuelles (Lee et *al.*, 2022). Elles se traduisent par une méfiance des entreprises américaines collectant les données. Ainsi, l'expansion de l'usine Tesla qui était prévue à Shanghai en 2023 est pour le moment en attente

[15] La guerre commerciale déclarée par les États-Unis à la Chine cherchait initialement à augmenter les droits de douane pour redresser sa balance commerciale, tout en dénonçant la concurrence déloyale de la Chine. Une liste noire d'entreprises chinoises pour lesquelles une licence d'exportation est requise apparaît en 2019 et s'accompagne de l'interdiction pour les entreprises technologiques américaines de traiter avec leurs homologues chinois. Suit rapidement la réduction des ventes des compagnies chinoises Huawei et ZTE. Depuis lors, l'armement de la technologie par le biais de contrôles à l'exportation, d'acquisitions, de blocages et d'exigences en matière de licences, a été de plus en plus utilisé pour paralyser le développement chinois dans des secteurs technologiques clés. L'arrivée de Joe Biden à la Maison-Blanche a renforcé cette tendance en mettant l'accent sur les restrictions concernant les puces. La dernière série de mesures dans ce domaine empêche les entreprises américaines et les filiales étrangères basées aux États-Unis d'exporter des puces avancées, ainsi que des équipements de fabrication pour les technologies inférieures à 14 nm. En imposant de telles barrières à l'offre et à la production potentielle de semi-conducteurs en Chine, les États-Unis tentent de pousser cette dernière vers un découplage forcé, et donc de conserver leur avance technologique.

d'autorisation et Starlink semble être également proscrit dans le pays (Bloomberg News, 2023).

c) La Russie

En Russie, « c'est avant tout une volonté de redynamisation et de projection de la puissance économique […] qui a guidé les politiques publiques en faveur des secteurs de l'informatique et du numérique » (Bertran, 2020 : 235) de 2008 à 2012. Après la révélation au grand jour de la surveillance massive exercée sur l'Internet mondial par les services de renseignement des Five Eyes (États-Unis, Royaume-Uni, Canada, Australie et Nouvelle-Zélande)[16] en 2013, les autorités russes se sont recentrées sur les enjeux stratégiques et de sécurité liés au numérique, et ont précisé leur vision du cyberspace par une série de lois (Douzet, 2020 : 8).

Afin de limiter les coûts et les risques de ses investissements, la Russie a largement encouragé l'emploi de logiciels libres, voie qu'elle avait déjà expérimenté en 2009 avec la création d'« ASTRA Linux Édition spéciale » (qui ne respecte ironiquement pas les exigences du libre), répondant ainsi aux besoins de confidentialité des administrations relevant de la défense nationale. Cela étant dit, l'externalisation des compétences informatiques vers des entités privées, qu'on constate au fil des ans en Russie comme ailleurs, n'est pas sans risques, comme le prouve la plus importante fuite de données connue de l'histoire des services de renseignement du pays, celle de l'entreprise SyTech, le 13 juillet 2019 (Bertan, 2020).

[16] L'alliance des Five Eyes est issue de la guerre froide et la surveillance à grande échelle qu'elle réalise a été dévoilée par Edward Snowden. Si le partage d'information collectée via le programme de surveillance américain ECHELON devrait également être la norme, les États-Unis ont déjà transmis des informations issues de ce programme à une entreprise pour lui donner un avantage sur les entreprises étrangères soumissionnant pour le même contrat (Dixon, 2016 : 133), remettant en question la ligne tracée entre surveillance et espionnage industriel, mais aussi la confiance des membres de l'alliance sur la nature des renseignements partagés.

Enfin, le cyberspace est également conceptualisé par la Russie comme un territoire culturel avec la mise en place de la doctrine RuNet comme sous-espace linguistique, ethnique et culturel post-soviétique dans le monde numérique (Limonier, 2018 cité par Douzet ; Salamatian et *al.*, 2020).

Soupçonné de recourir à de nombreux mercenaires, le cyber-espionnage russe s'est intensifié dès le début de la seconde invasion de l'Ukraine (Smith, 2022), et selon Clint Watts, dont un article sur le blogue *Microsoft On the Issue* établit une liste des cyberattaques russes en Ukraine et en Pologne, les derniers changements de tactique russe (multiplication de destructions d'infrastructures à utilité civile) « *suggest that the world should be prepared for several lines of potential Russian attack in the digital domain over the course of this winter* » (Watts, 2022).

Nous voyons à travers un rapide survol des politiques adoptées et des ressources accordées au cyberspace par les trois superpuissances actuelles qu'il existe des différences majeures dans leur positionnement. Sur le plan diplomatique, les États-Unis prêchent pour un cyberspace égalitaire et transparent régulé par l'ensemble des États, dans lequel les échanges sont la norme et les comportements conflictuels à punir. Mais, sur les plans géopolitique et géoéconomique, le pays ne semble pas respecter lui-même cette vision politique. De son côté, la Russie insiste sur un Internet qui respecte la souveraineté des États, comme elle le fait en dehors du monde numérique. La Chine, qui est sur ce point alignée avec la Russie, est poussée par la confrontation géoéconomique (et géopolitique) qui l'oppose aux États-Unis à ajuster son comportement vis-à-vis du cyberspace.

Il est à ce sujet intéressant de souligner que la Chine et les États-Unis ont signé un accord en 2015 dans lequel les deux pays s'engagent à ne pas utiliser le cyberespace à des fins d'espionnage économique. Cet accord s'est traduit par une réduction significative (bien que temporaire) de la cyberactivité chinoise dans les mois qui ont suivi (Barrinha et Renard, 2020 : 761). Le contexte géopolitique extrêmement tendu

en dehors du cyberspace comme l'approche proactive des États-Unis au sujet du cyberspace laisse songeur sur les possibilités de renouveler cet accord dans le futur.

Un autre point intéressant est l'utilisation par la Russie des logiciels libres pour rattraper son retard au tournant des années 2010, surtout lorsqu'on apprend que la compagnie chinoise Tencent a, pour contourner les sanctions américaines sur les puces, rejoint l'année dernière RISC-V, soit le plus grand consortium mondial sur les semi-conducteurs, lequel propose une architecture *open source* (Pan, 2022).

Tel qu'indiqué plus haut, ces trois pays sont également intégrés dans d'autres alliances en matière de cyberspace. L'analyse de la cyberdiplomatie de chacun d'eux ne peut donc se faire de façon isolée. De plus, comme dans la diplomatie classique, les comportements et les actes ne sont pas nécessairement le reflet des engagements pris. Il faut également souligner que cette cyberdiplomatie découle de la multiplication de cyberattaques, mais que celles-ci sont tout sauf homogènes.

3- Les différents types de cyberattaques

« La propagande, […] c'est la guerre poursuivie par d'autres moyens » (Domenach, 1950 : 19)

En l'absence de règles internationales encadrant le cyberspace, de nombreux pays ont adopté leur propre doctrine ainsi que des outils pour les mettre en œuvre. L'idée ici n'est pas de dresser un inventaire exhaustif des cas existants, mais plutôt de faire ressortir les différents types de menaces, tout en signalant que ce sont les États les plus actifs dans le monde militaire qui le sont dans le cyberspace.

D'après Kaiser (2015), la première cyberattaque répertoriée a visé l'Estonie en 2007. En juillet 2008, une vague de cyberattaques précédait la pénétration de chars russes en Géorgie. Au cours de ces deux années, 103 pays ont également été victimes de cyberattaques d'origine chinoise (Hartnett, 2011). Les attaques se sont par la suite multipliées et complexifiées, pour culminer sur 2016, année marquant la première

attaque mobilisant l'Internet des objets (Douzet et Géry, 2020). Le nombre de belligérants avait lui aussi augmenté et au moins 30 pays avaient développé des capacités offensives dans le cyberspace à la fin de cette année d'après une note déclassifiée d'un rapport du Sénat américain daté du 5 janvier 2017 (James et *al.*, 2017).

Si les cyberattaques entre États sont en voie de devenir la norme, il existe des types d'attaques très différents selon leurs objectifs et leur opérationnalisation. Cette partie s'appuiera sur des cas documentés pour présenter la diversité recensée à ce jour dans ce domaine.

- **Opérations psychologiques**

Les opérations psychologiques sont la concrétisation d'une véritable « guerre de l'information » (Colon, 2021 : 361) et c'est la Russie qui semble être à la pointe de ce type d'attaque. Le pays utilise l'Internet Research Agency pour lancer des « campagnes de désinformation » et de déstabilisation à l'étranger, particulièrement aux États-Unis (Howard et al., 2019) et en Europe (Innes et al., 2020), le tout de manière coordonnée avec les chaînes médiatiques russes RT et Sputnik. Des hackers russes ont ainsi tenté d'influencer les élections américaines de 2016 et ont été rejoints par des hackers chinois et iraniens lors de l'élection présidentielle de 2020, selon le blogue *Microsoft On the Issues* (Burt, 2020). Consciente des effets possibles de la propagande dans le cyberspace, la Russie a, dès le début de la seconde invasion de l'Ukraine, interdit des compagnies étrangères (Facebook, Instagram, Twitter, Apple, Cisco, Microsoft, Oracle, etc.) sur son territoire (Segal et Goldstein, 2022 : 8).

L'exemple le plus marquant des opérations cyber-psychologiques s'est déroulé dans le cyberspace africain, région où la propagation et la normalisation des récits russes et chinois sont devenues monnaie courante (voir Douzet ; Limonier et al., 2020).

Cette opération a mis en confrontation directe des agents français[17] et russes, avant d'être démantelée par Facebook, qui en décembre 2020 a supprimé une série de comptes pour avoir adopté « un comportement inauthentique coordonné au nom d'un gouvernement étranger ». Les comptes des personnes ayant « des liens avec des personnes associées à l'armée française » visait essentiellement la Centrafrique et le Mali, et dans une moindre mesure le Niger, le Burkina Faso, l'Algérie, la Côte d'Ivoire et le Tchad. Ils donnaient la parole à de faux habitants de ces pays qui exprimaient un soutien à la politique française dans la région et à son armée. Utilisant le français et l'arabe, ils colportaient aussi que les élections en République centrafricaine avaient connu de nombreuses ingérences russes. La Russie justement, dont les comptes associés diffusaient principalement dans la République centrafricaine, à Madagascar, au Cameroun, en Guinée équatoriale, au Mozambique et auprès de la diaspora centrafricaine, et qui avait investi près de 38 000$ américains dans leurs campagnes de communication dénigrant la politique française dans la région. Facebook en a aussi profité pour radier d'autres comptes russes, dont certains sur Instagram, lesquels ciblaient entre autres la Libye et le Soudan (Gleicher et Agranovich, 2020).

Cet exemple est intéressant à plus d'un titre. D'abord, c'est le premier face-à-face documenté de campagnes de propagande opposées et organisées par deux États rivaux dans le cyberspace. Ensuite, fait majeur, c'est une entreprise privée (Meta) qui non seulement y met fin, mais communique à son propos. Il n'est pas non plus

[17] La thèse de Desforges (2018) retrace la prise de conscience et la mise en place d'outils par la France pour tenter de contrer les nouveaux risques géopolitiques découlant du monde numérique. L'article de Coustillière (2020) traite pour sa part de la transformation numérique du ministère des armées lancée en septembre 2017. Voir également Cataruzza (2019), Douzet (2020) et Renault et *al.*, (2022).
Pour les développements actuels, il faut noter que la Loi de programmation militaire en cours d'adoption prévoit un doublement des budgets du renseignement militaire de la capacité de traitement des menaces cyber majeures (Tertrais, 2023) et que le pays s'est mis à utiliser des systèmes de chiffrement pouvant sur le papier résister à un déchiffrement par ordinateur quantique (France Diplomatie, 2022).

anodin que de nombreuses informations citées dans le présent texte soient produites par des compagnies privées ayant de lourds intérêts dans le cyberspace, ce qui invite le chercheur comme le lecteur de ce texte à la réflexivité, à s'interroger sur le pourquoi et le comment de ces communications, et donc à leurs effets psychologiques, mais démontre aussi à quel point ces compagnies sont des acteurs incontournables de la géopolitique du cyberspace.

Plus généralement, les « campagnes de désinformation » sont légion, bien qu'il soit difficile de remonter avec certitude vers chaque commanditaire. Mais le cyberspace ne se limite pas à la propagande et est aussi utilisé pour réaliser des opérations d'espionnage.

- **Opérations de renseignement**

L'espionnage par le truchement du cyberspace est sans doute le type de cyberattaque le plus médiatisé. Les effets qu'il engendre dépassent largement le cyberspace, comme le démontre le licenciement du chef de la cybersécurité allemande[18] en octobre 2022 en raison de ses liens équivoques avec des agents russes (Reuters, 2022), ou encore l'espionnage du siège de l'Union africaine de 2012 à 2017 par la Chine (Kadiri, 2018).

Notons que de nouveaux acteurs veulent combler leur retard en la matière, notamment l'Inde, qui investit massivement dans le cyberespionnage en ciblant particulièrement le Pakistan, la Chine, le Moyen-Orient et l'Asie du Sud, même si le pays reste en retard par rapport aux principaux joueurs (Leyden, 2021). Inversement, des chercheurs pakistanais estiment que le pays est victime de cyberespionnage et de cyberattaques pilotées par l'Inde, et appellent les décideurs

[18] Outre son engagement sur les questions de cybersécurité au sein de l'OTAN et de l'UE, l'Allemagne établit la cybersécurité en tant que tâche commune de l'État, des milieux économique et scientifique, et de la société. Elle vise depuis 2021 une approche transparente dans la mise en œuvre et le contrôle de la stratégie adoptée. Apparemment consciente de son retard dans le domaine, l'agence allemande chargée de la cybersécurité travaille de concert avec son homologue français (Federal Office for Information Security, 2023).

du pays à investir massivement dans le domaine (Mirza et Akram, 2022). Comme dans le renseignement classique, les moyens et les expertises sont névralgiques et entraînent une course en avant.

Également à l'instar du renseignement classique, certaines techniques utilisées dans le cyberspace sont traditionnelles. Ainsi, en février 2020, le porte-parole de l'armée israélienne mettait ses troupes en garde contre de faux profils émanant du Hamas. Ces faux profils affichaient des jeunes femmes et envoyaient des photos intimes avec l'objectif d'infecter les téléphones des soldats (Arpagian, 2022 : 56).

Soulignons enfin que dans le renseignement, il ne semble pas y avoir de véritables alliés. La NSA américaine a espionné la chancelière allemande Angela Merkel en 2013; le BND (services secrets allemands) a espionné des politiciens français en 2015; les États-Unis et le Royaume-Uni auraient tenté de hacker des drones de surveillance israéliens en 2016, selon le gouvernement israélien; etc.

- **Des opérations permettant de contourner des embargos**

Ce type d'opération permet à des régimes frappés de lourdes sanctions, dont l'Iran et la Corée du Nord au premier chef, de les contourner. Ainsi, des actifs numériques sud-coréens d'une valeur de près de 1,2 milliard de dollars américains auraient été dérobés par la Corée du Nord au cours des cinq dernières années, selon le Service national du renseignement sud-coréen (NIS) (Kim, 2022). Le Threat Analysis Group (blogue de Google/Alphabet) a également publié une note concernant des profils fictifs créés sur Linkedin et Telegram par Pyongyang afin d'infecter les comptes des spécialistes du secteur de la cybersécurité. Selon les analystes, Pyongyang multiplie les offensives numériques afin de s'assurer des entrées d'argent et de contourner les sanctions internationales qu'il subit, mais aussi pour voler des informations lui permettant de rattraper son retard industriel (Weidemann, 2021).

- **Les cyberattaques visant les infrastructures physiques et les personnes**

« En 2015, les États-Unis ont utilisé un drone pour tuer le Britannique Junaid Hussain, hacker en chef de l'État islamique en Syrie. » (Amsellem, 2020 : 281)

Les cyberattaques visant les infrastructures physiques et les personnes sont de plus en plus communes. Elles peuvent être déployées rapidement, comme le montre l'attaque contre le Parlement européen après qu'il eut qualifié la Russie de « promoteur de terroristes » (Libération et AFP, 2022). Selon les rapports d'entreprises américaines de cybersécurité, la Russie multiplierait depuis trois ans ce type d'attaque en sol ukrainien (Area 1, 2020 ; Watts, 2022).

L'une des cyberattaques de ce type les plus médiatisées a été découverte en 2010 : des installations nucléaires iraniennes ont été infectées par le ver informatique Stuxnet. Cette attaque serait d'origine américaine et israélienne[19] et aurait incité l'Iran à renforcer la sécurité de son réseau (Alimardani 2019). Téhéran a ainsi lancé en 2013 le *National Network Information,* intranet national qui permet d'éviter les échanges non protégés de données avec le réseau Internet mondial (Tajdin, 2013). Dans ce domaine aussi, les actions offensives et réactions défensives s'enchaînent et culminent vers une course aux investissements et aux expertises. Tel qu'annoncé dans de nombreuses stratégies étatiques, les infrastructures sont parfois ciblées de « manière classique » pour contrecarrer des actions se déroulant dans le monde numérique. Ainsi, Israël a bombardé le 4 mai 2019 un immeuble en zone palestinienne servant à lancer des cyberattaques contre des intérêts israéliens (Amsellem, 2020).

Le cyberspace partage donc de nombreuses caractéristiques avec les autres espaces : un champ d'influence et de bataille lié à l'ensemble des intérêts

[19] Israël a adopté une politique officielle au sujet du cyberspace dès 2011, l'ensemble des institutions créées étant réunis au sein du *National Cyber Directorate* en 2017. Soupçonné d'avoir mené de nombreuses cyberattaques en Syrie, mais aussi au Liban, et même en Autriche et en Suisse (où se déroulaient les négociations sur le programme nucléaire iranien), l'État hébreux se fait aussi régulièrement attaquer et espionner par l'Iran, mais aussi par la Syrie, le Hezbollah libanais ou encore la Corée du Nord. (Amsellem, 2020)

géostratégiques des États. Les attaques dans le cyberspace sont rarement revendiquées. Ce sont donc généralement des analystes ou les États ciblés, lesquels estiment souvent connaître le pays commanditaire, qui permettent de suivre les affrontements.

Un autre type d'attaque est celui des infrastructures sur lesquelles repose le cyberspace. Ces attaques, qui doivent prendre en compte la géographie locale des infrastructures, se déplacent parfois le long des lignes de front des « guerres classiques », comme lors du conflit ukrainien de 2014 (Douzet ; Salamatian et *al.*, 2022). Parfois, l'attaque des infrastructures précède les attaques classiques. Par exemple, des logiciels malveillants capables d'effacer les disques durs ont été découverts dans les réseaux du gouvernement ukrainien dans les semaines qui ont précédé son invasion (Segal et Goldstein, 2022 : 8-10).

Conclusion

« Vous pouvez avoir la plus grande puissance militaire du monde, si vos bâtiments, troupes et infrastructures sont incapables de communiquer, d'un seul coup, votre puissance se trouve considérablement affaiblie » (Thibout, 2018).

Le cyberspace est donc devenu un espace comme les autres. Il est investi par les États et, en l'absence de règles globales et efficaces, est devenu un lieu de confrontation suivant les intérêts géopolitiques et géoéconomiques de chacun, produisant des cyberattaques nombreuses et variées. Des politiques nationales poussées par des intérêts géopolitiques globaux se multiplient donc de manière éparse, et sont accompagnées d'investissements économiques majeurs dont la croissance est dans les dernières années exponentielles. La recherche de la maîtrise du cyberspace par les États est donc devenue une priorité, et ce Cahier a cherché à en expliquer les raisons, et a souligné que les entreprises privées empiètent largement sur la prérogative des États en la matière. Il faut ajouter que ces entreprises ont un rôle central pour la maîtrise du cyberspace.

Si certaines prennent politiquement position comme Méta[20], d'autres participent financièrement à la cybersécurité de leurs pays d'attache comme Microsoft, Google, Amazon, Apple et IBM. Mais cette générosité soudaine suite à d'un discours de Joe Biden[21] suivant l'adoption de l'*Infrastructure Investment and Jobs Act*[22], semble calculée pour empêcher de se voir imposer des impôts qui redonneraient à l'État américain, la capacité de décider seul des investissements requis pour assurer la cybersécurité du pays. Le fait que certaines de ces entreprises collaborent également avec des compagnies chinoises sur des sujets reliés aux enjeux de cybersecurité (Savolle, 2021) renforce d'ailleurs cette hypothèse.

La maîtrise du cyberspace se joue aussi sur la maîtrise des données, et les compagnies privées ont parfois là aussi des intérêts financiers limitant leurs coopérations avec les États (Kokas, 2022). En ce qui concerne les voies de communications, soulignons juste que le trafic de la zone Atlantique passe à 95 % en 2022 par des câbles appartenant aux Gafam (Arpagian, 2022 : 22), ou encore la volonté de Taïwan d'acheter à la compagnie Starlink un réseau de satellites à orbites basses pour rester maître des communications en cas d'invasion (The Strait Times, 2023).

Aux données collectées et aux voies de communication s'ajoute le savoir faire technique, qui est aujourd'hui médiatisé autour de l'emplacement des fonderies de microprocesseurs. Reste également à sécuriser un approvisionnement en minéraux

[20] Meta a adopté une politique spécifique à la suite de l'invasion de l'Ukraine (Meta, 2022),

[21] « [the] *government will only buy tech products that meet certain cybersecurity standards, which will have a ripple effect across the software industry, in our view, ultimately improving security for all Americans.* […] *And because cybersecurity is a global issue, we've also rallied G7 countries to hold nations who harbor ransomware criminals accountable.* […] *But the reality is, most of our critical infrastructure is owned and operated by the private sector, and the federal government can't meet this challenge alone. So I've invited you all here today because you have the power, the capacity, and the responsibility, I believe, to raise the bar on cybersecurity* » (Biden, 2021).

[22] Enveloppe de 1000 milliard de dollars américains investis dans les voitures électriques, le haut-débit et les infrastructures

critiques par le truchement de groupes minier. L'ensemble de ces impératifs (analyse des données, fluidité des communications, savoir techniques et ressources premières) ne sont donc pas du ressort des seuls États, et une étude approfondie de leurs liens (économiques, législatifs, etc.) avec les compagnies privées du secteur reste à être menée. Les recherches empiriques et les analyses entourant la géopolitique et la géoéconomie du cyberspace se multiplieront donc fort probablement dans les années à venir.

Références

Alimardani, M. (2019)' Stuxnet, American Sanctions, and Cyberwar Are Legitimizing Iranian Internet Controls', *Vice* (3 juillet), (c. le 9 janvier 2023: https://www.vice.com/en/article/vb9859/stuxnet-american-sanctions-and-cyberwar-are-legitimizing-iranian-internet-controls).

Alshabib, H.N. et Martins, J.T. (2022) 'Cybersecurity: Perceived Threats and Policy Responses in the Gulf Cooperation Council', *IEEE Transactions on Engineering Management*, 69, 6: 3664-3675.

Álvarez-Valenzuela, D. et Vera-Hott, F. (2022) 'Cyber Operations in South America', *Baltic Yearbook of International Law Online*, 20, 1: 163-186.

Amsellem, D. (2020) 'Le cyberespace israélien, un enjeu de puissance', *Hérodote*, 2, 177/178 : 281-296.

Ang, B. (2022) 'Small States Learn Different Survival Lessons', *The Cyber Defense Review*, 7, 1: 93-100.

Area 1 (2020) *Phishing Burisma Holdings* (c. le 18 janvier 2023 : https://cdn.area1security.com/reports/Area-1-Security-PhishingBurismaHoldings.pdf).

Arpagian, N. (2022) *Frontières.com*, Paris : Éditons de l'Observatoire / Humensis.

Barrinha, A. et Renard, T. (2017) 'Cyber-diplomacy: the making of an international society in the digital age', *Global Affairs*, 3, 4/5: 353-364.

Barrinha, A. et Renard, T. (2020) 'Power and diplomacy in the post-liberal cyberspace', *International Affairs*, 96, 3 : 749–766.

Bergé, J.-S. et Grumbach, S. (2016) ' La sphère des données et le droit : nouvel espace, nouveaux rapports aux territoires', *Journal du Droit International Clunet*, 4.

Bertran, M.G. (2020) 'La place des logiciels libres et *open source* dans les nouvelles politiques du numérique en Russie', *Hérodote*, 2, 177/178 : 235-252.

Biden, J. (2021) *Remarks by President Biden on Collectively Improving the Nation's Cybersecurity*, Briefing Room, White House (c. le 1er décembre 2022: https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/08/25/remarks-by-president-biden-on-collectively-improving-the-nations-cybersecurity/).

Bloomberg News (2023) 'Tesla China Plant Expansion in Doubt over Starlink Concerns', *Bloomberg News* (12 janvier) (c. le 20 janvier 2023: https://www.bloomberg.com/news/articles/2023-01-12/tesla-china-factory-expansion-plans-in-doubt-amid-data-concerns#xj4y7vzkg).

Bommakanti, K. (2022) *India and Cyber Power: The Imperative of Offensive Cyber Operations*, Occasional Paper of the Observer Research Foundation, 377 (c. le 23 janvier 2023: https://www.orfonline.org/programme/tech-and-media/cybersecurity-and-internet-governance/).

Brent, L. (2019) 'Nato Roles in CyberSpace', *NATO* (c. le 9 janvier 2023 : https://www.nato.int/docu/review/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/EN/index.htm).

Burt, T. (2020) 'New cyberattacks targeting U.S. elections', *Microsoft On the Issues* (10 septembre) (c. le 18 janvier 2023: https://blogs.microsoft.com/on-the-issues/2020/09/10/cyberattacks-us-elections-trump-biden/).

Cattaruzza, A. (2019) *Géopolitique des données numériques. Pouvoir et conflits à l'heure du big data*, Paris : Le Cavalier Bleu.

Cheng, T.F. et Shunsuke, T. (2022) 'Breaking Through. How Huawei and other tech champions are stealthily building g up China's domestic semiconductor supply chain as US sanctions continue', *Nikkei Asia* - Special excerpt from Dec. 5-11.

Colon, D. (2021) *Propagande. La manipulation de masse dans le monde contemporain*, Paris : Flammarion.

Conseil de l'UE (2017) *Cyberopérations russes contre l'Ukraine: déclaration du haut représentant au nom de l'Union européenne*, Communiqué de presse (c. le 18 janvier 2023 : https://www.consilium.europa.eu/fr/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/).

Conseil de l'UE (2022) *Cyberopérations russes contre l'Ukraine: déclaration du haut représentant au nom de l'Union européenne*, Communiqué de presse (c. le 18 janvier 2023 : https://www.consilium.europa.eu/fr/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/pdf).

Coustillière, A. (2020) 'La transformation numérique du ministère des Armées', *Hérodote*, 2, 177/178 : 165-177.

Creemers, R. (2020) 'Comment la Chine projette de devenir une cyber-puissance', *Hérodote*, 2, 177/178 : 297-311.

CyberTechAccord (2021) *Towards Effective Cyber Diplomacy: A Guide to Best Pratices and Capacity Building* (c. le 10 janvier 2023: https://cybertechaccord.org/uploads/prod/2021/10/TowardsEffectiveCyberDiplomacy.pdf).

Danet, D. et Desforges, A. (2020) 'Souveraineté numérique et autonomie stratégique en Europe : du concept aux réalités géopolitiques', *Hérodote*, 2, 177/178 : 179-195.

Delerue, F. (2020) *Cyber Operations and International Law*, Cambridge: Cambridge University Press.

Demchak, C. C. et Spidallieri, F. (2022) 'Tallying Unlearned Lessons from the First Cybered Conflict Decade, 2010-2020', *The Cyber Defense Review*, 7 , 1: 15-20.

Desforges, A. (2018) *Approche géopolitique du cyberespace : les enjeux pour la défense et la sécurité nationale : l'exemple de la France*, Thèse de doctorat en géopolitique soutenue le 27 août, Paris 8.

Dixon, P. (2016), *Surveillance in America: An Encyclopedia of History, Politics, and the Law*, Vol. 1, Santa Barbara: ABC-CLIO.

Domenach, J.-M. (1950) *La propagande politique*, Paris : Presses Universitaires de France.

Douzet, F. (2018) 'L'expansion de la puissance chinoise dans le cyberespace', *Revue Défense Nationale*, 7, 812 : 89-94.

Douzet, F. (2020) 'Du cyberspace à la datasphère. Enjeux stratégiques de la révolution numérique', *Hérodote*, 2, 177/178 : 3-15.

Douzet, F. et Géry, A. (2020) 'Le cyberespace, ça sert, d'abord, à faire la guerre. Prolifération, sécurité et stabilité du cyberespace', *Hérodote*, 2, 177/178 : 329-350.

Douzet, F.; Limonier, K.; Mihoubi, S. et René, É. (2020) 'Cartographier la propagation des contenus russes et chinois sur le Web africain francophone', *Hérodote*, 2, 177/178 : 77-99.

Douzet, F.; Salamatian, L.; Salamatian, K.; Pétiniaud, L.; Limonier, K. et Alchus, T. (2020) 'Measuring the Fragmentation of the Internet: The Case of the Border Gateway Protocol (BGP) During the Ukrainian Crisis', *in* Jančárková, Lindström, Signoretti, Tolga et Visky (Eds.), *12th International Conference on Cyber Conflict.*

20/20 Vision: The Next Decade. Proceedings 2020 (c. le 18 janvier 2023: https://ccdcoe.org/library/publications/12th-international-conference-on-cyber-conflict-20-20-vision-the-next-decade-proceedings-2020/).

Dragos (2023) 'Threat Groups We're Tracking' (c. le 24 janvier 2023: https://www.dragos.com/threat-groups/).

Eveno, E. (2004) 'Le paradigme territorial de la Société de l'Information', *Netcom*, 18, 1-2 : 89-132.

Federal Office for Information Security (2023) *State of IT Security in Germany reports* (c. le 27 janvier 2023: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Lageberichte/lageberichte_node.html).

Ford, C.A. (2022) 'Conceptualizing Cyberspace Security Diplomacy', *The Cyber Defense Review*, 7, 2: 35-54.

France Diplomatie (2022) 'La France transmet son premier message diplomatique en cryptographie post quantique (1er décembre 2022)', *France Diplomatie* (c. le 23 janvier 2023 : https://www.diplomatie.gouv.fr/fr/le-ministere-et-son-reseau/actualites-du-ministere/actualites-du-ministere-de-l-europe-et-des-affaires-etrangeres/article/la-france-transmet-son-premier-message-diplomatique-en-cryptographie-post).

Gao, J. (2022) 'What the 20th Party Congress Report Tells Us About China's AI Ambitions', *The Diplomat* (5 novembre) (c. le 20 janvier 2023: https://thediplomat.com/2022/11/what-the-20th-party-congress-report-tells-us-about-chinas-ai-ambitions/).

Gao, C.; Guo, Q.; Jiang, D.; Wang, Z.; Fang, C. et Hao, M. (2019) 'Theoretical basis and technical methods of cyberspace geography', *Journal of Geographical Sciences*, 29, 12: 1949-1964.

Gleicher, N. et Agranovich, D. (2020) 'Removing Coordinated Inauthentic Behavior from France and Russia', *Meta* (15 décembre) (c. le 19 janvier 2023: https://about.fb.com/news/2020/12/removing-coordinated-inauthentic-behavior-france-russia/).

Gold, J. (2020) *The Five Eyes and Offensive Cyber Capabilities: Building a 'Cyber Deterrence Initiative'*, The NATO Cooperative Cyber Defence Centre of Excellence (c. le 12 janvier 2023: https://ccdcoe.org/uploads/2020/10/2020-Josh-Gold-Five-Eyes-and-Offensive-Cyber-Capabilities.pdf).

Hartnett, S.J. (2011) 'Google and the 'Twisted Cyber Spy' affair: US–Chinese communication in an age of globalization', *Quarterly Journal of Speech*, 97, 4: 411–434.

Henrikson, A. (2019) 'The end of the road for the UN GGE process: The future regulation of cyberspace', *Journal of Cybersecurity*, 5, 1: 1-9.

Housen-Couriel, D. (2017) 'An analytical review and comparison of operative measures included in cyberdiplomatic initiatives', *Briefing n^{o} 2 from the Research Advisory Group*, Global Commission on the Stability of Cyberspace: 49-84.

Howard, P.N.; Ganesh, B.; Liotsiou, D.; Kelly, J. et François, C. (2019) 'The IRA, Social Media and Political Polarization in the United States, 2012-2018', *U.S. Senate Document* (c. le 23 janvier 2023: https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1004&context=senatedocs).

Ibragimova, G. (2013) 'Podhody gosudarstv Central'noj Azii k voprosam upravleniâ Internetom i obespečeniâ informacionnoj bezopasnosti' [Approches politiques des États d'Asie centrale en matière de gouvernance de l'Internet et de sécurité de l'information], *Indeks Bezopanosti*, 1, 104: 103-128.

Innes, M.; Grinnell, D., Innes, H.; Harmston, D. et Roberts, C. (2020) 'Normalisation et domestication de la désinformation numérique : les opérations informationnelles d'interférence et d'influence de l'extrême droite et de l'État russe en Europe', *Hérodote*, 2, 177/178 : 101-123.

James, R.C.; Lettre, M. et Rogers, M.S. (2017) *Foreign Cyber Threats to the United States*, (c. le 12 janvier 2023: https://www.armed-services.senate.gov/imo/media/doc/Clapper-Lettre-Rogers_01-05-16.pdf).

Kadiri, G. (2018) 'A Addis-Abeba, le siège de l'Union africaine espionné par Pékin', *Le Monde* (26 janvier) (c. le 9 janvier 2023 : https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html).

Kaiser R. (2015) 'The Birth of Cyber War', *Political Geography*, 46: 11-20.

Kim, K.-J. (2022) 'Seoul: North Korean hackers stole $1.2B in virtual assets', *AP Press*, (22 décembre) (c. le 18 janvier 2023: https://apnews.com/article/technology-crime-business-hacking-south-korea-967763dc88e422232da54115bb13f4dc).

Kokas, A. (2022) 'Data Trafficking and the International Risks of Surveillance Capitalism: The Case of Grindr and China', *Television & New Media*: 1-18.

Lee, J.; Zhang, E. et Creemers, R. (2022) 'China's Standardisation System – trends, implications and case studies in emerging technologies', *Leiden Asia Centre Report* (c. le 23 janvier 2023: https://leidenasiacentre.nl/wp-content/uploads/2022/04/Chinas-standardisation-system.pdf).

Leyden, J. (2021) 'Indian cyber-espionage activity rising amid growing rivalry with China, Pakistan', *The Daily Swig* (25 février) (c. le 12 janvier 2023: https://portswigger.net/daily-swig/indian-cyber-espionage-activity-rising-amid-growing-rivalry-with-china-pakistan).

Libération et AFP (2022) 'Après le vote d'un texte qualifiant la Russie d' 'Etat promoteur du terrorisme', le Parlement européen victime d'une attaque informatique', *Libération* (23 novembre) (c. le 23 janvier 2023 : https://www.liberation.fr/international/europe/apres-le-vote-dun-texte-qualifiant-la-russie-detat-promoteur-du-terrorisme-le-parlement-europeen-victime-dune-attaque-informatique-20221123_6AOTH7ONBBCDHKKOSDJHXLPNYE/).

Limonier, K. (2018) *Ru.Net: Géopolitique du cyberespace russophone*, Paris: L'Inventaire.

Maurer, T. (2011) *Cyber Norm Emergence at the United Nations – An Analysis of the Activities at the UN Regarding Cyber-security*, Discussion Paper #2011-11 (Explorations in Cyber International Relations Discussion Paper Series) du Belfer Center for Science and International Affairs de l'Université Harvard (c. le 9 janvier 2023: https://www.belfercenter.org/sites/default/files/files/publication/maurer-cyber-norm-dp-2011-11-final.pdf).

Maurer, T. (2018) *Cyber Mercenaries*, Cambridge : Cambridge University Press.

Meta (2022) 'Meta's Ongoing Efforts Regarding Russia's Invasion of Ukraine', *Meta* (26 février) (c. le 19 janvier 2023: https://about.fb.com/news/2022/02/metas-ongoing-efforts-regarding-russias-invasion-of-ukraine/).

Mirza, M.N. et Akram, M.S. (2022) *3-Cs of Cyberspace and Pakistan: Cyber Crime, Cyber Terrorism and Cyber Warfare*, Institute Strategic Studies Islamabad (c. le 12 janvier 2023: https://issi.org.pk/3-cs-of-cyberspace-and-pakistan-cyber-crime-cyber-terrorism-and-cyber-warfare/).

Moreau Defarges, P. (2023) 'Géopolitique', *Encyclopædia Universalis* [en ligne], (c. le 9 janvier 2023 : www.universalis-edu.com/encyclopedie/geopolitique/).

Mueller, M.L. (2020) 'Against Sovereignty in Cyberspace', *International Studies Review*, 22: 779-801.

Nations Unies (2019) *L'ère de l'interdépendance numérique*, Rapport du Groupe de haut niveau sur la coopération numérique crée par le secrétariat général de l'Organisation des nations unies (c. le 9 janvier 2023 : https://www.un.org/sites/www.un.org/files/uploads/files/Ere_Interdependance_numerique.pdf).

Nations Unies (2023) *Construire une architecture plus efficace pour la coopération numérique* (c. le 9 janvier 2023 : https://www.un.org/techenvoy/fr/content/global-digital-cooperation).

Nocetti, J. (2020) 'Un « cyber-mariage » arrangé ? Réalités et implications de la coopération cyber entre la Russie et la Chine', *Études Internationale*s, 51, 2 : 261-285.

Nye, J. (2014) *The Regime Complex for Managing Global Cyber Activities*, Global Commission on Internet Governance Paper Series No. 1 du Centre for International Governance Innovation (c. le 9 janvier 2023: https://www.cigionline.org/publications/regime-complex-managing-global-cyber-activities/).

Official Journal of the European Union (2020) *COUNCIL DECISION (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States* (c. le 30 janvier 2023: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020D1127&from=EN).

OTAN (2021) *Communiqué du sommet de Bruxelles publié par les chefs d'État et de gouvernement participant à la réunion du Conseil de l'Atlantique Nord tenue à Bruxelles le 14 juin 2021* (c. le 30 janvier 2023 : https://www.nato.int/cps/en/natohq/news_185000.htm?selectedLocale=fr).

Pan, C. (2022) 'Tencent joins open-source chip design community RISC-V as China seeks to mitigate impact from US sanctions', *South China Morning Post* (22 décembre) (c. le 24 janvier 2023: https://www.scmp.com/tech/big-tech/article/3204265/tencent-joins-open-source-chip-design-community-risc-v-china-seeks-mitigate-impact-us-sanctions).

Patel, K. et Chudasama, D. (2021) 'National Security Threats in Cyberspace', *National Journal of Cyber Security Law*, 4, 1: 12-20.

Pétiniaud, L. (2022) 'Les routes des données, enjeu géopolitique de la guerre en Ukraine', *Hérodote*, 3, 186 : 113-134.

Renard, T. (2018) 'EU cyber partnerships: assessing the EU strategic partnerships with third countries in the cyber domain', *European Politics and Society*, 19, 3: 321-337.

Renault, C.; Charon, P. et Laurençon, F. (2022) ' Renseigner autrement ? Trajectoires de l'Osint dans les services de renseignement', *Hérodote*, 186, 3 : 19-30.

Reuters (2022) 'Arne Schönbohm: German cybersecurity chief sacked over alleged ties with Russia', *Euronews* (18 octobre) (c. le 12 janvier 2023: https://www.euronews.com/2022/10/18/arne-schonbohm-german-cybersecurity-chief-sacked-over-alleged-ties-with-russia).

Riordan, S. (2019) *Cyberdiplomacy: managing security and governance online*, Cambridge: Polity Press.

Samaran, S. (2023) 'L'Organisation du traité de sécurité collective en état de mort cérébrale ?', *Brève Stratégique de l'IRSEM*, 53 (c. le 27 janvier 2023 : https://www.irsem.fr/media/bs-53-samaran-otsc.pdf).

Savolle, A. (2021), 'Le Soft Power chinois à l'heure des algorithmes', *Regards géopolitiques*, 7, 2.

Segal, A. (2017) 'Chinese Cyber Diplomacy in a New Era of Uncertainty', *Aegis Paper Series*, 1703, Hoover Institution, Stanford University (c. le 10 janvier 2023: https://www.hoover.org/sites/default/files/research/docs/segal_chinese_cyber_diplomacy.pdf).

Segal, A. et Goldstein, G.M. (2022) 'Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet', *Independent Task Force Report*, 80 (c. la 10 janvier 2023: https://www.cfr.org/report/confronting-reality-in-cyberspace/download/pdf/2022-07/CFR_TFR80_Cyberspace_Full_SinglePages_06212022_Final.pdf).

Smith, B. (2022) 'Defending Ukraine: Early Lessons from the Cyber War', *Microsoft On the Issues* (22 juin) (c. le 23 janvier 2023: https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/).

Tajdin, B. (2013) 'Will Iran's national internet mean no world wide web?', *BBC* (c. le 9 janvier 2023: https://www.bbc.com/news/world-middle-east-22281336).

Taillat, S. (2020) 'Cyber opérations offensives et réaffirmation de l'hégémonie américaine : une analyse critique de la doctrine de *Persistent Engagement*', *Hérodote*, 2, 177/178 : 313-328.

Tertrais, B. (2023) 'La cohérence sans l'abondance ? La nouvelle programmation militaire se dessine', *Institut Montaigne* (23 janvier) (c. le 24 janvier 2023 : https://www.institutmontaigne.org/analyses/la-coherence-sans-labondance-la-nouvelle-programmation-militaire-se-dessine).

Teurtrie, D. (2017) 'L'OTSC : une réaffirmation du *leadership* russe en Eurasie *post*-soviétique ?', *Revue Défense Nationale*, 7 : 153-160.

The New York Times (2022) 'Chinese Hackers Tried to Steal Russian Defense Data, Report Says', *The New York Times* (19 mai) (c. le 23 janvier 2023: https://www.nytimes.com/2022/05/19/world/asia/china-hackers-russia.html).

The Strait Times (2023) 'Taiwan plans domestic satellite champion to resist any China attack', *The Strait Times* (6 janvier) (c. le 24 janvier 2023: https://www.straitstimes.com/asia/east-asia/taiwan-plans-domestic-satellite-champion-to-resist-any-china-attack).

Thibout, C. (2018), 'Cyberespace : vers quelle gouvernance ?', *Entretien de l'IRIS* (c. le 18 janvier 2023 : https://www.iris-france.org/123908-cyberespace-vers-quelle-gouvernance/).

TSCIOPRC [The State Council Information Office of the People's Republic of China] (2017) *International Strategy of Cooperation on Cyberspace* (c. le 10 janvier 2023: http://www.scio.gov.cn/32618/Document/1543874/1543874.htm).

U.S. Department of State (2019) *Joint Statement on Advancing Responsible State Behavior in Cyberspace* (c. le 20 janvier 2023: https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/).

Van Puyvelde, D. (2019) *Outsourcing US Intelligence. Contractors and Government Accountability*, Édimbourg: Edinburgh University Press.

Voo, J.; Hermani, I. et Cassidy, D. (2022) *National cyber power index 2022*, Rapport du Belfer Center for Science and International Affairs (c. le 12 janvier 2023: https://www.belfercenter.org/sites/default/files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf).

Watts, C. (2022) 'Preparing for a Russian cyber offensive against Ukraine this winter', *Microsoft On the Issues* (3 décembre) (c. le 10 janvier 2023: https://blogs.microsoft.com/on-the-issues/2022/12/03/preparing-russian-cyber-offensive-ukraine/).

Weidemann, A. (2021) 'New campaign targeting security researchers', *Threat Analysis Group* (25 janvier) (c. le 30 janvier 2023: https://blog.google/threat-analysis-group/new-campaign-targeting-security-researchers/).

Woo, S. (2020) 'The U.S. vs. China: The High Cost of the Technology Cold War', *The Wall Street Journal* (22 octobre) (c. le 25 janvier 2023: https://www.wsj.com/articles/the-u-s-vs-china-the-high-cost-of-the-technology-cold-war-11603397438).

Xinhua (2016) 'China announces cybersecurity strategy', The State Council, The People's Republic of China (c. le 10 janvier 2023: https://english.www.gov.cn/state_council/ministries/2016/12/27/content_281475526667672.htm).

Zagaris, B. (2022) 'U.S. Unseals Indictment Charging Three Iranian Nationals with Hacking and Extortion', *International Enforcement Law Reporter*, 38, 9: 368-371.