Le cyber, un facteur d'instabilité internationale

Laurent Prosperi

laurent.prosperi@ens-paris-saclay.fr

18 octobre 2020

La dernière décennie a vu de nombreuses cyberattaques défrayer la chronique, que ce soit en 2017 avec les deux vagues mondiales de cryptovirus (WannaCry et NotPetya), les diverses actions visant à influencer les élections en Europe comme aux États-Unis ou encore les offensives répétées contre les systèmes de santé, souvent à des fins cybercriminelles. Le cyber apparait comme un domaine facilitateur de l'extension de la conflictualité contemporaine. La flexibilité d'emploi et la difficulté à attribuer une attaque d'origine cyber permettent d'agir en évitant les pénalités liées au recours à la force armée par un contournement par le bas de l'ordre établi, en restant en dessous du stade de la légitime défense ou en étant par exemple dans la zone grise de l'article 5 de l'OTAN. L'usage de groupes non-étatiques comme proxy permet le déni plausible et donc favorise un usage décomplexé de la force. Dans le même temps, le droit international ne peut jouer son rôle de régulateur du fait des deux points précédents même si son applicabilité au cyberespace a été reconnu.

1 Le retour des États

L'une des idées fondatrices d'Internet était de constituer un réseau mondial sans frontière géographique, n'étant pas soumis aux contraintes juridiques préexistantes mais plutôt à des règles fixées par le bas (i.e utilisateur). La déclaration d'indépendance du cyberespace en 1996 par John Perry Barlow et la construction de la société du logiciel libre vont dans ce sens. Bruce Schneier [1] explique la tension entre pouvoir

1. The battle for power on the Internet : Bruce Schneier at TEDxCambridge 2013 », vidéo publiée le 25 septembre 2013 par TEDxTalks dans (F. Douzet. « La géopolitique pour comprendre le cyberespace ». In : *Hérodote* 152-153.1 [2014], p. 3-21, p. 9)

« distribué » (communauté du logiciel libre, militants, dissidents, hackers, criminels) et « traditionnel » (états, grandes entreprises et institutions) de par les caractéristiques initiales d'Internet : décentralisation, neutralité et accessibilité. Celles-ci ont favorisé les petits acteurs de tous bords en leur permettant d'atteindre une grande efficacité et une bonne réactivité.

Les actions des États ont été, et sont, contestées dans le cyberespace par de puissantes multinationales contrôlant la technologie (et son développement), les données et noyautant l'économie numérique ; par des individus seuls ou coalisés dans le cadre d'actions cybercriminelles, d'influence ou de militantisme et poursuivant des objectifs politiques, idéologiques ou culturels ; par des organisations non étatiques (par exemple terroristes) utilisant le milieu cyber pour se structurer, comme plateforme opérationnelle et pour mener une lutte asymétrique contre des États. Même de petite taille, ces acteurs « peuvent avoir un effet systémique, déstabilisant une entreprise, une organisation ou même un État. » [2] « La suprématie des acteurs étatiques est donc battue en brèche : les acteurs non étatiques accèdent au statut de sujets des relations internationales, tandis que les États glissent vers une position de dépendance vis-à-vis de ces derniers. » [3]

La contestation de l'ordre westphalien, dans le cyberespace, est accéléré par la « révolution dans les capacités individuelles » [4] avec l'accès à des vecteurs d'influence, que sont les réseaux sociaux et les plateformes de contenus avec des effets potentiellement stratégiques ; par la disponibilité d'outils offensifs clé en main facilitant la mise en œuvre tactique ; par la généralisation de moyens de communication chiffrés et outils d'anonymisation tel que Tor [5] ou I2P ; par le développement de cryptomonnaies compliquant le traçage des transactions. Cependant, cet état de fait est à nuancer car la majorité des outils disponibles sont génériques, bruyants bien qu'avec un fort potentiel de nuisances contre des cibles faiblement durcies, et avoir une action stratégique efficace dans le spectre informationnel n'est pas chose aisée (en quantifier les effets est tout aussi difficile) malgré la disponibilité des outils et vecteurs. Enfin, la capacité d'action d'un acteur dépend étroitement de ses ressources et de la sophistication de son organisation [6].

Pour autant, les relations entre les États et les autres acteurs du cyberespace ne

2. « Cybersécurité : Extension du domaine de la lutte ». In : *Politique étrangère* 2 (2018), p. 9-230, p. 11.

3. S. Taillat. « Le cyberespace et la conflictualité internationale ». In : *La Cyberdéfense*. U. Paris : Armand Colin, 2018, p. 26-33, p.32 Buchanan 2017.

4. Ibid., p.31 Rosenau, 1990.

5. Initialement développé par des chercheurs de United States Naval Research Laboratory.

6. Taillat, op. cit., p.32 Buchanan 2017.

peuvent se résumer à un rapport d'opposition. Premièrement, les États construisent [7] une cyberdéfense s'articulant avec le secteur privé : en Occident, la tendance est à la coopération ; en Russie et en Chine, l'heure est à l'intégration. Deuxièmement, les États ont recours à des proxies afin de mener des opérations non attribuables (ou d'en réduire les risque) ou pour profiter du savoir faire et des ressources des acteurs employés. La nature des proxies est très variée : individus isolés (pouvant louer leur services) ; des réseaux d'hacktivistes agissant pour des motifs politiques ; des réseaux cybercriminels motivés par le profit (l'espace post-soviétique en abrite un certain nombre) ; des sociétés militaires ou de cybersécurité privée. L'utilisation de proxies entraine un certain nombre de conséquences : un accroissement de l'instabilité, la complication de l'étude des phénomènes à l'œuvre dans le cyberespace et cela pose la question du contrôle de l'effecteur par le commanditaire, les deux pouvant poursuivre des buts différents.

Initialement, les États ont été pris de cours. Seuls quelques uns d'entre eux [8] avaient anticipé l'importance future du domaine cyber. Une centralisation du pouvoir est en œuvre depuis près d'une décennie, avec la maturation et la consolidation d'acteurs initiaux (géants du web, regroupement des hackers en organisations structurées) mais aussi par le retour en force des acteurs étatiques sur fond de sécurité nationale et défense de leurs pouvoirs régaliens [9]. Le concept de cyberespace réapparait à partir des années 2000 dans les discours et la doctrine étatique. Les années 2007 (Estonie), 2008 (Géorgie), 2013 (Snowden) et 2015 (Ukraine) servent de catalyseur à la réappropriation étatique en Occident. Le cyberespace apparait alors comme « un territoire sur lequel il faut faire respecter ses frontières, sa souveraineté, ses lois ; et surtout, une menace pour la sécurité nationale et les intérêts de la nation » [10]. Initialement, les États sont pris de court. Seuls quelques uns d'entre eux avaient anticipé son importance future : les États-Unis de par leur rôle d'avant garde dans le développement de la technologie (réflexion dès le début des années 1990) mais aussi la Russie (publication en 2000 de leur doctrine de sécurité informationnelle) et la Chine (dès la fin des années 1990) autour des problématiques de contrôle de l'information vitales pour leur stabilité politique. Au-delà de la protection des infrastructures critiques, l'enjeu est aussi la maîtrise de l'information. Les printemps arabes ont mis en exergue l'importance des réseaux sociaux dans la structuration de mouvements de contestation mais aussi leur influence sur la po-

7. Ou tentent de construire pour les plus faible d'entre eux.
8. En particulier les Etats-Unis, la Chine, la Russie et Israël.
9. Douzet, loc. cit.
10. Ibid., p. 7-8.

pulation. Depuis, les États tentent de se réapproprier la couche sémantique dans un objectif de supériorité informationnelle et de défense nationale (contre-ingérence, contre-influence), pour un contrôle de la population ou pour s'opposer de manière asymétrique à d'autres puissances.

Le domaine cyber est l'un des vecteurs du retour à des politiques de puissance [11] et de remise en cause de l'ordre mondial [12]. En effet, le numérique favorise le conflit du fait de l'absence de conception partagée permettant de cadrer les enjeux, de l'utilisation du cyber à des fins politiques (États-Unis, Russie, Chine ou puissance émergentes), du contournement par le bas (sous le seuil de l'agression armée [13]) et enfin par l'incertitude sur l'intention et les actions des autres protagonistes. Les règles du jeu international et les modèles stratégiques existants semblent inadaptés [14] et surtout la vitesse des évolutions technologiques et opérationnelles dépasse celle de l'élaboration d'un consensus international et d'un nouveau corpus juridique. Par ailleurs, le cyberespace se militarise (par exemple avec les cyberopérations menées par la NSA et GCHQ contre l'État Islamique ou alors le soutien cyber en appui des forces russes en Crimée et des séparatistes en Ukraine) rapidement en parallèle d'un mouvement de« souverainisation » [15] du cyber. Par ailleurs, il tend à supprimer la frontière entre sécurité intérieure et extérieure.

Les enjeux géopolitiques sous-jacents pour les sociétés occidentales sont, pour F.Douzet [16], tout d'abord la paix et la sécurité. Par ailleurs « les stratégies nationales contribuent à façonner l'Internet » [17] en entrainant une fragmentation politique et physique du réseau (souvent appelée balkanisation de l'Internet) ce qui pose la question du futur de l'Internet. D'autres problématiques apparaissent : la gouvernance du cyberespace et la remise en cause de la puissance étatique. Un géant du numérique pourrait presque être défini comme un État numérique, en voyant ses utilisateurs comme sa population, les infrastructures, les services et les données qu'il détient comme son territoire et les CGU comme ses lois.

11. Taillat, op. cit., p. 29.
12. *Cybersécurité : Extension du domaine de la lutte*, p. 11 note 7.
13. Selon l'ouvrage du journaliste David E. Sanger, « Confront and Conceal : Obama's secret wars and surprising use of american power » les forces américaines serait attachées à élaborer Olympic Games de telle sorte que les règles du DCA ne s'y appliquent pas : pas d'imputabilité, discrétion des effets et effets diffus dans le temps pour ne pas dépasser un certain seuil.
14. Douzet, op. cit.
15. J. Nocetti. « Géopolitique de la cyber-conflictualité ». In : *Politique étrangère* Été.2 (2018), p. 15-27, p. 22.
16. Douzet, op. cit.
17. Ibid., p. 19.

2 Vers une escalade cyber ?

Les capacités cyber sont relativement répandues dans le monde. Selon l'ancien directeur de la NSA, Richard Ledget [18], une centaine de pays seraient en mesure de lancer des cyberattaques, à des intensités diverses. Certains, les APT notamment, sont capables de mener des opérations d'une complexité similaire à ce qui peu être fait par un état. Cette grande diversité d'acteurs couplée aux propriétés du cyberespace (incertitude, attribution, avantage à l'offensive) tend à dégrader la sécurité internationale, à favoriser une escalade des tensions. Celle-ci est favorisée par quatre facteurs, *la courses aux cyberarmements et au développement capacitaire*. *Le dilemme entre pénétration et retenue* [19] provenant de la confusion entre défense et attaque du fait que les acteurs sont incités à la pénétration préventive de systèmes pour des raisons défensives ou pour la préparation opérationnelle qui nécessite de compromettre une cible potentielle plusieurs mois ou années à l'avance ; sachant que toute intrusion est perçue comme menaçante. *Le doute quant à l'attribution* accroit le risque d'escalade en cas de représailles du fait de l'incertitude sur les intentions de l'adversaire et des opérations sous "false flag" (utilisation de proxy, usurpation d'identité, obfuscation du code ou encore opération sous "faux-uniformes"). Enfin, il n'y a *pas de cadre partagé au niveau stratégique* car il n'y a pas de représentation commune des menaces ni des enjeux entre les différents acteurs. Les Occidentaux se préoccupent de la menace technique pesant sur leurs activités économiques, financières et sociales bien qu'il y ait une prise en compte croissante de la menace informationnelle depuis trois ans entrainant la mise en évidence d'un risque politique. A l'inverse, la Russie et la Chine (mais aussi l'Iran) considèrent qu'une menace existentielle pèse sur leur stabilité politique et ils tendent à transformer le cyber en outil de puissance afin de remettre en question l'ordre international post guerre froide. Les points de divergence entre les deux modèles portent sur le point de la gouvernance d'Internet, les questions d'applicabilité du droit international, la lutte contre la cybercriminalité (qui a proliféré dans le monde post-soviétique), la rédaction d'accords contraignants sur les "arsenaux numériques" et, enfin, sur la définition de la légitime défense (doit elle être stricte, préemptive ou préventive afin de s'adapter aux contraintes du cyberespace).

18. Durant son intervention à Georgetown Law School dans A. Cattaruzza. « Chapitre 1. La construction politique de l'espace numérique. Penser l'espace numérique comme un espace stratégique ». In : *La Cyberdéfense*. U. Paris : Armand Colin, 2018, p. 19-25, p. 90

19. Taillat, loc. cit.

3 Limiter l'escalade

« La retenue joue un rôle central dans la gestion des crises » [20], par exemple avec une absence de toute déclaration publique et d'attribution officielle suite au piratage massif de JP Morgan en 2014 ou lors de celui des messageries de la Maison Blanche. Les attributions peuvent se faire par médias ou sociétés de sécurité interposés. Entre 2009 et 2010, Moscou et Washington ont mené des politiques d'apaisement avec la mise en place d'un partage d'informations, pour lutter contre la cybercriminalité, ainsi que d'une ligne de déconfliction afin de prévenir une escalade entre les deux nations. Toutefois, le retour de Vladimir Poutine en 2012, suivi par le conflit ukrainien, a stoppé net les politiques de coopération. Cependant, la société civile tend à être un facteur limitant. En effet, contrairement au nucléaire, les capacités cyber s'appuient sur de la technologie et des acteurs civils. Ce qui fait dire à Edward Roche [21] que les entreprises auront un rôle au moins égal à celui des états dans le développement des capacités cyber et dans leur contrôle mais aussi dans la paix et la sécurité du cyberespace. Outre la retenue, les états et les grandes entreprises sont engagés, officiellement du moins, dans un long processus de développement d'une lutte efficace contre la cyberprolifération et d'une gouvernance permettant de limiter les tensions.

3.1 La lutte contre la cyberprolifération

La cyberprolifération tient à une grande diversité de fins (profits, défense d'une idéologie, recherche d'avantages stratégiques, espionnage), aux propriétés intrinsèques des armes cyber (les outils sont facilement copiés, réutilisés, détournés et échangés), au développement de marchés parallèles (utilisés aussi par les états) et à une dualité entre attaque et défense. La Convention de Budapest, du 23 novembre 2001, est le premier instrument international visant à lutter spécifiquement contre la prolifération cyber. L'objectif est de mettre sur pied une politique pénale commune pour lutter contre la cybercriminalité et contre la détention et le transfert intentionnel de certains outils, tout en prenant en compte la dualité des technologies (par exemple ceux permettant de tester la protection des systèmes). Son action est limitée car elle n'est ratifiée que par 56 états, une bonne part sont des membres de l'Union Européenne, et parce qu'elle ne couvre pas les marchés parallèles.

Les normes se renforcent suite à la vente par des entreprises européennes de

20. Nocetti, op. cit., p. 23 note 26.

21. E. M. Roche. « La course au cyber armement ». In : *Netcom. Réseaux, communication et territoires* (2019).

systèmes de surveillance et d'interception à la Libye (l'entreprise française Amesys), à la Syrie de 2011 à 2013. Cela mène en 2014, sur proposition franco-britannique, à l'inscription, sur la *Liste des biens et technologies à double usage* de l'agrément de Wassenaar, des logiciels d'intrusion et des système de surveillance IP. Le régime de contrôle est non contraignant et ne regroupe que 42 états, incluant la Russie, les États-Unis ainsi que de nombreux états européens (déjà soumis au régime de contrôle de l'Union Européenne). Enfin la liste doit être transposée dans le droit national des états pour être effective. Le GEG de juin 2015 propose une norme non contraignante, n'entrainant pas de contrôle et garantissant l'intégrité de la chaîne logistique afin que les utilisateurs finaux aient confiance dans la sécurité des produits informatiques ; par exemple les États s'engagent à ne pas introduire volontairement de backdoors. Suite à l'échec du cycle de 2017, de nombreux points sont restés sans consensus, comme le contrôle des actions offensives menées par des acteurs privés, l'établissement de critères [22] de précision visant à restreindre les effets de masse afin de prévenir les risques systémiques hors conflit ouvert, l'obligation de durcissement ou d'auto-destruction des charges utiles pour limiter les risques de détournement et l'engagement de signaler les failles informatiques, notamment zero-days. Enfin, de nouvelles exceptions relatives aux contrôles des logiciels ont été ajoutées à l'agrément Wassenaar en 2017, afin d'autoriser certains outils nécessaires à la recherche et à la cyberdéfense car la précédente version s'appliquait aux briques logicielles et non aux usages qui en sont faits. Cependant, ces démarches se heurtent, comme dans le cas de l'application du droit international, à l'absence d'une définition officielle partagée de ce qu'est une cyberarme et à défaut de consensus entre États, parmi les différentes parties prenantes d'un même État. Les instruments existants sont non contraignants, d'une portée non universelle, d'une précision variable et il manque une articulation entre eux.

3.2 Quelle gouvernance ?

Le modèle de gouvernance d'Internet est développé autour de « multi-parties prenantes » [23] que sont l'industrie, la communauté technique (universitaires, logiciel libre), les gouvernements et la société civile. Par ailleurs, les principaux enjeux internationaux de cette gouvernance sont la cybersécurité, la problématique des données

22. A. Géry. « Droit international et prolifération des cyberarmes ». In : *Politique étrangère* Été.2 (2018), p. 43-54, p. 53.

23. J. Nocetti. « Internet et sa gouvernance : crispations internationales et nouveaux enjeux ». In : *La Cyberdéfense*. U. Paris : Armand Colin, 2018, p. 130-135, p. 130.

(notamment le défit posé par les géants du web pour la souveraineté des états), l'adoption de standards techniques, la liberté d'expression ou le statut des entreprises de contenus et de services. Depuis une quinzaine d'années, une coopération internationale encore balbutiante est en construction autour des problématiques de gouvernance du cyberespace. Elle tend à regrouper les acteurs centraux, étatiques ou non (géants du numérique en premier, le secteur privé, la société civile, la communauté scientifique).

En 2004 est constitué un Groupe d'experts gouvernementaux (GGE) au sein de l'ONU sur la cybersécurité ; celui-ci s'est réuni cinq fois depuis 2004. En 2013, ce groupe conclut à l'applicabilité du droit international existant, notamment la Charte des Nations unies, à l'action des États dans le cyber-espace. En 2015, un socle non contraignant de bonne conduite des états hors du contexte d'opérations militaires (comme ne pas endommager les infrastructures critiques, coopération avec les états victimes de cyberattaques, lutte contre la prolifération) est adopté par l'assemblée générale des Nations Unies [24]. Une interdiction de principe (non contraignante) d'utilisation des moyens cyber à des fins d'espionnage économique est prise lors du G20 de 2015. La déclaration de Lucques, lors du G7 2017, approfondit la reconnaissance de l'applicabilité du droit international au cyber. Cependant la même année marque un coup d'arrêt au développement d'une gouvernance onusienne avec l'échec du nouveau cycle du GGE (encourageant le signalement des failles de sécurité et l'échange d'informations entre acteurs étatique ou non) se soldant par une absence de consensus final (et donc de rapport). D'autres initiatives intégrant d'avantage les partenaires du privé et de la société civile continuent, comme le consacre la Revue, les « Etats ne seront pas en mesure de créer et d'imposer seuls des règles à tous les acteurs du cyberespace » [25]. En effet, le secteur privé (à minima les géants) sont devenus des acteurs systémiques incontournables de la régulations du cyberespace par leur maîtrise technologique, leur taille, leur rôle dans la normatisation technique et dans le développement de l'infrastructure du cyberespace (rappelons que les câbles et les réseaux ne sont pas possédés par les états, et que les futures constellations de satellites proviennent du secteur privé américain). Les états n'ont qu'un rôle consultatif au sein de l'ICANN alors que les géants ont un rôle décisionnaire. Les Nations Unies intègrent les grands acteurs du secteur privé dans des échanges sur la gouvernance depuis octobre 2006 avec la première édition du Forum sur la Gouvernance de l'Internet (avec une édition chaque année jusqu'à ce jour). Son mandat est de faciliter la

24. Assemblée générale des Nations Unies, A/70/174, 22 juillet 2015
25. SGDSN. *Revue stratégique de cyberdéfense*. 2018, p. 36.

discussion entre les différentes parties prenantes. En 2011, en marge du 37ème Forum du G8 s'est tenu l'e-G8 à Paris, rassemblant, outre des représentants des membres du G8, les acteurs de l'économie numérique (au premier rang desquels les PDG de Google, Facebook, Alibaba, Amazon mais aussi des responsables de l'Electronic Frontier Foundation ou de Wikipedia). Les différents échecs de régulation inter étatique ont donné l'occasion au secteur privé de devenir une cheville ouvrière de la construction de la gouvernance en déployant des stratégies diplomatiques similaires à celles des états. Depuis 2014, Microsoft promeut un ensemble de règles de comportement et d'accords (TechAccord) rassemblant le secteur privé et les acteurs étatiques. En février 2017, Microsoft a appelé à la signature d'une « Convention de Genève du numérique » avec obligation de révéler les failles de sécurité. En février 2018, Siemens dévoile sa « Charte de confiance » lors de la conférence de Munich sur la sécurité. En janvier 2018, le Forum économique mondial a annoncé le lancement d'un Centre mondial de cybersécurité afin d'améliorer la coopération entre gouvernements et acteurs privés. En 2016, Paris dénonce la mainmise des géants américains sur la gouvernance d'Internet [26]. L'année 2017, est marquée par la reconnaissance du numérique comme un espace diplomatique à part entière, et par des géants comme interlocuteurs de premier plan, avec la nomination d'un ambassadeur spécialisé en France [27] et au Danemark, dédié à la Silicon Valley pour ce dernier. En 2018, l'Appel de Paris réunit près de 80 États et nombre d'acteurs de la société civile autour des questions de gouvernance et de sécurité dans le monde numérique. Les participants s'engagent, de manière non contraignante, à lutter contre la cybercriminalité et la cyberprolifération, à prendre des mesures contre les actions offensives des acteurs non étatiques, à protéger la propriété intellectuelle et à prévenir les interférences dans les processus électoraux. Notons que la Chine, la Russie et les États-Unis n'y ont pas participé, et ne sont donc pas signataires de l'appel. Les géants américains étaient tous au rendez-vous, les grandes entreprises chinoises absentes.

Deux formes de régulation "décentralisées", initialement peu soumises à l'action des états, favorisent le secteur privé : la régulation par le code [28] et la régulation du contenu. La première vient du constat que le choix de l'architecture du Net et des technologies utilisées tend à façonner la société dans laquelle nous vivons et les lois "physiques" du cyberespace. Par exemple, des choix techniques peuvent maximiser la

26. Nocetti, loc. cit.

27. L'ambassadeur français pour le numérique a pour missions de concourir à la paix et à la stabilité dans le cyberespace, de participer à la construction de la gouvernance, de renforcer le secteur numérique français et de faire de l'influence quant aux valeurs, models et normes français.

28. Cattaruzza, op. cit., p. 36.

vie privée (et limiter l'identification) ou à l'inverse récolter un maximum de données. Pour Laurence Lessig « le code régule » et donc la question est de savoir qui va avoir un rôle dans le choix de la construction technique, souvent dépendante de considérations économiques. La deuxième vient du constat que les géants concentrent une majorité des contenus, que ce soit dans le domaine de la recherche en ligne (Google détient plus de 90% des parts de marché en Europe), la vidéo (Facebook et Google avec leurs différentes plateformes dominent le secteur), la messagerie (à travers les stratégies de rachat de Whatsapp par Facebook ou de Skype par Microsoft). Ce sont leurs Conditions Générales d'Utilisation (CGU) qui s'appliquent et définissent le cadre des conduites permises ou non, avec pour action coercitive le déréférencement ou la suppression de la plateforme. Cependant, une offensive légale est en cours en Europe avec le RGPD en 2016, le *Réglement européen relatif à la prévention de la diffusion de contenus à caractère terroriste en ligne* de 2019 puis la loi française Avia visant à lutter contre des contenus haineux. Cette dernière a été partiellement vidée de sa substance avec la suppression de la mesure phare : le retrait des contenus en moins de 24 heures. Un effet indirect de ces règlements sur le contrôle des contenus est la probable accentuation de la place centrale des solutions techniques, souvent non connues du grand public, de ces géants. En effet, rares sont les entreprises capables de mettre en place les infrastructures permettant de traiter leurs contenus dans les délais impartis, ce qui donne lieu à une externalisation du contrôle vers les géants qui mettent à disposition des solutions s'appuyant sur leur recherche en classification automatique et sur leurs infrastructures cloud, comme par exemple dans le cadre de l'Azure Content Moderator de Microsoft.

Les tendances sont une montée en puissance de la Chine et de la Russie avec une volonté d'affirmation à l'échelle internationale de la prééminence des États sur les autres acteurs et d'une revendication à l'échelon national du pouvoir souverain de l'État sur le contrôle du fonctionnement d'Internet. Le tout est présenté sur fond d'ordre public, de lutte contre la cybercriminalité et d'intérêts économiques. Le centre de gravité d'Internet se déplace vers l'Asie [29]. Cette dernière représentera près de 40% de la population mondiale connectée d'ici à la prochaine décennie et près de 75% des internautes vivront en dehors du monde occidental, la remise en cause de la gouvernance américaine (qu'elle soit étatique ou issu du secteur privé) va s'accélérer. Déjà en 2017, la Chine comptait 739 millions d'internautes pour 718 millions en Occident (Union Européenne et Etats-Unis). De plus, une coopération régionale sous l'égide de la Chine et la Russie se développe au sein de l'Organisation

29. Nocetti, op. cit., p. 131.

de coopération de Shanghai, notamment en matière de sécurité de l'information. A cela s'ajoute traditionnellement l'opposition de la Maison-Blanche à toute initiative multilatérale pouvant brider sa prééminence en matière numérique ou un contrôle des armements qui jouerait en défaveur des États-Unis, qui se considèrent comme dotés des capacités cyberoffensives les plus significatives [30]. Les révélations d'Edward Snowden ont eu l'effet d'un détonateur au sein des puissances émergentes mais n'ont pas eu de rôle unificateur. L'Inde et le Brésil ont une approche fondée sur la coopération internationale, à la différence des positions souverainistes de la Chine et de la Russie. L'Inde reste économiquement et sécuritairement proche des Etats-Unis, son approche s'inscrit dans la promotion d'une voie de type onusien. Depuis 2003 (et jusqu'en 2019), le Brésil s'est opposé frontalement à la domination américaine avec une intensification post-Snowden sous la présidence de Dilma Rousseff qui s'est traduite par une offensive diplomatique en avril 2014 avec l'organisation du NetMundial (rassemblant les représentant de près de 98 pays). L'objectif de cette conférence est de créer un écosystème distribué en charge de la gouvernance d'Internet afin d'éviter que les Américains ne concentrent trop de pouvoir.

Conclusion

Si initialement, la plupart des États se sont laissés dépasser par le numérique, aujourd'hui, le domaine cyber est l'un des vecteur du retour à des politiques de puissance car il facilite une remise en cause de l'ordre mondial et le contournement par le bas du seuil de l'agression armée. Les outils traditionnels permettant d'assurer la paix et la stabilité s'avèrent bien faibles et inadaptés pour lutter contre les dynamiques à l'œuvre. Certes le droit international est applicable en principe, cependant il ne l'est pas et ne peut l'être en pratique. La construction d'une gouvernance internationale est à l'arrêt depuis 2017. Les outils de lutte contre la prolifération sont très faibles, et n'incluent pas de contrôle externe, à la différence des armements nucléaires. La Maison Blanche s'oppose à toute initiative multilatérale pouvant brider sa prééminence en matière numérique ou voulant mettre en œuvre un contrôle des armements. Par ailleurs, la Russie et la Chine lient contrôle de l'information et cybersécurité, ce qui complique d'autant plus une co-construction commune.

30. Idem, *Géopolitique de la cyber-conflictualité*, p. 25.

Bibliographie

Réglement européen relatif à la prévention de la diffusion de contenus à caractère terroriste en ligne. 17 avril 2019. URL : https://www.europarl.europa.eu/doceo/document/TA-8-2019-0421_FR.html.

Roche, E. M. « La course au cyber armement ». In : *Netcom. Réseaux, communication et territoires* (2019).

Cattaruzza, A. « Chapitre 1. La construction politique de l'espace numérique. Penser l'espace numérique comme un espace stratégique ». In : *La Cyberdéfense*. U. Paris : Armand Colin, 2018, p. 19-25.

« Cybersécurité : Extension du domaine de la lutte ». In : *Politique étrangère* 2 (2018), p. 9-230.

Géry, A. « Droit international et prolifération des cyberarmes ». In : *Politique étrangère* Été.2 (2018), p. 43-54.

Nocetti, J. « Géopolitique de la cyber-conflictualité ». In : *Politique étrangère* Été.2 (2018), p. 15-27.

— « Internet et sa gouvernance : crispations internationales et nouveaux enjeux ». In : *La Cyberdéfense*. U. Paris : Armand Colin, 2018, p. 130-135.

SGDSN. *Revue stratégique de cyberdéfense*. 2018.

Taillat, S. « Le cyberespace et la conflictualité internationale ». In : *La Cyberdéfense*. U. Paris : Armand Colin, 2018, p. 26-33.

Douzet, F. « La géopolitique pour comprendre le cyberespace ». In : *Hérodote* 152-153.1 (2014), p. 3-21.