Géopolitique de la cyber-conflictualité

Par **Julien Nocetti**

Julien Nocetti est chercheur à l'Ifri. Ses travaux portent sur la diplomatie du numérique et de l'intelligence artificielle, la gouvernance de la cybersécurité, et les manipulations de l'information.

Les cyberattaques tendent à se multiplier et à devenir plus complexes. Les auteurs, comme les victimes, peuvent être des États ou des acteurs privés. Le champ de la cyber-conflictualité est particulièrement difficile à appréhender du fait de la multiplicité des acteurs impliqués, de la difficulté à attribuer précisément les attaques et de l'émergence de nouvelles formes de guerre de l'information. Les tentatives de régulation internationale du cyberespace ont abouti à des résultats modestes.

politique étrangère

Les événements internationaux des deux dernières années ont placé les problématiques de cybersécurité au cœur des agendas diplomatiques et stratégiques. Les piratages successifs de grands acteurs de la *tech*, comme Yahoo !, l'apparition de nouvelles menaces à grande échelle comme les « rançongiciels[1] » *WannaCry* et *NotPetya*, ainsi que la confirmation d'une course aux cyber-armements, traduisent la volatilité d'une politique internationale bouleversée par la dissémination des moyens numériques. Les soupçons d'ingérence russe dans l'élection présidentielle américaine en 2016, *via* une campagne d'influence sur internet, ajoutent à ces préoccupations une dimension informationnelle que les Occidentaux ont longtemps négligée. La cybersécurité est devenue un objet de « grande politique », aiguisant les appétits des grandes puissances, mais aussi d'acteurs privés qui ambitionnent de peser sur l'élaboration des normes de comportement dans le cyberespace.

1. Un rançongiciel (*ransomware*) est un programme malveillant reçu par courriel ou mis à disposition sur un site internet, qui rend les données d'un ordinateur chiffrées, donc inaccessibles. Une rançon, généralement en *bitcoins*, est exigée en échange d'une clé de déverrouillage. Une fois qu'un rançongiciel a infecté un ordinateur, il peut se propager à d'autres ordinateurs dans le réseau, empêchant ainsi toute activité normale.

Le cyberespace, perturbateur du système international

La politique internationale s'articule désormais largement autour du cyberespace. Dès l'origine de l'internet, l'action des États a été contestée dans ce domaine, tant par de puissantes plates-formes privées, majoritairement californiennes (les « GAFAM », Google, Apple, Facebook, Amazon et Microsoft), que par des individus, seuls ou coalisés, dont les registres d'action empruntent des formes variées (militantisme, influence, criminalité, etc.[2]). Les applications de messagerie chiffrée (Telegram, WhatsApp, etc.), et les outils d'anonymisation des connexions comme Tor, rendent le contrôle du cyberespace très difficile.

Voici une décennie, on ne pouvait être assuré que des acteurs comme Google, Facebook ou Twitter seraient en mesure de défier la souveraineté des États sans s'exposer à de puissantes ripostes. Les faits sont aujourd'hui plus clairs. L'affaire des fuites de données de millions d'utilisateurs de Facebook témoigne de cette évolution, sur fond de campagne d'influence numérique de la Russie dans l'élection présidentielle américaine en 2016, et avec deux auditions tendues de Mark Zuckerberg au Congrès américain.

Auparavant, les révélations d'Edward Snowden, en 2013, ont déstabilisé les relations internationales et reconfiguré la géopolitique du cyberespace. La présidence de Barack Obama avait installé l'industrie numérique américaine comme axe prioritaire d'un redéveloppement économique organisé autour des acteurs de cette industrie et de la stratégie de sécurité du pays. L'échelle de collecte des données par la National Security Agency (NSA) a dépassé tous les soupçons passés sur le degré d'intrusion et de surveillance numérique des agences américaines. Si la Russie s'est alors opportunément distinguée en accordant l'asile à l'ancien contractuel de la NSA, le Brésil a pris la tête d'une croisade contre l'hégémonie perçue des États-Unis sur le fonctionnement technique et le mode de gouvernance de l'internet[3]. L'épisode a permis à une puissance dite alors émergente, le Brésil, de suggérer de nouvelles alliances dans la géopolitique du cyberespace, tirant profit du discrédit moral des États-Unis.

L'essor d'une cyber-conflictualité protéiforme ne peut en effet être dissocié d'un contexte géopolitique en mutation accélérée. La Chine se pose en *challenger* des États-Unis pour la maîtrise du cyberespace. Elle défend

2. A. Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*, New York, PublicAffairs, 2017.
3. J. Nocetti, « Puissances émergentes et internet : vers une "troisième voie" ? », *Politique étrangère*, vol. 79, n° 4, 2014.

ardemment son marché national, tout en projetant ses champions à l'international (les « BATX[4] »), en industrialisant ses capacités de cyber-espionnage, et en se livrant à des tests réguliers de l'architecture physique de l'internet[5]. La Russie, quant à elle, conteste le récit occidental sur les affaires du monde, ambitionnant de reformater un ordre international autour de ses propres intérêts. Le cyberespace lui permet de déployer des opérations d'influence à une échelle inédite, tout en jouant de l'effet d'asymétrie propre à ce domaine pour transformer ses faiblesses en atouts[6].

Des menaces informatiques protéiformes et intenses

Les cyber-menaces affichent aujourd'hui de multiples visages. Les actions offensives menées contre des réseaux et des infrastructures numériques peuvent se manifester de diverses manières. Elles peuvent tout d'abord se traduire par des attaques par déni de service, qui ont pour effet de paralyser les serveurs visés. Au printemps 2007, l'Estonie avait été paralysée pendant près de deux semaines par ce type d'attaque[7]. Deuxième exemple : un virus peut être dirigé délibérément sur une infrastructure précise, comme les centrifugeuses d'uranium iraniennes en 2010, ciblées par *Stuxnet*, virus développé par Israël et les États-Unis pour ralentir le programme nucléaire de Téhéran[8]. Entreprise coûteuse, planifiée dès 2006, *Stuxnet* intégrait un niveau inédit de sophistication technique et de précision opérationnelle[9]. Troisièmement : on peut propager des virus de différents types, visant à extorquer des données et/ou de l'argent (cas de la cybercriminalité classique), ou à saboter et détruire. C'est le cas du logiciel malveillant (*malware*) *NotPetya* qui, ciblant massivement l'Ukraine en juin 2017, cherchait à fragiliser cet État. Plus de 70 % des machines infectées se trouvaient en Ukraine, le programme ayant amplement ciblé les infrastructures critiques du pays (système bancaire, aéroports, télécommunications, énergie, etc.), et pas seulement ses institutions[10]. Quatrième exemple, enfin : l'espionnage informatique, *via* le vol de données, qui reste une dimension sous-évaluée de la cyber-conflictualité.

---

4. Baidu, Alibaba, Tencent et Xiaomi.
5. La Chine a par exemple diffusé en 2010 37 000 fausses informations de routage dans le système ; China Telecom a détourné 15 % du trafic internet mondial pendant 20 minutes, prouvant la capacité de Pékin à couper internet temporairement et à faire passer le trafic mondial par ses appareils de surveillance.
6. J. Nocetti, « Cyber Power », *in* A. Tsygankov (dir.), *Routledge Handbook of Russian Foreign Policy*, Londres, Routledge, 2018.
7. A. Klimburg, *The Darkening Web: The War for Cyberspace*, New York, Penguin Press, 2017, p. 233-235.
8. B. Valeriano et R. Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*, Oxford, Oxford University Press, 2015, p. 151-156.
9. J. Healey (dir.), *A Fierce Domain: Conflict in Cyberspace 1986-2012*, Washington D.C., Cyber Conflict Studies Association, 2013, p. 212.
10. A. Greenberg, « Ukrainians Say *Petya* Ransomware Hides State-Sponsored Attacks », *Wired*, 28 juin 2017, disponible sur : <www.wired.com>.

Depuis l'été 2016, les cyber-menaces sont entrées dans une phase de prolifération. L'attaque massive qui a visé la société Dyn en octobre 2016 – qui gère une partie essentielle de l'infrastructure de nombreux services numériques – a été perçue comme une « brique » supplémentaire dans les tests successifs ciblant l'architecture physique de l'internet[11]. L'aspect novateur de cette attaque est qu'elle s'est appuyée sur l'utilisation d'objets connectés comme robots d'attaques. Des objets ou services de la vie quotidienne (radio-réveils, distributeurs de boissons, caméras de contrôle, etc.), peu sécurisés et faisant rarement l'objet de mises à jour de sécurité, peuvent ainsi servir à des cyberattaques de grande ampleur.

Types d'agresseurs et de victimes dans le cyberespace.

		Agresseur	
		État	**Acteur privé**
Victime	**État**	Un État attaque les infrastructures d'un autre État (ex : *Stuxnet*)	Des acteurs non étatiques (groupes militants ou « hackers patriotiques ») ciblent les réseaux d'un autre État (ex : Estonie, Géorgie)
	Acteur privé	Un État attaque les réseaux privés d'un autre État à des fins stratégiques ou commerciales (ex : Saudi Aramco, Sony Pictures)	Échanges d'hostilités entre acteurs non étatiques (ex : attaques de groupes affiliés aux Anonymous contre le groupe État islamique)

Une plus grande intensité

Au printemps 2017, en l'espace de deux mois, deux attaques informatiques d'une intensité inédite ont ravivé le spectre d'une cyber-conflictualité aux contours très mouvants. Le logiciel malveillant *WannaCry*, tout d'abord, a servi au plus grand piratage à rançon de l'histoire d'internet. Plus de 300 000 ordinateurs dans 150 pays ont été atteints par cette attaque qui visait principalement des entreprises, mais aussi des infrastructures sensibles (le système national de santé britannique, des réseaux internes de la police chinoise, les systèmes de transport en Allemagne, etc.). Exploitant une faille de sécurité des systèmes d'exploitation de Microsoft, le *malware* chiffre des données – dès lors rendues inaccessibles à leur propriétaire – et exige une rançon en *bitcoins* pour leur déchiffrement.

Quelques semaines plus tard, *NotPetya* (ou *exPetr*) apparaît en Ukraine. Doté de capacités de réplication très avancées, il se propage très rapidement dans tout le pays, touchant par ricochet de nombreuses entreprises en Europe et dans le monde. Il s'est révélé par la suite que *NotPetya* n'était

11. B. Schneier, « Someone Is Learning How to Take Down the Internet », *Blog Schneier on Security*, 13 septembre 2016.

en réalité pas un rançongiciel classique, comme *WannaCry*, mais un virus destiné à détruire les données des ordinateurs infectés, faisant des entreprises touchées les victimes collatérales d'une agression visant délibérément l'Ukraine. En février 2018, Washington et Londres, ainsi que les autres pays de l'alliance des *Five Eyes*, ont publiquement attribué l'origine de *NotPetya* à la Russie.

De manière générale, cette cyber-conflictualité cible de plus en plus les infrastructures critiques. Les cyberattaques se sont ainsi multipliées dans le secteur de l'énergie[12] : le piratage des systèmes informatiques de la compagnie pétrolière saoudienne Aramco, et la mise hors-service du réseau électrique ukrainien en décembre 2015, sont deux exemples connus d'actes de sabotage ayant nécessité des moyens financiers conséquents, dans deux régions soumises à de fortes crises – tensions russo-occidentales consécutives à l'occupation russe du Donbass ukrainien, et rivalité irano-saoudienne au Moyen-Orient. Les systèmes de télécommunication et les médias sont également visés (TV5 Monde en 2015), de même que les institutions financières, ou les organisations gérant des crypto-monnaies, pour l'appât du gain financier et l'accès à des données confidentielles[13].

Les cyberattaques se sont multipliées dans le secteur de l'énergie

« Guerre de l'information » et cyberespace

Les actes de cyber-malveillance décrits ci-dessus, surtout lorsqu'ils émanent d'États, ne peuvent plus être dissociés de leur versant informationnel. Ainsi la guerre de l'information est-elle partie intégrante de cette cyber-conflictualité, à laquelle se livrent grandes puissances, pays en marge de l'ordre international, voire acteurs privés et individus seuls ou coalisés. Si les menaces cyber et informationnelles sont bien souvent analysées séparément, le contexte international a évolué, et pose la question de l'adoption d'une approche plus intégrale, ne serait-ce que pour appréhender plus finement les stratégies d'États comme la Chine et surtout la Russie, pour qui les cyberopérations sont subordonnées aux opérations informationnelles (propagande, désinformation, etc.).

Une cyberattaque émanant d'un État, au-delà de son résultat destructeur, a pour objectif premier de produire de l'incertitude politique. La Conférence sur la sécurité de Munich de février 2017 a précisément abordé

12. G. Desarnaud, « Cyberattaques et systèmes énergétiques. Faire face au risque », *Études de l'Ifri*, Ifri, janvier 2017, disponible sur : <www.ifri.org>.
13. M. Boer et J. Vazquez, « Cyber Security and Financial Stability: How Cyber-Attacks Could Materially Impact the Global Financial System », Institute of International Finance, septembre 2017.

ce point, postulant que la cyber-conflictualité ne visait plus seulement les infrastructures dites critiques, mais aussi, désormais, le système politique occidental et les valeurs sur lequel ce système est fondé (démocratie représentative, séparation des pouvoirs, liberté d'expression, etc.). Certains responsables occidentaux ont ainsi suggéré que la démocratie et ses attributs devaient désormais être traités comme une infrastructure critique face aux attaques informatiques et aux manipulations d'internet[14].

Dans une vie politique internationale où, selon certains, « la géopolitique est de retour[15] », la rivalité pour façonner les perceptions et tenter d'imposer un récit dominant se développe. L'exemple du conflit syrien l'illustre : la guerre de l'information y tient une place prépondérante. Dans la foulée des attaques chimiques de Douma menées en avril 2018 par les forces loyalistes, la Russie a déployé une stratégie informationnelle tous azimuts qui désoriente les opinions publiques occidentales et divise leurs dirigeants (production de faux reportages, exagérations outrancières, etc.[16]).

Les acteurs : États, *proxies*, individus

Les technologies numériques ont aussi permis l'émergence de nouveaux acteurs sur la scène internationale. Les organisations « hacktivistes » comme Anonymous, WikiLeaks ou Telecomix, ont des objectifs qui peuvent être politiques, idéologiques ou culturels[17]. Par ailleurs, des acteurs non étatiques plus classiques, comme des groupes terroristes, utilisent le web social comme une véritable « plate-forme opérationnelle », notamment pour planifier des opérations et recruter des combattants[18].

Les débats sur la notion de cyberguerre ont surtout porté sur l'action des États et sur les hypothèses de cyber-conflits interétatiques. Cette focalisation s'est faite au détriment de l'appréhension du rôle que les hackers privés pouvaient jouer comme intermédiaires (*proxies*), et de la manière dont ceux-ci interagissaient avec les États, en leur permettant notamment de développer leurs capacités de lutte informatique offensive[19]. Il est désormais

14. Munich Security Conference, *Munich Security Report 2017*, « Post-Truth, Post-West, Post-Order? », disponible sur : <www.securityconference.de>.
15. W. Russell Mead, « The Return of Geopolitics: The Revenge of the Revisionist Powers », *Foreign Affairs*, vol. 93, n° 3, mai-juin 2014.
16. J. Nocetti, « Russian Information Warfare in the Middle East », *EuroMeSCo Policy Brief*, 2018 (à paraître).
17. T. Owen, *Disruptive Power: The Crisis of the State in the Digital Age*, Oxford, Oxford University Press, 2015.
18. M. Hecker, « Web social et djihadisme : du diagnostic aux remèdes », *Focus stratégique*, n° 57, Ifri, juin 2015, disponible sur : <www.ifri.org>.
19. L. Kello, *The Virtual Weapon and International Order*, New Haven, Yale University Press, 2017, p. 190-192.

reconnu que certains acteurs non étatiques disposent de capacités techniques et de moyens financiers leur permettant de causer des dégâts majeurs *via* des actes de piratage informatique. En réalité, certains acteurs non étatiques ne disposant que de faibles ressources peuvent faire peser un risque encore plus sérieux que des acteurs étatiques puissants. En effet, il manque souvent à ces acteurs privés les compétences pour développer des codes sophistiqués qui permettraient de maîtriser les effets de leurs *malwares*. Le rançongiciel *WannaCry* a ainsi montré les conséquences de la diffusion de ce type de programme malveillant par un acteur aux ressources relativement modestes[20].

Maîtriser les effets des *malwares*

Plusieurs types d'acteurs peuvent être rangés sous le terme de *proxies* : des individus isolés, comme des hacktivistes opérant seuls ou des hackers malveillants louant leurs services ; des réseaux d'hacktivistes agissant pour des motifs politiques ou des cybercriminels motivés par le profit (l'espace postsoviétique disposant de nombreux réseaux cybercriminels) ; des sociétés militaires ou de sécurité privée[21].

D'une grande complexité, les relations entre États et *proxies* peuvent revêtir plusieurs formes selon des logiques de coopération, de coordination ou d'intégration. D'un côté, puisque l'exploitation et la maintenance de la plupart des réseaux numériques sont confiés à des acteurs privés, l'intégration des *proxies* dans les dispositifs de cybersécurité pourrait permettre un meilleur partage de l'information. De l'autre, certains États se servent de hackers pour entretenir le doute sur l'origine d'une attaque.

Il demeure difficile d'évaluer le degré d'intrication de ces acteurs privés – hackers, sociétés privées – et des organes de sécurité et de renseignement des États. Ce défi est au demeurant indissociable de la difficulté à s'assurer du contrôle de leurs actions, et de la convergence de ces dernières avec les objectifs politiques poursuivis. Mais le recours à des acteurs non étatiques permet aussi de profiter des savoir-faire et des ressources provenant du secteur privé légal ou criminel[22].

Favoriser des liens plus souples *via* un soutien indirect, permet de réfuter plus aisément son implication, mais questionne l'autonomisation d'acteurs dont les logiques peuvent diverger. Les opérations sous fausse

20. Entretien avec un expert en cybersécurité, Aix-en-Provence, juin 2017.
21. T. Maurer, *Cyber Mercenaries: The State, Hackers, and Power*, Cambridge, Cambridge University Press, 2018.
22. *Ibid*.

bannière (*false flag*) constituent un facteur supplémentaire d'instabilité dans le cyberespace. L'attribution de l'intrusion dans les serveurs de la Convention nationale du Parti démocrate américain en 2016 au hacker prétendument roumain Guccifer 2.0, était en réalité une tentative de couvrir l'implication directe de l'État russe[23].

Les États s'adaptent aux cyber-menaces

Face à cette conflictualité protéiforme, les États ont progressivement élaboré des structures et des doctrines de cyberdéfense afin de développer des capacités offensives et défensives au profit de leurs forces armées ou parallèlement à celles-ci. Dès 2011, les États-Unis se sont dotés d'une *Stratégie internationale pour le cyberespace*. Plus récemment, la France s'est lancée dans un effort de rattrapage capacitaire qui concerne son outil de sécurité, de défense et de renseignement[24]. Paris formalise également sa doctrine cyberoffensive, en coordination avec les efforts de l'OTAN.

De manière générale, les capacités numériques se militarisent de façon exponentielle. Qu'il s'agisse des cyberopérations menées par la NSA et le Government Communications Headquarters (GCHQ) britannique contre le groupe État islamique, ou du soutien des hackers aux forces russes et séparatistes en Ukraine, on assiste à un mouvement de « souverainisation » du cyberespace.

Cyber-diplomatie : la nouvelle frontière

La prolifération des cyber-menaces, qui concerne tant les moyens employés que la transformation de l'espace numérique en théâtre d'affrontement international, requiert l'élaboration de nouvelles normes de régulation. Or, face à la pluralité d'origine des menaces, à la nature mouvante des attaques, et au problème de l'imputabilité de celles-ci, réguler les conflits dans le cyberespace s'est jusqu'à présent révélé délicat.

Risque d'escalade et attribution des cyberattaques

Dans le cyberespace, il est impossible d'identifier avec certitude l'origine d'une attaque, ce qui rend difficile la mise en œuvre du droit à la légitime défense. En conséquence, toute décision de représailles est risquée. L'incertitude quant aux intentions de l'adversaire se manifeste par un « dilemme de sécurité » propre au cyberespace. Pour garantir leur cybersécurité, les États sont

23. K. Poulsen et S. Ackerman, « "Lone DNC Hacker" Guccifer 2.0 Slipped Up and Revealed He Was a Russian Intelligence Officer », *The Daily Beast*, 22 mars 2018, disponible sur : <www.thedailybeast.com>.
24. Voir l'article de Louis Gautier dans le présent dossier, « Cyber : les enjeux pour la défense et la sécurité des Français », page 29 de ce numéro.

contraints à une confusion entre les modalités tactiques de l'attaque et de la défense, ce qui ne peut se traduire que par un accroissement des tensions et de l'insécurité générale pour l'ensemble des acteurs[25].

Face au risque élevé d'escalade dans le cyberespace, la retenue joue un rôle central dans la gestion des crises[26]. Après le piratage massif de la banque américaine JP Morgan, à l'été 2014, l'administration Obama s'est abstenue de toute déclaration publique, préférant l'option de fuites dans la presse pointant la responsabilité de hackers russes. Il en fut de même en avril 2015 après le piratage des messageries de la Maison-Blanche et du département d'État, supposément le fait de hackers soutenus par Moscou. Dans les deux cas, l'envoi d'un signal par médias interposés appelant la Russie à la retenue s'est substitué à une attribution en bonne et due forme.

Les crises cyber sont indissociables du contexte géopolitique du moment. Le *reset* des relations russo-américaines en 2009-2010 a conduit Moscou et Washington à rechercher la voie d'un apaisement en cas de conflit dans le cyberespace. De multiples rencontres bilatérales ont donné lieu à des échanges de vues sur les usages militaires du cyberespace, à des partages d'informations, et à la mise en place d'une *hotline* cyber. Le retour de Vladimir Poutine au Kremlin en 2012 a espacé le dialogue russo-américain, stoppé net avec le conflit ukrainien, puis relancé de manière indirecte[27].

L'attribution d'attaques informatiques est une manœuvre rare, qui procède moins d'une certitude technique que de la volonté politique de faire passer un message. En d'autres termes, la question consiste plus à savoir *quand* l'imputabilité est possible que *si* elle l'est[28]. Il reste que le problème de l'attribution demeure « la marque de la puissance dans le cyberespace[29] ». Seulement appuyée d'un faisceau d'indices, puisque les auteurs peuvent dissimuler leurs traces numériques derrière des hackers ou des ordinateurs installés dans un pays tiers, la capacité d'attribution d'une attaque varie grandement d'un État à l'autre. L'exercice repose sur l'analyse des traces techniques, mais aussi sur un travail de renseignement humain.

L'attribution d'une attaque varie grandement d'un État à l'autre

25. B. Buchanan, *The Cybersecurity Dilemma. Hacking, Trust, and Fear between Nations*, Londres, Hurst, 2016.
26. B. Valeriano et R. Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System, op. cit.*, p. 195-196.
27. Entretiens à Moscou, 2012-2015.
28. T. Maurer, *Cyber Mercenaries. The State, Hackers, and Power, op. cit*.
29. L. Kello, *The Virtual Weapon and International Order*, *op. cit.*, p. 129.

Par extension, les cyberopérations du XXIe siècle ne sauraient être appréhendées sans une solide connaissance des pratiques du renseignement du XXe siècle[30].

Une difficulté supplémentaire, pour les États, vient du nombre croissant d'entreprises de sécurité informatique, une partie de leurs équipes étant spécialisées dans le repérage et l'analyse des programmes espions. En révélant publiquement le contenu de leurs recherches sur ce nouveau type d'outils à disposition des États, ces entreprises médiatisent des opérations d'espionnage entre États qui seraient restées, pendant la guerre froide, dans le secret[31]. La société russe Kaspersky Lab, par exemple, s'est distinguée à plusieurs reprises par la divulgation d'actes malveillants dans le cyberespace, dont l'attaque *Red October* dévoilée en janvier 2013, qui visait plusieurs centaines de sites gouvernementaux et commerciaux en Occident, et dont les lignes de code laissaient supposer une origine russophone[32].

Les normes internationales du cyberespace

L'essor d'une menace cyber protéiforme contraint les États à investir de nouveaux champs diplomatiques pour apaiser les tensions et rechercher le consensus. C'est le cas des normes internationales du cyberespace – domaine d'action que les acteurs étatiques ont investi pour défendre leurs propres intérêts nationaux et esquisser une cyber-diplomatie.

Nul traité contraignant ne régit le cyberespace. Un fossé conceptuel sépare, d'un côté Américains (et Occidentaux) enclins à parler de cybersécurité, et de l'autre Russes et Chinois qui privilégient la « sécurité de l'information ». Cette ligne de fracture complique les débats internationaux sur la cybersécurité depuis le milieu des années 1990. Peut-être plus que tout autre État, la Russie craint autant la dimension technique du cyberespace que sa dimension cognitive, donc humaine. Pour ce pays comme pour d'autres, les négociations internationales sur la cybersécurité comportent un double niveau : l'un global – il s'agit de se positionner par rapport aux États-Unis perçus comme la menace principale dans le cyberespace – ; l'autre national, puisque la stabilité et la survie du régime dépendent en partie de sa capacité à maîtriser les usages que fait sa population

30. T. Rid, audition au Sénat américain, Commission permanente du renseignement, 30 mars 2017, disponible sur : <www.intelligence.senate.gov>.
31. M. Untersinger, « Attribuer l'origine d'une attaque informatique, un puzzle aux ramifications infinies », *Le Monde*, 5 octobre 2017, disponible sur : <www.lemonde.fr>.
32. B. Valeriano et R. Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System, op. cit.*, p. 180-184.

des technologies numériques[33]. Les approches russe, mais aussi chinoise et iranienne, montrent bien que les politiques étrangères de ces États en matière de cybersécurité sont largement motivées par des considérations de politique intérieure.

Depuis 1998, Moscou soumet chaque année aux Nations unies un projet de traité sur le désarmement dans le cyberespace, qui reflète la préoccupation des autorités russes à l'égard de la liberté de circulation de l'information. Les initiatives russes restent construites sur une opposition aux États-Unis, qui affirme la légitimité des seuls États à assurer leur souveraineté numérique. Les codes de conduite successifs proposés par Moscou aux Nations unies – et soutenus par Pékin – ont suscité la résistance de Washington. D'une part la Maison-Blanche s'est toujours opposée à toute initiative multilatérale pouvant brider sa prééminence en matière numérique. D'autre part, une approche traditionnelle de contrôle des armements appliquée au cyberespace – comme la Russie le souhaite – jouerait en défaveur des États-Unis, pays possédant les capacités cyberoffensives les plus significatives[34].

L'approche chinoise diffère peu des positions russes ; la nuance porte sur la priorité qu'accorde Moscou aux manœuvres informationnelles, quand Pékin privilégie les opérations cyberoffensives. Les deux pays coopèrent en matière de « sécurité de l'information » au sein des organes onusiens et de l'Organisation de coopération de Shanghai (OCS). Surtout, la Chine a fait de l'internet une composante-clé de son ambition de remodeler la gouvernance mondiale selon ses intérêts. La Conférence mondiale de Wuzhen, qui réunit annuellement depuis 2014 autour du président chinois de nombreux représentants officiels et des PDG de la *tech* mondiale, vise à légitimer la vision chinoise du cyberespace et les normes internationales que Pékin souhaite promouvoir.

Élargir la régulation au secteur privé ?

Depuis 2004 s'est réuni, à cinq reprises, un groupe d'experts gouvernementaux de l'ONU sur la cybersécurité (UNGGE). En 2013, le groupe s'est accordé sur la reconnaissance de l'applicabilité du droit international existant, et notamment de la Charte des Nations unies, à la conduite des États dans le cyberespace. En 2015, les experts du groupe se sont accordés sur un socle d'engagements volontaires de bonne conduite. Les États

33. J. Nocetti, « Contest and Conquest: Russia and Global Internet Governance », *International Affairs*, vol. 91, n° 1, janvier 2015, disponible sur : <www.chathamhouse.org>.
34. J. Markoff et A. Kramer, « U.S. and Russia Differ on Treaty for Cyberspace », *The New York Times*, 28 juin 2009, disponible sur : <www.nytimes.com>.

ont ainsi été encouragés à adopter un comportement coopératif vis-à-vis d'États victimes d'attaques informatiques, à lutter contre la prolifération d'outils informatiques malveillants, ou à s'engager à ne pas endommager les infrastructures critiques d'un autre État, hors contexte d'opérations militaires[35].

En revanche, ainsi que l'a montré l'échec du dernier cycle de négociations du groupe en juin 2017, la régulation interétatique ne peut apporter à elle seule une solution efficace et durable à ces défis de sécurité. L'irruption du numérique comme outil et espace de confrontation confère au secteur privé un rôle et une responsabilité inédits[36]. En février 2017, Microsoft a appelé à la signature d'une « Convention de Genève du numérique », avec l'introduction de normes qui obligeraient les États à révéler aux éditeurs de logiciels les failles de sécurité en leur possession. Ambitionnant de développer des capacités d'attribution d'attaques informatiques, qui seraient mises en commun dans une future organisation internationale, Microsoft pointe aussi la responsabilité des États dans la course aux cyber-armements. Siemens prolonge les efforts de Microsoft avec sa « Charte de confiance » annoncée à la Conférence de sécurité de Munich en février 2018. En janvier 2018, le Forum économique mondial a annoncé le lancement d'un Centre mondial de la cybersécurité, chargé d'améliorer la coopération entre gouvernements et acteurs privés face aux cyber-menaces.

Ces enjeux de gouvernance doivent intégrer la problématique du renforcement des capacités cyber, qui concerne tant les États que les organisations internationales, les entreprises et les grandes structures de recherche. Pour certains acteurs, ce *capacity building* est même devenu un instrument de politique étrangère, puisqu'il permet de défendre un modèle de gouvernance précis d'internet, de promouvoir certains standards techniques, ou de faciliter l'ouverture de marchés pour leurs acteurs nationaux[37].

***

Le numérique possède un pouvoir égalisateur inédit en politique internationale. Accessible à tous les acteurs – bienveillants ou non –, il place les groupes criminels sur un pied de quasi-égalité avec des entreprises

35. Assemblée générale des Nations unies, A/70/174, 22 juillet 2015.
36. Discours de J-Y. Le Drian, 72e Assemblée générale des Nations unies, « Cybersécurité – Le rôle et la responsabilité des acteurs privés dans le renforcement de la stabilité et de la sécurité internationale du cyberespace », 18 septembre 2017.
37. P. Pawlak, « Capacity Building in Cyberspace as an Instrument of Foreign Policy », *Global Policy*, vol. 7, n° 1, février 2016, disponible sur : <https://onlinelibrary.wiley.com>.

mondiales ou des grandes puissances. À court et moyen termes, l'essor et la sophistication croissants de l'intelligence artificielle risque pourtant de produire de nouveaux bouleversements en matière de cyber-conflictualité, tant par une fuite en avant des cyber-puissances que par la multiplication de *proxies* aux loyautés variables.

Mots clés
Internet
Cybersécurité
Cyberdéfense
Hackers

politique étrangère

PE

Découvrez nos nouvelles offres d'abonnement sur le site www.revues.armand-colin.com

- ✔ Bénéficiez de services exclusifs sur le portail de notre diffuseur
- ✔ Accédez gratuitement à l'ensemble des articles parus depuis 2007
- ✔ Choisissez la formule papier+numérique ou e-only

TARIFS 2018

▶ *S'abonner à la revue*		France TTC	Étranger HT*
Particuliers	papier + numérique	☐ 80,00 €	☐ 100,00 €
	e-only	☐ 65,00 €	☐ 80,00 €
Institutions	papier + numérique	☐ 175,00 €	☐ 195,00 €
	e-only	☐ 130,00 €	☐ 150,00 €
Étudiants**	papier + numérique	☐ 70,00 €	☐ 75,00 €
	e-only	☐ 50,00 €	☐ 55,00 €

* Pour bénéficier du tarif **Étranger HT** et être exonéré de la TVA à 2,1 %, merci de nous fournir un numéro intra-communautaire
** Tarif exclusivement réservé aux étudiants sur présentation d'un justificatif

▶ *Acheter un numéro de la revue*	Tarif	**Numéro** (format X-20XX)	Quantité
Numéro récent **(à partir de 2014)**	☐ 23,00 €	.....	.....
Numéro antérieur à 2014	☐ 20,00 €	.....	.....

TOTAL DE MA COMMANDE ..... €

Bon de commande à retourner à :

DUNOD ÉDITEUR - Service Clients - 11, rue Paul Bert - CS 30024 - 92247 Malakoff cedex, France
Tél. 0 820 800 500 - Fax. 01 41 23 67 35 - Étranger +33 (0)1 41 23 66 00 - **revues@armand-colin.com**

Adresse de livraison

Raison sociale : .....
Nom : .....Prénom : .....
Adresse : .....
Code postal : |_|_|_|_|_| Ville : .....Pays : .....
Courriel : .....@.....

Règlement à l'ordre de Dunod Éditeur

☐ **Par chèque** à la commande
☐ **À réception de facture** (institutions uniquement)
☐ **Par mandat administratif** (institutions uniquement)

Date : _ _ /_ _ /_ _ _ _

Signature (obligatoire)

Je souhaite effectuer mes démarches en ligne ou par courriel/téléphone

- ✔ Je me connecte au site **www.revues.armand-colin.com**, onglet « ÉCO & SC. POLITIQUE »
- ✔ Je contacte le service clients à l'adresse **revues@armand-colin.com** ou au **0 820 065 095**

ifri ARMAND COLIN