ANNUAIRE FRANÇAIS DE RELATIONS INTERNATIONALES

2014

Volume XV

PUBLICATION COURONNÉE PAR
L'ACADÉMIE DES SCIENCES MORALES ET POLITIQUES

(Prix de la Fondation Edouard Bonnefous, 2008)

Université Panthéon-Assas
Centre Thucydide

L'IMPACT DU CYBERESPACE DANS LES RELATIONS INTERNATIONALES

Révolution géopolitique ou continuité stratégique par d'autres moyens ?

PAR

Vincent JOUBERT (*)

Le cyberespace s'est imposé ces dernières années comme une question prioritaire de sécurité dans les agendas diplomatiques internationaux. L'appropriation de ce domaine par les gouvernements répond à un besoin né des enjeux sociétaux, économiques, politiques, diplomatiques et militaires émergeant de la dépendance de la société et de ses acteurs aux technologies de l'information et de communication (TIC) qui constituent le cyberespace. En effet, la quasi-totalité de l'activité des Etats repose sur l'utilisation des technologies du cyberespace, poussant certains analystes à les considérer comme de véritables « colonnes vertébrales des sociétés modernes ». Le vocabulaire officiel employé dans les stratégies nationales de cybersécurité (infrastructures critiques, opérateurs d'importance vitale, etc.) ne laisse d'ailleurs aucune place au doute quant à l'importance de ces structures pour les Etats. Si on peut considérer que l'élection de Barack Obama à la présidence des Etats-Unis en 2008 a accéléré la mise en avant de ces questions dans l'agenda politique international, il convient d'analyser dans quelle mesure, cinq ans après l'effervescence politico-médiatique qui a accompagné le traitement du sujet à ses débuts, le cyberespace a influencé la conduite des relations internationales. Au-delà des prédictions alarmistes qui ont largement monopolisé les attentions des débats, une lecture plus objective des événements dans et par le cyberespace ayant eu un impact décisif sur les relations internationales ces cinq dernières années nous permettra de dresser un premier bilan quant à l'impact de ce domaine sur le système international.

(*) Chargé de recherche à la Fondation pour la recherche stratégique (FRS, France) et doctorant à l'Institut français de géopolitique (IFG) de l'Université Paris VIII (France).

La mise en avant des enjeux du cyberespace dans l'agenda politique international

L'exposition politique et médiatique des enjeux du cyberespace a été déclenchée par l'élection de Barack Obama à la présidence des Etats-Unis en 2008. Dès la campagne présidentielle, ce dernier avait promis de renforcer la sécurité des systèmes d'informations et des réseaux (SI) américains critiques pour le fonctionnement et la sécurité de la nation. Une fois élu, il a rapidement réorganisé les institutions gouvernementales, défini une stratégie nationale et internationale et alloué des parts budgétaires en hausse permanente pour se doter des capacités permettant d'atteindre les objectifs fixés par cette politique, quand bien même le pays traversait une période de coupure budgétaire généralisée (1). Le résultat, au terme du premier mandat de l'administration Obama, est éloquent : une réorganisation bureaucratique et institutionnelle profonde permettant une répartition claire des tâches et des responsabilités, la création en 2010 de l'US Cyber Command comme structure dédiée à la défense des SI américains contre les attaques extérieures et une position stratégique résolument orientée vers l'affirmation de la puissance américaine dans le cyberespace, considéré comme espace stratégique prioritaire par la Maison-Blanche et défendu comme tel.

Cette mise en avant des besoins de cybersécurité repose sur la perception que la menace créée par des attaques contre les infrastructures critiques des Etats-Unis pourrait potentiellement avoir des conséquences plus dramatiques qu'une attaque à l'arme de destruction massive ou qu'une attaque terroriste semblable aux événements du 11 septembre 2001 (2). On constate ainsi aux Etats-Unis, dès la fin des années 1990, l'apparition et la multiplication de scénarios catastrophistes résultant de cyber-attaques lancées contre les infrastructures critiques des Etats-Unis. Or la réalité est que, jusqu'à présent, aucun de ces scénarios, aucune des hypothèses alarmistes ne s'est réalisé(e). Les attaques informatiques sont une réalité, mais la menace principale qui en découle actuellement concerne l'espionnage industriel par lequel des multinationales se font dérober des quantités importantes de données relatives à la propriété intellectuelle, induisant des coûts financiers conséquents, par la perte de réputation commerciale, la perte de marchés et, plus simplement, les coûts de réparations et de remplacement du parc informatique corrompu et/ou endommagé.

(1) Selon les chiffres de l'Office of Management and Budget, le total des investissements américains dans les technologies de l'information est passé de 6,7 milliards de dollars pour la *Fiscal Year* (FY) 2008 à 8,9 milliards pour la FY 2014. A noter qu'à partir de la FY 2011, les documents font la différence entre les investissements de défense et ceux relatifs au secteur civil. A titre d'exemple, pour illustrer l'importance accordée par l'administration au sujet, le budget « cybersécurité-cyberdéfense » prévu pour l'année fiscale 2014 (FY 2014) était initialement de 3,9 milliards de dollars, mais la Maison-Blanche a décidé de le relever à 4,7 milliards.

(2) En 1999, le député C. Weldon (R-Pennsylvania) déclarait lors d'une conférence sur l'« InfoWar » à Washington : « *in my opinion, neither missile proliferation nor weapons of mass destruction are as serious as the threat of cyberterrorism* ». En 2003, dans une lettre ouverte au président G. W. Bush rédigée par R. Clarke et 50 experts en informatique, il est dit : « *our nation is at grave risk of a cyberattack that could devastate the psyche and the economy more broadly than did the 9/11 attacks* ».

La dramatisation rhétorique et l'alarmisme scénarisé développés par une partie de la communauté de la défense est ainsi dénoncée par leurs opposants, les « sceptiques ». Ces derniers n'ignorent ni n'écartent la menace malgré tout : ils reconnaissent que la complexité des architectures de réseaux et l'imprévisibilité de l'évolution des technologies de l'information empêchent de dénigrer toutes les hypothèses, mais ils dénoncent ouvertement l'exagération et la manipulation actuelle de la représentation de la « cyber-menace ». Cette surestimation de la menace pour la sécurité nationale profite au secteur industriel, qui trouve là un marché extrêmement lucratif, provoqué par l'apparition soudaine d'un besoin urgent de produits et services de cybersécurité. On perçoit pourquoi, dans ces conditions, le secteur industriel a tout intérêt à ce que cette demande persiste et, pour qu'elle persiste, la perception d'une menace imminente et imprévisible doit demeurer.

La menace cyber s'inscrit dans cette catégorie de « nouvelles menaces » apparues au sortir de la Guerre froide, où les grilles de lectures de l'environnement stratégique se sont soudainement retrouvées inapplicables. Ces nouvelles menaces sont incertaines, car immatérielles, inquantifiables, difficilement localisables, difficilement attribuables, et leurs motivations échappent parfois aux acteurs ciblés. Ces menaces, souvent non étatiques, non militaires ou asymétriques, ont posé beaucoup de problèmes aux Etats : il a fallu repenser la manière d'appréhender ces nouvelles menaces et, dans le cas du cyberespace, c'est le modèle de gestion du risque (*risk management*) qui a prévalu. Ce modèle propose ainsi de réduire au maximum les risques, entendus comme l'impact d'une menace sur un système d'information, en diminuant les vulnérabilités inhérentes du système d'information pour limiter l'impact de leur exploitation. Cette méthode, couramment utilisée pour la sécurisation des systèmes d'information, pose cependant des problèmes nouveaux lorsqu'elle s'applique à une stratégie de cybersécurité dans le système international. En effet, si la sécurisation des SI et des infrastructures critiques d'un Etat est indispensable, elle n'est, à l'heure actuelle, pas autosuffisante. Autrement dit, aucun système d'information n'est impénétrable, cela, en dépit de sa protection par des dispositifs de sécurité. Aussi, dans ces conditions, devient-il difficile de dissuader un adversaire d'attaquer les SI. Un Etat doit donc trouver d'autres moyens de dissuader un adversaire d'attaquer ses infrastructures. C'est précisément ce qu'ont fait les Etats-Unis sous l'administration Obama : d'une part, ils ont considérablement investi dans le développement de capacités technologiques et techniques, qui, de par la dualité de leur usage, peuvent avoir des applications offensives et défensives : d'autre part, afin de palier la non-applicabilité d'une dissuasion dans le cyberespace calquée sur le modèle de la dissuasion nucléaire (3), ils ont adopté une stratégie de dissuasion globale, manifestée par une escalade dans la rhétorique stratégique, dont le seuil est explicité dans l'*International Strategy for Cyberspace* (2011) − si les Etats-Unis sont attaqués par

(3) Sur ce sujet, l'ouvrage de référence est celui de M. Libicki, *Cyberdeterrence and Cyberwar*, RAND Corp., 2009.

une cyberattaque de grande ampleur, ils répondront comme contre tout autre type d'attaque et se réservent le droit d'utiliser tous les moyens pour protéger leurs intérêts (4).

L'accroissement de l'implication du militaire dans le cyberespace a été perçu aux Etats-Unis comme une véritable « militarisation » du cyberespace et a été dénoncé par de nombreux spécialistes de la sécurité informatique. Pour eux en effet, les méthodes de défense et de protection militaires n'auraient que très peu d'efficacité sur la sécurité des systèmes d'information. Cependant, la perception de cette militarisation du cyberespace par les Etats-Unis a déclenché une course à l'armement dans le cyberespace au sein du système international. Si nombre de grandes puissances avaient depuis plusieurs années établi des structures gouvernementales dédiées à la cybersécurité, le soudain accroissement d'intérêt pour ces sujets de la part des premières puissances militaires mondiales a entraîné une explosion de la demande en capacités de cybersécurité et de cyberdéfense. La compétition militaire dans le cyberespace créée par le développement de capacités défensives et offensives par de nombreux Etats affecte inévitablement la représentation de la menace et pourrait, à terme, engendrer un véritable « dilemme de la cyber-sécurité ». Le risque de tomber dans le conflit interétatique est d'autant plus élevé que les actions dans le cyberespace sont « invisibles », ce qui laisse une place considérable à la perception et à l'interprétation.

Ainsi, à la suite de l'impulsion donnée par les Etats-Unis à ce sujet, les stratégies nationales de cybersécurité se sont multipliées, la question a été portée dans les agendas des rencontres internationales, dans le cadre d'institutions existantes (OTAN, UE, ASEAN, etc.) comme dans les forums de discussions plus spécifiques (G8, G2 sino-américain). Aujourd'hui, la cybersécurité est presque systématiquement abordée dans les discussions diplomatiques et, parce que les enjeux sociétaux, économiques, politiques et militaires associés ont pris une ampleur colossale, elle cristallise les divergences à l'origine de tensions internationales existantes et est devenue véritablement incontournable.

La conflictualité dans le cyberespace : différentes formes, différents objectifs

Si les scénarios catastrophiques ne tarissent pas d'inventivité pour décrire les effets de cyber-attaques d'ampleur majeure sur un pays, force est de constater que les affrontements dans le cyberespace sont polymorphes et visent divers objectifs. La conflictualité dans le cyberespace, qu'elle soit envisagée ou réelle, se place ainsi sur les plans militaires et du renseignement, économiques ou encore politico-diplomatiques.

(4) « When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. [...] We reserve the right to use all necessary means – diplomatic, informational, military, and economic – as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests ». Il faut entendre ici par « tous les moyens » le recours à l'arsenal traditionnel (frappes aériennes, missiles longues portées, etc.).

L'accroissement d'acquisition de capacités cyber par les Etats renvoie d'abord au problème, évoqué plus haut, de la course à l'armement et de ses conséquences dangereuses, théorisées dans le dilemme de la sécurité (5). Cependant, de l'avis des experts militaires et des experts en sécurité informatique, un conflit dans le cyberespace a très peu de chances d'avoir lieu à un niveau stratégique ; il faut entendre par là qu'il y a peu de chances que des cyber-attaques puissent à elles seules garantir la victoire militaire et politique. On retombe ici dans ce que les scénarios catastrophes décrivent et un consensus au sein de la communauté scientifique et militaire s'accorde à réfuter ces hypothèses pour le moment. Cependant, cela ne veut pas dire que l'utilisation de cyber-attaques ne peut pas produire des effets permettant d'acquérir un avantage stratégique militaire sur son adversaire. En utilisant par exemple des attaques informatiques ciblées sur les capacités C2 (commandement et contrôle) des adversaires, on peut envisager de l'empêcher de mener à bien l'opération militaire initialement prévue en coupant ses capacités de communication, en rompant la chaîne de commandement ou en lui opposant un déni d'accès au théâtre des opérations. C'est précisément ce type de scénario, beaucoup plus réaliste, que redoutent les états-majors des armées des différentes puissances militaires (6), bien qu'à ce jour aucun cas ne soit à rapporter.

En parallèle à ces actions qui entrent dans le cadre d'une opération militaire classique, certains Etats ont recours à des opérations clandestines (*covert actions*) qui ont pour objectif d'atteindre une cible sans engager publiquement ni officiellement la responsabilité de l'Etat. L'opération « Olympic Games » (7), matérialisée par l'implantation du virus Stuxnet dans les systèmes utilisés pour contrôler des centrifugeuses d'enrichissement d'uranium dans la centrale iranienne de Natanz, est l'exemple le plus connu. Néanmoins, le succès de ces opérations réside normalement dans leur discrétion et donc, à moins d'une fuite, il est impossible d'en avoir connaissance. L'autre volet des opérations clandestines concerne le renseignement. Les TIC et la complexité du cyberespace ont offert de nouvelles possibilités d'écoute et de surveillance et permettent aux Etats ayant massivement investi dans des capacités cyber d'étendre leur champ d'action au bénéfice de leurs services de renseignement. Si la pratique est tacitement reconnue, son ampleur et ses techniques ne l'étaient pas jusqu'aux révélations d'Edward Snowden, ancien consultant de la National Security Agency (NSA), qui a révélé l'existence des programmes américains de surveil-

(5) Le dilemme de sécurité dans les Relations internationales a été théorisé par J. Hrez en 1951, puis repris par R. Jervis. Cette théorie pose qu'un Etat interprétera l'acquisition de capacités militaires comme nécessaire à sa protection et, dans le même temps, percevra l'acquisition de capacités militaires par d'autres Etats comme une menace. Dès lors, chaque Etat est tenté d'acquérir d'autant plus de capacités et aggravera ainsi le processus, ce qui, à terme, peut conduire à un conflit à l'origine non désiré.

(6) *Cf.* notamment M. Libicki, « Chinese use of cyberwar as an anti-access strategy: Two scenarios », RAND Corp., 2011.

(7) L'opération « Olympic Games » est décrite par D. Sanger, journaliste au *New York Times*, dans un article du 1er juin 2012, « Obama order sped up wave of cyberattacks against Iran ».

lance à très grande échelle PRISM (8). Grâce à ses révélations, il a été possible d'évaluer quantitativement et qualitativement la pratique du renseignement dans et par le cyberspace ; l'ampleur autant que la sophistication des processus employés ont étonné au sein de la communauté internationale. Bien que l'espionnage ne constitue pas un acte de guerre en soi, les révélations faites par E. Snowden ont immanquablement ébranlé la confiance existante entre partenaires internationaux et Etats alliés. Loin de favoriser la coopération interétatique, ces pratiques risquent de renforcer la prévalence de la souveraineté dans la protection et la défense des intérêts nationaux dans le cyberespace.

L'espionnage dans et par le cyberespace n'est pas uniquement interétatique ; l'espionnage industriel est en effet une pratique particulièrement développée, qui affecte tous les secteurs industriels et, par voie de conséquence, l'économie des nations. Si le secteur privé a su, dès les premiers instants de l'explosion des TIC, profiter des opportunités économiques et commerciales qu'elles créaient, il a été plus difficile d'intégrer que l'utilisation de telles technologies ne pouvait se faire sereinement sans y associer les dispositifs de sécurité idoines. En conséquence, les pertes financières associées au vol de propriété intellectuelle ou de bases de données commerciales ont été considérables pour certaines multinationales (9). Malgré cette réalité, le secteur privé est encore frileux à l'idée d'investir massivement dans des capacités de cybersécurité, mais également de mettre en place une véritable politique de cybersécurité au sein des entreprises. Cette réticence s'explique par le fait que le secteur privé a, avant tout, une logique de profit et de rentabilité. Or, les besoins associés à la cybersécurité en entreprise leur semblent être des dépenses à perte, puisqu'ils ne rapporteront *a priori* rien. Cette logique se révèle évidemment fausse lorsque ces investissements empêchent ou limitent les pertes financières beaucoup plus élevées associées à la compromission de son parc informatique et des données de l'entreprise (10). Si la révélation publique de cyberespionnage peut affecter la réputation commerciale des entreprises et que ces dernières préféraient jusqu'alors passer la découverte d'attaques sous silence, on assiste néanmoins depuis quelques années à un changement de position, où les multinationales n'hésitent plus à désigner ouvertement ceux qu'ils pensent être les auteurs de l'espionnage industriel. La République populaire de Chine a ainsi été de nombreuses fois accusée de pirater les réseaux et centres de données de multinationales américaines. L'implication directe ou indirecte d'un Etat dans de telles manœuvres n'est pas sans renforcer les tensions diplomatiques qui

(8) Les révélations d'Edward Snowden ont été rapportées par le quotidien britannique *The Guardian*, puis reprises dans *Le Monde*. Les différentes facettes des programmes de surveillance américains sont rapportées au fur et à mesure depuis juillet 2013.

(9) On pourra lire l'étude de Kaspersky & CSIS, *The Economic Impact of Cybercrime and Cyberespionnage*, juil. 2013.

(10) L'exemple de l'entreprise HBGary est à ce titre éloquent. Multinationale spécialisée dans la sécurité informatique, elle avait annoncée avoir démasqué des membres du collectif de hackers Anonymous et menaçait de les dénoncer aux autorités. En réponse, Anonymous a pénétré les centres de données de HBGary et divulgué les informations de ses clients, parmi lesquels de très importantes multinationales. En conséquence, HBGary a perdu toute crédibilité, ce qui a entraîné la fuite de ses clients et conduit à terme à la faillite de deux branches de l'entreprise, HBGary Fed. & HBGary Inc.

existent, notamment entre les Etats-Unis et la Chine. Néanmoins, le cyber-espionnage industriel est une forme d'intelligence économique illégale, dont la pratique est aujourd'hui courante et répandue, comme en témoignent les découvertes successives d'attaques de types « Advanced Persistent Threats » – et bien d'autres – ciblant les SI du secteur privé. Enfin, si les auteurs de ces attaques sont divers et multiples et peuvent impliquer des Etats, la finalité est toutefois commune : se procurer un avantage économique et commercial sur ses concurrents.

La conflictualité dans le cyberespace ne porte pas uniquement sur le contenant – la compromission des réseaux et des données – ; elle affecte aussi le contenu, cela, dans plusieurs dimensions. En premier lieu, il y a une opposition clairement marquée autour de la question du contrôle de ce contenu : d'un côté, certains pays prônent la liberté d'expression et donc un contrôle *a minima* – *i.e.* dans les limites de la législation nationale – ; de l'autre, nombres d'Etats souhaitent pouvoir contrôler ce contenu de manière plus approfondie. Ce clivage s'est révélé lors de la conférence de l'International Telecommunications Union (ITU) de l'ONU en 2012, où la proposition de texte émanant de la Chine et de la Russie (entre autres) a été rejetée par 55 Etats (dont les Etats-Unis, la France, et le Royaume-Uni). Ce refus a été justifié d'une part par l'ambiguïté du texte qui, en l'état, aurait permis d'exercer un contrôle sur le contenu des données et donc s'est trouvé dénoncé par nombre de pays européens comme étant de la censure allant à l'encontre des valeurs qu'ils défendent. D'autre part, la question de la gouvernance d'Internet, dont l'ICANN (11) a aujourd'hui la majeure responsabilité, soulève beaucoup d'indignation parmi les pays souhaitant que la gestion des noms de domaines et la gouvernance plus générale d'Internet ne repose pas uniquement sur cette société américaine : le texte de la conférence de l'ITU intégrant un paragraphe prévoyant que tous les gouvernements aient « *un rôle et une responsabilité identique en ce qui concerne la gouvernance mondiale de l'Internet* » (12), on comprend aisément que les Etats-Unis n'aient pas souhaité abandonner leur monopole actuel et que la situation reste pour l'instant dans une impasse diplomatique. L'opposition entre les Etats qui souhaitent bouleverser le *statu quo* et ceux qui au contraire veulent à tout prix le maintenir est d'une certaine manière un aboutissement logique de l'évolution des TIC : l'architecture d'Internet et les TIC ont été développés dans des pays occidentaux, avec une philosophie spécifique, qui ne correspond pas forcément à celle de tous les Etats du système international. La récupération politique du cyberespace et, donc, d'Internet vient se heurter à cette philosophie particulière et, conjuguée avec les enjeux sociétaux, économiques, politiques et militaires du cyberespace, devient un sujet politique international majeur, pour lequel les Etats vont chercher à préserver leurs intérêts.

(11) Internet Corporation for Assigned Names and Numbers, société américaine gérant l'attribution des noms de domaine et des « numerous » associés sur Internet.

(12) World Conference on International Communications, Final Acts, ITU, Dubaï, 2012.

L'impossibilité actuelle de trouver un consensus international traduit bien cette conflictualité latente qui existe entre les Etats dans le cyberespace. Les enjeux sont si importants que la préservation des intérêts nationaux prévaut actuellement sur la collaboration internationale, mais les frictions qui résultent de cette situation ne servent pas forcément les intérêts des Etats. Toute la difficulté consiste alors à trouver la bonne stratégie pour effectivement préserver les intérêts et la sécurité nationaux sans franchir un seuil faisant basculer cette conflictualité limitée à un conflit interétatique ouvert.

Le cyberespace, outil de redistribution des puissances ?

La notion de puissance en Relations internationales est primordiale. Si elle englobe nombre d'éléments constitutifs et n'est pas universelle, nous retiendrons la définition qu'en donne Joseph Nye : « *la puissance est la capacité d'influencer l'autre pour obtenir des résultats attendus par l'utilisation du* hard power *(la coercition et les amendes) et du* soft power *(influencer l'agenda politique, exercer une attraction, et une persuasion). Diverses ressources permettent l'application du* hard power *et du* soft power*, variant selon les contextes, et le cyberespace constitue un nouveau contexte* » (13). Comme l'énonce J. Nye, le cyberespace est un nouveau vecteur par et dans lequel les Etats peuvent exprimer et projeter leur puissance dans ses aspects principaux, politiques, informationnels, militaires, économiques, créant ainsi la notion de *cyber power*, définie comme « *la capacité à utiliser le cyberespace pour se créer des avantages stratégiques et influencer les autres environnements opérationnels, sur l'ensemble du spectre des instruments de puissance* » (14). En analysant attentivement les éléments constitutifs du cyberespace ainsi que les acteurs pouvant exercer leur puissance dans ce domaine, on constate que la complexité inhérente soulève des problématiques nouvelles susceptibles d'avoir un impact sur le système international.

En effet, le cyberespace peut se représenter comme une structure complexe composée de trois couches distinctes. La première est matérielle : on y retrouve les infrastructures indispensables au fonctionnement du domaine. Ces éléments physiques (câbles, routeurs, centres de données, ordinateurs, etc.), sont localisés sur un territoire géographique auquel s'applique une législation relevant de la souveraineté d'un Etat. De la même manière, les éléments mobiles de cette couche physique (les satellites de communication par exemple) relèvent d'une juridiction rattachée à un Etat. La deuxième couche, dite applicative, regroupe les logiciels, les applications, les protocoles, les données, les codes. Les éléments de cette couche sont en majorité immatériels et ont vocation à être diffusés dans et par le cyberespace ; ils constituent l'interface permettant d'utiliser les infrastructures de la couche matérielle (le contenant) pour diffuser

(13) Joseph S. Nye, « Power and national security in cyberspace », *in America's Cyber Future, Security and Prosperity in the Information Age*, vol. II, Center for a New American Security, juin 2011.

(14) F. Kramer / S. Starr / L. Wentz, *Cyberpower and National Security*, National Defense University Press, 2009, p. xvi.

le contenu, les idées, qui sont le cœur de la troisième et dernière couche, la couche cognitive. Dans cette couche, la notion de territorialité est inexistante, mais l'impact et la portée des éléments véhiculés représentent un enjeu majeur du *cyber power* et donc de la puissance étatique.

La couche cognitive est au cœur de la notion d'« influence » dans le cyberespace, qui correspond à l'application du *soft power* dans ce domaine : il s'agit, par des actions ciblées et étudiées, d'influencer et de convaincre les autres Etats, afin d'atteindre des objectifs spécifiques sans avoir besoin de recourir à la force. Maîtriser son influence dans le cyberespace revient pour un Etat à assurer un contrôle de sa puissance dans ce domaine. Cependant, contrôler les éléments de la couche cognitive afin de maîtriser son influence dans le cyberespace et empêcher ses adversaires d'accroître le leur est actuellement impossible : un Etat ne peut prétendre contrôler tous les contenus échangés dans le cyberespace et maîtriser la couche cognitive. Toutefois, puisqu'il est impossible d'empêcher l'émergence d'idées et d'opinions allant à l'encontre des intérêts d'un Etat, le plus simple est encore d'empêcher la diffusion de ces idées en exerçant son pouvoir de législateur souverain contre les fournisseurs d'accès aux réseaux. Autrement dit, étant donné que les Etats n'ont pas de contrôle direct sur la création du contenu, ils agissent sur les gestionnaires du contenant, en leur imposant de censurer le contenu jugé subversif. Evidemment, ce procédé n'est pas d'une fiabilité technique absolue : la complexité de l'architecture du cyberespace fait qu'il est possible de trouver des techniques ou des technologies permettant de contourner les censures et ainsi continuer la diffusion des idées dans le cyberespace. Dès lors, même les principales puissances mondiales, disposant de capacités cyber très avancées, ne peuvent atteindre le contrôle total ni la domination du cyberespace, comme cela avait pu être le cas dans les autres domaines physiques.

Les Etats ont dû accepter que la maîtrise de leur puissance dans le cyberespace ne réponde pas aux grilles de lecture traditionnelles et ont dû adapter leurs stratégies nationales de cybersécurité et de cyberdéfense pour en limiter la diffusion, par des mesures alliant protection des infrastructures physiques et un contrôle plus ou moins strict du contenu. Malgré ces mesures, le cyberespace offre des pouvoirs d'action et d'expression à des acteurs qui n'ont pas ces capacités dans les autres domaines physiques.

Une particularité du cyberespace est en effet d'offrir un seuil d'accès très bas ; on appelle « seuil d'accès » les conditions pré-requises pour devenir un acteur à part entière de ce domaine. Pour devenir un acteur du cyberespace, il suffit d'un ordinateur et d'une connexion Internet. Sans même avoir besoin d'être un expert en sécurité informatique, la diffusion d'idées reprises par une foule peut avoir un impact parfois bien plus puissant que certaines actions coercitives. De la même manière, un individu rompu aux techniques de sécurité informatique peut considérablement affecter le *cyber power* d'un Etat en exploitant les failles de sécurité de ses réseaux : les exemples de propagation de virus ou de ver informatique à l'échelle internationale affectant des systèmes d'information étatiques de première importance sont malheureusement nombreux. Le

virus Conficker a notamment infecté plusieurs ministères de la Défense de puissances militaires majeures (Etats-Unis, Royaume-Uni, France), obligeant ainsi, pour l'éradiquer, à couper certaines portions de leurs réseaux internes avec les conséquences que de telles opérations de maintenance impliquent. Ces attaques informatiques ne sont pas des opérations militaires ; elles sont le résultat de *hackers* talentueux qui exploitent les vulnérabilités des réseaux. Les *hackers* n'ont pas tous des intentions hostiles ; au contraire, la plus grande majorité d'entre eux apporte une aide considérable en rapportant la découverte de failles de sécurité aux propriétaires de réseaux. Pourtant, il suffit d'une simple faille pour qu'un individu s'introduise dans des réseaux ou des infrastructures critiques d'un Etat, lui conférant ainsi un pouvoir d'action considérable. De manière générale, il est effectivement beaucoup plus compliqué d'établir une bonne protection des réseaux et systèmes d'informations que de trouver la faille de sécurité permettant d'exploiter cette vulnérabilité et attaquer le système. Non pas que trouver une faille de sécurité soit à la portée de tout un chacun, bien au contraire, mais les ressources financières, humaines et temporelles nécessaires à la mise en place de dispositifs et de procédures de cybersécurité sont encore aujourd'hui largement supérieures à celles nécessaires pour trouver les failles de sécurité. Dans ces conditions, la capacité de coercition dans le cyberespace n'est plus l'apanage de l'Etat et un individu ou un groupe d'individus possède un pouvoir d'action qu'il ne possède pas dans les autres domaines.

Ce bouleversement de distribution de la puissance semble cependant s'estomper et tendre vers un retour de la prévalence de l'Etat comme acteur principal de la coercition dans le cyberespace. On a pu effectivement constater depuis quelques années qu'avec la prise de conscience des décideurs politiques de l'importance du cyberespace, qui a engendré une augmentation substantielle du niveau de sécurité sur les infrastructures critiques nationales et le déploiement de capacités de cyberdéfense, les attaques susceptibles de produire des effets affectant la puissance d'un Etat sont le fruit d'actions étatiques. Le virus Stuxnet, évoqué précédemment, en est là encore un exemple : il entre dans le cadre d'une opération clandestine ayant nécessité des moyens de renseignement et d'expertise humaine, ainsi qu'une structure hiérarchisée que seule quelques puissances militaires pouvaient déployer (15). Cet apparent retour au « monopole étatique de la violence » dans le cyberespace ne doit néanmoins pas occulter le vivier que représentent les experts civils en sécurité informatique, vivier qui est sollicité de différentes manières selon les régimes politiques des Etats et dont l'impact n'est pas négligeable (16). De la même manière, nous avons vu que la diffusion d'idées jugées subversives était fortement redoutée dans certains régimes politiques, ce qui conduit à la mise en place de dispositifs de contrôle et de censure. Or, avec la facilité d'accès au cyberespace, qui va croissante, tant en termes de diffusion géographique mondiale que d'amélio-

(15) Selon les informations du journaliste D. Sanger, à l'origine des révélations sur ce projet, Stuxnet serait le fruit d'une collaboration israélo-américaine.

(16) V. Joubert / G. Petkova, « L'intégration des citoyens dans une stratégie nationale de cyberdéfense : entre opportunités et contraintes stratégiques », *Note de la Fondation pour la recherche stratégique*, à paraître.

ration de la qualité des services d'accès, et qui engendre la multiplication des échanges de biens, de services, mais aussi d'opinions, maintenir cette censure afin de contenir la diffusion de la puissance sera une tâche complexe.

La complexité de la structure du cyberespace, qui empêche tout contrôle absolu, toute domination de la part d'un Etat, conjuguée à la multiplication des acteurs dans le domaine rendue possible par un seuil d'entrée très bas et des capacités d'actions favorisant l'attaque remettent en question la distribution de la puissance, jusqu'alors monopole des Etats. En dépit de la ré-accaparation politique du cyberespace amorcée depuis quelques années maintenant, l'imprévisibilité des évolutions techniques et technologiques, associée au contexte géostratégique, pousse des experts à affirmer que « *même les puissances dominantes possédant des capacités de coercition impressionnantes, comme les Etats-Unis, doivent partager la scène avec de nouveaux acteurs et ont plus de difficultés à contrôler leurs frontières dans le cyberespace. Le cyberespace ne remplacera pas l'espace géographique ni n'abolira le principe de souveraineté étatique, mais la diffusion de la puissance dans ce domaine prendra la forme d'une cohabitation, compliquant considérablement l'exercice du pouvoir en tant que nation souveraine et puissance étatique* » (17).

Quelles evolutions de la géopolitique depuis l'avènement du cyberespace ?

La dépendance des sociétés modernes aux technologies et infrastructures d'information et de communication, vitale pour la conduite des activités et la sécurité nationale des Etats, et le risque que constitue l'exploitation des vulnérabilités de ces systèmes par des adversaires ont contraint les gouvernements à investir massivement dans la protection de leurs intérêts dans le cyberespace.

L'investissement politique du cyberespace s'est alors traduit par plusieurs actions notables. D'une part, les Etats ont défini des stratégies nationales permettant de protéger leurs intérêts au niveau national : ils ont pour ce faire instauré des programmes de sensibilisation à la cybersécurité destinés au secteur privé et aux individus, incitant les entreprises comme les particuliers à adopter une hygiène informatique minimum et des comportements responsables limitant les risques de succès d'attaques sur les systèmes d'informations et réseaux qu'ils utilisent. La difficulté du succès de ces programmes réside dans le fait que les utilisateurs n'ont pas spontanément conscience de l'impact de leurs négligences et qu'il y a donc un véritable besoin d'éducation à grande échelle et devant s'inscrire dans la durée. Bien évidemment, ces programmes de sensibilisation ne permettent pas à eux seuls de faire avancer la situation,

(17) « *Even large countries with impressive hard power, such as the United States, find themselves sharing the stage with new actors and having more trouble controlling their borders in the domain of cyberspace. Cyberspace will not replace geographical space and will not abolish state sovereignty, but the diffusion of power in cyberspace will coexist and greatly complicate what it means to be a sovereign state or a powerful country* », écrit J. Nye, *Cyber Power*, Belfer Center for Science and International Affairs, Harvard Kennedy School, mai 2010.

c'est pourquoi les Etats ont recours à un dispositif législatif et réglementaire approprié pour fixer les standards de sécurité à respecter afin de prévenir les cyber-attaques, dispositif s'accompagnant parfois d'un renforcement des obligations qui incombent aux opérateurs d'infrastructures critiques pour détecter, notifier, et traiter toutes attaques touchant leurs systèmes (18). Cependant, ces tentatives de légiférer la cybersécurité n'aboutissent pas toujours, principalement en raison de contentieux politiques et économiques autour des obligations envisagées (19). D'autre part, les Etats ont établi une stratégie pour protéger leurs intérêts vitaux dans le système international : ils ont fait l'acquisition de capacités cyber qui, de par la dualité de leur fonction, permettent des actions offensives comme défensives afin d'assurer la protection des intérêts vitaux des nations, ou encore de préparer et d'accompagner les missions militaires. Cette militarisation du cyberespace s'inscrit dans le cadre de stratégies de dissuasion dites globales, par lesquelles les Etats se réservent le droit d'envisager toutes les options de riposte en cas de cyber-attaques contre leurs intérêts vitaux. Une telle stratégie, initiée par les Etats-Unis en 2011, a été reprise ouvertement ou tacitement par d'autres puissances (la Russie, la Chine, ou encore la France) (20). L'acquisition de capacités cyber associée à une dialectique stratégique ferme n'est pas pour apaiser les tensions interétatiques existantes. Comme nous l'avons expliqué, une telle situation tend à déclencher un nouveau dilemme de la sécurité dans le cyberespace et pose le risque d'aggraver des conflictualités, gérables en l'état, en conflit interétatique ouvert. Ce problème est pris très au sérieux par la communauté de défense américaine, laquelle met en garde les décideurs politiques contre les effets non désirés d'une politique non maîtrisée (21).

En dépit de l'évidente hyper-attention accordée aux enjeux de cybersécurité et de cyberdéfense par les puissances mondiales comme régionales, peut-on affirmer que le cyberespace a modifié la géopolitique internationale ? Les éléments relatifs à la diffusion de la puissance dans le domaine, par laquelle des individus tendent à acquérir un pouvoir d'action nouveau leur permettant de concurrencer celui des Etats, semble diminuer, voire fortement s'estomper, principalement grâce aux politiques nationales de cybersécurité instaurée depuis quelques années. L'Etat redevient progressivement l'acteur principal du cyberespace, auteur des actions et décisions ayant un impact sur l'environnement stratégique international. Cela ne signifie cependant pas que des

(18) *Ibid.*

(19) Il est intéressant de constater que, depuis son arrivée à la Maison-Blanche en 2008, B. Obama et son administration ne sont toujours pas arrivés à faire adopter le *Cybersecurity Act*, texte de loi devant permettre de renforcer la cybersécurité des infrastructures critiques américaines. L'administration s'est heurtée aux refus successifs du Congrès et du Sénat, principalement pour des raisons politiques, économiques et commerciales. Cette situation place les Etats-Unis dans un paradoxe entre la volonté affichée de rester le *leader* dans ce domaine technologique aux enjeux qu'on lui connaît et l'impossibilité d'arriver à un consensus politique national sur la cybersécurité des infrastructures du pays.

(20) Les dispositions du Livre blanc de la Défense et de la Sécurité nationale de 2013 sont, à ce sujet, très claires.

(21) *Cf.* notamment James Lewis, « Asia : the Cybersecurity Battleground », Statement before the House Foreign Affairs Committee, Subcommittee on Asia and the Pacific, CSIS, juil. 2013.

individus ou des groupes d'individus ont un rôle négligeable dans le cyberespace ; au contraire, l'implication collective des individus, coordonnée au niveau politique par des stratégies adaptées, permettent d'obtenir des résultats significatifs. C'est le but des programmes publics d'éducation et de sensibilisation à la cybersécurité, des programmes de réserves citoyennes de cyberdéfense ou encore des programmes de collaboration entre les secteurs publics-privés ou entre les opérationnels et la recherche.

Dans ces conditions, comment le cyberespace s'inscrit dans la géopolitique ? L'analyse des politiques étatiques ainsi que des stratégies nationales de cybersécurité et de cyberdéfense existantes nous permet de constater qu'il existe une géopolitique du cyberespace, en ce que les acteurs du domaine ont développé des représentations précises des enjeux intrinsèques qui viennent s'opposer à celles des autres acteurs, engendrant ainsi des rivalités de pouvoirs dans ce « territoire » nouveau. Cette géopolitique du cyberespace n'est pas autarcique, elle s'intègre pleinement dans la géopolitique internationale traditionnelle ; les acteurs internationaux ont plutôt cherché à utiliser ce nouveau domaine et saisir les opportunités stratégiques qu'il offre pour poursuivre leurs politiques extérieures. Si on observe attentivement les faits, on constate que les puissances majeures ayant massivement investi dans le cyberespace intègrent la dimension cyber à des stratégies classiques. La représentation américaine de la menace chinoise n'est pas apparue avec le cyberespace : toute une frange de la communauté de défense américaine l'avait évoqué depuis des années (22). De la même manière, les révélations d'Edward Snowden sur les programmes américains d'écoute et de surveillance dans le cyberespace semblent s'inscrire dans une certaine continuité de la politique de sécurité américaine dans le cadre de la lutte antiterroriste post-11 septembre 2001. Les techniques de récupération des données par les agences fédérales de renseignement américaines ont évolué qualitativement, ce qui leur a d'une certaine manière permis de les développer quantitativement en récupérant des données d'un nombre colossal de réseaux, mais cela ne veut pas dire que la finalité du renseignement a évolué. Les éléments de renseignements récoltés dans et par le cyberespace constituent un apport parmi d'autres aux opérations de sécurité américaine. Enfin, si on observe la Chine, on s'aperçoit que le cyberespace constitue un moyen d'atteindre les objectifs d'une politique globale ambitieuse replaçant le pays au sommet des puissances mondiales. Le cyberespace est utilisé comme levier pour accélérer la transformation du pays et permettre ce que l'ancien Secrétaire général du Parti communiste, Hu Jintao, a appelé le « *parachèvement de la grande renaissance de la nation chinoise* » (23).

(22) Jean-Loup Samaan, « La menace chinoise : une invention du Pentagone ? », *Vendémiaire*, oct. 2012.

(23) La notion de « *renaissance de la Chine* » (*zhonghua minzu weida de fuxing*) exprime une volonté du gouvernement chinois de rétablir l'« harmonie » en Asie, ce qui passe par une reconnaissance, par l'ensemble des autres puissances régionales comme de ses partenaires internationaux, de la suzeraineté naturelle de la puissance chinoise au niveau régional.

* *
*

Si l'exploitation du cyberespace est souvent présentée comme source de conflictualité interétatique, que ce soit par le cyberespionnage industriel, le cyberespionnage opéré par les services de renseignement étatiques ou encore l'application militaire des capacités cyber sur les théâtres de conflit, une analyse approfondie démontre que les acteurs principaux du domaine, au premier rang desquels se placent les Etats, maintiennent une politique extérieure classique, dans laquelle le cyberespace vient se greffer non comme unique enjeu mais plutôt comme domaine d'application supplémentaire. Une grande majorité des Etats ont ainsi investi dans l'acquisition de capacité cyber afin de préserver leurs intérêts vitaux contre des adversaires éventuels. Si certaines relations interétatiques peuvent se dégrader dans des régions du système international, ce ne sera pas à cause du cyberespace, mais parce que le cyberespace a cristallisé les rivalités et les conflictualités déjà existantes.