Études de l'Ifri

QU'EST-CE QUE LA PUISSANCE NUMÉRIQUE ?

Jean-Christophe NOËL

Novembre 2019

ifri 1979 2019
Institut français des relations internationales

L'**Ifri** est, en France, le principal centre indépendant de recherche, d'information et de débat sur les grandes questions internationales. Créé en 1979 par Thierry de Montbrial, l'Ifri est une association reconnue d'utilité publique (loi de 1901). Il n'est soumis à aucune tutelle administrative, définit librement ses activités et publie régulièrement ses travaux. L'Ifri associe, au travers de ses études et de ses débats, dans une démarche interdisciplinaire, décideurs politiques et experts à l'échelle internationale.

Capgemini est un leader mondial du conseil, des services informatiques et de la transformation numérique. À la pointe de l'innovation, le Groupe aide ses clients à saisir l'ensemble des opportunités que présentent le cloud, le digital et les plateformes. Fort de 50 ans d'expérience et d'une grande expertise des différents secteurs d'activité, il accompagne les entreprises et organisations dans la réalisation de leurs ambitions, de la définition de leur stratégie à la mise en œuvre de leurs opérations. Pour Capgemini, ce sont les hommes et les femmes qui donnent toute sa valeur à la technologie. Résolument multiculturel, le Groupe compte plus de 200 000 collaborateurs présents dans plus de 40 pays. Il a réalisé un chiffre d'affaires de 13,2 milliards d'euros en 2018.

Les opinions exprimées dans ce texte n'engagent que la responsabilité des auteurs.

Cette note a été réalisée dans le cadre du partenariat entre Capgemini et l'Ifri.

ISBN : 979-10-373-0072-0

© Tous droits réservés, Ifri, 2019

Comment citer cette publication :

Jean-Christophe Noël, « Qu'est-ce que la puissance numérique ? »,
Études de l'Ifri, Ifri, novembre 2019.

Ifri

27 rue de la Procession 75740 Paris Cedex 15 – FRANCE

Tél. : +33 (0)1 40 61 60 00 – Fax : +33 (0)1 40 61 60 60

E-mail : accueil@ifri.org

Site internet : Ifri.org

Auteur

Jean-Christophe Noël est chercheur associé au Centre des Études de Sécurité de l'Ifri. Il est un ancien officier de l'armée de l'Air. Après avoir mené une carrière de pilote de chasse, il a tenu diverses places en état-major, traitant notamment des affaires de doctrine ou de prospective.

Il a également été l'adjoint du chef de cabinet du chef d'état-major de l'armée de l'Air de 2006 à 2009, *Military Fellow* au Center for Strategic and International Studies à Washington D. C. en 2009 et expert chargé des affaires politico-militaires pendant cinq ans au Centre d'analyse, de prévision et de stratégie (CAPS) du ministère des Affaires étrangères de 2012 à 2017.

Résumé

La puissance numérique désigne la capacité d'un acteur à exploiter les flux de données numériques pour contribuer à modifier le comportement d'autres acteurs sur la scène internationale.

Bien que s'exerçant dans un milieu artificiel, l'influence de la puissance numérique sur le monde réel est grandissante. Elle dépasse par certains aspects la puissance étatique traditionnelle et rebat les catégories habituelles. Des formes de domination originales se sont mises en place, d'abord dans le champ économique puis dans celui de la sécurité, consistant à asservir avec son consentement le client ou la cible. Les informations échangées dans les réseaux peuvent être analysées par des opérateurs qui sauront transformer une envie en un besoin, une opinion en un fait incontestable. Ils jouent notamment sur des biais psychologiques pour rendre leurs cibles volontairement captives des services ou des messages proposés. Ces procédés donnent un nouvel élan à la « guerre politique » dans le domaine de la défense. Ce type de guerre offre la possibilité de contourner les niveaux tactiques, opératifs ou stratégiques pour influencer directement la population de son adversaire et atteindre son but sans combat sanglant.

Les formes les plus avancées de cette puissance ont un coût financier important et nécessitent un volontarisme politique pour être mises en œuvre. Un acteur doit être capable de créer un écosystème favorable, de pouvoir contrôler les données qui y circulent, de dominer les nœuds stratégiques des réseaux numériques et, surtout, de savoir articuler cette puissance d'un nouveau type avec les autres formes de puissance plus classiques. Aucun acteur ne parvient aujourd'hui complètement à maîtriser ce dernier aspect.

Pour autant, les acteurs traditionnels tentent de mobiliser les ressources dont ils disposent dans le monde réel pour influencer les comportements dans le monde numérique. De nouvelles formes de dissuasion, de coercition ou de régulation sont introduites pour tenter de limiter le pouvoir des plus importants acteurs digitaux. L'issue de cet affrontement déterminera en partie les contours futurs de la puissance numérique.

Sommaire

INTRODUCTION 9

Qu'est-ce que le numérique ? 9

Le numérique, enjeu politique 9

Qu'est-ce que la puissance ? 10

Qu'est-ce que la puissance numérique ? 11

COMMENT LE VIRTUEL INFLUENCE LE RÉEL 13

La puissance et le réseau 13

LES PRATIQUES DANS LE CYBERESPACE 19

Une nouvelle technologie au service d'objectifs classiques 19

La nécessité de définir de nouveaux paradigmes 21

LES COMPOSANTS DE LA PUISSANCE NUMÉRIQUE 29

Peut-on évaluer la puissance numérique ? 29

Les déterminants de la puissance numérique 30

COMMENT LE RÉEL INFLUENCE LE VIRTUEL 37

La riposte militaire 37

À la recherche d'une nouvelle régulation 39

Technologies numériques et cycle économique 41

Vers un morcellement plus prononcé ? 42

CONCLUSION 45

Introduction

Qu'est-ce que le numérique ?

Les données numériques peuvent être enregistrées, stockées, compressées, ou transférées sans aucune perte d'information et de qualité. La mise en valeur de ces caractéristiques a été essentielle pour le développement de l'informatique, à tel point que le terme numérique est entré dans le langage commun pour désigner de manière générique les applications des sciences informatiques[1]. Le développement d'algorithmes toujours plus sophistiqués, combinant ces données par le calcul, facilite la résolution de problèmes considérés jusqu'alors comme très complexes. La puissance constamment améliorée des microprocesseurs réduit sensiblement la durée de ces calculs. La mise en place de protocoles communs pour échanger aisément ces données entre ordinateurs redéfinit la notion de connectivité entre les hommes. Des informations, des ordres, des stimuli circulent toujours en plus grand nombre et bouleversent la manière d'échanger ou de gérer des systèmes complexes.

Le numérique, enjeu politique

Le mouvement de communication à distance initié par l'écriture, poursuivi par l'imprimerie, le télégraphe, le téléphone et la radio se poursuit donc.

La révolution numérique bouleverse, elle, de vastes secteurs de l'activité humaine. Elle accompagne la mondialisation en modifiant les distances entre les hommes. Les systèmes de transport, de logistique, de distribution d'énergie, de finance internationale, de gestion d'infrastructures critiques ne pourraient fonctionner sans ses applications. Le volume des échanges de messages électroniques impressionne également : 44,7 milliards de SMS et de MMS auraient été envoyés en France au premier trimestre 2018[2]. Au 12 août 2019, plus de 45 584 milliards de mails auraient été partagés à travers le monde depuis le début de l'année[3].

Dans le domaine militaire, les armées les plus avancées ont intégré la numérisation du champ de bataille dans leurs concepts. Les états-majors

1. D. Cardon, *Culture numérique*, Paris, Presses de Sciences Po, 2019, p. 18.
2. « Le nombre de SMS envoyés en France », *journaldunet.com*, 8 mai 2018.
3. « Emails envoyés dans le monde », *planetscope.com*, consulté le 12 août 2019.

fonctionnent de manière plus décentralisée en profitant des ressources qu'offre l'informatisation, concrétisant l'avènement d'une « révolution dans les affaires militaires[4] ».

D'un point de vue culturel, les jeux se pratiquent en réseau. Les joueurs les plus doués vivent de leurs participations à des tournois médiatiques. Les effets spéciaux envahissent les écrans de cinéma, donnant vie à des univers artificiels. Une culture numérique est en train d'émerger.

La technologie numérique est au cœur des enjeux économiques, militaires et culturels. Elle est entrée dans la vie quotidienne de l'ensemble des individus connectés à internet à travers le monde. Elle offre des ressources en termes d'enrichissement, de pouvoir, de contrôle de la société et de la vie privée. Conscient de ces enjeux, le Danemark a par exemple nommé dès 2017 un ambassadeur chargé des affaires technologiques. Il paraît légitime de parler de puissance numérique.

Qu'est-ce que la puissance ?

Définir la notion de puissance est cependant un défi. Le sens commun retient que la « puissance » sur la scène internationale est l'équivalent du « pouvoir » au sein des sociétés. Mais une telle intuition est d'une utilité limitée. Les scènes nationale et internationale fonctionnent selon des règles différentes. Les auteurs qui cherchent à l'appréhender reconnaissent qu'il s'agit d'un des termes les plus controversés des relations internationales[5].

Pour autant, deux grandes thématiques reviennent régulièrement dans les réflexions. La première tente de rendre ce concept opératoire. Si la puissance existe, il doit être possible de définir ses composants et de les évaluer, de les mesurer pour agir rationnellement. Dans ce cadre, la puissance a longtemps été réduite par l'école réaliste à la position géographique et à la somme des moyens militaires, démographiques ou économiques. Des composants plus immatériels comme le sentiment national, la qualité du personnel, politique pouvaient compter aussi. Cette approche comptable et analytique est cependant critiquée en ce qu'elle ne dévoile que le potentiel de la puissance. Elle ne garantit aucune performance, si un acteur étatique ne parvient pas à les combiner efficacement. L'Union soviétique disposait de nombre de ces avantages. Elle s'est pourtant effondrée sans lutter.

4. A. F. Krepenevich, « Cavalry to Computer: The Pattern of Military Revolutions », *The National Interest*, n° 37, automne 1994, p. 30-42 ; E. A. Cohen, « A Revolution in Warfare », *Foreign Affairs*, mars-avril 1996, p. 37-54 ; J.-C. Noël, « Intelligence artificielle : vers une nouvelle révolution militaire ? », *Focus stratégique*, n° 84, Ifri, octobre 2018.
5. R. Gilpin, *War and Change in World Politics*, New York, Cambridge University Press, 1981, p. 18.

Un autre thème revient souvent dans les réflexions sur l'essence de la puissance. La puissance est ce qui décide de l'issue de l'interaction entre deux entités étatiques ou acteurs du système international. Elle ne désigne plus un potentiel, mais le « passage à l'acte[6] ». Dans un article séminal, Robert Dahl la définit comme « la capacité de A d'obtenir de B l'accomplissement de quelque chose que B n'aurait pas fait[7] ». La puissance contraint, mais pas nécessairement de manière violente. Elle peut s'exercer par la séduction, plutôt que par l'imposition brutale d'une volonté[8]. La puissance correspond finalement à la capacité d'un acteur à modifier le comportement d'autres acteurs de la scène internationale dans un sens favorable.

Qu'est-ce que la puissance numérique ?

Dans ce cadre, comment qualifier la puissance numérique, parfois désignée comme la cyberpuissance ? Pour notre part, la puissance numérique sera considérée comme la capacité d'un acteur quelconque à exploiter les données numériques pour contribuer à modifier le comportement d'autres acteurs de la scène internationale et à atteindre ses propres fins.

Elle dépasse le cadre étatique classique et rebat les catégories habituelles, puisque tous les acteurs connectés sont théoriquement susceptibles d'en détenir une part. Par ailleurs, les sources de la puissance numérique se trouvent dans l'exploitation d'un milieu et de données artificiels. Cette étude a pour but de comprendre comment une puissance « immatérielle » parvient à influencer les événements dans le monde réel et de caractériser son potentiel, ses applications comme ses limites.

La puissance numérique transforme le monde réel grâce à la mise en valeur des propriétés réticulaires du cyberespace (1) et des nouvelles pratiques de domination qui s'y sont imposées (2). Ses composantes peuvent en être déduites (3). Il est cependant probable que son exercice sera altéré dans l'avenir par un volontarisme plus affirmé des acteurs du monde réel (4). Elle est finalement comme un kaléidoscope, présentant plusieurs facettes, dont l'articulation suscite parfois de fortes tensions.

6. T. de Montbrial, « Qu'est-ce qu'une puissance au 21e siècle ? », Discours à l'Académie des sciences morales et politiques, 7 janvier 2013.
7. R. A. Dahl, « The Concept of Power », *Behavioral Science*, n° 2, 1957, p. 201-215.
8. J. Nye, *Soft Power*, New York, PublicAffairs, 2005.

Comment le virtuel influence le réel

La puissance et le réseau

Jelle van Haster définit en 2016 la cyberpuissance comme « la variété d'expression de pouvoirs qui circulent dans le cyberespace et qui modèlent les expériences de ceux qui agissent dans et à travers le cyberespace[9] ». Selon cet expert néerlandais, la puissance numérique est intimement liée au cyberespace, milieu dans lequel elle émerge, se déploie et s'exerce.

Aborder la puissance numérique par le cyberespace semble de fait une approche pertinente pour mieux dessiner ses contours. Mais définir le cyberespace est encore une fois une gageure tant les perceptions sont discordantes. Il est dépeint alternativement comme un domaine, un théâtre d'opérations, un environnement, un espace, un substrat, un milieu ou un moyen[10]. Cette abondance de définitions ne reflète pas qu'un simple débat académique entre universitaires sourcilleux. Des pensées stratégiques originales soutiennent ces différents points de vue. Ainsi, Moscou ne considère pas le cyberespace comme un lieu singulier possédant des spécificités propres qui imposent des règles et des conduites particulières. Pour les Russes, le numérique est un média comme un autre qui participe à la maîtrise de l'information[11]. Il remplit plus une fonction régalienne qu'il n'occupe un espace.

Qu'il soit considéré comme un médium[12] ou comme un environnement[13], le cyberespace se ramène peu ou prou aux intranets et à

9. J. van Haster, « Assessing Cyber Power » *in* N. Pissandis, H. Rölgas et M. Veenendaal, *8th International Conference on Cyber Conflict*, Tallinn, NATO CCD COE Publications, 2016, p. 13.
10. A. Desforges, « Les représentations du cyberespace : un outil géopolitique », *Hérodote*, n° 152-153, 2014, p. 67.
11. K. Limonier, « La Russie dans le cyberespace : représentations et enjeux », *Hérodote*, n° 152-153, 2014, p. 143.
12. Selon P. Cornish, le cyberespace est « un medium mondial pour les échanges dans le domaine de la communication et l'information entre des ordinateurs et leurs opérateurs humains, un environnement dans lequel il est possible que des signaux numériques soient envoyés, reçus et traités ». Voir P. Cornish, « Governing Cyberspace through Constructive Ambiguity », *Survival*, vol. 57, n° 3, 2015, p. 153.
13. Pour W. H. Boothby, le cyberespace est « l'environnement formé par des composants physiques et non physiques défini par l'usage d'ordinateurs et du spectre électromagnétique pour emmagasiner, modifier et échanger des données utilisant des réseaux d'ordinateurs ». Lire W. H. Boothby, *Conflict*

internet. Son organisation est celle d'un réseau décentralisé, qui ne possède pas de centre, de frontières, mais où certains nœuds ont plus de valeur que d'autres[14].

La puissance offerte par un réseau diffère singulièrement de la puissance classique, qui se résume souvent à un simple rapport de force. Le réseau valorise le lien, le flux, la mobilité des biens par rapport au lieu, à la position, à l'enracinement. Pénétrer et faire partie d'un réseau est une expérience immersive et englobante. Tout corps plongé dans un réseau devient un réseau ; l'objet ou l'individu connecté acquiert la puissance du réseau ; et un réseau lent sera toujours avalé par un réseau plus agile (ou plus rapide, plus efficace)[15].

La puissance numérique doit donc d'abord se comprendre et s'étudier comme un phénomène s'exerçant à travers un réseau. Or la puissance réticulaire a déjà été au fondement de la domination de certains États.

Puissance navale

La puissance navale en est un formidable exemple. Les Athéniens, Carthaginois et Étrusques pendant l'Antiquité, les Génois et Vénitiens au Moyen Âge en définissent les premiers contours en Méditerranée. Mais leur influence est principalement commerciale et s'opère surtout sur le littoral. C'est l'émergence de l'Empire britannique à partir du XVIe siècle, en rivalité avec les Provinces unies[16], qui porte ce concept à maturité.

Alors que les Espagnols ou les Portugais considèrent le Nouveau Monde comme une réserve à piller, les Anglais partent à la conquête des espaces vides pour les valoriser et imposer leur système politique. La maîtrise des océans doit permettre d'asseoir la domination par le commerce et les échanges, l'expansion de l'idéologie libérale et de l'utilitarisme. La maîtrise des voies de communication accélère la croissance des flux de marchandises, de soldats et… d'idées entre les ports tenus par les Britanniques. Londres est le centre du réseau et les bases maritimes forment les différents nœuds du réseau qui sont autant de

Law: The Influence of New Weapons Technology, Human Rights and Emerging Actors, Hague, TMC Asser Press, 2014, p. 123.

14. P. Cardon, *op. cit.*, p. 27-36.

15. P. Bellanger, *La Souveraineté numérique*, Paris, Stock, 2014, p. 30-31. Lire aussi A.-M. Slaughter, *The Chessboard and the Web: Strategies of Connection in a Networked World*, New Haven, Yale University Press, 2017 ; D. S. Grewal, *Network Power: The Social Dynamics of Globalization*, New Haven, Yale University Press, 2008.

16. C. Schmitt, *Le nomos de la terre*, Paris, Presses universitaires de France, 2001 ; P. Forget et G. Polycarpe, *Le réseau et l'infini*, Paris, Economica, 1997, p. 53-77 ; F. Gipouloux, *La Méditerranée asiatique*, Paris, Presses du CNRS, 2009.

points d'entrée vers des territoires vierges. La puissance navale britannique est d'abord au service d'une vision politique.

Cette conquête des océans est rendue possible par les progrès des sciences et le déchiffrement mathématique de la Nature. Leurs applications dans la cartographie ou dans l'astronomie donnent les moyens de se repérer et de sillonner les vastes étendues des océans sans s'égarer. Le monde est décrit mathématiquement par une suite de nombres appelée latitudes et longitudes, dont l'origine se situe évidemment près de Londres, à Greenwich. Il est décodé. Il peut être instrumentalisé pour se déplacer et agir.

Des acteurs d'origines très diverses évoluent conjointement dans ce milieu. Militaires, marchands, migrants, voyageurs côtoient des pirates, et même autrefois des corsaires dont le statut brouille allégrement les catégories régaliennes et criminelles.

Puissance numérique

Si la mer est un milieu naturel, le cyberespace a été créé artificiellement par l'homme. Il est constitué de trois couches. La première est matérielle (*hardware*) et comprend toute l'infrastructure physique nécessaire pour que les données transitent d'un point du réseau vers un autre. Elle inclut notamment les câbles sous-marins, les serveurs, les ordinateurs et les objets connectés. La deuxième couche est immatérielle et correspond aux applications nécessaires pour traiter les informations (*software*). Elle est formée des logiciels, des systèmes d'exploitation. La dernière couche est appelée la couche cognitive. Elle renvoie au contenu des informations stockées ou échangées dans le réseau.

Différentes lois ou observations caractérisent les vertus de ce réseau. Selon Robert Metcalfe, l'inventeur d'Ethernet, « l'utilité d'un réseau est proportionnelle au carré du nombre de ses utilisateurs[17] ». Un réseau constitué par cinq ordinateurs a une utilité de 25. Si l'on double le nombre d'ordinateurs pour arriver à 10, l'utilité quadruple et atteint 100[18]. L'entrepreneur Gordon E. Moore observe pour sa part qu'« à prix égal, la capacité de calcul d'un microprocesseur double tous les 18 mois. Sur les 15 dernières années, la puissance de calcul des machines a été multipliée 1 000 fois[19] ». Le mathématicien allemand Martin Grötschel complète cette

17. P. Bellanger, *op. cit.*, p. 27.
18. Des nuances ont été apportées à cette loi. Voir B. Briscoe, A. Odlyzko et B. Tilly, « Metcalfe's Law Is Wrong », *spectrum.ieee.org*, 1er juillet 2006.
19. P. Bellanger, *op. cit.*, p. 27. Entre 1971 et 2001, la densité de transistors a doublé chaque 1,96 années.

loi empirique et affirme que « la vitesse de calcul des machines, grâce à la croissance de l'efficacité des algorithmes, progresse 43 fois plus vite que la loi de Moore[20] ». Les possibilités offertes par le cyberespace augmentent à un rythme exponentiel. La puissance numérique est une puissance émancipatrice qui démultiplie les capacités d'action des internautes.

Le cyberespace n'est pas un milieu figé où les lois de la physique encadrent étroitement l'innovation. Il évolue sans cesse, notamment grâce aux intuitions et aux initiatives d'acteurs individuels et privés qui élaborent des logiciels qui se diffusent de manière virale s'ils satisfont un besoin[21]. Les applications numériques se font et se défont également très rapidement. La concurrence est féroce entre les entrepreneurs, comme en Chine, où pour paraphraser un célèbre proverbe, « tout est permis à la guerre et… entre start-up[22] ». Les progrès de la technologie et la demande du marché s'inspirent mutuellement et accouchent sans cesse de nouvelles solutions. La 5e génération de standards (5G) est sur le point d'être mis en place dans le domaine de la téléphonie mobile. Pourtant, les champions d'hier comme Ericsson sont tombés de leur piédestal pour n'avoir pas su anticiper les évolutions du marché. Huawei a su au contraire investir dans des projets qui lui assurent aujourd'hui une place essentielle pour accroître ses débouchés. La puissance numérique s'exerce dans un environnement de destruction/création très concurrentiel, où l'innovation est généralement ascendante. Elle sera éphémère si son propriétaire ne dispose pas des outils à la pointe de la technologie.

Comme sur la mer, de nombreux acteurs possédant des statuts hétéroclites ont accès au cyberespace. Des États, des entreprises, des individus peuvent interagir entre eux, en tentant d'atteindre des buts très variés. Cette connexion permet d'initier des rapports de puissance plus directs qu'autrefois, de soulever des leviers originaux pour influencer son interlocuteur ou son rival. La puissance numérique est une puissance partagée, ou encore décentrée entre la multiplicité d'acteurs qui interviennent dans le cyberespace[23].

Ce phénomène est accentué par le fait qu'internet est conçu initialement selon une logique libertaire, où chaque individu connecté se voit offrir une part de liberté et d'initiative en court-circuitant le monopole des institutions traditionnelles. Par ailleurs, le cyberespace n'est pas un

20. *Ibid.*, p. 29.
21. D. Cardon, *op. cit.*, p. 101-110.
22. Kai-Fu L., *AI Super-powers: China, Silicon Valley and the New World Order*, New York, Houghton Mifflin Harcourt Publishing Company, 2018, p. 40-50.
23. T. Gomart, « Entre concentration et dispersion : le bel avenir de la puissance », *Politique étrangère*, n° 1, Ifri, mars 2019, p. 11-21.

commons, terme qui définit un espace où aucune souveraineté ne s'exerce mais dont l'usage peut profiter à tous[24]. Il peut plutôt être comparé à un condominium, où « un ensemble de bits se déplaçant d'un ordinateur vers un autre sont généralement sur un réseau que quelqu'un possède et qui est physiquement situé dans un pays souverain[25] ». Les câbles sous-marins qui transportent les données au travers de fibres optiques peuvent par exemple appartenir à des acteurs privés qui en ont l'usage réservé ou qui louent une partie de leurs capacités. Ils peuvent aussi être la copropriété de différents acteurs réunis au sein de consortiums[26]. Les États n'ont donc pas le monopole de ces réseaux et ne peuvent imposer aisément leurs règles.

L'évolution entamée au XVIe siècle sur les océans se poursuit enfin aujourd'hui. Les algorithmes sont une extension dans le monde digital des êtres humains et de leurs cerveaux. Ils traduisent les choix, les décisions, les préférences et les goûts des hommes dans un langage différent. Ils codent numériquement leurs comportements et transforment l'homme en une quantité mesurable[27]. Ainsi, la découverte des lois physiques et la traduction en langage mathématique de la Nature ont rendu possible l'ère des grandes découvertes et de la conquête du monde par les Européens. La numérisation partielle des êtres humains et le dévoilement de leurs capacités cognitives pourraient à son tour provoquer de grands bouleversements, débordant du cyberespace vers le monde réel.

Le cyberespace est un milieu où un nouveau rapport entre l'homme et les réseaux s'instaure. La maîtrise de la mer a permis l'émergence de thalassocraties. Le contrôle de l'espace numérique pourrait susciter le développement de numérocratie. Reste à voir selon quelles pratiques.

24. B. R. Posen, « The Command of Commons: The Military Foundation of U.S. Hegemony », *International Security*, vol. 28, n° 1, 2003, p. 8.
25. J. A. Lewis, « Cybersecurity: Next Steps to Protect Critical Infrastructure », *Testimony to the US Senate Committee on Commerce, Science and Transportation*, 23 février 2010.
26. Intervention de Jean-Luc Vuillemin lors d'un séminaire fermé à l'Ifri, le 11 juillet 2019.
27. P. Bellanger, *op. cit.*, p. 101.

Les pratiques dans le cyberespace

La manière dont les ressources numériques sont exploitées dans le cyberespace est au cœur de la définition de la puissance numérique. Un débat oppose à ce propos ceux qui estiment que l'exercice de la cyberpuissance ne s'inscrit que dans les formes de compétition classiques et d'autres qui affirment que la nature de la rivalité entre les États est au contraire bouleversée et que de nouveaux modèles doivent être privilégiés[28].

Une nouvelle technologie au service d'objectifs classiques

Dès le début des années 1990, le cyberespace est identifié comme un nouveau théâtre d'opérations où la violence va immanquablement se déchaîner[29]. Mais rien de significatif n'advient. Les analyses s'affinent et en 2012, Thomas Rid explique dans un article séminal que la cyberguerre n'a jamais existé, qu'elle n'existe pas, et qu'il est hautement probable qu'elle n'éclate pas dans le futur[30]. Les cyberattaques les plus médiatiques ne sont que des versions modernisées et sophistiquées d'actes de subversion, d'espionnage ou de sabotage. Les États adaptent juste les modalités des opérations avec les nouveaux moyens à leur disposition.

La crainte qu'un jeune surdoué maléfique parvienne à paralyser depuis son sous-sol les organisations de sécurité semble plus tenir du fantasme que renvoyer à la réalité. Certes, des opportunités existent et des brèches dans les systèmes peuvent être élargies pour obtenir des résultats parfois impressionnants médiatiquement, mais très éphémères opérationnellement. Un Allemand de 20 ans est par exemple parvenu à publier sur internet des informations personnelles appartenant à environ un millier de personnalités politiques allemandes, dont la chancelière Angela Merkel. Sans posséder de grands talents de hacker, il avait réussi à

28. W. Hoffman, « Is Cyber Strategy Possible? », *The Washington Quaterly*, vol. 42, n° 1, 2019, p. 134.
29. J. Arquila et D. Ronfeldt, « Cyberwar Is Coming! », *Comparative Strategy*, vol. 12, n° 2, 1993, p. 141-165.
30. T. Rid, « Cyberwar Will not Take Place », *Journal of Strategic Studies*, vol. 35, n° 1, 2012, p. 6.

extraire du web l'ensemble des informations disponibles sur ses victimes, avant de les compiler et de les diffuser[31].

Obtenir des effets militaires réclame en revanche une mobilisation importante de moyens, similaire à la préparation d'une action militaire classique de ciblage[32]. Une analyse systémique de l'objectif doit être accomplie. Il faut connaître parfaitement son architecture et son fonctionnement. Des renseignements précis doivent être obtenus pour pénétrer discrètement le système de l'adversaire. La rédaction du logiciel d'attaque doit être suffisamment élaborée pour éviter les dommages collatéraux. Pour autant, l'échec est toujours possible. Le simple changement de mot de passe d'un opérateur adverse peut ruiner des mois d'investigations[33].

Les logiciels d'attaque ne servent qu'une fois. Ce sont des armes à un coup, qui cessent d'être opérationnelles dès que l'adversaire comprend qu'il a été joué et qu'il corrige les défauts de sa cuirasse[34]. Paralyser un système ne suffit pas toujours pour obtenir un effet militaire durable. Seule la destruction de l'objectif le peut. Comme le résume le stratégiste Colin Gray, la principale valeur ajoutée de la cyberpuissance dans le domaine de la confrontation militaire est sûrement d'être un catalyseur, un facilitateur (*enabler*) dans les opérations interarmées[35]. *Orchard* est le nom de l'opération menée par Israël en 2007 au-dessus de la Syrie pour détruire un site en construction qui devait accueillir des facilités nucléaires. Des cyberopérateurs israéliens se sont introduits dans le système de détection aérien syrien et ont masqué les échos radar des avions de l'armée de l'Air israélienne. Leur contribution s'est révélée décisive pour surprendre l'adversaire et conserver la liberté de manœuvre. Si la cyberpuissance ne peut résoudre les problèmes militaires, elle permet de les aborder en meilleure position.

Enfin, la puissance numérique ne semble pas apporter de rupture dans le domaine de la coercition[36]. Son usage y est particulièrement délicat, tant l'adversaire peut mal percevoir l'intention de l'attaquant. L'attaquant devra d'abord décider s'il informe son rival de son assaut. S'il ne le fait pas, ce dernier pourra croire qu'il est victime d'une panne informatique ou

31. « Cyberattaque en Allemagne : le hacker vivait chez ses parents », *latribune.fr*, 8 janvier 2019.
32. Entretien avec un membre du ministère des Armées, le 20 juin 2019.
33. *Ibid.*
34. Ces algorithmes peuvent en revanche servir de « souche » et muter si des hackers chevronnés les recomposent en partie. Ils sont alors réutilisés avec succès.
35. C. Gray, *Making Strategic Sense of Cyber Power: Why the Sky is not Falling*, Carlisle, Strategic Studies Institute and US Army War College Press, 2013.
36. Pour nuancer ce point de vue, lire S. Taillat, « Dissuasion et coercition » *in* S. Taillat, A. Cattaruzza et D. Danet, *La Cyberdéfense : politique de l'espace numérique*, Paris, Armand Colin, 2018, p. 147-148.

craindre au contraire qu'il est la cible d'une attaque préventive et réagir d'une manière outrancière en cas de crise grave. Mais s'il choisit d'informer son adversaire de son coup, ce dernier sera en mesure d'analyser le mode d'action de l'attaquant et d'y parer. Démonstration de force et efficacité semblent peu compatibles.

En outre, la teneur du signal envoyé peut être difficile à saisir pour le défenseur si l'ampleur des dommages dépasse le seuil qui est envisagé initialement, du fait d'une programmation défaillante d'un logiciel. La maîtrise de l'escalade peut échapper au contrôle de l'attaquant. Le virus Stuxnet, destiné à saboter l'enrichissement en uranium du programme nucléaire iranien, s'est ainsi propagé vers d'autres ordinateurs à travers le monde[37]. Si d'autres fonctions très sensibles sont atteintes, la réaction peut enclencher un cycle de représailles difficile à arrêter.

En première analyse, la cyberpuissance participe avec ses caractéristiques propres à l'exercice de la puissance traditionnelle. L'avènement du numérique n'a pas modifié les intérêts et les motivations des États, ni même des individus, qui demeurent constants[38]. Elle contribue surtout aux formes de compétitions et d'affrontements classiques. Le défi est de l'intégrer de manière juste avec les autres outils de la puissance traditionnelle, comme la force militaire.

La nécessité de définir de nouveaux paradigmes

Malgré ces restrictions, la fréquence et le volume des agressions ne cessent d'augmenter dans le cyberespace. Plus de 200 événements pouvant être considérés comme des cyberattaques d'un État contre un autre ont été en tout recensés[39]. Les actions criminelles prolifèrent sur internet également. Le nombre de harcèlements commis par l'intermédiaire d'un service de communication en ligne a doublé en France entre 2016 et 2018[40]. Si les caractéristiques du réseau numérique ont déjà été évoquées, la description des avantages qu'offre le cyberespace est utile pour comprendre cette augmentation sensible des attaques et mieux aborder la puissance numérique.

37. « Stuxnet also Found at Industrial Plants in Germany », *h-online.com*, 17 septembre 2010.
38. J. A. Lewis, « Étude préliminaire sur les analyses en cybersécurité ; l'affaire Snowden comme étude de cas », *Hérodote*, n° 152-153, 2014, p. 33.
39. M. Willett, « Assessing CyberPower », *Survival*, vol. 61, n° 1, p. 85.
40. « L'état de la menace liée au numérique en 2019 », *interieur.gouv.fr*, 9 juillet 2019.

Principes d'action dans le cyberespace

La diffusion des messages et des données est d'abord immédiate et globale dans le cyberespace. Deux ordinateurs quelconques peuvent échanger des informations instantanément pourvu que leurs protocoles de communication soient compatibles. La géographie physique ne compte plus. Les effets d'échelle sont sans commune mesure avec ce qui était pratiqué avant. Si une attaque est possible, elle peut largement s'étendre rapidement. Les théâtres d'action militaires prennent une dimension mondiale. Si les actions cinétiques sont bien contenues dans les zones de guerre pendant les conflits, des sympathisants habitant dans des zones très éloignées des combats, voire même dans le pays d'un ennemi, peuvent aussi tenir un rôle. Les concepts traditionnels de frontière, de souveraineté sont remis en cause.

Les moyens d'action offensifs sont favorisés. L'accès au réseau est aisé et demande un investissement modeste. Le rapport coût/résultat est particulièrement faible et peut inciter des assaillants à agir. L'échec n'aura que peu de conséquences. L'attaquant dispose aussi de l'initiative. Un système informatique est comparable à une forteresse. Il est figé. Il peut être observé, ses défenses peuvent être testées, ses failles décelées et exploitées. Le défenseur peut difficilement concevoir toutes les possibilités de pénétration de ses réseaux et s'en prémunir. Un des modes d'action favoris des assaillants est de repérer une vulnérabilité appelée « zéro jour », correspondant à un défaut de sécurité du logiciel ou du système d'exploitation dont les concepteurs n'ont pas conscience[41]. L'imagination est la plus grande force des hackers.

L'attaquant agit aussi masqué. Il s'avère très difficile de détecter immédiatement une attaque, puis de remonter les arcanes du réseau pour identifier les initiateurs. La priorité initiale est plutôt de comprendre la nature de l'attaque pour en limiter les effets. La phase d'attribution ne vient qu'après. Et il est très improbable de trouver un « smoking gun » indiquant avec certitude l'origine de l'attaque. Des faisceaux d'indices doivent être rassemblés et interprétés[42]. Les États peuvent brouiller les pistes en confiant la réalisation de certaines missions sensibles à des acteurs privés. Cette furtivité renforce en tout cas l'incitation à agir des hackers puisqu'ils savent qu'ils disposeront d'une relative immunité.

Enfin, des règles d'engagement communes ou un code de bonnes pratiques partagé par tous n'existent pas dans le cyberespace. Les conduites des acteurs peuvent être très disparates et imprévisibles du fait

41. J.-L. Gergorin et L. Isaac-Dognin, *Cyber. La guerre permanente*, Paris, Le Cerf, 2018, p. 109.
42. *Ibid.*, p. 150.

d'un déficit de régulation. L'incertitude et la méfiance règnent du fait que les acteurs ignorent les capacités de leurs rivaux et les limites qu'ils se fixent.

La puissance numérique est donc également une puissance asymétrique, réduisant l'écart de pouvoir et les capacités d'action entre les différents acteurs[43].

Puissance numérique et économie[44]

Les entrepreneurs économiques privés ont été les premiers à comprendre comment articuler le mieux possible toutes ces ressources. Ils ont imaginé une nouvelle forme d'organisation, bouleversant les chaînes de valeurs et renversant la domination d'entreprises séculaires.

Les start-ups s'affranchissent du modèle taylorien et promeuvent la « scalabilité ». Puisqu'elles peuvent théoriquement accéder à tous les internautes à des coûts financiers très modiques, elles élaborent de nouveaux produits qu'elles pourront continuer à « fabriquer » en cas de choc de croissance, si la demande explose rapidement.

De petites équipes disposant d'une grande autonomie sont mises en place. Wikipédia rassemble par exemple huit personnes initialement. Facebook compte 450 employés en 2007 (contre 35 000 en 2018)[45]. Les clients se chargent de fournir librement et gratuitement les composants nécessaires au développement de la start-up. Une idée originale est exploitée en imaginant un prototype simple. L'objectif est par exemple de fabriquer une voiture de luxe, mais seul le moteur est installé sur un châssis et sur quatre roues. Le reste est conçu par les clients. Leurs préférences et leurs désirs sont connus et exploités grâce aux échanges directs entretenus avec eux. Il suffit de leur proposer ce qui leur convient le mieux. Les entrepreneurs tirent profit de l'intelligence collective du réseau tout en individualisant le service. L'offre et la demande se rencontrent directement, sans médiateurs. Les pertes financières sont parfois importantes au départ, mais elles sont largement compensées par les gains futurs. La croissance est assurée grâce aux technologies de marketing et à des ressorts psychologiques créant une dépendance. La fidélité est récompensée par des avantages, des remises exclusives.

43. *Ibid.*, p. 157.
44. N. Colin et H. Verdier, *L'âge de la multitude : entreprendre et gouverner après la révolution numérique*, Paris, Armand Colin, 2015.
45. « Nombre d'employés de Facebook 2004-2018 », *Statista.com*, consulté le 16 août 2019.

Les plates-formes numériques ne fabriquent évidemment pas des voitures, mais elles offrent des services. Elles les agrègent pour les rendre encore plus attractifs et pour dominer le marché. On ne vend plus un véhicule, mais une expérience de vie. On ne vend plus une chambre d'hôtel, mais un voyage. Les logiciels remplacent les intermédiaires et les services de transaction. Ils se chargent de trouver les propositions les plus attrayantes pour les touristes potentiels, leur faisant gagner du temps et de l'argent. Ils combinent les offres des groupes hôteliers avec celles des compagnies de transport.

Outre le contrôle de la chaîne de valeur, ces plates-formes sont tentées de contrôler les infrastructures numériques pour gérer plus étroitement les flux de données. La maîtrise des interfaces, comme les téléphones mobiles, est essentielle pour que les clients accèdent exclusivement aux applications de ces plates-formes. Amazon a commencé par vendre des livres. La firme américaine en a ensuite numérisé le contenu, qui était uniquement lisible sur le *Kindle*. Elle fabrique désormais les puces qui équipent ces lecteurs électroniques.

Les clients deviennent captifs d'un écosystème qui est partagé de manière inégale. Développant un monde où les besoins, plus ou moins artificiels, de ses habitants sont satisfaits, les plates-formes deviennent incontournables. Elles prélèvent en contrepartie une dîme invisible, constituée par les données que fourniront de manière asymétrique ses clients sur leurs comportements et leurs préférences. Elle est à l'origine de la richesse des plates-formes qui les font fructifier. La publicité (Facebook, Twitter) est individualisée. Les services de cartographie renseignent bien sûr les usagers sur leurs positions mais ils leur indiquent aussi quelques adresses proches susceptibles de déclencher une envie irrépressible de consommer. Cette dîme endette encore plus ses clients en les rendant toujours plus dépendants des services fournis par la plate-forme.

Mais ces données ne leur appartiennent plus. Elles sont aux mains des grands groupes, qui les transforment en instruments de pouvoir. Les données ne sont pas le nouveau pétrole de l'économie (*oil* en anglais), mais son nouveau terreau (*soil* en anglais)[46]. Tous les individus connectés sont les nouveaux serfs de l'ère numérique. Ce sont des métayers qui cultivent, entretiennent et développent le sol numérique, qui ne leur appartient pas et dont ils peuvent se voir interdire soudainement l'accès si leurs maîtres le décident[47].

46. L. Kirchner, « Data is the New Soil: David McCandless' TED Talk on Visualizing Data », *Columbia Journalism Review*.
47. Entretien avec un membre du ministère des Affaires étrangères, 10 mai 2019.

Le but de ces plates-formes est de créer un système fermé, hyper-concentré, où elles éteindraient toute concurrence. Elles pourraient alors ordonner les données selon leur propre logique et avoir une influence dans de nombreux domaines comme le travail, la vie privée ou la fiscalité. Facebook veut par exemple battre sa propre monnaie avec le Libra. Elles incarnent une version moderne des grandes entreprises coloniales qui ont acquis des fonctions commerciales, puis régaliennes et militaires comme l'*East India Company* entre le XVIIe et le XIXe siècle, qui mit l'Inde sous sa coupe[48].

Entre guerre et paix

Les recettes appliquées avec succès dans le domaine économique sont progressivement adoptées dans le domaine de la conflictualité. L'exercice de la puissance numérique semble particulièrement s'étendre dans la « zone grise » qui ne correspond plus à l'état de paix mais ne peut être encore considéré comme un état de guerre. Le but n'est pas de porter un coup décisif. L'intention est plutôt de pénétrer lentement les réseaux numériques de l'adversaire pour s'y implanter durablement et les exploiter si des opportunités se présentent ou des circonstances l'imposent. La somme des coups portés sur l'ensemble de ces réseaux doit fragiliser à terme l'ennemi.

La scalabilité et le changement d'échelle permettent de redéfinir les conditions de l'affrontement et de reconsidérer certaines catégories de la compétition internationale. Pour paraphraser Valery Gerasimov, le rôle des moyens non militaires pour atteindre des buts politiques et stratégiques augmente[49]. Les cyberactions s'avèrent parfois plus efficaces que la force armée, brouillant le rapport à la violence de nos sociétés.

Le niveau de conflictualité où la puissance numérique semble la plus décisive est celui de la « guerre politique[50] ». Ce terme date du début de la guerre froide. Georges Kennan le définit le premier comme l'application logique de la doctrine de Clausewitz en temps de paix, c'est-à-dire de l'emploi de tous les moyens à la disposition d'une nation, à l'exception de la guerre, pour atteindre ses objectifs nationaux[51]. Une définition plus récente l'interprète comme « l'usage intentionnel d'un ou plusieurs composantes de la puissance (diplomatique, informationnelle, militaire et économique)

48. J. Keay, *The Honourable Company: A History of the English East India Company*, Londres, Harper Collins, 1991.
49. M. Galeotti, « The Gerasimov Doctrine and Russian Non-Linear War », *kcl.rl.talis.com*, 2013.
50. Traduction du terme Political Warfare.
51. L. Robinson, T. C. Helmus, R. S. Cohen, *et al.*, *Modern Political Warfare,* Santa Monica, Rand, 2018, p. XIII.

pour affecter la composition politique ou le processus de décision à l'intérieur d'un État[52] ».

La puissance numérique influe sur cette guerre politique. Les niveaux tactique, opératif ou stratégique sont délaissés par rapport au conflit conventionnel. Il ne s'agit plus de s'imposer sur un champ de bataille classique, de mieux manœuvrer que les armées adverses ou de détruire les moyens de production d'armement et de soutien logistique. Le but est de contourner tous ces niveaux traditionnels de la guerre et de cibler directement les citoyens, en agissant sur leur perception de la réalité et l'orientation de leurs préférences politiques.

Les débats politiques domestiques sont formatés et la légitimité de certains dirigeants est affaiblie ou renforcée en utilisant des procédés semblables à ceux du marketing commercial. Les mêmes biais psychologiques permettent d'attirer et de retenir les internautes. Qu'importe qu'on rende compte exactement des événements. Les histoires fausses, mais dont le narratif est excitant, circulent par exemple six fois plus vite que les faits réels sur internet. La viralité dépasse la vérité. Le sentiment d'appartenance à un groupe, possédant des idées, sentiments ou valeurs similaires est également un puissant moteur pour rassembler sous un même thème des individus dispersés. L'impression d'avoir raison est encore plus forte. Le fait que les hommes n'aiment généralement pas avoir tort et détestent encore plus qu'un tiers leur démontre leurs erreurs accentue la difficulté de rétablir la vérité[53].

Des « monarques » émergent sur la Toile qui savent jouer de la psychologie humaine, séduire un vaste auditoire et confisquer les débats à leur profit. Le phénomène d'hyper-concentration à l'œuvre dans l'essor des plates-formes se retrouve ici. Une étude sur 330 millions d'utilisateurs chinois de Weibo a montré que moins de 200 000 membres avaient plus de 100 000 *followers*, et que seuls 3 000 d'entre eux étaient suivis par plus d'un million d'individus. Les opinions se forment essentiellement à partir des messages émis sur seulement 300 comptes[54].

Ces principes ont été déclinés de plusieurs façons par des entrepreneurs politiques. Le Mouvement 5 étoiles en Italie a connu une expansion rapide et a conquis le pouvoir grâce à Gianroberto Casaleggio, véritable expert du marketing sur internet. Il s'est appuyé sur l'image populaire et sympathique de Beppe Grillo, comique italien critique des partis politiques traditionnels, en lui proposant de rédiger les billets de son

52. *Ibid.*, p. 7.
53. *Ibid.*, p. 118-147 pour ce paragraphe.
54. P. W. Singer et E. T. Brooking, *Like War: The Weaponization of Social Media*, New York, Houghton Mifflin Harcourt, 2018, p. 130.

blog. En l'espace de deux ans, le blog de Beppe Grillo est devenu l'un des dix blogs les plus lus dans le monde. Les réactions des Internautes étaient scrutées et analysées. Les thèmes les plus *likés* étaient repris et développés. L'objectif était bien de capter l'attention des internautes et de les fidéliser en leur offrant ce qu'ils souhaitaient. Le passage au monde réel et à la compétition politique s'est fait en conservant le même principe. Il fallait toujours déceler, valoriser et entretenir les croyances de la population, mais aussi proposer une raison simple et consensuelle pouvant expliquer la cause de leurs frustrations. L'explication trouvée en Italie fut la faillite des élites. Bien que très sommaire, ce « narratif » permit de souder diverses communautés aux sensibilités politiques très diverses, voire contradictoires. Chacune estimait que sa situation était le résultat de la gestion catastrophique du pays par un personnel politique constitué d'incapables[55].

Des variations existent dans cette forme renouvelée de la propagande. Moscou joue moins sur le populisme qu'il ne cherche à agrandir des fractures sociales et profiter des crises quand elles apparaissent[56]. Daech préférait une approche plus décentralisée et recourait à un système de propagande redondant dans plusieurs langues, avec de multiples relais qui proclamaient l'avènement d'un régime rompant radicalement avec les valeurs occidentales[57].

Les démocraties ont déjà été visées par des interférences étrangères pour influencer la perception et le vote de leurs citoyens[58]. Mais leur vulnérabilité est accentuée par les caractéristiques de la puissance numérique et elles sont souvent désemparées. Identifier, influencer, isoler et opposer des groupes de citoyens dénature le fonctionnement d'un régime fondé sur le consensus. Afficher péremptoirement ces idées est plus efficace que de débattre. Il est désormais question de rejet plutôt que de projet. Plus besoin d'affronter militairement l'adversaire pour lui imposer ses vues. L'ennemi se fragilise seul en se divisant.

La situation actuelle pourrait même empirer avec les avancées technologiques. Les réactions pourront être analysées au travers des expressions corporelles, comme l'observation des visages, pour saisir discrètement l'adhésion ou non des individus à certaines thèses. Des bots seront capables de diffuser automatiquement de fausses nouvelles adaptées

55. G. da Empoli, *Les ingénieurs du chaos*, Paris, JC Lattès, 2019.
56. L. Robinson, T. C. Helmus, R. S. Cohen, *et al.*, *Modern Political Warfare*, *op. cit.*, p. 41-124. B. Jensen, B. Valeriano et R. Maness, « Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist », *tandfonline.com*, 2019.
57. L. Robinson, T. C. Helmus, R. S. Cohen, *et al.*, *Modern Political Warfare*, *op. cit.*, p. 207.
58. E. Wilson, « Don't Call It a Comeback: Foreign Interference in US Elections Has Been here for Years », *War on the Rocks*, 30 juillet 2019.

précisément à leurs cibles. Bref, la compétition internationale s'élargit au champ politique domestique de manière renouvelée, qui tend à brouiller les catégories traditionnelles de la guerre et la sécurité. La puissance numérique pourrait être un facteur d'instabilité de la scène internationale.

Une puissance révolutionnaire ?

La puissance numérique est un formidable atout pour qui sait s'en servir. Elle peut s'exercer au profit d'activités traditionnelles comme la subversion, l'espionnage ou le sabotage pour reprendre la typologie de Thomas Rid. Elle peut contribuer aux opérations militaires aux niveaux tactique, opératif ou stratégique.

Mais la capacité de la puissance numérique à asservir sa cible tout en la satisfaisant, en s'introduisant dans son processus de fonctionnement (cerveau pour les hommes, SCADA pour les systèmes industriels) est probablement sa plus grande force. Elle s'exerce avec le plus d'efficacité dans le domaine des services en économie et au niveau de la guerre politique pour les affaires de défense. Son déploiement correspond alors moins à une tentative de contrainte ou de séduction que de sujétion.

La connectivité entre les individus ou les objets connectés et leur maître est assurée par le réseau. La cible fournit elle-même les conditions de son contrôle en dévoilant de manière asymétrique ses particularités. Ces informations se transforment en savoir et en pouvoir pour peu qu'elles soient traitées et enrichies. La structure algorithmique ou psychologique de la cible devient transparente. L'identification d'une faille dans le système informatique, d'un trait de comportement ou de caractère chez un individu peut causer sa perte. Il suffit de l'examiner et de l'accentuer pour qu'il devienne le maillon faible qui fragilise l'équilibre général de l'édifice.

La puissance numérique pourrait altérer dans l'avenir les formes de la compétition entre acteurs du système international, comme elle l'a fait pour la concurrence économique. Jouer sur la violence et la peur physique pour entamer la volonté de son adversaire pourrait apparaître suranné dans certaines circonstances. Il s'agit moins de contrôler les corps que les cerveaux. La puissance numérique est aussi une puissance de contournement de la violence.

Les composants de la puissance numérique

Peut-on évaluer la puissance numérique ?

Mesurer la puissance numérique revient à se heurter aux mêmes obstacles que dans les démarches de quantification de la puissance classique. Il est d'abord nécessaire de disposer d'un grand volume d'informations. Des chercheurs du Global Cyber Security Capacity Centre de l'université d'Oxford ont déjà entrepris de rassembler ce type de documentation. Les études et les données sont mises en libre accès. Néanmoins, elles risquent de rester toujours incomplètes. Un des critères du succès des cyberattaques est leur discrétion, de sorte qu'il est impossible de s'appuyer sur un état des lieux précis de la réalité dans ce domaine.

Évaluer la puissance numérique réclame ensuite un effort d'analyse, en étudiant le concept selon ses différents champs d'application, que sont la défense, l'économie ou la culture par exemple. Ces champs possèdent à leur tour plusieurs facettes qui doivent être prises en compte[59]. L'exercice de la puissance militaire dans les airs, la mer ou le sol ne réclame pas les mêmes aptitudes. Il en va de même pour la puissance numérique selon qu'elle soit mobilisée pour espionner, saboter ou même participer à des opérations de guerre. Le nombre d'aptitudes peut cependant rapidement devenir imposant selon le degré d'exhaustivité visé, et une telle liste peut perdre de son intérêt.

C'est pourquoi des auteurs comme Joseph Nye[60] ou David J. Betz et Tim Stevens[61] ont préféré sélectionner quelques capacités qu'ils jugent essentielles. Joseph Nye insiste par exemple sur l'importance de pouvoir mener des attaques de déni de service, de dresser des *firewalls*. David Betz et Tim Stevens notent l'importance de la production des normes ou de l'influence des structures internationales. Mais là encore, un effort d'analyse est indispensable pour déterminer les déterminants de ces

59. M. Willett, « Assessing CyberPower », *op. cit.*, p. 87.
60. J. Nye, *Cyber Power*, Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School, mai 2010, p. 5.
61. D. J. Betz et T. Stevens, *Cyberspace and the State: Towards a Strategy for Cyberpower*, New York, Routledge, 2012, p. 45-53.

capacités. Robert J. Bebber, de l'*US Cyber Command*, estime ainsi que 25 domaines contribuent à l'efficacité de la cyberpuissance[62]. L'industrie technologique, les réseaux d'information, les partenariats avec l'étranger, le système d'éducation, le nombre de personnes impliqués dans la cybersécurité et dans l'économie numérique en sont quelques-uns. Pouvoir les apprécier exige un travail minutieux qui dépasse le cadre de cette étude.

Une autre approche consiste à s'inspirer de ce qui existe pour le transposer au monde numérique. Marcus Willett note ainsi que les points communs entre la puissance aérienne[63] et la cyberpuissance sont nombreux[64]. La possession des moyens nécessaires pour protéger son espace souverain et éviter toute action agressive doit être une composante de la puissance aérienne et de la puissance numérique. La capacité à recueillir du renseignement pour apprécier la situation opérationnelle en est une autre. La faculté d'agir dans le monde entier grâce à un réseau de base aérienne ou à la connexion globalisée des acteurs complète ce bref tableau. Il n'existe pas d'études académiques qui classent les différentes armées de l'Air entre elles, mais des critères pourraient être élaborés, comme le nombre d'avions de chasse de 5e génération ou la capacité de mener des raids punitifs à longue distance. Transposés au monde numérique, ces éléments pourraient se comparer à la mise en œuvre des ordinateurs dont les capacités de calcul sont les plus puissantes ou à l'habileté pour pénétrer des réseaux protégés. Des travaux plus complets seraient nécessaires pour juger de l'intérêt d'un tel exercice.

Les déterminants de la puissance numérique

Une autre démarche consiste plus simplement à proposer des capacités à détenir pour agir efficacement dans le cyberespace. Quatre items peuvent être mis en avant.

Créer un écosystème favorable

Le premier item est la capacité à créer un écosystème numérique favorable. Nul acteur international ne possède intrinsèquement les qualités indispensables pour assurer seul son développement. Il doit exploiter l'intelligence collective du réseau pour attendre sa fin. Il doit donc être

62. R. J. Bebber, « Cyber Power and Cyber Effectiveness: An Analytic Framework », *Comparative Strategy*, vol. 36, n° 5, 2017, p. 426-436.
63. Pour approfondir cette notion, lire : John A. Olsen (dir.), *Routledge Handbook of Air Power*, New York, Routledge, 2018.
64. M. Willett, « Assessing CyberPower », *op. cit.*, p. 88-89.

capable de rassembler tous les morceaux de puissance qui sont répandus entre l'ensemble des membres du réseau pour les concentrer entre ses mains. Un acteur devra valoriser l'hybridité de l'écosystème, c'est-à-dire la variété de ses membres qui apporteront chacun une part d'intelligence précieuse, originale, même si elle est parfois inamicale. Il devra aussi savoir gérer la tension suscitée par cette extrême dissémination de la puissance et l'hyper-concentration du pouvoir qu'il tente d'entretenir.

Les plates-formes numériques parviennent à maîtriser cette tension en offrant apparemment des services avantageux à ses clients. Mais l'État a également une carte à jouer. C'est peut-être même l'acteur qui détient le plus de ressources dans ce cadre. Certes, il ne dispose pas des atouts de certains acteurs économiques. Google recrute par exemple régulièrement les meilleurs ingénieurs informaticiens, dispose de l'essentiel des données circulant sur internet et ces algorithmes fonctionnent grâce à une puissance de calcul très forte[65]. Il ne pourra pas se substituer aux entreprises, mais leur déléguera une part d'autonomie pour en bénéficier en retour.

L'État peut ainsi servir de creuset. Il peut soutenir des projets incertains qui seront repris et améliorés par des entrepreneurs privés et contribueront à la richesse nationale. Il peut également investir dans le capital humain et développer des parcours professionnels qui formeront les futurs acteurs de la puissance numérique. Le domaine de la défense peut servir d'incubateur. Le réseau ARPANET, ancêtre d'internet, a une vocation militaire à l'origine. Il devait permettre aux autorités de continuer à pouvoir échanger pendant une attaque nucléaire soviétique. Il bénéficie des apports de la recherche fondamentale menée par des ingénieurs employés par le Département de la Défense. L'unité 8200 de *Tsahal* recrute chaque année des centaines de jeunes cyberopérateurs israéliens qui font face à des attaques sophistiquées et ripostent à leur tour. Ils sont à la pointe de la recherche. Ces jeunes israéliens, une fois démobilisés, se fondent aisément dans le tissu économique local. Ils entretiennent la bonne santé de l'industrie digitale israélienne grâce à leur formation assurée par l'État. L'investissement initial de l'État israélien améliore sa défense et augmente sa richesse.

L'État peut par ailleurs tenir un rôle d'investisseur et de protecteur en favorisant la recherche et la prise de risque dans un environnement financier, légal et culturel adapté. Il peut enfin être un coordinateur dans les domaines humain, technique ou organisationnel, en apportant son expertise ou sa vision quand elles manquent dans le secteur privé.

65. Entretien avec un membre du ministère des Affaires étrangères, le 10 mai 2019.

D'une manière générale, les liens entre le public et le privé doivent être affermis. Entrepreneurs et universitaires doivent pouvoir mieux échanger pour favoriser la recherche appliquée. L'identification des opérateurs d'importance vitale (OIV) renforce en France la sécurité générale des systèmes d'information en imposant la prise de mesures de protection indispensables par la réglementation.

À terme, une division du travail doit clairement s'instituer entre acteurs publics et privés lorsqu'ils collaborent sur des projets étatiques ambitieux. L'État doit rester le donneur d'ordres et énoncer le « quoi ». Le secteur privé élaborera en revanche le « comment ».

Pour assumer ces rôles, l'État doit prendre conscience de l'importance des enjeux liés au numérique et se donner les moyens d'y répondre par une action volontariste[66]. Il doit savoir définir ses intérêts et mobiliser des ressources en énonçant ses priorités. Cette condition est essentielle pour réussir.

Contrôler les données

Le deuxième déterminant de la puissance numérique est celui du contrôle des données. Elles sont au fondement de la richesse numérique. Mais l'enjeu est également politique. Les citoyens fournissent à leurs administrations de nombreuses informations privées. Si elles sont piratées, les conséquences peuvent être dramatiques sur le long terme. Des mutuelles privées qui accéderaient librement aux données médicales des Français pourraient proposer des offres avantageuses à court terme et menacer par exemple la pérennisation de notre système de santé. L'État doit protéger de manière exclusive ce type de données[67].

La localisation des données ou des centres administratifs de ces données sont des enjeux essentiels. Les réflexions sur la mise en place de *data centers* nationaux, les doutes qui subsistent sur l'évaporation éventuelle de données vers l'étranger[68] ou les enjeux liés au développement des *clouds* souverains montrent la sensibilité de ces questions[69]. Elles suggèrent aussi que les rôles sont déjà bien distribués et que la remise en cause de la hiérarchie actuelle imposerait des investissements colossaux.

66. Ce thème revient régulièrement dans les entretiens effectués.
67. Entretien avec un membre du ministère des Armées, le 20 juin 2019. Voir également « La stratégie nationale du renseignement », *sgdsn.gouv.fr*, 15 juillet 2019.
68. A. Cattaruzza, « Quelle souveraineté pour l'espace numérique ? » *in* S. Taillat, A. Cattaruzza et D. Danet, *op. cit.*, p. 84-86.
69. T. Gomart, J. Nocetti et C. Tonon, « L'Europe : sujet ou objet de la géopolitique des données ? », *Études de l'Ifri*, Ifri, juillet 2018.

Tenir les points hauts du cyberespace

La puissance s'exprime également par la capacité à tenir des « points hauts » dans les trois couches du cyberespace. Ces points hauts peuvent être physiques. Les Chinois s'approprient par exemple les terres rares qui sont essentielles pour la fabrique des ordinateurs. Mais ils peuvent aussi dépendre de l'innovation, conceptuelle ou technologique. Les entrepreneurs qui ont porté les GAFAM[70] au sommet avaient une vision avancée par rapport à leurs concurrents. Ils les ont écrasés en imposant leurs solutions. Du point de vue technologique, les plus grandes entreprises numériques mondiales entretiennent des rapports étroits avec les start-ups israéliennes. Celles-ci améliorent sans cesse leurs algorithmes et conservent leurs avantages par rapport à leurs concurrents. Les grands groupes intègrent systématiquement leurs applications dans leurs produits de pointe[71].

Le point haut peut parfois être tenu grâce à la cryptologie. La maîtrise complète du réseau importe peu. Ce sont ses segments stratégiques qui comptent le plus. Ce sont eux qu'il faut défendre grâce au chiffrement. L'architecture globale des systèmes, mis en œuvre éventuellement par des opérateurs étrangers, doit être finement analysée pour identifier les parties les plus utiles ou sensibles. Crypter leur accès permet de conserver sa liberté d'action. Une frontière physique est réinstaurée dans le réseau qui assure une part de souveraineté.

La maîtrise de l'intelligence artificielle (IA) tend à devenir également de plus en plus décisive. Elle donne un sens, qui échappe souvent aux opérateurs, au volume de données en augmentation exponentielle qui circulent sur les réseaux numériques. Les acteurs qui disposeront des modèles les plus compétitifs jouiront d'un avantage cognitif qu'ils pourront exploiter en agissant plus précocement et plus sûrement que leurs rivaux[72].

Le point haut peut enfin être la forme du réseau lui-même. Un acteur peut redessiner son contour en limitant les accès, en contrôlant les interfaces avec une autre part du réseau. Il isole ainsi les usagers et peut surveiller leurs pratiques. Il filtre le contenu des données venant de l'extérieur et impose ses propres règles de fonctionnement.

Ces initiatives coûtent toujours très cher. Des acteurs privés offrent parfois des solutions moins onéreuses pour assurer de tels services, qui peuvent inciter à leur déléguer une part de sa souveraineté. Une telle option est incompatible avec l'exercice de la puissance étatique, qui ne se

70. Google, Apple, Facebook, Amazon, Microsoft.
71. Entretien avec un entrepreneur franco-israélien, le 30 janvier 2019.
72. J.-C. Noël, « Intelligence artificielle : vers une nouvelle révolution militaire ? », *op. cit.*

cède pas. La puissance repose sur une ambition et des moyens. Transiger avec l'un ou l'autre est déjà une cause de déclin.

Articuler la puissance numérique avec les autres formes de puissance

Le quatrième item est essentiel d'un point de vue opératoire. La cyberpuissance est aussi « la capacité d'utiliser le cyberespace pour créer des avantages et influencer les événements dans tous les environnements opérationnels et à travers tous les instruments de puissance[73] ». La puissance numérique n'est qu'une des facettes de la puissance d'un acteur. Elle doit nourrir les autres volets ou parvenir à s'articuler avec eux. À la manière dont la puissance navale a stimulé la puissance britannique, la puissance numérique doit être intégrée dans la grande stratégie d'un État pour livrer tout son potentiel. La puissance numérique des acteurs économiques, bien que forte, reste relative sur la scène internationale puisqu'il lui manque un pan. Elle ne se décline pas dans le domaine militaire dans le cyberespace ou le monde réel.

Il n'existe pas de modèle parfait pour transformer la puissance numérique en puissance globale. Son apport dépend surtout des liens et de la bonne harmonisation qui existent entre les cultures stratégique et économique nationales.

Ainsi, les États-Unis sont peut-être la nation la plus avancée dans ce domaine, mais de larges progrès semblent encore à accomplir[74]. Ils disposent en effet d'atouts dans les domaines économique, militaire, culturel et idéologique. Le modèle de puissance numérique est libéral. Il favorise l'expansion des entreprises et la création de richesses. Les données accumulées profitent indirectement au secteur de la défense. Pour autant, les liens restent ténus entre les compagnies privées et les militaires. La collaboration semble surtout dépendre des arguments financiers du Pentagone.

La Chine est l'autre superpuissance numérique. Reconnaissant l'intérêt économique de cette nouvelle industrie, Pékin considère le numérique comme un domaine primordial dans sa compétition stratégique contre Washington et comme un moyen d'assurer le contrôle politique de sa population[75]. Si l'État chinois est étroitement adossé au secteur privé,

73. D. T. Kuehl, « From Cyberspace to Cyberpower: Defining the Problem » *in* F. D. Kramer, S. H. Starr et L. K. Wentz, *Cyberpower and National Security*, Potomac Books , 2009, p. 38.
74. V. N. Weber, « Linking Cyber Strategy with Grand Strategy: The Case of the United States », *Journal of Cyber Policy*, publié en ligne le 17 août 2018.
75. N. Inkster, « China's Cyber Power », IISS *Adelphi* 456, Routledge, New York, 2016.

il n'hésite cependant pas à sanctionner les entreprises quand elles n'agissent selon la ligne du Parti communiste, préférant la stabilité politique à l'innovation.

Les autres nations sont des puissances numériques plus modestes. Israël est performant dans le domaine économique et militaire, mais s'intéresse moins aux aspects culturels et idéologiques. La Russie, la Corée du Nord ou l'Iran favorisent les actions de nuisance mais peinent à exister économiquement. L'Europe agit essentiellement dans le champ de la régulation en promouvant ses valeurs au travers d'une défense de l'éthique dans le cyberespace, mais peine à disposer de capacités coercitives pour les faire appliquer en toutes circonstances. L'intégration harmonieuse des différents volets de la puissance numérique reste à ce jour un défi pour tous les acteurs étatiques.

Comment le réel influence le virtuel

La riposte militaire

Les effets de la puissance numérique ont été parfois difficilement contenus dans le domaine de la défense et de la sécurité. Pourtant, quelques signes montrent que la situation évolue progressivement.

La cybersécurité se durcit par exemple. La défense s'organise de plus en plus dans la profondeur pour faire échouer les attaques, avec la constitution de labyrinthes dans les systèmes informatiques pour égarer le hacker. La sécurité de ces systèmes est par ailleurs prise en compte dès leur conception. Le rajout de patchs sur les programmes revenait souvent à ravaler la façade des logiciels plutôt qu'à repenser leurs fondements. Leur efficacité était relative. Désormais, des boucliers sont intégrés dans la conception des logiciels, compliquant les phases d'infiltration et d'implantation.

Des progrès sensibles ont également été accomplis dans le domaine de l'identification et de l'attribution des attaques, même si la discrétion entoure ce domaine très sensible. Certes, les preuves évidentes pointant immédiatement l'origine d'une agression restent rares. Le doute subsiste. Mais les experts ont amassé avec le temps de plus en plus d'informations utiles pour discriminer les traces laissées. Le nombre de hackers capables d'agir dans le haut du spectre est limité, même si cette communauté est mouvante. Ils ne prolifèrent pas. Chacun possède un style, privilégie des modes d'action qui sont autant d'indices pour les pister. Le phénomène d'extrême concentration déjà noté pour les plates-formes ou le nombre de bloggeurs influents sur internet peut se transformer en faiblesse[76].

L'attribution publique des attaques demeure une décision politique. Si la France reste prudente, les États-Unis ont décidé de revoir leur politique. Washington, en coopération avec d'autres capitales anglo-saxonnes, a par exemple rapidement attribué en février 2018 le virus *NotPetya* aux équipes

76. Insistons sur le fait que l'ensemble de ces remarques concerne principalement le haut du spectre de la cyberdéfense. Dans le domaine de la cybersécurité, beaucoup d'acteurs disposent de capacités réduites et restent vulnérables aux hordes de hackers sûrement moins doués, mais qui restent assez performants pour améliorer régulièrement leurs modes d'action et menacer le fonctionnement des entreprises à des fins criminelles.

de hackers militaires russes. Le Département de la justice a inculpé huit équipes de hackers chinois, russe, iranien ou nord-coréen en 2018 contre seulement une en 2014[77]. Les conséquences de l'augmentation des *naming and shaming* et des poursuites judiciaires sont à court terme plutôt faibles. L'accusé peut nier les accusations, exigeant des preuves solides de son implication. Néanmoins, à plus long terme, une telle posture pourrait favoriser la coopération entre certains États, accélérer la réflexion sur l'établissement de règles communes dans le cyberespace et nuire à l'image de certains acteurs sur la scène internationale.

Ce volontarisme des États-Unis semble s'étendre dans tous les domaines de la cyberdéfense[78]. Les règles américaines encadrant le déclenchement de cyberopérations offensives deviennent plus lâches. Afin d'endiguer les multiples tentatives de pénétration des réseaux numériques américains, Washington menace de contre-attaquer en neutralisant les systèmes informatiques des assaillants. Le risque d'escalade existe, même si des officiels du Département de la Défense insistent sur le fait qu'un relâchement des règles n'impliquait pas que le cyberespace devienne un Far West[79].

Les formes de la dissuasion dans le cyberespace se dessinent progressivement[80]. La dissuasion, qui désigne l'acte d'empêcher un adversaire d'entreprendre une action, ne saura prohiber toute action dans l'espace numérique. Elle ne peut se concevoir qu'à partir d'un seuil ou d'un volume d'actions. Elle pourrait être organisée à la manière d'une police qui doit s'assurer du maintien de l'ordre dans l'espace public. L'assaillant doit savoir que certains actes seront systématiquement réprimandés en fonction de leur fréquence et de leur portée[81]. Joseph Nye propose par exemple que des tabous normatifs soient définis que les différents acteurs s'engageraient à respecter. Il croit également à la valeur d'une dissuasion par intrication : les intérêts des acteurs dans la sphère numérique sont tellement mêlés qu'une action dans un domaine finirait par nuire à l'attaquant dans un autre domaine du fait des conséquences qu'elle déclencherait[82].

77. K. Charlet, « How the US Approach to Cyber Conflict Evolved in 2018 – and What Could Come Next », *worldpolitics review.com*, 26 décembre 2018.
78. *National Cyber Strategy of the United States of America*, Washington D. C., Maison-Blanche, septembre 2018.
79. K. Charlet, « How the US Approach to Cyber Conflict Evolved in 2018 – and What Could Come Next», *op. cit*.
80. Le lexique stratégique français retient le terme de « découragement » pour marquer la différence avec la dissuasion nucléaire.
81. S. Taillat, « Dissuasion et coercition » *in* S. Taillat, A. Cattaruzza et D. Danet, *La Cyberdéfense : politique de l'espace numérique*, *op. cit.*, p. 144.
82. J. Nye, « Deterrence and Dissuasion in Cyberspace », *International Security*, vol. 41, n° 3, 2017.

Joseph Nye pense que la cyber-dissuasion peut s'exercer entièrement dans le cyberespace. Ce point constitue un des enjeux essentiels de la réflexion des prochaines années. Les Occidentaux ont pour l'instant fait un usage responsable et modéré de leurs capacités numériques et physiques pour gérer la violence dans le cyberespace. Mais leurs réactions pourraient s'étendre de plus en plus au monde réel, que ce soit dans le cadre de la dissuasion, de la coercition ou plus simplement des affaires militaires. En 2015, J. Hussain, un hacker de Daech, a été tué par un drone pour avoir notamment publié en ligne des informations sur du personnel américain[83]. Début mai 2019, un bâtiment accueillant les cyberopérateurs du Hamas a été détruit par une frappe aérienne israélienne pour empêcher une cyberoffensive contre des cibles israéliennes[84]. La réflexion des Occidentaux s'articule plus autour de l'impact et des effets produits par les cyberattaques que des moyens employés pour les mener. Il n'y a plus, selon eux, de déconnexion entre le virtuel et le réel.

Moscou et Pékin réfutent cette approche et accusent les Occidentaux de vouloir militariser le cyberespace. Russes et Chinois souhaiteraient conserver leur liberté d'action et bénéficier des ressources asymétriques offertes par ce milieu virtuel. Ils n'ont aucun intérêt à étendre les affrontements au monde réel, où leur infériorité face aux armées américaines est encore patente. Le coût d'une attaque pourrait devenir prohibitif.

L'avantage que possèdent les attaquants dans le cyberespace est donc en train d'être contesté. Les initiatives prises dans ce domaine pourraient indiquer qu'une nouvelle phase du numérique est en train de s'annoncer.

À la recherche d'une nouvelle régulation

Un mouvement de réaction similaire semble se développer dans d'autres secteurs touchant le numérique. Les États testent plusieurs types de stratégie pour fragiliser l'hyper-concentration de puissance de certains acteurs privés et rééquilibrer le partage des richesses créées par leur développement[85].

Une première posture est la confrontation directe. C'est une des voies que la France a choisies en imposant la taxe GAFA, avant que l'Organisation de coopération et de développement économiques (OCDE) ne s'empare de cette initiative. Le manque d'enthousiasme d'autres pays

83. Z. Doffman, « Israel Responds to Cyber Attack with Air Strike on Cyber Attackers in World First », *forbes.com*, 6 mai 2019. Je remercie B. Pajot de m'avoir alerté sur cet événement.
84. *Ibid.*
85. Entretien avec un membre du ministère des Affaires étrangères, le 12 juillet 2019.

européens, les risques de délocalisation fiscale des entreprises ou de rétorsion par l'administration américaine montrent que le succès d'une telle mesure n'est pas assuré. D'autres expressions plus radicales de cette stratégie ne sont cependant pas à négliger dans le temps. La promulgation d'une loi *anti-trust* aux États-Unis pourrait défaire les plates-formes numériques et réintroduire de la concurrence là où elle a disparu[86].

Une variation de cette posture est la création de champions nationaux ou continentaux qui entreront en compétition avec les entreprises déjà en place. Le moteur de recherche français *Qwant*, dont l'une des caractéristiques était de ne pas tracer ses utilisateurs, en est un exemple. La volonté de promouvoir un champion européen dans la course à la 5G en est un autre. Suivre cette voie est cependant très difficile, compte tenu des rentes de situation que possèdent déjà les grandes plates-formes. Le prix d'entrée est très élevé pour des chances de succès discutables.

La « régulation douce » est une autre option. L'Union européenne (UE) la poursuit avec la mise en place du Règlement général sur la protection des données (RGPD). Le RGPD est une loi extraterritoriale qui permet d'imposer des normes correspondant aux valeurs défendues par l'UE dans le cyberespace. Les intérêts des citoyens de l'UE sont défendus quel que soit l'endroit du monde d'où ils se connectent. L'individu conserve la souveraineté de ses données en consentant à les partager et en recevant l'assurance qu'elles seront protégées. La faillite, même non intentionnelle, à ce principe peut coûter cher aux entreprises. *British Airways* a été sanctionné à hauteur de 200 millions d'euros, après avoir été victime d'un piratage informatique qui avait aspiré les données financières d'environ 500 000 de ses clients[87].

Une dernière possibilité est de coopérer avec les plates-formes pour fixer des modes de fonctionnement agréés de tous. Le rapport sur la mission de régulation des réseaux sociaux, dite « Mission Facebook », menée par Benoît Loutrel en est un exemple[88].

La société civile ne reste pas inactive de son côté. Les sites d'*Open Source Intelligence* (OSINT) produisent des résultats impressionnants qui stigmatisent l'action de compagnies privées ou des États. *Bellingcat* est l'un d'entre eux. Ses membres sont parvenus à démontrer l'implication de la Russie dans la destruction du vol MH 17 de la *Malaysian Airlines* au-dessus de l'Ukraine malgré les dénégations répétées de Moscou[89].

86. « Domestiquer les géants du numérique », *Le Monde*, 12 septembre 2019.
87. D. Filippone, « Violation RGPD : une amende de 200 M d'euros pour British Airways », *Le Monde Informatique*, 8 juillet 2019.
88. « Régulation des réseaux sociaux-Expérimentation Facebook », *economie.gouv.fr*, mai 2019.
89. W. Singer et E. T. Brooking, *Like War: The Weaponization of Social Media*, *op. cit.*, p. 71-77.

Travaillant en toute transparence en exploitant les données mises à disposition de tous sur internet, les OSINT peuvent de nos jours recueillir et traiter les informations d'une manière plus efficace que ce que la CIA ou le KGB pouvaient faire il y a encore une génération[90].

Il est encore trop tôt pour dire si de telles pratiques annoncent une nouvelle forme de participation politique des citoyens poussant à la transparence ou si les initiatives étatiques vont freiner l'expansion des grandes plateformes numériques. La défense des valeurs ne suffit pas toujours quand elle n'est pas soutenue par des capacités d'action politiques ou militaires avérées. Néanmoins, ces tentatives d'instaurer une autre logique dans le cyberespace montrent que le sens de l'histoire s'inverse peut-être et que le réel tente de plus en plus de s'imposer dans le monde virtuel.

Technologies numériques et cycle économique

Pour mieux saisir la transformation de l'ancienne dynamique, il est stimulant de changer d'échelle et de considérer l'avènement du numérique comme une révolution technologique, à l'image de la révolution industrielle, ou de l'introduction plus récente de la vapeur, de l'acier et du pétrole dans les cycles de production.

Les travaux de Carlota Perez consacrés à l'impact des technologies sur les cycles économiques offrent à ce titre un modèle pouvant rendre compte des évolutions actuelles[91]. Elle montre que ces révolutions technologiques engendrent des cycles comportant régulièrement deux phases séparées par un point d'inflexion. Dans la première phase, la nouvelle technologie prend progressivement la place d'une autre, plus ancienne. Ses applications sont nombreuses et séduisantes, et les retours sur investissement sont importants. L'enthousiasme des inventeurs entretient une créativité débridée. Cette exaltation est partagée par les entrepreneurs tentant de satisfaire leur *hubris* et les financiers à la recherche de gains faciles et immédiats. Ces derniers captent l'essentiel de la richesse, dominent la scène et multiplient des bulles de prospérité reposant sur des bases fragiles.

Cette période d'euphorie s'arrête soudainement quand ces bulles explosent, provoquant une récession. C'est le moment du point d'inflexion, correspondant à la période où les intérêts privés et les intérêts collectifs

90. *Ibid.*, p. 75.
91. C. Perez, *Technological Revolutions and Financial Capital: The Dynamics of Bubbles and Golden Ages*, Cheltenham, Edward Elgar, 2003.

s'affrontent pour trouver un nouvel équilibre. La durée de cette étape est variable et dépend des rapports de force entre les différents acteurs impliqués dans le contrôle de la technologie.

Ce point d'inflexion annonce généralement une seconde phase, appelée « âge d'or » par Carlota Perez, quand ce rapport de force s'est stabilisé dans le sens de l'intérêt général. Le contrôle des investissements devient plus institutionnel et passe du côté des industriels, soutenus par les autorités étatiques. Les applications technologiques sont encadrées et régulées pour que la prospérité soit mieux partagée. Cet âge d'or se terminera avec l'émergence de nouvelles technologies.

Nous traverserions actuellement la période du point d'inflexion. Le volontarisme de la superpuissance américaine dans le domaine de la défense en est un indice. La recherche de solutions pour maîtriser les GAFAM ou les initiatives de la société civile pour imposer plus de transparence en sont d'autres. La puissance numérique est une puissance qui pourrait être contenue dans l'avenir.

Vers un morcellement plus prononcé ?

Les cycles économiques ne mettent toutefois pas fin à la compétition internationale. Celle-ci demeure avec des acteurs divisés, soutenant des approches opposées sur la géographie et la gouvernance du cyberespace. Certains, comme la Chine ou la Russie, considèrent le cyberespace en termes hobbesiens. Ils refusent l'anarchie et l'autorégulation qui régneraient sur le Web, sources de désordre. Ils soutiennent une gouvernance étatique, seule capable selon eux de faire respecter les notions de souveraineté et de sécurité, aux fondements d'un ordre international harmonieux. L'organisation de l'Union internationale de télécommunications est leur modèle. Le problème est que cette recherche effrénée de l'ordre peut cacher des formes d'autoritarisme beaucoup plus pervers, qui sape le fonctionnement actuel du monde numérique.

D'autres, comme les pays anglo-saxons, préfèrent une approche plus décentrée. Ils souhaitent que l'ensemble des acteurs du monde numérique puissent contribuer à son fonctionnement. Si chacun participe à la fabrication des normes, des règles, des sanctions autour d'une table de négociations, il sera plus enclin à les respecter. La légitimité et l'autorité des institutions de régulation n'en seront que meilleures. L'affaire Snowden, qui a montré la collusion d'intérêt entre les États-Unis et certains acteurs privés, a cependant affaibli cette vision.

Aussi le risque de partition du cyberespace est réel. Il est même en train de se fragmenter si l'on considère que les internets russe et chinois sont en partie déconnectés du réseau mondial. La puissance numérique pourrait se morceler. La gouvernance de l'espace numérique pourrait varier selon les zones et se déterminer à l'avenir entre des organisations régionales regroupant des États aux régimes politiques similaires. Un des moyens de sauvegarder certaines règles internationales communes peut être de chercher à produire des normes sur des domaines limités et restreints, comme le droit intellectuel par exemple, sans grands enjeux stratégiques immédiats[92]. La tendance semble cependant être à la constitution de deux espaces numériques différenciés[93]. L'opposition classique en géopolitique entre un *Heartland* et un *Rimland*, entre une partie finie, fermée sur elle-même et une autre plus ouverte, qui l'entoure, pourrait retrouver une nouvelle jeunesse[94]. Son issue reste toutefois incertaine.

92. S. Patrick, « The Unruled World: The Case for Good Enough Global Presence », *Foreign Affairs*, vol. 93, 2014, p. 58-73.
93. Entretien avec un membre du ministère des Affaires étrangères, le 5 juillet 2019.
94. N. Spykman, *Geography of the Peace*, San Diego, Harcourt, Brace and Company, 1944.

Conclusion

La puissance numérique est un objet complexe et multiforme. C'est une puissance à la fois classique et réticulaire, émancipatrice et asservissante, partagée et morcelée, asymétrique et contenue, fragile et éphémère mais qui peut contourner les obstacles. Elle continue d'évoluer à mesure que les hommes imaginent de nouvelles pratiques.

Son avenir dépendra d'abord du développement de nouvelles applications technologiques. L'intelligence artificielle jouera un rôle déterminant. L'automatisation de certaines tâches pourrait s'accentuer, obligeant à repenser le rapport entre l'homme et la machine, entre l'espace numérique et le réel[95]. La puissance de calcul des ordinateurs pourrait changer d'échelle avec l'informatique quantique. Le chiffrement des logiciels, qui est une des solutions privilégiées actuellement pour protéger les systèmes informatiques, pourrait être aisément défait. L'imprimerie 3D pourrait révolutionner le mode de production des objets et augmenter le pouvoir des individus. Les nanosciences vont accélérer la miniaturisation du monde.

Les formes de la puissance numérique dépendront aussi de choix politiques. À court terme, le concept encore flou d'identité numérique va probablement déclencher des controverses. Les hommes sont déjà identifiés par leurs empreintes digitales ou des spécificités biologiques. Les données individuelles qu'ils partagent sur les réseaux pourront-elles fonder à terme une identité numérique ? Réguler l'usage de ces données sera indispensable. Un opérateur qui a accès à ces données pourra numériser le passé d'un homme et anticiper son avenir en extrapolant les connaissances[96]. Celui qui possède ces données pourra même les contrefaire ou les effacer, condamnant l'individu à une mort virtuelle. Le droit à l'oubli… et au souvenir sur internet pourrait devenir deux droits fondamentaux. Mais comment les ordonner ? À plus long terme, d'autres débats comme l'avènement programmé de l'homme augmenté deviendront sûrement inévitables.

95. J.-C. Noël, « Intelligence artificielle : vers une nouvelle révolution militaire ? », *op. cit*.
96. P. Bellanger, *op. cit,* p. 101.

Institut français
des relations
internationales