Histoire et géopolitique de l'Internet. Une généalogie de la guerre cognitive.

Henri ISAAC, Université Paris-Dauphine, PSL, DRM CNRS UMR 7088

Conférence du 25 octobre 2022

Université de Montréal, Chaire LexUM en information juridique

Table des matières

Histoire et géopolitique de l'Internet. Une généalogie de la guerre cognitive.....1

Préambule.....3

Introduction.....5

De la Seconde Guerre Mondiale à la Chute du Mur de Berlin (1942-1989) : émergence du réseau Internet.....7

Aux origines de l'Internet et du monde numérique.....7

Vannevar Bush et le Memex.....7

La cybernétique, fondement du monde numérique.....7

L'ordinateur, conséquence des programmes militaires de la Seconde Guerre Mondiale.....8

L'ordinateur en réseau : menace soviétique et émergence progressive de l'Internet aux Etats-Unis pendant la Guerre Froide.....9

La chute du Mur et les autoroutes de l'information : nouvel espace, nouvelle frontière, nouvelle gouvernance (1989-2001).....11

La révision de la doctrine géostratégique américaine.....11

Le World Wide Web devient américain.....13

Les autoroutes de l'information, un discours pour propager le World Wide Web.....14

L'Internet repose sur une gouvernance contrôlée par les Etats-Unis.....15

Le retour de l'Histoire et le déploiement de la guerre cognitive : terrorisme, émergence chinoise, retour russe, comment l'Internet est devenu un espace de conflictualités entre puissances mondiales (2001-).....16

Vers la fragmentation de l'Internet, le Splinternet.....17

La Russie et la souveraineté de l'espace numérique russe.....18

La montée des tensions : la guerre sino-américaine dans l'Internet et les technologies de communication.....19

Internet et la guerre cognitive.....20

Les contours de la guerre cognitive.....21

La guerre par Internet.....23

La guerre sur Internet.....24

La guerre informationnelle : désinformation, fuite d'informations, fausses informations.....24

La rivalité technologique au-delà de l'Internet.....26

La guerre pour le contrôle des infrastructures.....26

Le contrôle des micro-processeurs et de la puissance de calcul.....28

La maîtrise de la sécurité des communications et la course à l'ordinateur quantique.....28

Conclusion.....29

Bibliographie.....31

« *… et l'Histoire reprend ses droits, montrant combien ces « guerres cognitives » se préparent de longue haleine, et se gagnent sur la durée. Entre l'instantanéité de la technologie, panoptique, discriminatoire, omniprésente ; et la construction lente et patiente de capacités cognitives supérieures, la polémologie des conflits futurs est riche et pleine de défis.* » P. Baumard, 2002.

Préambule

N'étant ni historien, ni spécialiste de géopolitique, il faut donc considérer mon propos comme celui d'un spécialiste du numérique qui depuis longtemps s'intéresse à ses origines historiques. Étant également investi dans les débats de politique publique du numérique au niveau français et européen depuis de nombreuses années, j'ai pu mesurer l'importance des enjeux géopolitiques des questions relatives au numérique, particulièrement depuis l'entrée en vigueur du Règlement général sur la protection des données (RGPD), premier texte eurpoéen à portée extraterritoriale qui a accru les tensions américano-européennes sur les questions numériques. De nombreux faits récents en attestent encore, comme les discussions transatlantiques entre la Commission européenne et l'administration américaine à propos de l'invalidation du *Privacy Shield* à la suite de l'arrêt de la Cour de Justice de l'Union européenne (CJUE) dit Schrems II, les propositions récentes américaines et le contexte énergétique singulier de l'Europe depuis ces discussions. Les tensions géopolitiques sino-américaines sur la question technologique se sont brusquement renforcées ces dernières années avec l'interdiction des équipements Huawei aux Etats-Unis, la tentative d'interdiction de TikTok, et plus récemment le CHIPS Act.

Faire l'histoire de cette géopolitique nécessite de fournir un découpage historique qui fasse sens. C'est donc une approche diachronique[1] que j'ai retenue pour cette conférence. On aurait pu préférer une approche diatopique, considérant que la recomposition des espaces par l'Internet est un sujet central de sa contribution à la reformulation des enjeux géopolitiques. Mais l'approche historique permet selon moi une mise en perspective unique d'enjeux géopolitiques dont il faut comprendre l'origine. Aussi, je voudrais réinterroger la question des origines souvent débattue dans les recherches sur l'histoire d'Internet (Brügger & alii, 2017). Si l'on s'en tient à l'origine d'Internet, beaucoup la date à celle des débuts du réseau ARPANet, c'est-à-dire à la fin des années 1960 et au contexte de la Guerre Froide (Abbate, 2003 ; Hafner & Lyon, 1996 ; Paloques-Bergès, Schaffer, 2019). Compte-tenu de la perspective suggérée pour cette conférence, j'ai opté pour un début plus ancien, je m'en expliquerais, en choisissant de dater les débuts d'une réflexion qui est le fruit d'un contexte géopolitique très particulier, celui de la Seconde Guerre Mondiale. J'espère vous convaincre de mon choix de découpage des périodes de cette histoire en cours. J'ai conscience que certains historiens de l'Internet pourraient questionner ce choix. Mais si l'on s'intéresse à la géopolitique de l'Internet, je trouve intéressant que l'on se penche sur le contexte géopolitique qui a produit les idées qui ont contribué à son émergence. Tant d'erreurs ont été

[1] En suivant Yves Lacoste dans les trois approches du sujet géopolitique

véhiculées sur le choix de l'architecture ARPANet, nourrissant des interprétations erronées de son origine.

S'intéresser à la géopolitique de l'Internet, c'est également s'intéresser aux autres enjeux géopolitiques dans lesquels la question de l'Internet s'insère ou trouve un rôle particulier. Dès lors, cette histoire doit tenir compte des enjeux géostratégiques majeurs pour mieux comprendre en quoi, l'Internet est devenu à la fois un champ spécifique des rivalités des grandes puissances mondiales et à la fois un instrument particulier pour atteindre d'autres objectifs géopolitiques. A cet égard, il n'est jamais simple de dégager ces objectifs géopolitiques, tant ceux-ci se sont multipliés dans les deux dernières décennies avec l'avènement de la puissance chinoise et des nombreuses rivalités régionales qui se sont faites jour dans un monde plus multipolaire que jamais.

Mais au-delà de cette histoire, quel qu'en soit le découpage historique que l'on retient, c'est la modification profonde que le projet cybernétique a introduit dans la société qui doit être analysée à l'aune des rivalités géopolitiques classiques. C'est la transformation de la nature de la guerre qui est à l'œuvre avec des acteurs nationaux s'appuyant sur l'espace informationnel et cognitif pour bâtir des stratégies de domination spécifiques. A mesure que nous développpons nos usages de l'Internet (Web 1.0, Web 2.0, IoT), nous développons une prothèse cognitive comme l'analysait Michel Serres dès 2007[2]. Avec les révélations d'E. Snowden sur l'ampleur des programmes et disposotifs de surveillance des communications électroniques, la prise de conscience de nombreux Etats a accéléré la transformation des rivalités dans cet espace devenu une arène des rivalités des puissances mondiales et régionales.

[2] M. Serres, Conférence 40 ans de l'INRIA, https://www.youtube.com/watch?v=ZCBB0QEmT5g

Introduction

Le développement d'Internet est souvent présenté dans les récits des origines comme un projet, qui possède des origines militaires. On évoque alors l'épisode ARPANet. Cependant le récit se nourrit surtout de nombreux récits sur les pionniers, les premières communautés d'utilisateurs en ligne, parfois c'est un récit sur les cypherpunks (Jarvis, 2022), ou les hackers et autres profils innovants qui est mis en évidence afin de souligner la dimension profondément libertaire et libératrice de l'Internet. Ce discours dominant masque des origines différentes, plus anciennes, qui s'ancrent dans la transformation que les Etats-Unis ont connu au cours de la Seconde Guerre Mondiale et qui ont durablement établi la puissance de cette nation dans l'ordre mondial jusqu'à aujourd'hui. Ce discours occulte *de facto* la dimension stratégique d'Internet qui s'est progressivement construite entre 1945 et 1990 pour devenir un axe majeur de la politique mondiale américaine et un instrument essentiel de sa puissance économique et militaire.

Le développement de l'Internet auprès du grand public débute dans la dernière décennie du XXème siècle. Il est concomitant d'un nouvel ordre mondial caractérisé par l'effondrement du bloc soviétique et la fin de la Guerre Froide, ce que d'aucun qualifie « la fin de l'Histoire » (Fukuyama, 1992). Internet est alors présenté comme un moyen de réaliser une utopie démocratique mondiale et le moyen de faire advenir la société de la connaissance. Robert Cailliau et Tim Berners-Lee, co-inventeurs du World Wide Web en 1990, contribueront largement à propager cette ambition d'une société ouverte de la connaissance grâce à la connectivité généralisée des documents et des individus, s'inscrivant parfaitement dans la vision historique de Vannevar Bush et de Ted Nelson.

Le World Wide Web est alors pensé comme un nouvel espace de libertés qui ne peut être approprié par les États, qui dès 1996, aux Etats-Unis (*Telecommunication Act*), tentent de le réguler. La *Déclaration d'indépendance du cyberespace* de John Perry Barlow (1996) exprime à cet égard que l'Internet est un espace où les États ne doivent pas s'immiscer et doivent laisser libres les utilisateurs. Cette vision contribue à forger l'idée qu'une cinquième dimension s'ajoute aux espaces stratégiques traditionnels, terre, air, mer et que l'espace numérique est un espace qui échappe aux États.

Ces utopies, qu'elles visent la liberté ou la connaissance universelle, se heurtent cependant à d'autres visions qui renvoient à l'origine des technologies qui ont permis l'émergence de l'Internet.

Les racines de l'Internet trouvent leurs origines dans la pensée cybernétique qui naît au cœur du conflit de la Seconde Guerre Mondiale. Il est intéressant de se pencher sur ces origines plus anciennes que celles généralement retenues (ARPANet), car elles incarnent une ambiguïté fondatrice éclairante pour comprendre comment cette connectivité sera instrumentalisée par les États, au premier rang desquels les Etats-Unis, dans leur rivalité avec l'Union Soviétique, puis dans le monde post-soviétique après la chute du Mur de Berlin.

Une dualité d'origine qui porte en elle l'instrumentalisation actuelle du numérique par les États dans leur volonté de puissance.

Cependant, si la progression de cette connectivité de l'humanité – 4,9 milliards d'humains sont connectés à Internet en 2021[3], trouve son origine aux Etats-Unis, en partie grâce à plusieurs inventions européennes (UDP, URL, http, HTML), nous y reviendrons, elle se trouve désormais confrontée à des visions et des usages très différents de ceux imaginés par les fondateurs de ces technologies.

La Chine, la Russie, l'Inde en autres, réagissent à cette expansion réticulaire, car ils ne perçoivent pas celle-ci comme une libération quelconque mais plutôt comme une menace, politique, culturelle et économique. Rapidement, plusieurs visions de l'Internet s'affrontent et les puissances chinoise et russe en développent des visions alternatives de la vision originelle américaine, conduisant à une fragmentation progressive de l'Internet, le « Splinternet ».

De facto, Internet est devenu un espace de plus en plus central de conflictualités géopolitiques. Les Etats ont en effet développé des composantes militaires pour se défendre ou attaquer une puissance étrangère ou des groupes rattachés à celle-ci, dans l'espace numérique. Cyberattaques, cyberdéfense et cyberguerre sont désormais du vocabulaire que l'on apprend dans les écoles militaires. Mais celle-ci est souvent comprise comme une attaque de personnes physiques (usurpation d'identité, compromission, rançon) ou morales (entreprises, établissements publics, infrastructures). Sans nier l'importance et le développement croissant de cette conflictualité bien réelle, il faut comprendre que l'Internet est devenu le lieu d'une guerre cognitive (Baumard, 1997) qui a transformé la notion même de guerre, puisque cette conception place l'action militaire comme un élément d'un ensemble d'actions plus vastes (Encel, 2022 ; Galeotti, 2022). Le développement d'une infrastructure informationnelle mondiale a constitué une rupture dans les logiques d'affrontement en offrant un espace et des ressources nouvelles aux nations pour tenter d'imposer leur domination.

[3] Source: ITU

De la Seconde Guerre Mondiale à la Chute du Mur de Berlin (1942-1989) : émergence du réseau Internet

Aux origines de l'Internet et du monde numérique

L'idée d'une connectivité entre documents naît à la fin du programme scientifique et industriel américain de la Seconde Guerre Mondiale en la personne de Vannevar Bush. La Seconde Guerre Mondiale est également le moment des prémices de la cybernétique avec les conférences de Macy (1942-1953) qui déboucheront, en autre, sur le livre de Norbert Wiener – *Cybernetics* (1948) - et les premières ébauches de ce qui sera par la suite, nommé intelligence artificielle, dont les développements récents reposent sur les données rendues disponibles par le réseau Internet.

Vannevar Bush et le Memex

Vannevar Bush a dirigé le programme scientifique américain pendant la Seconde Guerre Mondiale. En 1940, il est chargé de l'organisation du nouveau « National Defense Research Committee » (NDRC) voulu par le Conseil de défense nationale et le président Franklin D. Roosevelt. En 1941, Bush prend la tête du OSRD et devient le maître d'œuvre de la recherche scientifique des États-Unis en guerre, avec d'importants effectifs, environ 6 000 scientifiques. Il sera une des têtes pensantes du projet Manhattan qui conférera l'arme atomique aux États-Unis. Cette structure de coordination scientifique à vocation militaire est l'ancêtre de l'ARPA (1958) puis de la DARPA (1972) qui portera le projet ARPANet, ancêtre d'Internet jusqu'en 1983.

Vannevar Bush est une incarnation de ce que l'on dénomme, à la suite d'Enseinhower, le complexe militaro-industriel américain, dans lequel il occupera de nombreux postes jusqu'en 1955, qui articule financement de la recherche académique fondamentale, des programmes expérimentaux, de la coordination de différents travaux entre composantes des armées, et des programmes industriels spécifiques. Vannevar Bush au cours de cette période est confronté à d'innombrables défis scientifiques, de coordination des connaissances, des équipes.

Dans un article publié en 1945 - « *As We May Think* » - dans la revue « The Atlantic Monthly », il décrit une machine liée à une bibliothèque capable d'afficher des livres et de projeter des films. Cet outil est aussi capable de créer automatiquement des références entre les différents médias. Le memex permettrait aussi à l'utilisateur de créer des informations, comme ajouter des photos ou du texte sur un microfilm à partir d'un écran tactile semi-transparent. Le memex apparaît aujourd'hui comme une vision qui préfigure l'Internet tel qu'il a pu se développer de nos jours.

La cybernétique, fondement du monde numérique

La Seconde Guerre Mondiale est l'occasion d'un débat intellectuel intense aux Etats-Unis ou dès 1942 des chercheurs issus de nombreuses disciplines scientifiques s'interrogent sur l'avenir de

l'Homme à l'aune des avancées scientifiques. Des ponts sont ainsi établis entre biologie, sciences sociales, physique et bien d'autres champs théoriques. Parmi les réflexions issues de ces travaux, Norbert Wiener publie en 1948 *Cybernetics* qui ouvre la voie à la modélisation et la gestion de systèmes complexes et à leur matérialisation dans des systèmes d'information au sein des organisations.

Le neurophysiologiste Warren McCulloch affirme qu'il incombe aux scientifiques de construire un ordre social avec suffisamment de rétroaction cybernétique pour empêcher un prochain holocauste mondial, possiblement final et total[4].

On mesure donc l'ambition initiale, bâtir une méta-science qui permet une nouvelle ère, dans laquelle on évitera les conflits destructeurs par une meilleure gouvernance des sociétés humaines grâce à la cybernétique. Le contrôle d'une couche informationnelle par le bais de systèmes d'information est donc envisagé comme le moyen d'empêcher une destruction de l'humanité. Les conditions de son émergence, totalement marquée par les traumatismes de la destruction à l'œuvre au cours de la Seconde Guerre Mondiale sont bien présentes à l'esprit de Norbert Wiener, qui explique que la cybernétique que lui et ses collègues ont développée impose « *great possibilities for good and for evil. We can only hand it over into the world that exists about us, and this is the world of [the German death camp] Belsen and Hiroshima.* ». Wiener est donc conscient dès le début de la crête étroite sur laquelle la cybernétique avance et son potentiel de contrôle autoritaire de l'être humain.

Le monde franchit donc une étape dans sa mathématisation, tendance pluri-séculaire. La mise en données du monde est envisagée comme le moyen de créer une harmonie humaine grâce au pilotage des comportements humains en accédant à une couche informationnelle, envisagée comme le moyen par lequel on les oriente.

La concrétisation du projet cybernétique s'appuiera sur des machines intelligentes, l'ordinateur, dont l'origine est totalement déterminée par les enjeux scientifiques de l'effort de guerre américain. Si les principes de la machine générale sont posés dès 1937 par Turing, sa matérialisation dans l'ordinateur moderne repose sur la vision portée par Von Neumann, Shannon et les cybernéticiens.

L'ordinateur, conséquence des programmes militaires de la Seconde Guerre Mondiale

Pendant la Seconde Guerre Mondiale, Shannon travaille pour les services secrets de l'armée américaine, en cryptographie, chargé de localiser de manière automatique dans le code ennemi les parties signifiantes cachées au milieu du brouillage. Son travail est exposé dans un rapport secret (déclassifié dans les années 1980 seulement), qui donne naissance après-guerre à un article, *A Mathematical Theory of Communication* (1948). C'est un apport fondamental à l'avènement

[4] Warren S. McCulloch, "A Recapitulation of the Theory, with a Forecast of Several Extensions," Annals of the New York Academy of Sciences 50, no. 4 (1948): 264.

de l'informatique puisque la codification de l'information permettra la technologie de la machine intelligente, l'ordinateur, que nous connaissons.

Von Neumann, mathématicien juif d'origine hongroise, participe activement au projet Manhattan et à la mise au point de l'explosion de la première bombe atomique. Il est reconnu comme l'un des contributeurs fondamentaux à l'émergence de l'ordinateur auquel il apporte une architecture logique toujours à l'œuvre de nos jours.

La Seconde Guerre Mondiale fait émerger aux Etats-Unis une articulation singulière entre la science, l'industrie et l'État, ce qu'Einsenhower nommera le « complexe militaro-industriel » en 1961[5]. L'extraordinaire effort de mobilisation de la nation américaine s'accompagne d'une vision scientifique entièrement nouvelle, la cybernétique, dont les principales idées mettront un demi-siècle à se concrétiser grâce notamment aux budgets militaires liés à la Guerre Froide. C'est au cours de cette période que les Etats-Unis bâtiront l'essentiel de l'architecture de l'Internet.

L'ordinateur en réseau : menace soviétique et émergence progressive de l'Internet aux Etats-Unis pendant la Guerre Froide

Le projet cybernétique se déploie lentement mais sûrement au cours de la Guerre Froide, période au cours de laquelle des avancées technologiques majeures permettent de concrétiser les idées de la cybernétique en établissant un réseau mondial d'ordinateurs, Internet.

Deux logiques de recherche cohabitent durant les années 1950 jusqu'au début des années 1990. Un premier champ de recherche et d'applications travaille à connecter des ordinateurs entre eux dans un contexte où la puissance de calcul est rare et coûteuse. Un second champ distinct se préoccupe de l'accès à l'information et à la connaissance. C'est la fusion de ces deux logiques qui conduira au World Wide Web du début des années 1990.

Les Etats-Unis et principalement les forces militaires développent un système de détection et de défense anti-aérienne pour se prémunir d'une attaque atomique soviétique. Dans ce contexte particulier, la mise au point d'un système d'alerte et de riposte nécessite de déployer un réseau de communication et de commandement sur le territoire américain. Ce sont les projets SAGE, Semi-Automatic Ground Environment (*SAGE*) et SABRE qui reposeront sur les réseaux téléphoniques et constituent une sorte d'ancêtre de réseaux interconnectés.

Joseph Licklider, qui travaille pendant la Guerre Froide sur le projet énonce pour la première fois des idées relatives à un réseau global d'ordinateurs en 1962, dans une série d'articles traitant du concept de réseau galactique. Ces idées englobaient déjà presque tout ce qu'Internet est aujourd'hui. L'article *L'ordinateur comme outil de communication*, dans *Science and Technology* en avril 1968, illustre sa vision des applications en réseau.

[5] https://en.wikipedia.org/wiki/Eisenhower%27s_farewell_address

Les forces militaires américaines développent ensuite ARPAnet (Advanced Research Projects Agency Network) qui est l'acronyme du premier réseau à transfert de paquets de données conçu aux États-Unis par la DARPA. Le projet fut lancé en 1962, mais ARPAnet ne vit le jour qu'en 1969. Sa première démonstration officielle date d'octobre 1972. Rapidement, de nouveaux raccordements sont ajoutés au réseau, portant le nombre de « nœuds » à 23 en 1971, puis à 111 en 1977.

En 1974, le protocole TCP/IP est créé pour uniformiser le réseau, mais ne sera adopté qu'en janvier 1983 par ARPAnet. Développé par B. Kahn et V. Cerf, avec des idées de L. Pouzin et H. Zimmerman, TCP/IP deviendra le protocole fondamental d'Internet.

En 1980, ARPAnet se divise en deux réseaux distincts, l'un militaire (MILNET qui deviendra le Defense Data Network, DDN) et l'autre, universitaire (NSFnet), que les militaires abandonnent au monde civil. En 1984, DDN et NSFNET comptent déjà près de 4 millions de nœuds interconnectés et plus de 1 000 ordinateurs à travers le monde y sont reliés.

En parallèle des travaux militaires américains, d'autres approches existent qui nourriront le Web tel que nous le connaissons. En 1960, Théodore Nelson (Ted Nelson), âgé de 27 ans, étudiant en sociologie à Harvard, réfléchit à un concept de système d'information « au bout des doigts ». Il imagine une machine permettant à chacun de stocker des données, de les mettre à disposition de tous, partout, en quelques instants. Nelson invente ainsi le concept d'hypertexte. Il s'inscrit donc dans la lignée des idées énoncées par V. Bush en 1945.

Les idées de Ted Nelson donne naissance au projet Xanadu. Celui-ci connaît des développements informatiques difficiles et le premier serveur opérationnel Xanadu ne sera disponible qu'en 1981. Le projet ne décollera jamais et sera vite dépassé par l'arrivée du World Wide Web de Cailliau et Berners-Lee.

Avant le World Wide Web en 1990, Internet est donc une double réalité à la fois militaire et académique et essentiellement américaine.

Les technologies qui permettront le basculement dans le grand public ne seront pas inventées par les Etats-Unis. Elles trouvent leur origine au cœur de l'Europe, à Genève au CERN, mais seront très rapidement récupérées par les Etats-Unis avec le départ en 1994 de Tim Berners-Lee au MIT et le refus de la Commission européenne de financer le développement du WWW (Jardon, 2017). Cette erreur majeure d'appréciation des enjeux liés au World Wide Web, dans un contexte marqué par la puissance encore forte des opérateurs téléphoniques européens qui voient d'un mauvais œil un protocole alternatif venir concurrencer les leurs (X25), accélère le déclin technologique de celle-ci, déjà identifié par Jean-Jacques Servan Schreiber dès 1967 dans son ouvrage « le Défi américain », dans lequel il s'inquiétait de l'absence de l'Europe dans l'industrie des micro-processeurs.

La chute du Mur et les autoroutes de l'information : nouvel espace, nouvelle frontière, nouvelle gouvernance (1989-2001)

La période qui s'ouvre avec l'apparition du World Wide Web est une période géostratégique qui rompt avec la précédente. La chute du Mur de Berlin en 1989 place les Etats-Unis comme la puissance mondiale dominante, sans rival, la Chine n'ayant pas encore pleinement débuté son développement ni intégré l'OMC[6]. Les Etats-Unis établissent alors une révision stratégique majeure qui s'appuiera sur une vision nouvelle de l'information et des réseaux de communication. Elle s'accompagne d'un discours mobilisateur sur l'Internet porté par l'administration Clinton (1993-2001) et Al Gore en particulier, pour développer les usages du réseau comme une nécessité économique et démocratique au niveau mondial annonçant une ère nouvelle de la mondialisation. De fait, l'Internet est un nouvel eldorado économique et une nouvelle frontière démocratique qui se heurtera rapidement à des multiples oppositions.

La révision de la doctrine géostratégique américaine

A partir de cette époque, la situation géopolitique a radicalement évolué avec la Chute du Mur de Berlin en 1989. La fin de la Guerre Froide ouvre une période nouvelle qui nécessite une révision stratégique profonde pour les Etats-Unis qui apparaissent comme les vainqueurs de la Guerre Froide. La disparation de la menace d'une guerre nucléaire oblige à une révision des doctrines stratégiques américaines, une « *Revolution in Military Affairs* » (Noyer, 2002).

Le concept de « guerre de l'information » émerge ainsi principalement de publications américaines, au moment où la légitimité du renseignement d'Etat est remise en cause aux Etats-Unis. Contrairement à la période précédente, la dissuasion nucléaire ne suffit plus aux États-Unis pour imposer ses vues aux autres pays sur les échiquiers géopolitique, économique, culturel et sociétal. Seule une maîtrise absolue de la production de connaissances en amont (circuits éducatifs) et en aval (Internet, médias audiovisuels) peut assurer aux Etats-Unis une légitimité durable sur le contrôle des affaires mondiales.

« *On imagine dès le milieu des années 1990 une transposition des logiques d'affrontement de la sphère géopolitique traditionnelle vers une sphère géoéconomique où les États, devenus « non spatiaux » doivent déployer des stratégies de dominance fondées sur le contrôle des infrastructures d'information et les flux de savoir technologique et économique (Baumard, 1997). Les efforts classiques d'analyse de la vulnérabilité des infrastructures critiques des nations englobent désormais l'infrastructure d'information. La forte croissance des cas de piratage encourage les États à créer des organisations ad hoc chargées de contrôler et surveiller l'émergence de cette nouvelle forme de criminalité.* » (Baumard, 2002)

[6] La Chine intègre l'OMC le 11 décembre 2001.

La doctrine américaine est à cet égard très explicite. Dans la *Joint Publication 3-13*[7], s'annonce comme suit : « *Les opérations d'information (IO) capitalisent sur la fiabilité, la connectivité et la sophistication croissante des technologies de l'information. Les IO visent les technologies d'information ou les systèmes d'information pour perturber les processus d'information rivaux, humains ou automatiques. Ces processus informationnels peuvent être les systèmes de commandement nationaux adverses aussi bien que les systèmes d'information automatisés d'infrastructures commerciales, de télécommunication ou de production d'énergie* »

Ce nouvel environnement post-guerre froide et cette nouvelle doctrine conduisent à une restructuration des dépenses militaires et les agences fédérales tentent de justifier un maintien et un redéploiement de leurs budgets vers la sécurité économique (Baumard, 2002). Les agences de sécurité comprennent également que les financements privés peuvent compenser les diminutions de moyens publics.

Les agences de renseignement ont donc financé un vaste programme de recherche par le biais d'un programme non classifié et fortement compartimenté qui a été géré pour la CIA et la NSA par de grands entrepreneurs militaires et de renseignement : le projet Massive Digital Data Systems (MDDS). Celui débute dès 1995: "*Birds of a Feather Session on the Intelligence Community Initiative in Massive Digital Data Systems" took place at the Fairmont Hotel in San Jose in the spring of 1995*".

Au cours des années suivantes, l'objectif déclaré du programme est de fournir plus d'une douzaine de subventions de plusieurs millions de dollars chacune pour faire progresser ce concept de recherche d'information dans des très grandes bases de données. Les subventions sont dirigées en grande partie par l'intermédiaire de la NSF afin que les efforts les plus prometteurs et les plus fructueux puissent être capturés en tant que propriété intellectuelle et constituer la base des entreprises attirant des investissements de la Silicon Valley.

C'est la naissance du complexe militaro-numérique américain (Gomart, 2021), pendant du complexe militaro-industriel de la période précédente de la Guerre Froide. Google est illustratif de cette alliance. En partie issue du programmem MDDS[8], Google signe des accords avec les agences de sécurité américaines (CIA, NSA). C'est une étape importante dans l'approche de l'instrumentalisation de l'Internet (Thibout, 2021). Les liens entre l'appareil d'Etat et Google sont nombreux. Google passe par exemple un accord avec Geoeye, pour ses services Google Earth et Google Maps. Geoeye est typique de ces sociétés travaillant pour l'armée américaine et le secteur civil.

Se met alors en place une alliance entre l'appareil d'État américain et les grandes plateformes du numérique qui vont faciliter le déploiement du *soft power* américain dans le monde, et de plus

[7] Joint Chiefs of Staff, (1998), Joint Doctrine for Information Operations, October, p.9.
[8] Voir https://qz.com/1145669/googles-true-origin-partly-lies-in-cia-and-nsa-research-grants-for-mass-surveillance/

en plus du *hard power* au travers des infrastructures de réseau que celles-ci financent : câbles sous-marins, datacenters, centres de recherche, écosystèmes logiciels deviennent autant de moyens d'affirmer un pouvoir.

L'emprise des Etats-Unis sur l'Internet passe à la fois par des agences de renseignement redimensionnées et centrées sur la surveillance et l'écoute des réseaux de communication et à la fois par des acteurs économiques puissants comme Yahoo!, eBay, Google, Amazon, Facebook.

Là où le pouvoir géopolitique a longtemps été affirmé par les voies maritimes, les Etats-Unis et les grandes plateformes américaines bâtissent grâce à l'Internet un nouveau pouvoir infrastructurel mondial pour tenter d'assoir leur pouvoir sur le monde. Cela nécessite de contrôler l'architecture de l'Internet et ses évolutions. Dès lors, les Etats-Unis déploient de nombreux moyens pour y parvenir.

Le World Wide Web devient américain

Les technologies qui propulseront l'Internet à une échelle mondiale dans le grand public sont d'origine purement européennes puisque c'est au CERN, à Genève, qu'un Belge et un Anglais mettent au point les protocoles du World Wide Web grâce à trois composants : une technique d'adressage (URL), un protocole rendant possible l'hypertexte, les hyperliens (http), et un langage de description de contenus (HTML).

Malgré les tentatives nombreuses de R. Cailliau, la Commission européenne ne fournit pas les budgets nécessaires pour le développement du WWW en Europe. Dans ce contexte, Tim Berners-Lee se voit offrir des conditions matérielles et financières au MIT qui le conduisent à rejoindre les Etats-Unis en 1994. Il occupe alors au MIT la chaire *Computer Communication Compatibility* au *Laboratory for Computer Science* (LCS).

C'est un tournant fondamental pour l'Internet : il aurait pu connaître un développement différent si l'Europe avait saisi à cette époque l'importance des protocoles de Cailliau et Berners-Lee. Mais l'Europe ne se saisit pas de cette opportunité, et c'est sans doute, une erreur qu'elle continue de subir, dans la mesure où elle ne pèsera plus jamais sur le développement de l'Internet, dont elle est déjà largement absente avant cette date.

Le véritable décollage des usages de l'Internet par le biais du World Wide Web sera permis par la mise au point d'un logiciel de navigation entre sites Web, le Navigateur Mosaïc NCSA. Une partie de l'équipe qui a développé Mosaïc à l'Université d'Illinois à Urbana-Champaign la quitte en 1994 pour fonder Netscape qui sera absorbée par un fournisseur d'accès Internet et de contenus en ligne AOL en 1998.

Le développement des usages ne repose pas exclusivement sur la technologie et les contenus mais également sur un discours mobilisateur construit par le gouvernement américain.

Les autoroutes de l'information, un discours pour propager le World Wide Web

Al Gore, sénateur, propose dès 1991 un texte "*High Performance Computing and Communication Act*" dans la suite du rapport de 1988 "*Toward a National Research Network*" soumis au Congrès par un groupe piloté par le professeur Leonard Kleinrock (UCLA), l'un des personnage clé du projet ARPAnet.

A partir de 1993, Al Gore, vice-président des Etats-Unis, entame alors une campagne de sensibilisation de l'opinion américaine et mondiale à l'Internet. Il popularise l'Internet sous le terme d'« autoroutes de l'information » (*information highways*)[9].

Ce discours vise la mobilisation de l'ensemble des acteurs de la société qu'ils soient scientifiques, économiques ou militaires. « *Our new ways of communicating will entertain as well as inform. More importantly, they will educate, promote democracy, and save lives. And in the process they will also create a lot of new jobs. In fact, they're already doing it* »[10]. Ce discours puissamment relayé par les médias donnera progressivement naissance à une nouvelle industrie, celle du numérique avec des acteurs de taille mondiale qui contribueront à assoir la puissance économique américaine au niveau mondial. Les liens entre les hommes politiques et les plateformes numériques sont nombreux : Al Gore siège au conseil d'administration d'Apple[11] et sera un important conseiller de Google dont il est un important actionnaire.

En janvier 1994, Al Gore organise à UCLA une importante conférence au cours de laquelle il expose les promesses de l'Internet pour la société américaine : « *We have a dream for...an information superhighway that can save lives, create jobs and give every American, young and old, the chance for the best education available to anyone, anywhere* »[12]. L'Internet est vu comme une « National Information Infrastructure » de la même ampleur que le chemin de fer.

Les Etats-Unis pensent donc l'Internet comme une nouvelle infrastructure qui permettra de déployer un pouvoir infrastructurel (au sens de M. Mann ; Isaac, 2022) au niveau mondial. Le choix politique est clairement de laisser les acteurs privés développer cette infrastructure et les services numériques sur la base de cette infrastructure. Le financement est laissé au secteur privé et plus spécifiquement à l'industrie du financement de l'innovation, le Venture Capital, qui est

[9] Voir https://en.wikipedia.org/wiki/Al_Gore_and_information_technology

[10] Discours d'Al Gore, 11 Janvier 1994, Los Angeles, Clinton Foundation

[11] Depuis 2003

[12] Voir le discours prononcé à cette occasion : https://web.archive.org/web/20060929192826/http://www.clintonfoundation.org/legacy/011194-remarks-by-the-vp-on-television.htm

une industrie très fortement structurée aux Etats-Unis (Nicholas, 2019). La commande publique contribuera également au financement de cette nouvelle industrie[13].

C'est donc une configuration assez inédite qui associe puissance publique, militaire, agences de renseignement et entreprises privées qui se met en place à l'orée des années 2000 et qui propulsera sur la scène mondiale des acteurs privés très puissants comme Oracle, Microsoft, Adobe, Salesforce, Amazon, Google, Facebook, Apple et bien d'autres, moins visibles car centrés sur la gestion de l'infrastructure elle-même comme Cloudfare, Equinix, Akamai.

Certains de ces acteurs acquièrent une taille et un pouvoir économique sans précédent, ce que leur capitalisation boursière exprime largement. Ces acteurs souvent décrits comme plus puissants que certains Etats deviennent des acteurs majeurs du jeu géopolitique en contrôlant des infrastructures de communication et de calcul (réseaux sous-marins, datacenters), flux d'informations, services numériques souvent gratuits (Thibout, 2021, 2022). Ils génèrent, notamment en Europe, une défiance accrue qui conduit à vouloir les contrôler ou limiter leurs pouvoirs. Ce que l'Europe fait en 2022 en adoptant le DMA[14] et le DSA[15].

L'Internet repose sur une gouvernance contrôlée par les Etats-Unis

Ce nouveau réseau électronique s'accompagne d'une gouvernance inédite puisque les États n'y ont pas directement leur place. Réseau issu de recherches militaires et académiques, devenu un réseau grand public, la question de sa gestion et son évolution est rapidement posée. Les Etats-Unis opteront pour une gouvernance multipartite essentiellement technique et internationale, dans laquelle l'influence américaine demeure déterminante et présente depuis les origines.

Différentes instances de gouvernance voient ainsi le jour : ISOC (1992), IETF (1993), W3C (1994), ICANN (1998). L'ICANN illustre l'ambiguïté forte de ces instances. C'est un organisme dépendant du gouvernement américain auquel il est contractuellement lié (Department of Commerce). Les gouvernements y sont représentés mais n'ont qu'un rôle consultatif.

L'architecture de cette gouvernance, qui écarte les États, est une source constante de revendications au niveau mondial. De nombreux pays réclament une véritable gouvernance mondiale. De vives discussions existent, notamment en 2012 au congrès de l'IUT à ce propos. La Chine, l'Inde, le Brésil, la Russie, mais aussi la Commission européenne réclament une évolution de l'ICANN.

Après les révélations des programmes de surveillance américains par E. Snowden, la Russie demandera la fin du contrôle américain sur l'ICANN sans obtenir gain de cause. L'ICANN elle-même demandera la fin de son lien avec le gouvernement américain. Depuis 2016, le contrat entre

[13] Exemple le contrat du Pentagone sur les intrastructures cloud, (ex-contrat JEDI), « Joint Warfighter Cloud Capability », https://www.silicon.fr/cloud-jwcc-pentagone-eviter-fiasco-435237.html
[14] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R1925&from=EN
[15] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2022:277:FULL&from=EN

l'ICANN et le gouvernement américain n'existe plus et l'ICANN est désormais une organisation de droit californien à but non lucratif.

Depuis, les appels se multiplient pour que la gouvernance de l'Internet migre à l'ONU, comme le président Macron l'a réclamé à l'IGF 2018 à Paris. Mais pour certains, cela remettrait en cause la nature même de ce réseau qui *de facto* reviendrait sous le contrôle des États.

C'est précisément ce que plusieurs Etats viendront remettre en question au sein de leur espace souverain pour tenter de reprendre la main sur cette infrastructure communicationnelle qui leur échappe. Dès lors, on assiste à un double mouvement : une reprise en main de l'Internet dans plusieurs États et une instrumentalisation croissante de l'Internet par plusieurs grandes puissances (Russie, Inde, Chine) dans leur rivalité avec d'autres nations. L'internet devient un lieu de conflictualités multiples.

Le retour de l'Histoire et le déploiement de la guerre cognitive : terrorisme, émergence chinoise, retour russe, comment l'Internet est devenu un espace de conflictualités entre puissances mondiales (2001-)

L'évolution de la nature menace géopolitique à laquelle les Américains sont confrontés à l'orée des années 2000, les amène à considérablement repenser les moyens d'écoute et de surveillance électronique avec l'apparition des attaques terroristes sur leur territoire. La doctrine américaine élaborée au début des années 1990 va ainsi brutalement se durcir avec les attentats du 11 septembre 2001 qui conduisent les Etats-Unis à considérablement renforcer les moyens des agences de renseignement (FBI, CIA, NSA) et démultiplier les capacités d'écoute et de surveillance des réseaux électroniques aux Etats-Unis et à l'étranger grâce à une loi adoptée 45 jours seulement après les attentats, le Patriot Act.

Cette loi prorogée à deux reprises est venue modifiée le FISA Act de 1978. Depuis, d'autres textes législatifs ont considérablement renforcé les capacités d'écoute et de surveillance de ces agences aux Etats-Unis et à l'étranger sans mandat judiciaire ou avis préalable de la Cour spéciale prévue par le FISA (Protect America Act, 2007). Le programme *Terrorism Information Awareness*[16] lancé en 2003 illustre l'utilisation des réseaux pour identifier des supposés terroristes. Les révélations d'E. Snowden en 2013 permettent au monde de prendre conscience des capacités d'écoute électronique développées sur Internet par les Etats-Unis. La captation d'informations par Internet à une aussi vaste échelle fait dire à l'amiral John Poindexter que ce programme est le *Manhattan Project* du contre-terrorisme.

[16] https://en.wikipedia.org/wiki/Total_Information_Awareness

Les attentats perpétrés par Al-Qaïda aux Etats-Unis conduiront ceux-ci à décider plusieurs interventions militaires au Moyen-Orient et en Afghanistan, déstabilisant profondément ces régions et le monde arabo-musulman. Ces offensives s'accompagnent également d'une promotion du modèle démocratique dans ces pays par les Etats-Unis.

Les Printemps arabes de la période 2010-2012 se caractérisent par des soulèvements et des manifestations de la jeunesse qui font usage des réseaux sociaux, Facebook en particulier, pour lancer des mobilisations et coordonner leurs actions. Nombreux sont les analystes qui voient dans ces mouvements politiques les premières manifestations de l'importance des réseaux sociaux dans la société et les effets politiques possibles de ceux-ci (Faris 2012). Ont-ils été l'instrument des Etats-Unis dans leur volonté de reconfigurer l'espace arabo-musulman ? On peut raisonnablement penser à une tentative d'instrumentalisation des réseaux sociaux, autrement dit d'Internet comme un outil de déstabilisation de régimes politiques.

Le narratif développé à propos de ces évènements visait à démontrer que les réseaux sociaux constituaient un outil aux mains des peuples pour se libérer de leur dictateur et faciliter l'action pour un passage à une démocratie, ce qui finalement n'adviendra pas dans ces pays. Les réseaux sociaux incarnaient une des promesses de l'Internet, l'*empowerment* des individus et l'émergence de la démocratie dans des pays qui ne l'avaient jamais connue.

Ce message a été interprété très différemment par d'autres régimes politiques dans le monde qui ont mesuré la menace, désormais réelle de leur point de vue, que l'Internet pouvait constituer pour leur régime. Dès lors, nombre de régimes politiques ont déployé des politiques restrictives d'usage d'internet dans leur pays. Surveillance, limitations ou encore blocage temporaire ou définitif de certains services numériques ou, plus radicalement, d'accès à Internet. Iran, Turquie, Égypte, par exemple, mettent Internet sous contrôle[17]. Des pays comme l'Inde bloquent de nombreuses applications chinoises. La conséquence des Printemps arabes sur l'Internet, c'est l'accélération de sa fragmentation.

Vers la fragmentation de l'Internet, le Splinternet

Dès lors, chaque puissance développe sa vision de l'Internet pour en faire un levier géopolitique de sa propre stratégie de puissance. Nombre d'états, rivaux ou hostiles aux Etats-Unis, contraignent largement les usages dans leurs pays et bannissent les services numériques américains.

[17] Sur le cas iranien voir les détails des nombreuses restrictions : https://en.wikipedia.org/wiki/Internet_censorship_in_Iran , voir également Salamatian & alii, 2020.

Le livre blanc du Forum économique mondial intitulé « Internet Fragmentation: An Overview »[18], publié en 2016, tout comme d'autres publications (Lemley, 2020), résumait déjà le sujet via trois thématiques : fragmentation technique autour des questions de protocoles, fragmentation gouvernementale autour des sujets de souveraineté et fragmentation économique autour de la question des "prés carrés" privés. Halal Internet (Iran), Runet (Russie), pour ne donner que quelques exemples de volontés nationales d'isoler un pays du reste de l'Internet, traduisent bien la transformation de l'Internet en ilots de plus en plus contrôlés et isolables du reste de l'Internet.

A cet égard, deux nations se distinguent nettement dans la prise de contrôle de l'Internet au sein de leur pays, la Russie et la Chine. La Russie développe une vision souveraine fondée sur la souveraineté territoriale et tente de contrôler les services numériques étrangers en leur imposant de nombreuses contraintes, notamment d'hébergement et d'accès aux données. La Chine constitue un cas différent du cas russe, dans la mesure où l'enjeu militaire et géopolitique de l'Internet est appréhendé dès la fin des années 1990 par l'armée chinoise. En outre le Parti Communiste Chinois (PCC) assoit une partie importante du développement économique de la Chine sur le développement d'un puissant secteur numérique apte à rivaliser avec les Américains.

La Russie et la souveraineté de l'espace numérique russe

La Russie, distancée technologiquement au sortir de la Guerre Froide, laisse dans un premier temps se déployer les services numériques liés à l'Internet. Progressivement, à partir de 2012, et plus encore après les révélations d'Edward Snowden, la Russie modifiera considérablement son approche en faisant émerger des plateformes russes rivales des plateformes américaines (Yandex, Vkontakte) et imposera des restrictions de plus en plus strictes et nombreuses pour les services étrangers et notamment leur imposera une localisation de leurs données sur le sol russe[19].

Plus encore, la Russie souhaite se déconnecter de l'Internet en cas de menace, grâce à la mise en œuvre d'un Internet purement russe, le RUNET (Nocetti, 2019 ; Limonier, 2021). En 2016, les « lois Yarovaya »[20], obligent les plateformes à stocker pendant trois ans les métadonnées de leurs utilisateurs, à aménager des portes dérobées et à communiquer leurs clés de déchiffrement afin de faciliter d'éventuelles enquêtes des services de sécurité. Enfin, en 2019, avec la loi dite sur « le Runet souverain », la Douma donne à l'État les moyens techniques et juridiques de contrôler non seulement les paquets IP entrant et sortant du territoire russe, mais également « d'isoler » le réseau russe du reste du monde en cas de menace extérieure[21].

---

[18] Forum économique international (2016), "Internet Fragmentation: An Overview", 76 pp. : https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf

[19] Loi fédérale n°242FZ de juillet 2014

[20] Lois fédérales n°374FZ et 375FZ du 6 juillet 2016

[21] Loi fédérale n° 90-FZ du 1er mai 2019

La montée des tensions : la guerre sino-américaine dans l'Internet et les technologies de communication

La Chine, quant à elle, développe une vision stratégique initiée dès la fin des années 1990 (Liang, Xiangsui, 2002) avec la volonté de contrôler son espace numérique et de contrer le développement des services numériques américains. Les services comme Yahoo!, Google, Facebook sont bloqués en Chine comme de très nombreux autres acteurs de la technologie américaine[22].

Loin de se limiter à une approche défensive, comme les Russes, les Chinois mobilisent l'Internet comme un levier d'action de leur développement économique et leur contrôle politique de leur population (Lee, 2018). A cet égard, le Parti Communiste chinois (PCC) contribue à faire émerger des acteurs publics (ZTE) et privés (Huawei) dans le numérique afin d'être en mesure de bâtir une autonomie technologique face aux Américains. Ce qu'ils parviennent à réaliser dans le domaine des infrastructures de téléphonie mobile dans la 4G et la 5G, au prix de plusieurs affaires d'espionnage industriel[23]. Huawei et ZTE[24] ne se contentent pas de bâtir l'infrastructure 4G et 5G de la Chine mais également celles de nombreux pays asiatiques ou africains. Ils deviennent un redoutable rival des acteurs des télécommunications occidentaux dans la maîtrise des infrastructures de communication à un moment où l'essentiel des usages de l'Internet transite par les réseaux mobiles. La Chine tente donc de rivaliser avec les Etats-Unis dans la maîtrise de l'infrastructure de l'Internet, même si son emprise sur les câbles sous-marin et les infrastructures de calcul (datacenters) est loin encore d'égaler celle des Américains.

Au-delà des infrastructures numériques, la Chine a développé une ambitieuse politique de développement d'un secteur numérique afin de moderniser son économie. Elle a fait émerger des plateformes pour faciliter son développement économique dans un pays où les infrastructures de paiement et logistiques sont très peu développées au début des années 2000. Alibaba, JD.Com, Tencent, Baidu, Meituan, ByteDance, Pinduoduo sont autant d'exemples de plateformes chinoises qui occupent désormais une place dominante dans les usages chinois. Alibaba est ainsi conçu comme une plateforme pour aider les PME chinoises à exporter et faciliter leur développement économique à l'étranger (Shen, 2022). WeChat, super-App possédant plus d'un milliard d'utilisateurs, devient un outil central de la vie chinoise et de son contrôle[25]. Le développement du numérique chinois, à l'exception des infrastructures et des appareils, s'effectue donc principalement derrière un Intranet géant, véritable muraille de Chine numérique.

---

[22] La liste des services numériques bloqués en Chine est longue : Google, Wikipedia, Dropbox, Microsoft OneDrive, Slack, HootSuite, Twitter, Facebook, Instagram, Snapchat, Pinterest, Tumblr, Flickr, Yahoo!, Tinder, WhatsApp, Twitch, YouTube, Vimeo, etc.

[23] Affaire Cisco en 2002, T-Mobile en 2012, voir https://www.ft.com/content/3174481a-4e8b-11ea-95a0-43d18ec715f5

[24] ZTE est une compagnie publique à la différence de Huawei.

[25] Voir les conséquences du partage de photos d'une des très rares manifestations politiques à Pékin en 2022 sur WeChat pour ces utilisatuers, qui tentent de récupérer l'accès à leur compte WeChat : https://www.technologyreview.com/2022/10/16/1061713/wechat-accounts-begging-tencent-beijing-protest/

Ce n'est que récemment que les acteurs chinois sont partis à la conquête des marchés occidentaux comme Alibaba avec AliExpress, ByteDance avec TikTok, Tencent avec les jeux vidéo (Ligue of Legends), Shein dans le e-commerce vestimentaire. En août 2020, la rivalité sino-américaine prend une nouvelle tournure avec la signature par D. Trump d'un bannissement sous 45 jours de l'application TikTok si ByteDance ne vend pas sa filiale à une entreprise américaine. TikTok devient une filiale ouverte à la participations capitalistique d'Oracle qui devient hébergeur des données de cette application pour le reste du monde (hors Chine). On constate que les Etats-Unis tentent de contrer la progression des services chinois qui viennent sérieusement concurrencer leurs services, en l'occurrence ici Facebook que ce dernier avait tenter d'acquérir.

Après un développement rapide des plateformes numériques chinoises, la Chine a récemment (2020) repris le contrôle sur les acteurs numériques privés en forçant au départ plusieurs de leurs dirigeants et en limitant le développement de plusieurs secteurs du numérique comme le e-learning ou encore le jeu en ligne. Cette reprise en main doit se comprendre dans le cadre d'une politique plus globale où la Chine tente d'équilibrer sa croissance et de parfaire son modèle de développement, politique connue sous le nom de « Common Prosperity »[26]. Le contrôle des plateformes numériques s'accompagnent d'un contrôle accru sur l'usage des données collectées par le biais d'une loi adoptée en août 2021 (PIPL, *Personal Information Protection Law*) qui comporte des possibilités de sanctions pécuniaires importantes et qui limite les transferts transfrontaliers de données par les fournisseurs traitant de grands volumes de données en imposant, sauf autorisation spécifique par le département d'Etat après analyse d'impact, de stocker l'intégralité des données exclusivement sur le territoire chinois.

Le modèle chinois diffère donc sensiblement du modèle américain par les modalités d'association des plateformes numériques privées avec les actions publiques.

Internet et la guerre cognitive

La notion de guerre informationnelle n'est en soi pas nouvelle et n'est pas le propre de l'époque que l'Internet a ouverte. La doctrine militaire russe intègre dès le XIXème siècle l'information comme une arme de déstabilisation de l'ennemi. La guerre informationnelle renvoie à une conception de la guerre qui dépasse les approches traditionnelles militaires. Dans la doctrine russe, la phase militaire constitue la conclusion d'un affrontement qui est permanent[27] (Giles, 2016). « *Les guerres du cognitif opposent des capacités à connaître et produire ou déjouer des connaissances. Les sciences cognitives portent sur l'ensemble des sciences qui concernent la connaissance et ses processus (psychologie, linguistique, neurobiologie, logique, informatique). La définition que nous donnons de la guerre cognitive est donc la manière d'utiliser la connaissance*

[26] Voir XI Sun, (2022), Decoding China's "Common Prosperity" Drive, April, https://www.lse.ac.uk/ideas/Assets/Documents/updates/LSEIdeas-Decoding-Chinas-Common-Prosperity-Drive.pdf

[27] Il est intéressant d'analyser l'attaque russe de l'Ukraine dans cette perspective.

dans un but conflictuel. » (Harbulot, 2002). Dit autrement « *On arrête un espion mais on ne jugule pas la pensée et encore moins le formatage de la connaissance* » (ibid).

Contrairement à l'action militaire qui se déploie dans l'espace topologique, la domination cognitive se situe à la frontière de l'espace psychologique et de l'espace électromagnétique. « *La maitrise de la synthèse de ces deux espaces non topologiques (spectres), envisageable avec l'avènement de l'ère de la cognition (information age*), amène celle d'un nouvel espace : l'espace cognitif. Maîtriser cet espace pourrait donner un pouvoir bien supérieur à celui donné par la maîtrise séparée de ses deux constituants, psychologique et électromagnétique, …* » (Rainaudi, 2002).

Les contours de la guerre cognitive

Le concept de « dominance stratégique » repose sur la capacité d'un État d'interdire ou de dissuader un État rival de remettre en cause ses règles de conduite et sa perception du monde. L'« *information dominance* », concept anglo-saxon qui n'en est qu'une variante, postule que le contrôle global des infrastructures et des flux d'information permet d'atteindre une dominance globale des économies et des politiques.

En suivant Baumard (2002), on peut distinguer deux approches principales de la domination cognitive, qui ne sont pas mutuellement exclusives (voir Figure 1). La première approche de la dominance cognitive est légale et compétitive. C'est une approche qui vise à améliorer les capacités cognitives d'une nation par la mobilisation de toutes les expertises individuelles et collectives. Elle repose sur une approche de la persuasion ouverte et consultative. Elle crée des rentes cognitives pour les acteurs qui fournissent des ressources cognitives critiques. La défense est liée à la supériorité des systèmes d'analyse en temps réel qui permettent de contrecarrer les stratégies de prolifération et d'influence ennemies. C'est l'approche majoritairement choisie par les Etats-Unis, même si ceux-ci ne s'empêchent jamais d'agir selon la deuxième approche.

	Dominance cognitive légale et compétitive	Dominance cognitive grise et clandestine
Doctrine 3-13 JCS (US)	Propriété et contrôle de l'infrastructure globale d'information permettant d'interdire des flux	Prolifération clandestine de désinformations, destructions des infrastructures d'information rivales.
Capacités cognitives	Meilleure coordination et mobilisation spontanée des expertises et des capacités cognitives individuelles et collectives.	Interdiction ou paralysie des expertises adverses (discrédit) ; contrôle de la formation des expertises (prosélytisme)
Persuasion	Gestion des parties prenantes de manière ouverte et consultative.	Opérations psychologiques visant à masquer la réalité ou favoriser une doctrine par le leurre.
Rentes cognitives	Mesures d'incitation et de récompense aux capitaux intellectuels critiques et gestion de la connaissance.	Restriction de la mobilité de l'expertise avec intimidation et rétention des savoir-faire critiques.
Défense	Supériorité des systèmes d'interprétation en temps réel permettant de contrecarrer des stratégies de prolifération et d'influence	Désinformation et manipulation des systèmes d'interprétation rivaux ; production de connaissances déformées ; manipulation des modèles mentaux

Figure 1: formes de stratégie de "dominance cognitive" Baumard, 2002

La seconde approche de la dominance cognitive diffère de la première en ce qu'elle agit aux frontières de la légalité ou de façon clandestine. Dans cette perspective, la collecte de renseignements de façon légale ou non, les opérations de désinformation, de manipulation sont permanentes. Les opérations sont également offensives en menant des cyberattaques sur des infrastructures privées et publiques en s'appuyant, soit sur des unités spéciales de l'armée, soit indirectement en s'appuyant sur des groupes de hackers recrutés de façon ad hoc. Les opérations visent des secrets industriels, testent la résilience d'infrastructures vitales, ou cherchent à obtenir des rançons[28]. Il est possible d'affirmer que les Russes sont plutôt adeptes de la seconde stratégie de dominance cognitive. Nous avons désormais de nombreux éléments qui constituent autant de preuves, de l'importance de cette approche dans la guerre cognitive actuelle. La désinformation est devenue une stratégie « industrielle » des Russes.

La désinformation est une ressource offensive aux caractéristiques particulières : c'est une « arme redoutable à sens unique, sans possibilité de rétorsion ; ses effets insidieux ne sont souvent décelables qu'avec le recul du temps » (Lacoste, 1986). Les campagnes de déstabilisation ont trois objectifs : (a) la perte des moyens psychologiques de l'adversaire, c'est-à-dire générer une paralysie décisionnelle dans le camp adverse ; (b) la perte de réputation ou de légitimité de l'adversaire ; et (c) la chute de ses soutiens notamment financiers.

Les cibles des campagnes de désinformation sont les systèmes de croyance (de l'opinion, des rivaux, des parties prenantes), le système de commandement (des rivaux et des partenaires), et l'opinion publique.

Dans les faits, la dominance cognitive recherchée s'exprime selon trois logiques dans l'espace numérique. La première logique consiste à se servir de l'Internet pour détruire, bloquer des

[28] C'est le cas de la Corée du Nord qui finance en partie son économie à partir de ce type d'opérations.

ressources d'un acteur. C'est la guerre par Internet. La seconde logique est d'utiliser l'Internet pour ce qu'il est un espace de communication et d'information qui permet de s'attaquer aux systèmes de croyance. C'est la guerre sur Internet. Enfin, de façon plus récente, une logique déployée par les Américains vise à réduire la capacité à utiliser Internet en limitant l'accès à des composants clés. C'est la guerre au-delà de l'Internet.

La guerre par Internet

La connectivité d'installations industrielles ou vitales à Internet les rend vulnérables à des cyberattaques qui n'ont cessé de se sophistiquer au fur et à mesure du temps, conduisant à développer des métiers spécifiques liés à la cybersécurité dans les organisations. Dans ce cas, l'Internet est devenu un lieu de conflictualité spécifique avec ses armes, ses méthodes qui mobilisent de nombreuses connaissances informatiques, en programmation, en architecture réseau, etc.

Il serait beaucoup trop long de décrire dans le cadre de cette conférence, les acteurs et la nature des attaques tant ceux-ci se sont multipliés et les cibles diversifiées (hôpitaux par exemple). Les attaques peuvent être le fait d'acteurs privés, de type mafia, qui rackettent au travers de demande de rançon différentes organisations en bloquant leur système d'information. Ce peut-être des groupes de hackers privés recrutés par des services d'États pour atteindre des cibles gouvernementales ou non gouvernementales.

Si l'on veut se convaincre que la guerre s'est déplacée dans cet espace pour atteindre des cibles civiles, militaires ou industrielles, il faut analyser l'attaque du système industriel de Siemens utilisé dans les centrifugeuses nucléaires iraniennes grâce à un ver informatique, Stuxnet, particulièrement sophistiqué qui a conduit à considérablement ralentir le programme nucléaire iranien[29].

Intrusion, espionnage, pillage de la propriété intellectuelle

La Chine comme la Russie accuse un retard important dans nombre de secteurs technologiques de pointe décisifs pour l'industrie de la Défense et plus généralement pour le développement économique[30]. Ces intrusions dans les systèmes d'information de nombreuses entreprises du monde entier est une préoccupation de sécurité nationale pour les Etats-Unis, qui a conduit à des accords entre les agences de sécurité électronique américaine (NSA) et certains acteurs du numérique comme Google[31].

---

[29] https://fr.wikipedia.org/wiki/Stuxnet

[30] Martin A., (2022), Fears grow of Russian spies turning to industrial espionage, September 14, https://therecord.media/fears-grow-of-russian-spies-turning-to-industrial-espionage/

[31] https://www.salon.com/2014/11/16/googles_secret_nsa_alliance_the_terrifying_deals_between_silicon_valley_and_the_security_state/

De facto, l'accès aux données des entreprises par l'ingénierie sociale (hameçonnage) ou par le biais d'attaques ciblées des systèmes d'information d'une entreprise est devenue une pratique généralisée qui a conduit la plupart des gouvernements à déployer des stratégies de protection/défense et dans le domaine militaire des pratiques cyber offensives. La France a ainsi créé en 2009 une agence gouvernementale dédiée, l'ANSSI. L'Union européenne a également légiféré en 2016 en la matière pour étendre les actions au niveau européen au travers de la directive NIS 2 (*Network & Information System Security*)[32] et Cyber Resilience Act. L'UE tente de coordonner les stratégies nationales de cyberdéfense au travers de l'agence ENISA[33], mais ne peut guère aller au-delà de la coordination du fait que les questions de défense demeurent des prérogatives des États membres.

La guerre sur Internet

Comme on l'a évoqué, la Russie a dans sa doctrine militaire depuis de nombreuses années considéré la guerre informationnelle comme une arme à part entière et a su démontrer sa maîtrise à de nombreuses reprises dans l'histoire. Internet, on l'a dit, est perçu comme une menace américaine par les Russes. Le refus des occidentaux d'intégrer la Russie dans l'UE, a conduit la Russie à un repositionnement stratégique qui repose sur des visions panslaves et la nécessité de repousser les frontières de l'OTAN. Depuis 2014, la Russie est à l'offensive, après avoir échoué en Géorgie, elle a repris l'initiative en Crimée et en Ukraine récemment en mettant en œuvre une stratégie d'affaiblissement des démocraties occidentales au travers de nombreuses techniques massives de désinformation et de nombreuses cyberattaques.

La guerre informationnelle : désinformation, fuite d'informations, fausses informations

Dans la guerre cognitive modifier les systèmes de croyance est un objectif fondamental. Avec l'espace numérique, l'atteinte de ces objectifs est largement facilitée à mesure que les usages se développent. L'internet est alors un vecteur essentiel de propagande et de nombreuses tentatives de manipulations des opinions de différents pays, particulièrement dans les situations de conflits (Mejias, Vokuev, 2017).

La Russie est une nation passée experte dans l'utilisation d'Internet comme vecteur d'attaque des systèmes de croyances occidentaux. Elle a par exemple déployé en Europe une vaste stratégie de propagande visant l'affaiblissement des institutions, cherchant à accentuer les dissensions dans la société britannique comme après la vague d'attentats terroristes en 2017 en Grande-Bretagne[34], et à influencer le vote en faveur du Brexit.

[32] https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016L1148

[33] https://www.enisa.europa.eu

[34] Voir Russian Influence And Interference Measures Following The 2017 UK Terrorist Attacks, https://crestresearch.ac.uk/download/2310/17-081-02.pdf

Le rapport du parlement britannique sur la désinformation et les fausses informations[35] est très illustratif des pratiques russes :

“ Kremlin-aligned media published significant numbers of unique articles about the EU referendum. 89Up researchers analysed the most shared of the articles, and identified with a clear anti-EU bias to the reporting. The two main outlets were RT and Sputnik, with video produced by Ruptly. The articles that went most viral had the heaviest anti- EU bias. The social reach of these anti-EU articles published by the Kremlin-owned channels was 134 million potential impressions, in comparison with a total reach of just 33 million and 11 million potential impressions for all content shared from the Vote Leave website and Leave.EU website respectively. The value for a comparable paid social media campaign would be between £1.4 and 4.14 million. »

“On 17 January 2019, Facebook removed 289 Pages and 75 accounts from its site, accounts that had about 790,000 followers and had spent around $135,000 on ads between October 2013 and January 2019. The sites had been run by employees at the Russian state- owned news agency Sputnik, who represented themselves as independent news or general interest Pages. Around 190 events were hosted by these Pages (the first was scheduled for August 2015 and the most recent was scheduled for January 2019)”

Les investissements dans les fausses informations par la Russie sont évalués à 300 millions d’euros depuis 2014[36].

Les fuites d’informations sur Internet (*data leaks*) constituent dans la guerre informationnelle une méthode très commune et utilisée par de nombreux acteurs privés ou étatiques (Gastineau & Vasset, 2017). La Russie use régulièrement de ce type de méthode comme dans le cadre de la campagne électorale française (Macron Leaks[37]) ou américaine avec la révélation des courriels d’Hillary Clinton sur Wikileaks[38].

La désinformation repose sur des méthodes sophistiquées prenant appui sur les caractéristiques des services numériques et spécialement les réseaux sociaux qui permettent d’atteindre des millions d’utilisateurs rapidement en industrialisant les outils de désinformation. Ainsi, les botnets créant des milliers de faux comptes et les fermes de trolls[39] sont des outils très largement utilisés dans les campagnes de désinformation russes. La vitesse de circulation des fausses informations sur Internet est plus rapide que celle des informations vérifiées (Vosoughi &alii, 2020), notamment celles des médias et atteint davanatge de personnes. Plus encore, certains

[35] House of Commons Digital, Culture, Media and Sport Committee, (2019), *Disinformation and ‘fake news’: Final Report,* https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf

[36] Le Monde, 23/10/2022, https://www.lemonde.fr/police-justice/article/2022/10/24/thierry-mariani-et-yves-pozzo-di-borgo-vises-par-une-enquete-pour-corruption-en-lien-avec-la-russie_6147139_1653578.html

[37] https://fr.wikipedia.org/wiki/MacronLeaks, voir aussi https://www.zdnet.fr/actualites/au-fic-viginum-esquisse-ses-contours-39943054.htm

[38] https://wikileaks.org/clinton-emails/ ; https://fr.wikipedia.org/wiki/Affaire_des_courriels_d%27Hillary_Clinton

[39] https://fr.wikipedia.org/wiki/Usine_à_trolls

individus on la capacité d'atteindre davantage de personnes que des médias établis (Bak & alii, 2022).

Ainsi, l'Internet, tant craint par les Russes, leur sert désormais de vecteur principal de leurs opérations de désinformation, dans un retournement tactique proche du combat de judo que pratique activement Vladimir Poutine. En utilisant les vulnérabilités de ses adversaires, la libre circulation de l'information et la liberté d'expression couplées aux mécanismes de viralité des réseaux sociaux et les nombreuses possibilités de les influencer[40], la Russie conduit des campagnes massives de manipulation de l'information comme dans le cas de l'élection de Trump, le Brexit, le mouvement des gilets jaunes.

Les démocraties occidentales ont mis du temps à comprendre la menace à laquelle elles faisaient face (Tenove, 2020). La France a mis en place en 2021 une cellule dédiée à la surveillance des campagnes de désinformation, Viginum[41] attestant de l'importance croissante de ces menaces informationnelles qui altèrent le débat public et la vie démocratique. Viginum est le service technique et opérationnel de l'État chargé de la vigilance et de la protection contre les ingérences numériques étrangères. Après une année d'existence, ce service a pu identifier de 84 campagnes de désinformation en France relevant d'un Etat étranger[42].

La rivalité technologique au-delà de l'Internet

La rivalité entre Nations, et particulièrement la rivalité sino-américaine, dans le domaine du numérique dépasse désormais l'utilisation d'Internet et l'affrontement sur Internet (Thibout, 2020). Désormais, la rivalité dans le domaine technologique vise à empêcher son rival d'accéder à des capacités technologiques ou rendre celles-ci inopérantes. On peut distinguer trois champs spécifiques dans lesquels cette rivalité s'exprime à plein depuis quelques années :

[1]. Les infrastructures de réseaux et l'accès à Internet ;
[2]. Le contrôle des micro-processeurs et de la puissance de calcul ;
[3]. La sécurité des communications électroniques et la suprématie quantique.

La guerre pour le contrôle des infrastructures

La concurrence technologique conduit les Etats-Unis à déclarer une véritable guerre contre Huawei et ZTE les accusant de déployer des infrastructures comportant des portes dérobées (*backdoors*) permettant aux services de renseignements chinois d'espionner les communications. Les Etats-Unis interdisent ainsi Huawei aux Etats-Unis en mai 2019. Ils font ensuite pression sur

[40] On peut citer l'astroturfing comme méthode de visibilité rapide sur de tels réseaux, voir https://fr.wikipedia.org/wiki/Astroturfing

[41] http://www.sgdsn.gouv.fr/le-sgdsn/fonctionnement/le-service-de-vigilance-et-de-protection-contre-les-ingerences-numeriques-etrangeres-viginum/

[42] Compte-rendu de l'audition de MM. Stéphane Bouillon, secrétaire général de la défense et de la sécurité nationale (SGDSN), et de Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information (Anssi) http://www.senat.fr/compte-rendu-commissions/20221003/etran.html

la Commission européenne[43] et les gouvernements européens pour que Huawei et ZTE soient bannies des cœurs de réseaux 5G des opérateurs télécoms européens comme c'est le cas aux Etats-Unis après la décision de Donald Trump. La Suède, la Roumanie, la Pologne, la Tchéquie, la Lituanie, l'Estonie ont interdit l'utilisation des technologies 5G de Huawei en 2020.

Les Etats-Unis imposeront cette décision à leurs alliés dans le renseignement (Five eyes)[44]. Le bannissement de Huwaei aux Etats-Unis est plus large que l'enjeu des cœurs de réseaux 5G, puisqu'il s'étend à l'utilisation de composants logiciels et matériels américains (Google, ARM, Qualcomm, Intel, Texas Instrument).

La question du contrôle de l'Internet et de son accès se manifeste également dans le développement de l'accès satellitaire avec le déploiement des réseaux privés américains de type LEO (*Low Earth Orbit*) comme GlobalStar, Starlink (SpaceX) ou Kuiper (Amazon). Le conflit russo-ukrainien a mis en évidence l'intérêt d'une telle infrastructure d'accès à Internet fournie aux forces ukrainiennes alors que les Russes avaient compromis l'infrastructure terrestre filaire. Les Chinois ont déjà contesté le positionnement du réseau de satellites Starlink et interdisent le service en Chine[45] comme d'autres pays (cf. figure 2).

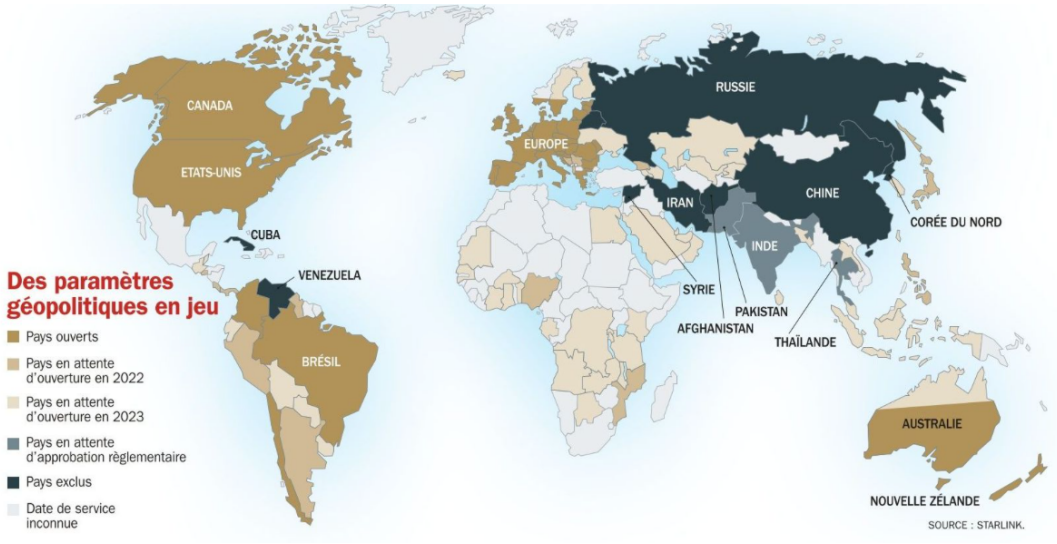

Figure 2: disponibilité du service Starlink fin 2022. Source Challenges, 20/10/2022

La maîtrise américaine de ces satellites, combinée à celles des smartphones (Apple, Qualcomm, Intel, Texas Instrument), articulée avec la virtualisation des réseaux mobiles sur le cloud (Telco Cloud sur Azure ou AWS) leur offre un retour dans le contrôle de l'accès Internet et des flux de données. Aucune nation autre que les Etats-Unis ne possèdent ces trois capacités en 2022.

---

[43] La Commission s'en tiendra à des recommandations de sécurité dans le déploiement de la 5G (5G ToolBox) https://digital-strategy.ec.europa.eu/en/library/secure-5g-deployment-eu-implementing-eu-toolbox-communication-commission

[44] Grande-Bretagne, Nouvelle-Zélande, Canada, Australie.

[45] https://www.ft.com/content/5ef14997-982e-4f03-8548-b5d67202623a

Le contrôle des micro-processeurs et de la puissance de calcul

La rivalité sino-américaine dans le domaine technologique s'amplifie au fur et à mesure des années. Celle-ci s'étend à tous les composants nécessaires à l'exploitation des infrastructures de télécommunications, notamment dans le domaine des semi-conducteurs et le cas spécifique de l'entreprise taïwanaise leader mondial TSMC.

Le récent CHIPS Act (août 2022) vient renforcer les capacités américaines en la matière dans un domaine où la Chine peine encore à s'imposer malgré de nombreux plans d'investissements successifs et où elle demeure dépendante des innovations américaines et taïwanaises. Cette guerre des puces électroniques connaît un nouveau tournant à l'automne 2022 avec la publication[46] par le BIS (Bureau of Industry & Security) de textes totalement restrictifs sur l'export vers la Chine de semi-conducteurs avancés, d'équipements de fabrication de puces et de composants de superordinateurs[47] et l'interdiction pour les citoyens américains de travailler pour une entreprise chinoise de semi-conducteurs.

La maîtrise de la sécurité des communications et la course à l'ordinateur quantique

La sécurité des communications sur Internet passe par leur encodage grâce à des algorithmes de cryptologie. Les progrès de la puissance de calcul ont fortement affaibli certains d'entre eux et on sait que les services de renseignement américains ont financé des entreprises dont ils possédaient les clés de cryptage. Les possibilités de la physique quantique commencent à être utilisées pour mettre au point des ordinateurs quantiques[48]. Si on reste en 2022 au stade du laboratoire, les progrès sont rapides en la matière et les conséquences importantes pour la sécurité des communications. Compte-tenu des capacités de calcul d'un tel type d'ordinateur, aucun algorithme de cryptage actuel ne serait en mesure de résister à un décodage rapide. Une course à l'ordinateur quantique a donc largement débuté. Elle implique les Etats-Unis, l'Europe et la Chine.

Ainsi, on assiste donc progressivement à une extension des rivalités qui ne se limitent plus aux réseaux ou à leur utilisation mais aux composants qui permettent de le bâtir, le gérer et le développer et le sécuriser. De fait, on peut interpréter cette extension comme une modification profonde de faire la guerre comme le décrit très bien Mark Galeotti dans son ouvrage « *The weaponisation of everyhting : A Field Guide to the New Way of War* » (2022).

---

[46] https://public-inspection.federalregister.gov/2022-21658.pdf

[47] Il s'agit d'un texte de portée extraterritoriale, puisque TSMC basé à Taïwan, a demandé si un export vers une de ses usines en Chine décidé avant l'entrée en vigueur du texte était concerné par le texte.

[48] Voir Ezratty O., (2022), Understanding Quantum Technologies 2022, Le Lab Quantique, 1024 p., https://www.oezratty.net/wordpress/2022/understanding-quantum-technologies-2022/

Conclusion

Dans ce début de XXIème siècle, où la connectivité n'a jamais été aussi développée, les risques majeurs n'ont jamais été aussi élevés : conflits armés aux frontières de l'Europe, crise écologique et énergétique, guerres informationnelles et cognitives, l'Internet apparaît loin des utopies fondatrices, si on considère que c'est leur principale origine. Les technologies qui constituent l'Internet sont majoritairement issues de programmes de recherche financés par la recherche militaire. Longtemps on a voulu voir le développement du réseau des réseaux comme un instrument de mise en capacité des individus et d'émancipation par la connaissance. C'est une réalité complexe, mais loin d'être la seule.

A mesure que l'humanité à déployer une surcouche cognitive mondiale grâce à l'Internet, les conflits se sont emparés de cette couche cognitive en l'instrumentalisant pour atteindre des objectifs militaires, mais plus encore en manipulant cette couche cognitive pour modifier les systèmes de croyances et de connaissances.

Force est de reconnaître que l'on a surtout eu à connaître une instrumentalisation de cette connectivité à des fins d'espionnage, de guerre (cyber-attaques), de campagnes massives de désinformation qui ont visé des démocraties dans un but évident de déstabilisation (USA, G-B, France). On ne peut s'empêcher de penser que l'Internet a été un instrument majeur dans la désinformation sur les énergies renouvelables qui a conduit à affaiblir durablement l'Europe en matière énéergétique, ce que les Russes et les Américains exploitent pleinement dans l'actuel conflit avec l'Ukraine. Ceci interroge sur la place de l'Europe dans la géopolitique de l'Internet, dont on peine, il faut bien le reconnaître, à identifier le rôle et l'importance. Les récentes initiatives pour réguler les grandes plateformes numériques étrangères, (DMA, DSA) sont souvent présentées et saluées comme des avancées substantielles face aux visées hégémoniques américaines. Alors que le DMA et le DSA ne sont pas encore appliqués, on peut douter de leur efficacité à contenir ces acteurs (Isaac, 2022), tant l'approche européenne peine à dépasser une stricte approche régalienne, incapable à elle seule à bâtir des contre-pouvoirs dans l'espace numérique. Dès lors, c'est la question du devenir du continent européen dans l'espace numérique qui est posée et plus généralement de sa relégation au troisième rang derrière la Chine et les Etats-Unis.

Des conclusions plus larges sur la nature de la conflictualité à l'ère numérique peuvent être dégagées, comme celles qui sont discutées par Encel et Galeotti (2022) :

1) Une nouvelle forme de rivalités permise par une réorganisation du champ informationnel et cognitif grâce aux infrastructures de communication de l'Internet, et de l'accès à l'information et à la connaissance ;
2) Une nouvelle catégorie d'acteurs privés aux côtés des États (GAFAM, BATX, NATU), qui jouent un rôle déterminant dans ce type de stratégie qui repose sur la privatisation de la gestion des infrastructures et de certains moyens de la guerre (réseaux satellitaires) ;

3) Un effacement de l'Europe devenue un terrain d'affrontements entre puissances rivales, comme en atteste la guerre de la 5G. L'Europe après avoir à deux reprises échappé de peu à son propre anéantissement devient un terrain de la conflictualité des grandes puissances mondiales (USA, Chine, Russie).

Bibliographie

Abbate, J. (2003). *Inventing the Internet*. Cambridge, MA: MIT Press.

Allcott H., Gentzkow M., (2017), Social media and Fake News in the 2016 Election, *Journal of Economic Perspectives*, Vol. 31, n°2, pp. 211–236

Borden A., USAF (1999), *What is Information Warfare?* Aerospace Power Chronicles.

Bak P.., Walter J. G., Bechmann A., (2022). Digital false information at scale in the European Union: Current state of research in various disciplines, and future directions. New Media & Society, 0(0). https://doi.org/10.1177/14614448221122146

Barlow J. P., (1996), *A declaration of the independence of cyberspace*, Electronic Frontier Foundation. https://www.eff.org/cyberspace-independence

Baumard P. (1996), "From Infowar to Knowledge Warfare: Preparing for the Paradigm Shift", in: *Cyberwar: Security, Strategy and Conflict in the Information Age*, A. Campen, D. Dearth, R. Goodden (editors), Fairfax, Virginia: Armed Forces Communications and Electronics Association, International Press, 1996, pp. 147-160.

Baumard, P. (1997), "Conquête de marchés, États et géoéconomie", *Revue Française de Géoéconomie*, Vol. 1, n°1., pp. 133-149.

Baumard, Ph. (2000), «From Inertia Warfare to Cognitive Warfare: Economics of Forces in Cognitive Arenas », *Martial Ecologies : Towards a New Strategic Discourse*, conférence organisée par l'Université de Tel Aviv et le *Jaffee Center for Strategic Studies*, Tel Aviv , Israël

Brügger N., Goggin G., Milligan I., Schafer V., (2017), Introduction: Internet histories, *Internet Histories*, 1:1-2, 1-7, DOI: 10.1080/24701475.2017.1317128

Cattaruzza A., (2019), *Géopolitique des données numériques. Pouvoir et conflits à l'heure du Big Data*, Paris, Le cavalier bleu

Chretien J., Isaac H., (2021), « Digital Markets Act : un remède aux maux de l'économie numérique européen ? », *Confrontations Europe*, n°131, Mai

Douzet F., (2014), l'art de la guerre revisité. cyberstratégie et cybermenace chinoises, Hérodote, n° 152-153, pp. 161-173.

Douzet F., (2014), « Géopolitique du cyberespace : La cyberstratégie de l'administration Obama », *Bulletin de l'association de géographes français* [En ligne], 91-2 | 2014, mis en ligne le 22 janvier 2018; DOI : https://doi.org/10.4000/bagf.1837

Encel F., (2022), Les voies de la puissance. Penser la géopolitique au XXIe siècle, Odile Jacob, 304 p.

Faris, D. (2012). La révolte en réseau : le « printemps arabe » et les médias sociaux. *Politique étrangère*, pp. 99-109. https://doi.org/10.3917/pe.121.0099

Fukuyama F., (1992), *La Fin de l'histoire et le Dernier Homme*, Paris, Flammarion, coll. Histoire, 452 p.

Galeotti M., (2022), *The Weaponisation of Everything: A Field Guide to the New Way of War*, Yale University Press, 248 p.

Gartzke E., (2013), The Myth of Cyberwar. Bringing War in Cyberspace back down to Earth, *International Security*, Vol. 38, No. 2, Fall, pp. 41–73, doi:10.1162/ISEC_a_00136

Gastineau P., Vasset P., (2017), *Armes de déstabilisation massive. Enquête sur le business des fuites de données*, Fayard, Paris.

Giles K., (2016), *Handbook of Russian Information Warfare*, Collège de Défense de l'OTAN, https://www.ndc.nato.int/news/news.php?icode=995

Giles K., (2022), *Russia's War On Everybody*, Bloomsberry Academic, 256 p.

Gomart T., (2021), Guerres invisibles. Nos prochains défis géopolitiques, Taillandier, Paris.

Hafner, K., & Lyon, M. (1996). *Where wizards stay up late: The origins of the Internet*. New York, NY: Simon & Schuster.

Harbulot, C. (2004), « De la légitimité de la guerre cognitive », *Revue internationale et stratégique*, 56, 63-67.

Heims S.J., (1991), *Constructing a Social Science for Postwar America: The Cybernetics Group,* MIT Press.

Isaac H., (2021), « Les super-plateformes et les plateformes internationales numériques », *Questions Internationales*, Septembre

Isaac H., (2022), « Quelle souveraineté numérique européenne ? », *Revue Française de Gestion*, Vol. 48, n°305, pp. 63-78, juillet-août.

Jardon Q., (2019), *Alexandria*, Gallimard, 256 p.

Jarvis C., (2022), Cypherpunk ideology: objectives, profiles, and influences (1992–1998), *Internet Histories Digital Technology*, Culture and Society, Volume 6, Issue 3, https://doi.org/10.1080/24701475.2021.1935547

Limonier K., (2021), Vers un « Runet souverain » ? Perspectives et limites de la stratégie russe de contrôle de l'Internet, EchoGéo, 56, http://journals.openedition.org/echogeo/21804

Kelly S., Truong M., Shahbaz A., Earp M., White J., (2017), Freedom on the net 2017: Manipulating social media to undermine democracy, Freedom of the Net project.

Lachlan Brumley et al. (2012), *Cutting Through the Tangled Web: An Information-Theoretic Perspective on Information Warfare*, October.

Lacoste P., (1986), Préface, in : Cathala, H.P., *Le temps de la désinformation*, Paris, Stock.

Lee K-F., (2018), *AI Super-powers. China, Silicon Valley, and the new order*, Houghton Mifflin Harcourt, 253 p.

Lemley M., (2020), The Splinternet, *Stanford Law and Economics Olin Working Paper*, n° 555, http://dx.doi.org/10.2139/ssrn.3664027

Liang Q., Xiangsui W. (2002), Unrestricted Warfare. China's Master Plan to Destroy America, Pan American Publishing Company (original edition PLA Literature and Arts Publishing House, Pékin, 1999) ; traduction française La Guerre hors limites, Rivages poches, Paris, 2006.

Mejias, A., Vokuev N., (2017), Disinformation and the media: the case of Russia and Ukraine, *Media, Culture & Society*, 39 (7), pp. 1027-1042

Mittelstadt J., Wilson M., (2022), *Military and the market*, Pensylvania University Press, 288 p.

Nicholas T., (2019), *VC. An American History*, Harvard University Press, 382 p.

Nocetti J. (2019), La Russie en quête de son « Internet souverain », INA, La Revue des Médias, 21 juin

Noyer, J. (2002). La guerre numérique au cœur de la stratégie : Changement de paradigmes, guerre de l'information, réseaux. *Les Cahiers du numérique*, 3, pp. 13-42.

O'Mara M., (2019), *The Code. Silicon Valley and the remaking of America*, Penguin, 496 p.

Paloque-Bergès C., Schafer V., (2019), Arpanet (1969–2019), *Internet Histories*, 3:1, 1-14, DOI: 10.1080/24701475.2018.1560921

Pornet, A. (2019). De l'atelier à la R&D : le rattrapage technologique comme outil de la puissance chinoise. *Revue internationale et stratégique*, 115, 117-126. https://doi-org-s.proxy.bu.dauphine.fr/10.3917/ris.115.0117

Rainaudi C., (2002), A la recherche de la suprématie cognitive : ou une doctrine de la domination douce, in Harbulot & Lucas Ed., *La guerre cognitive*, pp. 45-71, https://www.epge.fr/wp-content/uploads/2019/01/La-guerre-cognitive.pdf

Shen H., (2022), *Alibaba. Infrastructuring Global China*, Routledge, 77 p.

Tenove C., (2020), Protecting democracy from disinformation: normative threats and policy responses, *The International Journal of Press/Politics*, 25(3): pp. 517–537.

Thibout, C. (2020). La voie technologique du conflit sino-américain. *Revue internationale et stratégique*, 120, 59-70.

Thibout, C. (2021). Google et l'État fédéral états-unien : interdépendance, contestation et hybridation. *Entreprises et histoire*, 104, 142-163.

Thibout, C. (2022). Les GAFAM et l'État : réflexion sur la place des grandes entreprises technologiques dans le champ du pouvoir. *Revue internationale et stratégique*, 125, 75-88.

Van Puyvelde D., Brantly A., (2019), *Cybersecurity: Politics, Governance and Conflict in Cyberspace*, Wiley, 224 p.

Ventre D., (2016), *Information Warfare*, Wiley, ISTE, 2nd Ed.

Vosoughi S., Roy D., Aral S., (2018), The spread of true and false news online, *Science,* 359 (6380), pp. 1146–1151.