Objet conclusif : Le cyberespace, conflictualités et coopération entre les acteurs

Introduction : Le cyberespace est un terme emprunté à l'imaginaire cyberpunk, un sous genre de la science-fiction. Il a été forgé par W. Gibson dans son 1er roman, le ***Neuromancien***, paru en 1984, pour désigner l'espace en réseau qui découle de l'interconnexion des ordinateurs et de leur activité (échange, stockage et analyse des données). Le cyberpunk met en scène le combat d'individualités – humaines comme machiniques sous la forme d'intelligence artificielle – pour préserver leur autonomie face aux formes de domination renforcées qu'exercent sur les vies de grandes firmes grâce au contrôle du réseau des machines.

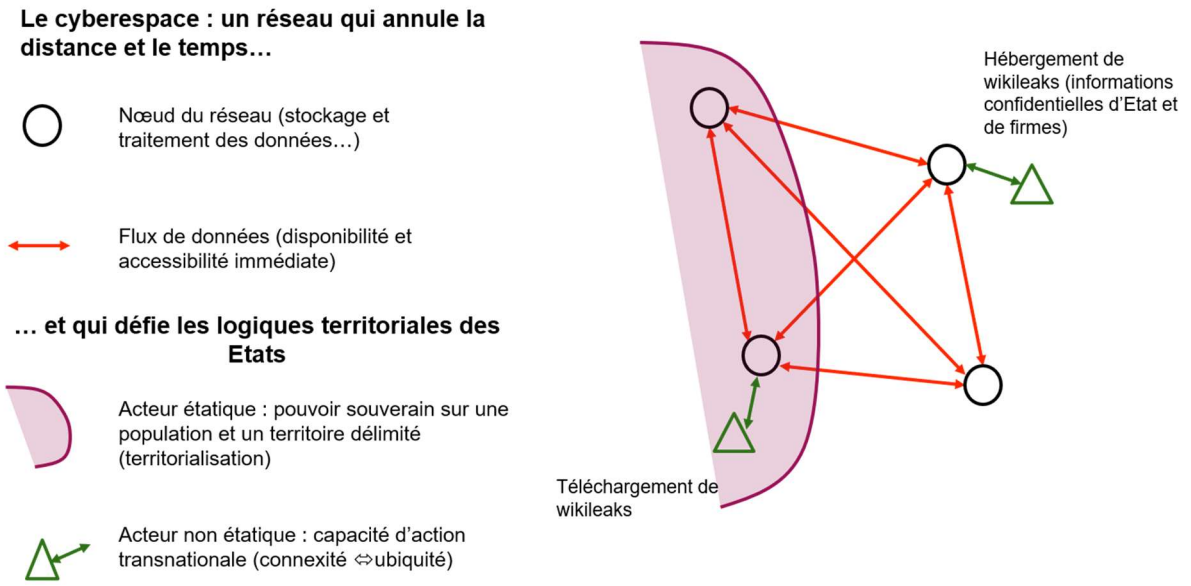
La thématique du cyberpunk s'organise ainsi autour des espoirs et angoisses que suscite la numérisation croissante des sociétés et des économies. D'un côté, le cyberespace peut être perçu comme un espace de nouvelles opportunités pour les individus et les firmes : partage de la connaissance, fonctionnement ouvert et décentralisé réalisant des aspirations démocratiques, nouveaux secteurs économiques (e-commerce, streaming…). De l'autre, il apparaît comme un espace de nouvelles vulnérabilités telles que des menaces pour protection de la vie privée ou pour la sécurité des États…

En témoigne une simple application comme Strava qui, pour ses utilisateurs/rices, représente un service gratuit pour mesurer et comparer leurs performances en course à pied, et qui, pour ses concepteurs, une firme, constitue une source de revenus considérables grâce à la marchandisation des données obtenues. Mais cette centralisation des données s'effectue au prix d'atteintes à la vie privée de toutes et tous, et à la sécurité des États. En effet, comme les informations sont accessibles à tous et toutes, il a été possible, par exemple, de déduire la localisation de sites secrets de bases et l'identité d'agents secrets à partir de leurs trajets de course à pied.

Problématique : Aussi convient-il d'analyser comment l'enjeu du contrôle du stockage, des flux, et de l'analyse des données suscite des coopérations et des rivalités entre les différents acteurs (États, firmes, individus) ? Est-ce que cela va déboucher sur une société de contrôle à rebours de l'idéal d'émancipation et d'autonomie porté par les premiers acteurs du cyberespace ?

Le cyberespace défie les schémas classiques de la géopolitique car il remet en cause la définition conventionnelle du pouvoir qui repose, comme dans le cas de la souveraineté étatique, sur son exercice sur une population et un territoire délimités. Le cyberespace semble échapper à l'emprise des gouvernements puisque c'est un réseau qui enjambe et brouille toute notion de limites comme le montre le schéma ci-dessous :

Qu'est-ce que le cyberespace ?



I) Le cyberespace : un réseau global et sans frontières qui consacre la prépondérance des EU

a) D'un projet militaire à un projet global et coopératif : Le cyberespace est, au départ, un projet militaire, déterminé par le contexte de la guerre froide. Ayant le sentiment d'avoir été surclassé technologiquement par l'URSS après le lancement réussi de Spoutnik en 1957 et d'être particulièrement vulnérable à un bombardement nucléaire de celle-ci en raison de sa domination spatiale, le gouvernement fédéral des EU consacre un effort budgétaire important à la recherche scientifique à des fins militaires pour rattraper son retard. Il crée la DARPA (Defense Advanced Research Project Agency). C'est dans ce cadre que les équipes de chercheur·es afin de mutualiser et d'accélérer la recherche décident mettre en réseau les ordinateurs afin de favoriser les échanges d'information : ARPANET.

Les principes de la communauté savante se substituent ainsi progressivement aux impératifs militaires : partage de la connaissance considérée comme un bien commun, coopération et évaluation entre pairs… Les centres universitaires des EU sont intégrés à ARPANET puis des centres étrangers. Leur mise en relation est facilitée par l'adoption d'un protocole d'échange commun, le protocole TCP/IP, en 1983, ce qui donne naissance à Internet, un réseau global. Mais ce sont les innovations d'un chercheur du CERN (Conseil Européen de la Recherche Nucléaire), Tim Berners-Lee, qui finalise l'architecture du cyberespace. Avec la mise au point

des liens hypertexte (langage HTML), des adresses URL et système http, il en fait un outil intuitif et accessible au plus grand nombre.

b) ***L'emprise croissante mais inégale du cyberespace :*** D'outil destiné à la communauté scientifique internationale, le cyberespace devient ainsi rapidement un vecteur de la globalisation des flux de données dans tous les domaines. Le nombre d'internautes passe de 500 000 millions en 2001 à 4,3 milliards en 2018, soit 53% de la population mondiale, tandis que ses usages n'ont cessé de diversifier, reflet de la numérisation croissante de nos vies : transactions financières de plus 1000 milliards de dollars par jour, commerce électronique, réseaux sociaux, objets connectés, streaming video, services en ligne des administrations publiques… Cette multiplication du nombre des utilisateurs/rices ainsi que des usages a pour conséquence une explosion du trafic des données comme en atteste son quintuplement entre 2017 et 2022.

Cette extension du cyberespace est cependant inégale suivant les régions qui reflète les inégalités de développement et de puissance. On observe, en effet, une fracture numérique entre les pays développés et les pays émergents, bien intégrés au cyberespace (plus de 50% de la population y a accès) et les pays en développement où moins de 50% de la population peut s'y connectée.

c) ***La centralité des EU dans les infrastructures du cyberespace :*** Le cyberespace se compose de trois couches superposées comme l'indique le tableau ci-dessous :

Couche matérielle	**Ordinateurs, serveurs, câbles sous-marins, datacenters...**
Couche logicielle	**Code et protocoles informatiques, système d'exploitation (Windows, Linux, macOS…), applications (Strava, netflix…)**
Couche sémantique (ou cognitive)	**Informations, contenus transmis et échangés par les utilisateurs/trices**

Dans chacune des couches nécessaires au fonctionnement du cyberespace, les entreprises et le territoire étatsuniens occupent une position dominante et stratégique. Pour la couche matérielle, les EU abritent ainsi 10 des 13 serveurs racines d'internet (qui assurent le nommage des sites internet) et près de 42 % des datacenters (les serveurs qui hébergent les données). De même, dans le domaine de la pose des câbles sous-marins par lesquelles transitent 97% du trafic internet, c'est la firme étatsunienne, Te Subcom, qui est leader avec 45% du marché des câbles posés entre 2013 et 2017, bien loin devant le conglomérat européen Nokia SNS/ANS et ce sont

les GAFA (Google, Amazon, Facebook et Apple) qui ont réalisé près de 50% des investissements dans ceux-ci en 2018.

Aussi, en raison de la qualité et du haut niveau de performance de leurs infrastructures, 97 % du trafic internet entre l'Asie et l'Europe transitent par leur territoire car la vitesse de débit y est plus rapide qu'un échange direct entre l'Asie et l'Europe. Cette primauté des EU se retrouve dans les autres couches comme en atteste le fait que, par exemple pour la couche logicielle, 90% des recherches s'effectuent par le biais de Google.

II) Le cyberespace : des acteurs variés aux conceptions opposées du cyberespace et aux capacités inégales

a) Des acteurs non étatiques en quête d'un espace libre et coopératif : Inspirés par les idéaux de la communauté savante (partage de la connaissance, autorégulation par la communauté, coopération), les premiers acteurs du cyberespace ont conçu celui-ci comme un territoire nouveau, autonome, dégagé de la tutelle des États, autoadministré par ses utilisateurs/rices où se réalise l'idéal d'une société de l'information marquée par la libre disponibilité et circulation des données pour tous et pour toutes. Face aux tentatives des EU de réglementer l'expression sur internet par la loi, le poète et militant, John Perry Barlow a ainsi proclamé l'indépendance du net en 1996. Pour lui, les acteurs étatiques n'ont aucune légitimité pour légiférer le cyberespace car ils ne représentent pas la communauté transnationale des utilisateurs/rices et, par ailleurs, ils ne disposent d'aucun pouvoir de coercition sur ceux-ci.

Cette vision du cyberespace comme un espace de citoyenneté cosmopolitique (à l'échelle du monde), collaboratif et ouvert s'est concrétisée sous la forme de l'**open data *i.e*** la gratuité et la disponibilité des données sans restriction de copyright, brevets ou autres mécanismes de contrôle. Wikipedia, l'encyclopédie libre et contributive, en est un exemple. Dans le même esprit, Richard Stallman, un savant étatsunien, a établi le cadre philosophique et juridique du logiciel libre dont Linux (système d'exploitation), Libre office (traitement de texte, tableur, diaporama) ou Gimp (outil de retouche d'image) sont des emblèmes. Face à l'emprise grandissante des États et des grandes firmes qui veulent contrôler, marchandiser et privatiser le cyberespace, des militant·es de la liberté sur le cyberespace utilisent pour défendre celle-ci les ressources du piratage (ou hacking) : des hacktivistes se revendiquant du mouvement ***Anonymous*** ont ainsi en 2011 par leurs attaques (en déni de service) contraint le site du FBI à fermer car celui-ci avait fait fermer le site Megaupload où pouvaient être téléchargés gratuitement films et séries.

b) ***Les géants du numérique ou le capitalisme de la surveillance comme nouvelle frontière du capitalisme :*** L'affaire du site Megaupload témoigne du très fort recul de la vision citoyenne dans le cyberespace au détriment de sa vision mercantile. Celui-ci constitue, en effet, un nouvel espace et une nouvelle frontière du capitalisme. Après avoir commercialisé des services sous forme payante, les grandes firmes du numérique ont repris à leur compte la logique de la gratuité pour collecter et monnayer les données de celles et de ceux qui utilisent leurs services. Les données collectées, agrégées et analysées par de puissants algorithmes sont vendues à d'autres entreprises afin de mieux cibler les publicités et de les rendre plus efficaces. D'autre part, grâce à ces données, les grandes firmes du numérique sont en mesure d'influer sur les comportements de leurs utilisateurs/rices. Ainsi Facebook manipulent-ils les contenus à forte charge émotionnelle, à l'instar d'autres réseaux sociaux (culture du buzz et du clash), afin d'augmenter l'activité de ses utilisateurs/rices et générer davantage de revenus publicitaires. La surveillance est ainsi à la base du capitalisme numérique avec comme conséquence la perte du contrôle de la vie privée et de l'autonomie par les utilisateurs/rices du cyberespace.

Les données qui alimentent ce capitalisme de surveillance sont centralisées par quelques firmes transnationales qui exercent une influence de plus en plus forte sur les contenus disponibles sur Internet. Dominent les firmes étatsuniennes, les GAFAM (Google , Amazon, Facebook, Apple, Microsoft), qui ont réalisé plus de 801 milliards de revenus en 2018. Face à elles, les firmes chinoises, les BATX (Badu – moteur de recherche, Alibaba – plateforme de commerce en ligne, Tencent – service de messagerie et Xiaomi – constructeurs de téléphones), avec 319 milliards de dollars de revenus en 2018, se positionnent en concurrentes. Très puissants face aux États car elles tiennent aujourd'hui les clés d'un réseau dont dépend l'économie mondiale, les géants du numérique sont cependant confrontés à l'action des États qui entendent affirmer leur souveraineté sur le réseau global cyberespace.

c) ***Les États, des acteurs qui cherchent à affirmer leur souveraineté sur le cyberespace :*** Les États tentent de réaffirmer leur souveraineté pour plusieurs raisons :

- D'abord, au nom de la protection de la vie privée et des droits humains : C'est en partie la conséquence du scandale de *Cambridge Analytica*, une firme qui a extraite et analysé des données sur les réseaux sociaux à l'insu de ces utilisateurs/rices pour prédire et influer sur leurs choix électoraux lors du référendum sur le Brexit au RU et lors des élections présidentielles des EU en 2016. Les firmes du numérique ne sont pas hostiles à une législation renforcée dans ce domaine car la confiance des utilisateurs/rices nécessaire à leur activité a été fortement ébranlée mais à la condition qu'elles puissent continuer d'exploiter et de monnayer les données qu'elles collectent, autrement dit, maintenir une surveillance à leur profit !

- Ensuite, en vertu des intérêts de puissance : Les révélations d'Edward Snowden en 2013 sur le système généralisé d'espionnage mise en place par la NSA sur le cyberespace comme l'enjeu du contrôle des données comme levier de puissance économique conduisent les États à vouloir territorialiser internet. La Russie impose ainsi l'hébergement des données numériques dans des datacenters sur son territoire, loin des grandes oreilles de la NSA, et encourage le développement de plateforme d'intermédiation russe de manière à damer le pion aux GAFAM tel Yandex, moteur de recherche russe qui s'est imposé dans la sphère d'influence russe devant Google. Dans le même esprit, la Chine soutient les BATX face aux GAFAM et fait poser des câbles terrestres et sous-marins par Huawei afin ne pas dépendre pour le transit des données d'un réseau sous contrôle des EU. On assiste ainsi à une territorialisation progressive du réseau global avec des sphères d'influence étatsunienne, russe et chinoise, à l'image du monde multipolaire.
- Enfin, au nom d'une conception autoritaire du pouvoir : les pouvoirs forts et antidémocratiques tels ceux de la Chine, la Russie, l'Iran ou encore l'Arabie Saoudite exercent une cybercensure pour filtrer et interdire les contenus, tout en exerçant une surveillance rapprochée des activités des internautes de leur pays. Le dispositif de filtrage des contenus mis en place par la Chine a ainsi instauré une véritable frontière numérique ; il est connu sous le nom Great Firewall (grand parefeu), en référence à la grande muraille de Chine.

III) Le cyberespace : entre conflits et coopérations

a) Un espace lourd de tensions, de menaces et de conflits : Conçu par la communauté savante comme un forum global, le cyberespace s'est transformé en arène où s'expriment les rivalités et les tensions entre États. La dépendance de plus en forte aux réseaux numériques des États et des sociétés en fait une cible pour déstabiliser, contraindre ou influencer les adversaires. C'est ainsi que la Russie a recouru aux cyberattaques contre l'Estonie en 2007 avec qui elle était en conflit larvé puis contre la Georgie en 2008 et l'Ukraine en 2014 avec qui elle était en conflit ouvert : elle notamment paralysé par des attaques en déni de service des sites gouvernementaux et de grandes entreprises. Elle est aussi accusée d'avoir voulu influencer les élections présidentielles des EU en hackant et rendant public des e-mails de Hillary Clinton afin de la discréditer et favoriser ainsi la victoire de Trump, plus favorable aux intérêts russes. Quant aux EU, ils ont utilisé un logiciel malveillant, le virus stuxnet, en 2010, pour ralentir le programme nucléaire iranien en contaminant leurs infrastructures informatiques et ils ont mis en place un système d'espionnage généralisé sur le cyberespace dévoilé l'analyste de la NSA, E. Snowden en 2013.

Espace où les États utilisent les attaques numériques pour s'affronter de façon ouverte ou larvée, le cyberespace offre aussi des opportunités considérables à la cybercriminalité. Trafiquants de drogue, d'armes, d'argent sales, pédocriminels profitent de l'anonymat que peut offrir le réseau pour se livrer à leurs activités et échapper ainsi au contrôle des États, en particulier, dans le darkweb, l'internet non référencé par les moteurs de recherche et non régulé. D'autre part, des cybercriminels envoient à des entreprises des ransomware (rançongiciels) qui exigent de l'argent pour débloquer des données (***cf*** Wannacry en 2017, 300 000 ordinateurs infectés, 150 pays touchés) , des logiciels espions ou de phishing (envoi de faux mails) pour voler des données.

b) La cyberdéfense et la cybersécurité comme réponses, l'exemple de la France et de l'UE – Jalon 2 : La protection des États et des sociétés face aux cybermenaces est délicate en raison même de la nature du cyberespace : difficultés à identifier les auteurs des agressions, absence de régulation internationale du réseau… Alors que l'UE aurait pu être l'échelle pertinente en raison du caractère global du réseau pour organiser les politiques de cyberdéfense et de cybersécurité, celle-ci a, dans les faits, un rôle très limité. En effet, la défense reste une prérogative attachée à la souveraineté des États qui se méfient les uns des autres en raison d'intérêts contradictoires. Aussi l'action de l'UE dans le domaine du cyberespace demeure cantonnée à la protection de la vie privée face aux firmes comme en témoigne en 2018 la mise en oeuvre du RGPD (Règlement Générale sur la Protection des Données). Cependant, face à la recrudescence des cyberattaques, émanant notamment de la Russie, le conseil de l'UE a adopté le ***Cybersecurity Act*** en juin 2019 : celui-ci prévoit des sanctions européennes (***i.e*** mises en œuvre par tous les États membres) face à toute cyberagression d'un acteur étatique ou non étatique. Il renforce également le rôle de l'ENISA (Agence européenne chargée de la sécurité des réseaux et de l'information) crée en 2014. Il établit enfin un cadre européen de certification de cybersécurité, autrement dit, des normes communes pour consolider la sécurité des produits connectés et des infrastructures critiques.

Quant à la France, plusieurs acteurs sont chargés de protéger sa souveraineté numérique. Créée en 2009 et employant aujourd'hui près de 600 personnes, l'ANSSI (Agence Nationale de Sécurité des Système d'Information) est l'autorité nationale en matière de cybersécurité. Elle est chargée de la prévention et de la réaction aux incidents informatiques visant les institutions sensibles (gouvernement, centrale nucléaire, hôpitaux…). Elle assure ainsi un service de veille, de détection, d'alerte et de riposte aux attaques informatiques, notamment sur les réseaux de l'État. Le ministère des Armées assure la protection des réseaux liées à ses opérations et intègre le combat numérique au cœur des opérations militaires. Á cette fin, a été créé en 2017 un commandement de cyberdéfense (COMCYBER). Il devrait avoir sous ses ordres près de 4000

cybercombattants en 2025. Depuis 2019, le dispositif a été étoffé avec la mise en oeuvre d'une doctrine officielle de lutte informatique offensive (LIO). En cas de cyberattaque, la France se réserve le droit de riposter et d'employer en opérations extérieures l'arme cyber à des fins offensives pour le recueil d'informations sur les capacités militaire adverses voire leur destruction. Enfin le ministère de l'Intérieur a pour mission de lutter contre toutes les formes de cybercriminalité, visant aussi bien les institutions et les intérêts nationaux, les acteurs économiques et les collectivités publiques, que les particuliers.

c) ***Une gouvernance mondiale du cyberespace en question :*** Deux tendances s'affrontent quant à la gouvernance du cyberespace. Les EU sont partisans d'un internet libre où les acteurs privés (GAFAM) et société civile ont un rôle à jouer aux côtés des États. C'est ainsi une société à but non lucratif, l'ICANN, réunissant représentants étatiques et acteurs économiques du réseau, qui est chargée du nommage et de l'adressage. Mais comme dans ces instances multi-acteurs dominent des acteurs attachés aux intérêts américains, la Chine et la Russie soutiennent une gouvernance étatique sur leurs réseaux. Cette revendication d'une souveraineté numérique forte sur les réseaux pourrait, selon Tim Berners-Lee, l'un des fondateurs d'Internet, aboutir à une « balkanisation du réseau », autrement dit, à son morcellement par les États.

De nombreux États militent pour une gouvernance élargie, notamment dans la cybersécurité et dans la protection des données. En effet, peu d'États disposent seuls des moyens techniques et financiers pour encadrer les comportements dans le cyberespace. Certaines entreprises numériques comme Microsoft ou Siemens appellent également à des normes de régulation contraignant les comportements dans le cyberespace : il s'agit pour elles de rétablir la confiance des usager·es dans le cyberespace après les scandales liés aux affaires de surveillance par des firmes et des États mais aussi de lutter contre « une balkanisation du net » qui serait préjudiciable à leurs affaires. L'Appel de Paris pour la confiance et la cybersécurité dans le cyberespace de 2018 a reçu 564 soutiens, dont 67 États, 358 entreprises (Microsoft, Facebook, IBM) et 139 organisations internationales. L'objectif est de promouvoir des règles internationales s'appliquant à tous les acteurs du cyberespace afin de protéger la vie privée et lutter contre la cybercriminalité. Mais les EU qui sont sur une ligne unilatéraliste, d'un côté, la Russie, la Chine qui défendent la gouvernance étatique contre des normes internationales, de l'autre, ont refusé d'y souscrire.