

La géopolitique du cyberspace Geopolitics of Cyberspace

*Messaouda Boulanouar**

Institut des Hautes Études de Sécurité Nationale, (Algeria)

mess.boulanouar@gmail.com

Date de soumission: 14/10/2025 **Date d'acceptation:** 12/11/2025 **Date de publication :** 31/12/2025

Résumé:

Dimension immatérielle transformant fondamentalement la nature des relations de pouvoir entre les États et redéfinissant les équilibres géopolitiques établis, le cyberspace prend une importance croissante. Souvent perçu comme un domaine intangible, il s'est rapidement imposé comme une dimension aux enjeux stratégiques, économiques et politiques, autant de facteurs contribuant aux rivalités de pouvoir. Il est devenu le théâtre de conflits réels où s'affrontent les États et d'autres acteurs internationaux, remodelant l'équilibre des puissances mondiales.

De par la nature des enjeux qu'il soulève et les défis concrets qu'il pose, le cyberspace peut se prêter à une approche géopolitique afin d'examiner les conflits d'ordre géopolitique dont il est l'enjeu.

Il sera question dans ce papier, dès lors, d'examiner comment on peut mobiliser le concept de géopolitique pour analyser le cyberspace, qui se présente en tant que dimension immatérielle.

Mots clés : *cyberspace, géopolitique du cyberspace, souveraineté numérique espace numérique*

Abstract:

Cyberspace, an intangible dimension fundamentally transforming power relations between states and redefining established geopolitical balances, is gaining increasing importance. Often perceived as an intangible domain, it has rapidly emerged as a sphere of strategic, economic, and political stakes, fueling power rivalries. It has become the theater of real conflicts where states and other international actors clash, reshaping the global balance of power.

Given the nature of its stakes and concrete challenges, cyberspace lends itself to geopolitical analysis of the conflicts it engenders. Accordingly, this paper examines how the concept of geopolitics can be mobilized to analyze cyberspace as an immaterial dimension.

Keywords: *cyberspace, geopolitics of cyberspace, digital sovereignty, digital space*

Introduction

Ces dernières années, le monde a connu une augmentation significative de l'ampleur des menaces sécuritaires, susceptibles de menacer la sécurité et la stabilité des États-nations. La mondialisation, variable d'évolution, pourrait également étendre les conséquences de ces défis au-delà des

** Correspondent Author*

frontières nationales, en raison de l'exposition créée par le développement technologique rapide. En l'espace de quelques années de la fin du XX^{ème} siècle à nos jours, l'internet, les technologies de l'information et les données numériques ont bouleversé le fonctionnement du monde, qu'il s'agisse du quotidien, des habitudes de consommation, de l'organisation de l'économie et des services publics, et des activités de surveillance.

Avec la pénétration de la technologie de communication numérique dans la plupart des secteurs de la vie, et en raison de la diffusion généralisée du World Wide Web dans nos vies humaines, le nombre d'utilisateurs d'Internet a augmenté à travers le monde. Internet a connu une croissance rapide au cours des trois dernières décennies, donnant naissance à une nouvelle dimension de la communication, représentation du cyberspace, l'une des réalisations les plus importantes de l'humanité moderne, comme un nouveau moyen de communication issu d'ordinateurs interconnectés à l'échelle mondiale. L'émergence du cyberspace représente la cinquième dimension, aux côtés de la terre, de la mer, de l'air et de l'espace.¹ Les pays cherchent à étendre leur souveraineté sur ce domaine, et son émergence comme espace stratégique engendre des menaces dont la gravité dépasse celle des espaces traditionnels.

L'interaction entre la société et le cyberspace génère des changements sociaux et pose des défis pratiques aux relations internationales, à commencer par le fait que le cyberspace devient un domaine distinct par rapport aux domaines traditionnels terrestres, aériens et maritimes. Alors que ces derniers sont régis par un concept territorial en raison de l'importance des frontières terrestres et des concepts d'espace aérien et maritime, le cyberspace se caractérise par son immatérialité partielle, exprimée par l'interconnexion des réseaux d'information.

Sur le plan stratégique, le cyberspace, de nature décentralisé, est considéré comme un domaine social, politique et technologique doté de caractéristiques uniques.² Ses caractéristiques influencent les principes fondamentaux de la souveraineté et de la territorialité, ainsi que l'État, considéré comme le détenteur exclusif et légitime du pouvoir et de la responsabilité, ce qui établit un contraste avec le domaine physique conventionnel.

Le cyberspace possède une dimension fortement géopolitique. Pour certains Etats, le cyberspace est devenu un espace de confrontations à part entière à l'image d'autres espaces tels que la terre, la mer ou l'air. En général, les conflits géopolitiques se structurent autour de territoires identifiables dans l'espace, marqués par des frontières naturelles, historiques ou politiques qui peuvent être plus ou moins distinctes. Avec la remise en question même des concepts d'espace, de frontière, de distance et

même de temps, l'apparition du cyberspace pose un défi majeur pour l'étude des conflits géopolitiques. Cependant, le cyberspace est soumis à un processus fort de « territorialisation » par ceux qui l'utilisent, ce qui en fait un défi pour les grandes puissances au XXI^e siècle, et ce, même s'il ne correspond pas à la conception traditionnelle d'un espace.

Ce papier, se proposant d'analyser les dynamiques géopolitiques structurant le cyberspace, la question qui se pose dès lors, est de savoir comment peut-on mobiliser le concept de géopolitique pour étudier les enjeux du cyberspace, relevant a priori de réalité non territoriale, alors que la géopolitique s'intéresse aux enjeux de pouvoir qui portent sur des territoires ? avant de répondre à ce questionnement nous aborderons tout d'abord ce qu'est le cyberspace.

I- Le cyberspace

Le terme cyberspace apparaît dans la littérature des années 1980 et fut popularisé par William Gibson dans son ouvrage *Neuromancien* (1984) qui décrit un espace tridimensionnel s'apparentant au cyberspace technique tel qu'on le conçoit aujourd'hui.³ Ce terme ne date donc pas d'hier.

Bien qu'il n'existe pas de définition consensuelle du cyberspace, la plupart des analyses réalisées confirment que son concept est vaste et englobe de nombreux systèmes interconnectés, allant des vastes réseaux administratifs (anciennement « réseaux domestiques ») – LAN privés – aux systèmes de communication longue distance basés sur l'espace, jusqu'aux bureaux, en passant par les systèmes de contrôle complexes de l'infrastructure. Il inclut également des technologies telles que les systèmes d'exploitation, les protocoles de communication, les applications logicielles, etc. Ces technologies sont utilisées dans des réseaux multifonctionnels tels que les services bancaires, l'industrie manufacturière, etc. Il est à noter que le concept de cyberspace comporte trois composantes : physique, non physique et un lien entre les deux, qui constituent des réseaux interconnectés.

Le cyberspace est un univers complexe à comprendre du fait de sa nature non matérielle et profondément technique, ainsi que du flou sémantique qui prédomine dans la littérature. Effectivement, il n'y a pas de définition universellement acceptée du cyberspace. Il est cependant possible de soutenir que le cyberspace est à la fois l'Internet et l'espace qu'il crée : un espace immatériel où se déroulent des interactions déterritorialisées entre des individus de tous horizons, à une vitesse fulgurante qui efface toute notion de distance.

On décrit souvent le cyberspace comme un univers virtuel, une zone autonome, sans limites définies, qui semblerait transcender les contraintes du monde physique, une perception accentuée par la montée en puissance du "cloud". Toutefois, cette illustration masque la complexité d'un espace

multidimensionnel, en partie immatériel mais fermement enraciné dans le monde physique et traversé de conflits géopolitiques bien réels.⁴

Pour le comprendre, il faut revenir sur le fonctionnement même du cyberspace. Si les données sont immatérielles et y circulent, il serait inadapté de croire, d'une part, que le cyberspace se limite à ces données et que l'internet constitue un réseau homogène. Ce réseau mondial peut être appréhendé en évoquant une structure en couches successives. A cet effet, trois niveaux sont évoqués (Olivier Kempf, 2012) :

-La première couche est dite physique et comprend l'infrastructure physique, à savoir: câbles, relais radio, satellites, ordinateurs et serveurs, qui sont déployés sur le territoire et donc sont soumis aux contraintes de géographie physique et politique.

-La seconde couche est dite logique et applicative, comprend tous les services permettant de transmettre les données entre deux points du réseau, à savoir: le nommage, l'adressage et le routage. L'infrastructure logique. Cependant, l'infrastructure logique s'appuie sur une base commune qui permet à tous les ordinateurs du monde de communiquer entre eux via le protocole Internet (TCP/IP) ⁵.

Là encore certains aspects peuvent être géolocalisables (logiciels utilisés, entreprise fournisseur, chemins empruntés, stockage des données, etc...). L'architecture logique repose toutefois sur une base commune, une harmonisation essentielle qui permet à tous les ordinateurs du monde de se comprendre entre eux, le protocole Internet (TCP/IP).

-La troisième couche est cognitive et sémantique. Elle rassemble les applications ou programmes informatiques qui permettent l'utilisation de l'internet. C'est le monde des utilisateurs de la couche logique, le monde de l'information, des réseaux sociaux, des discussions et des échanges en temps réel dans le monde. C'est la couche la plus intangible, et donc la plus difficile à géolocaliser.

Le cyberspace est également défini en tant qu'espace de communication constitué par l'interconnexion d'équipements de traitement automatisé de données numérisées, et ce, à l'échelle mondiale.⁶

Le cyberspace est aussi défini en tant que domaine opérationnel contrôlé, issu de l'interconnexion de systèmes et de leurs infrastructures connexes. Avec ses caractéristiques physiques et virtuelles, il se présente en tant que système hybride unique.⁷ Il est ainsi possible de lancer des attaques à faible coût depuis la couche virtuelle contre la couche physique, dont les ressources physiques sont rares et coûteuses. L'architecture gère les communications et les informations, les équipements informatiques, les infrastructures, les réseaux, les logiciels et les compétences humaines des utilisateurs. Elle s'applique uniquement aux dispositifs connectés à Internet,

mais couvre aussi les réseaux cellulaires internes et les technologies de communication spatiale.⁸

Le cyberspace est donc à la fois une réalité physiquement localisable et un espace de communication intangible et complexe. Il peut désigner tout ce qui circule, y compris un ensemble de réseaux informatiques (dont tablettes, smartphones, etc.), des réseaux humains, des flux de données et d'informations, via des réseaux informatiques interconnectés et partageant un langage commun. Les agendas politiques sont projetés sur ce domaine intangible. Que ce soit par un contrôle rigoureux de l'information comme en Chine ou par d'autres moyens, les gouvernements cherchent à y asseoir leur souveraineté. Cette volonté de contrôle fait d'Internet un lieu où sa maîtrise est perçue comme la clé pour influencer à la fois le monde réel et le monde numérique.

I-1-Une multiplicité d'acteurs

L'essor et la domination d'acteurs non étatiques en concurrence avec les puissances traditionnelles constituent une autre caractéristique distinctive du cyberspace. Aux acteurs traditionnels que sont les gouvernements et les grandes entreprises informatiques (GAFAM) s'ajoutent désormais des proxies-hackers isolés ou collectifs comme Anonymous, ainsi qu'une variété d'autres acteurs. Il est donc difficile d'identifier et d'attribuer des actions à des individus particuliers, comme les cybercriminels.⁹ L'attrait du cyberspace est évident : il offre un environnement inhabituel, accueillant un large éventail de participants internationaux, permettant de surmonter les contraintes géographiques et de fournir une quantité infinie d'informations. Cet environnement est complexe, varié et complexe à anticiper, voire à comprendre, les réactions de ses acteurs.

Le cyberspace est constitué de réseaux partagés par un large éventail d'acteurs, notamment des individus, des organisations politiques, des terroristes, des pirates informatiques, des activistes, des gouvernements et des entreprises. Ils sont omniprésents dans tous les aspects de notre vie quotidienne, de notre économie et de nos sociétés. Par conséquent, des défis et des dangers surgissent dans tous les secteurs. Grâce à sa capacité à accueillir davantage d'acteurs et à leur fournir des quantités suffisantes d'informations, cet espace minimise les distances, contourne les barrières physiques des États-nations. De plus, le cyberspace leur donne accès à des sources de pouvoir qui accroissent l'ampleur des menaces sécuritaires causées par leurs actions malveillantes. Même si cela n'assure pas une égalité totale entre les capacités des États et des acteurs non étatiques, cela signifie, en substance, de réduire l'écart qui les sépare en termes de pouvoir

et de capacité à recourir à la violence à travers des actions pour nuire aux infrastructures, aux individus et/ou aux institutions.¹⁰

En raison de cette fracture numérique, les frontières entre l'intérieur et l'extérieur s'estompent, ce qui entraîne une influence croissante des réseaux entre l'État et son extérieur, à mesure que les individus, les organisations et les gouvernements utilisent de plus en plus les nouvelles technologies connectées au cyberspace. La répartition du pouvoir permet à toute personne ou groupe en ayant les capacités de l'exercer Des appareils connectés peuvent exploiter la dépendance croissante du monde au cyberspace, même si l'État en est le seul détenteur légal. Des appareils connectés peuvent exploiter la dépendance croissante du monde au cyberspace. L'Etat se trouve ainsi confronté à la difficulté d'identification des auteurs d'attaques qui le ciblent.

I-2-Incertitude

Les aspects les plus insaisissables du cyberspace résultent de sa dynamique interne, ce qui rend difficile l'identification et l'attribution d'actions à des acteurs particuliers. Même si Internet semble de plus en plus ouvert et accessible au public, il demeure opaque. L'une des questions les plus débattues dans le débat public actuel est la protection de la vie privée dans le cyberspace. Cependant, de nombreux acteurs peuvent y interagir en dissimulant leur identité. Les États, ainsi que des acteurs individuels (tels que les pirates et autres hackers), ont recours à cette méthode. Cela, à son tour, fragilise les mécanismes actuels de responsabilisation dans les relations internationales, ce qui, conjugué à la multitude d'acteurs et à l'interconnexion du réseau, engendre une cyber incertitude.

L'une des fonctionnalités les plus attrayantes pour les utilisateurs est la possibilité de se dissimuler dans le cyberspace. Identifier les auteurs d'attaques est difficile, voire impossible, à réaliser avec certitude. Cette capacité de dissimulation pose problème dans le cyberspace, notamment en termes de développement de stratégies pour y faire face. L'identité de l'auteur d'une attaque étant inconnue, il serait, donc, difficile pour les Etas de s'en protéger (Centre d'études stratégiques aérospatiales, 2015, p.15).¹¹ L'absence de réglementation régissant le comportement des acteurs dans le cyberspace rend difficile la prévision des événements et, par conséquent, l'anticipation des réponses. Dans ce contexte, les enjeux pour la sécurité mondiale et la stabilité géopolitique sont considérables, et ce, compte tenu des difficultés à identifier avec certitude les auteurs des attaques, du potentiel d'escalade et de l'absence de normes internationales contraignantes ce qui favorise la création d'un environnement instable.

Certains défis sont propres au cyberspace, comme la difficulté d'identifier et de prouver l'origine d'une attaque, la difficulté de l'anticiper,

de la prévenir ou de la stopper. Sans parler des progrès rapides de la technologie et de la reconfiguration continue des réseaux, qui exigent tous deux une adaptation constante et rapide à l'évolution de l'environnement et l'enchevêtrement des juridictions et de la souveraineté.

I-3- Le cyberspace, une source de conflits

La conflictualité dans le cyberspace implique une diversité d'acteurs aux motivations et moyens variés. Ils peuvent être catégoriser par leur nature (géopolitique, économiques criminels, idéologiques, ...), leurs acteurs (Etat-nation, entreprise, organisation criminels, acteurs privés, ...) et leurs objectifs (espionnage, sabotage, déstabilisation, influencer l'opinion, ...).

Le cyberspace est un environnement conflictuel, alimentant des rivalités de pouvoir entre Etats, mais aussi avec des acteurs privés et criminels. Ces conflits peuvent se manifester par des cyberattaques comme celle du « Stuxnet » qui a ciblé le programme nucléaire iranien en 2010, ou de l'espionnage, à l'instar, des révélations d'Edward Snowden En 2013 qui ont démontré comment les pratiques d'espionnage pouvaient atteindre une ampleur inédite grâce à l'interconnexion planétaire des systèmes d'information et de communication.¹² Ces conflits peuvent également se manifester à travers des campagnes de désinformation remettant en cause la souveraineté et la stabilité internationale.

Les menaces numériques qui pèsent sur Internet sont nombreuses. Les formes les plus courantes de cyberattaques incluent l'hameçonnage, l'espionnage (économique, militaire), le sabotage (Ransomware) et la subversion. Elles reflètent également les tensions mondiales entre les grandes puissances, notamment entre les États-Unis et la Russie, accusée d'ingérence dans l'élection présidentielle américaine de 2016, à travers la manipulation de l'information, par des hackers. Le cyberspace reflète ainsi les tensions géopolitiques mondiales et génère également, au niveau local, des conflits d'aménagement par l'implantation de Data Centers.¹³

Au printemps 2007, la première cyberattaque de l'histoire paralyse l'ensemble du réseau informatique de l'Estonie. En 2017, le logiciel malveillant Wanna Cry prend en otage les données de centaines de milliers d'ordinateurs (Ransomware). C'est ainsi que le risque de paralysie lié aux cyberattaques, la diversité des menaces numériques pesant sur la sécurité nationale, notamment l'espionnage économique, la cybercriminalité, la cyberguerre et le cyberterrorisme,¹⁴ incitent les Etats à se mobiliser et à agir pour préserver leur sécurité et leur souveraineté, et de faire du contrôle du cyberspace une priorité stratégique.¹⁵

Le cyberspace se présente, ainsi, pour l'Etat, comme un territoire à conquérir et à contrôler, où sa souveraineté, ses frontières et sa puissance

doivent être établies. De fait, il occupe une place importante dans les discours des Etats confrontés aux cyberattaques de plus en plus nombreuses et complexes, favorisant des rivalités entre les puissances et ce, à travers l'adoption de stratégies de cyberdéfense pour protéger leurs infrastructures vitales et être capables de se défendre contre d'éventuelles attaques.

II- Une démarche géopolitique pour le cyberspace

La géopolitique étudie les rivalités de pouvoir et d'influence sur les territoires et les populations qui y vivent, à différents niveaux d'analyse, car elle s'intéresse à la dynamique de tout conflit sur le terrain, aux contradictions et aux stratégies des acteurs pour contrôler, répartir et défendre leurs intérêts au sein de ce territoire. La géopolitique peut aussi être appréhendée en tant que l'étude de l'espace en tant qu'enjeu.¹⁶

Par géopolitique, on entend toute forme de rivalité pour le contrôle ou la possession d'un territoire. Toutefois, toute rivalité de pouvoirs n'est pas forcément **géopolitique**. Pour qu'elle le soit, il est nécessaire que les acteurs se disputent principalement l'influence ou la souveraineté d'un territoire. La conception du territoire, selon les géographes, est vitale pour le raisonnement géopolitique : il ne s'agit pas d'une simple portion d'espace abstrait, mais bien d'un territoire délimité par ses frontières et ses limites, ses reliefs variés, les contours de ses côtes, le tracé de ses rivières, la répartition de sa population, l'emplacement de ses villes, ses axes de circulation et évidemment, sans négliger aucunement ses ressources géologiques et maritimes.¹⁷

De ce point de vue, il est utile de se poser la question suivante : dans quelle mesure le concept de géopolitique, fondée sur la matérialité des frontières, peut-il être mobilisé pour analyser le cyberspace, et lui appliquer les grilles de lecture classiques des rivalités et de pouvoir entre Etats (et autres acteurs), alors que le cyberspace n'est pas un territoire physique mais plutôt immatériel ?

Certes, le cyberspace perçu comme un milieu immatériel et déterritorialisé, semble à priori échapper aux grilles de lecture classiques de la géopolitique, traditionnellement centrées sur le contrôle des territoires terrestres et maritimes, pourtant, il est devenu un théâtre central de rivalité de pouvoir, d'influence et de souveraineté entre les acteurs internationaux. Face à ces considérations, il paraît suffisamment utile que l'on mobilise le concept de géopolitique pour analyser le cyberspace, et ce, non pas en transposant des concepts traditionnels sur une réalité nouvelle, mais en la adaptant à cette dimension immatérielle.

Pour saisir les logiques de puissance et de conflit à l'ère numérique, il est question d'examiner comment les principaux piliers de la géopolitique à

savoir la territorialité, la souveraineté, les acteurs et les rapports de force entre les États peuvent s'adapter et s'appliquer dans le cyberspace.

II-1 Le cyberspace et reconstruction des frontières

Rappelons avant tout ce qu'est un territoire. Il est défini en tant qu'une zone où un groupe humain réside et qu'il considère comme sa propriété collective, ou pour les États, en tant qu'une étendue terrestre délimitée par ses frontières dans laquelle est applicable son autorité et sa juridiction.¹⁸

C'est un espace géographique délimité par des frontières physiques, sur lequel on projette un projet politique, ce qui implique son appropriation, pour exercer une domination directe ou une influence indirecte. Le problème ici est que, si le cyberspace est un espace numérique sur lequel on peut très bien projeter un projet politique (filtrer les contenus Web qui favorisent l'image du gouvernement), sa domination reste fortement floue étant donné qu'Internet peut être contrôlé par tous types d'acteurs à la fois, qu'il s'agisse de groupes terroristes tout comme d'États.

Concernant le cyberspace, bien qu'on puisse y concevoir un projet politique à travers, à titre d'exemple, filtrer les contenus en ligne qui renforcent l'image du gouvernement, le défi réside dans sa domination, du fait qu'Internet peut être manipulé par une variété d'acteurs, allant des groupes terroristes aux États.

Par ailleurs, dans un univers mondialisé marqué par la fusion des réseaux, les avancées en matière de communication se traduisent, entre autres, par l'efficacité des interactions sociales à travers le cyberspace. Cette fluidité confère au cyberspace une légitimité en tant que terrain de pouvoir au XXI^e siècle et remet en cause les notions territoriales basées sur la logique des territoires physiques. Dans cette perspective, le cyberspace ne se définit pas comme une zone géographique, mais plutôt comme un domaine où des individus (les utilisateurs d'internet) interagissent, régulé par sa propre forme de gouvernance.¹⁹

Le cyberspace est souvent associé à la mondialisation du fait qu'il entretient des liens anciens avec cette dernière, puisqu'il en fut l'instrument premier à partir des années 1990. En effet, il est central dans la dématérialisation des échanges financiers, dans l'augmentation des échanges d'informations, mais aussi dans celles très rapides des échanges de biens, de services et entre les individus. Autrement dit, le cyberspace accompagne la mondialisation comprise comme une augmentation exponentielle des flux, alors que le cyberspace est, par construction, celui qui organise les flux. En effet, la multiplication des flux intensifs et continus de données massives, contribue à la disparition des frontières dans le cyberspace, entraînant ainsi la formation d'espaces corporatifs

déterritorialisés, fondés sur des réseaux économiques et des circuits de production qui se déploient à l'échelle planétaire.

On associe fréquemment le cyberspace à la mondialisation, étant donné qu'il a entretenu une relation étroite avec cette dernière, ayant été son principal outil depuis les années 1990.

On associe fréquemment le cyberspace à la mondialisation, étant donné qu'il a entretenu une relation étroite avec cette dernière, ayant été son principal outil depuis les années 1990. En effet, il joue un rôle crucial dans la dématérialisation des transactions financières, l'expansion du partage d'informations et l'échange rapide des biens, de produits, de services et d'interactions entre les individus.

Autrement dit, le cyberspace est par définition celui qui organise les flux, tandis qu'il accompagne la mondialisation, comprise comme une croissance exponentielle des flux. La multiplication de flux de données massifs, intenses et continus contribue, en effet, à la disparition des frontières du cyberspace, ce qui conduit à la création d'espaces corporatifs indépendants d'un territoire spécifique et fondés sur des réseaux économiques et des processus de production qui se déploient à l'échelle planétaire.

De ce fait, le cyberspace présente des défis pratiques et théoriques au concept de territoire comme espace de pouvoir en raison de sa nature intangible et des dynamiques de pouvoir qui caractérisent les interactions sociales modernes.

Par opposition à la notion de territoire, comme accès à l'espace physique au-delà des limites contrôlables, la nature immatérielle du cyberspace, au moins dans ses dimensions logique et informationnelle, garantit la liberté de circulation dans le monde globalisé, permettant le libre passage des frontières et la pénétration des territoires sans difficulté majeure.

La notion de territorialité est traditionnellement basée sur le domaine physique, où la société intègre le réseau du cyberspace. Les flux du cyberspace peuvent être appréhendés comme la territorialité des différents acteurs, exprimée à travers un champ artificiel et quasi immatériel. Contrairement aux domaines traditionnels, les activités du cyberspace ne sont pas limitées par des frontières territoriales ou des contrôles aux frontières.²⁰

Internet étant principalement utilisé pour manipuler l'information, les États les plus avertis comprennent la nécessité de contrôler et de protéger cette information spécifique, ce qui nécessite la mise en œuvre de certaines mesures. D'où la nécessité de disposer d'une cyberdéfense performante, ce qui va permettre à l'État de se concentrer sur l'établissement et la protection

des frontières de la communauté. Il s'agit d'un nouveau type de frontière, qui, contrairement aux anciennes frontières juridiques et administratives, englobant les frontières physiques réelles (terrestres, maritimes ou aériennes).²¹

Par conséquent, il convient de souligner le caractère paradoxal des facteurs qui contribuent à la territorialisation et à la déterritorialisation du cyberspace. D'une part, l'infrastructure de la couche physique relève de la juridiction des États, les frontières sont définies par les frontières des États et sont donc soumises à tous les principes territoriaux traditionnels. Tous les principes territoriaux traditionnels sont donc remis en question. D'autre part, après l'activation de la couche virtuelle et les données binaires sont transmises via Internet à une vitesse fulgurante, les concepts territoriaux fondés sur les éléments physiques ne sont plus valables. Par conséquent, la géolocalisation est complexe, car il s'agit d'une zone intangible et sans frontières.

De même, Internet a établi des frontières universelles qui ne correspondent plus aux frontières traditionnelles entre les États, et dont la circulation est devenue une question intangible qu'il s'agisse de communications, des transactions bancaires, du commerce, de la finance ou même de l'argent. Dans ce contexte, l'exercice de la souveraineté des États se trouve confronté à de multiples difficultés, allant de la puissance des acteurs impliqués au caractère international du réseau.

II-2 -Le cyberspace et la souveraineté étatique

La notion de souveraineté, concept westphalien par excellence, définissant l'autorité absolue et exclusive d'un État sur son territoire et sa population, se heurte à la nature transfrontalière, décentralisée et immatérielle du cyberspace. Alors que le concept de souveraineté dans son sens traditionnel est étroitement lié à la géographie et implique le contrôle et la domination complets d'un État sur son territoire, l'émergence du cyberspace a soulevé la relativité de ce concept face à l'absence de frontières et au changement de nature des conflits.

En effet, la notion de souveraineté a radicalement évolué avec l'avènement des communications. L'intégration et la connexion au réseau mondial d'information ont rendu plus difficile le contrôle total de l'information, devenue l'un des facteurs les plus importants du pouvoir politique, d'une part, et une source de faiblesse pour les États, d'autre part.

Ces mutations sociales et technologiques posent de nouveaux défis en termes de taille du marché, de modèles de gouvernance, de cadres réglementaires, de pratiques en matière de progrès technologique, et d'exercice la souveraineté de l'État sur le territoire numérique, notamment

vis à vis de la dépendance croissante des États à l'égard des technologies sous le contrôle d'acteurs privés multinationaux.

Il est donc essentiel de réguler l'espace numérique pour faire face à cette dépendance envers ces grandes sociétés technologiques qui possèdent une puissance et une influence transnationales (fiscalité, protection des données). Le besoin est constamment souligné par l'augmentation d'attaques cybernétiques de plus en plus coûteuses, ciblant aussi bien les particuliers que les sociétés et les États. Bien que la régulation du cyberspace vise principalement à instaurer un environnement numérique plus sûr, les États cherchent également à renforcer leur souveraineté sur un domaine qui devient de plus en plus stratégique.

L'exercice de la souveraineté des États est devenu plus complexe à mesure que les frontières entre juridictions dans le cyberspace se sont estompées et se sont imbriquées. Dans une large mesure, il défie la logique traditionnelle de territorialité. L'information circule à travers les continents, ignorant les frontières nationales.²²

Les activités du cyberspace transcendent les frontières nationales, et il peut être difficile pour un gouvernement de faire respecter ses réglementations et ses lois, même sur son propre territoire et par ses citoyens, en particulier lorsque le service utilisé est proposé par une entreprise étrangère. De plus, il existe une asymétrie de pouvoir marquée entre les nombreux acteurs en présence, notamment les États, les entreprises, les hackers et les citoyens. La souveraineté des États est menacée par cette fluidité, car ils peinent à faire respecter leurs lois sur des infrastructures souvent sous le contrôle d'organisations multinationales (GAFAM, opérateurs de réseaux). Cela dit, il est admis que dans le cyberspace, les juridictions sont souvent déterminées par des rivalités de pouvoir plutôt que par une définition juridique largement acceptée.²³

Cette dilution du contrôle entraîne une fragmentation d'Internet à l'échelle mondiale en sphères d'influence régionales, ce qui remet en cause son universalité. De fait, de nombreux États tentent de réaffirmer leur souveraineté numérique dans le cyberspace en ayant recours à divers moyens : soit en installant de « grands pare-feu », et en imposant la localisation des données telles que la Chine et la Russie ; Soit en adoptant une législation comme l'Union européenne pour restreindre l'hégémonie d'une autre puissance;²⁴ Soit en déclarant le cyberspace en tant que « champ de bataille », comme c'est le cas des États-Unis, et d'autres pays qui ont suivi (DodD, 2018, p. 2).²⁵

Compte tenu de la nature transfrontalière du cyberspace et des défis liés à l'application des lois nationales et au maintien d'un contrôle exclusif sur son propre territoire, le cyberspace remet en question les notions

traditionnelles de la souveraineté étatique, il ne la supprime pas, pour autant, mais la transforme. De ce fait, le monde numérique a créé, dans cette nouvelle ère, un environnement extrêmement concurrentiel pour son expansion et sa réaffirmation.

La souveraineté numérique dans le cyberspace ne peut plus reposer uniquement sur le contrôle territorial ; elle doit également disposer des capacités technologiques nécessaires pour la soutenir. Outre l'établissement d'un cadre juridique adapté à l'extraterritorialité du droit, elle vise également à garantir la cybersécurité, la résilience technologique (un cloud souverain) et la coopération judiciaire. Internet semble redéfinir la souveraineté en la complexifiant. Elle est désormais davantage une question de compétences à réglementer, protéger et influencer un environnement en mutation, qu'une question de frontières. C'est ainsi, que dans le cyberspace, la puissance, est davantage liée à la capacité d'influencer les normes et les infrastructures qu'au contrôle territorial.²⁶

II-3- Les enjeux géopolitiques du cyberspace

La maîtrise de ce nouveau territoire, qu'est le cyberspace, soulève des défis stratégiques majeurs, tant pour les Etats que pour les autres acteurs internationaux. Il est souvent question, au sujet de la géopolitique du cyberspace, d'enjeux stratégiques, de sécurité, de surveillance, d'espionnage, de pérennité du fonctionnement d'un réseau de plus en plus fondamental pour la plupart des sphères d'activité de la société.

Ces enjeux **stratégiques** ou économiques incluent à la fois la protection de l'intégrité des données et des réseaux contre les cyberattaques fréquemment ciblées. Elles favorisent également les entreprises capables de fournir les équipements ou les services nécessaires au fonctionnement des réseaux et de gagner des parts de marché.²⁷ Cependant, malgré leur importance, ces enjeux de pouvoir, comme ceux liés à la propriété intellectuelle, les domaines des négociations commerciales, des normes industrielles, des mouvements de capitaux ou des investissements ne sont pas immédiatement ancrés dans le territoire.

Parmi les particularités du cyberspace est son pouvoir égalisateur et sa capacité à uniformiser les règles du jeu en offrant des opportunités à différents acteurs, tels que les groupes de pirates informatiques, les groupes criminels pour défier des puissances étatiques ou de grandes entreprises et de leur causer des dommages considérables, modifiant ainsi les dynamiques traditionnels de pouvoir et rééquilibrant les relations asymétriques du monde réel, ce qui constitue un phénomène inédit en géopolitique.

De plus, les conflits dans ou autour du cyberspace sont indissociables des rivalités de pouvoir géopolitiques traditionnelles. D'autre part, ils représentent à la fois une nouvelle dimension et une expression de celle-ci,

qui doit être appréhendée dans une approche multiscalaire et demeure présente à tous les niveaux d'analyse. Comprendre le cyberspace comme un enjeu géopolitique nécessite de considérer les modes dont le pouvoir s'exprime dans un cet espace.

En effet, le cyberspace est virtuel et ses frontières sont difficiles à définir, d'où l'émergence de nouvelles stratégies de régulation, de surveillance et de réappropriation, ainsi que de nouvelles façons de se protéger et de se défendre. Par conséquent, la rivalité géopolitique pour la domination et la quête d'avantages stratégiques ne peut que s'étendre aux multiples couches du cyberspace.

Tout d'abord, comme indiqué précédemment, Internet ne peut exister sans un réseau physique permettant aux ordinateurs de fonctionner. L'Internet repose sur des infrastructures physiques géographiquement localisées, telles que les câbles sous-marins, les centres de données et les satellites, qui constituent un enjeu géopolitique et un point de vulnérabilité stratégique.

De plus, des rivalités pour le développement de câbles à haute capacité permettant de relier tel pays à tel autre se sont apparues, afin de se créer des clients mais aussi de se protéger de la vulnérabilité causée par une défaillance potentielle de ces câbles. La concentration géographique de l'infrastructure qui soutient le réseau dans un Etat donné, lui confère automatiquement une forme de pouvoir, comme c'est le cas des États-Unis d'Amérique.²⁸

Des stratégies de déploiement de serveurs puissants ont émergé sur les territoires des États, afin de mieux contrôler les données et de se protéger tant des cyberattaques que des décisions prises par les géants du web (les GAFAM), motivées par une logique de centralisation des traitements et de l'archivage des données, ce qui, contredit de façon flagrante la conception de plus en plus répandue d'un internet dématérialisé et libre de toute contingence géographique et politique.²⁹

De ce point de vue, les termes employés pour décrire le cyberspace comme un bien public mondial ou une ressource partagée sont inadaptés, dans la mesure où un bien public est un bien dont chacun peut profiter sans qu'il y ait d'exclusion. On pourrait considérer que certaines procédures d'information sur Internet appartiennent à cette catégorie, mais il ne s'agit pas de la structure physique, un bien précieux situé au sein des limites des États souverains et dont la maîtrise représente une domination des flux d'information mondiaux.

On peut évoquer une géopolitique du cyberspace principalement parce que le cyberspace n'est pas complètement déconnecté de l'espace réel. Les flux de données traversent des infrastructures matérielles situées à des

endroits spécifiques et empruntent des routes physiques concrètes, telles que les relais radio, les satellites ou les câbles sous-marins. De plus, les flux de données sont renforcés par le fait que les serveurs interagissent entre eux via des protocoles susceptibles de restreindre ou d'autoriser l'accès à leurs services. Ces données sont devenues la ressource stratégique du XXI^e siècle, avec leur contrôle et leur existence virtuelle au sein d'une réalité topologique ancrée dans la géographie réelle. La nature fondamentale de la guerre économique et des opérations d'influence est l'exploitation.

Les opérateurs de ces serveurs sont libres de prendre des décisions en fonction de facteurs commerciaux ou politiques. Par conséquent, l'accès à certaines routes peut être restreint aux utilisateurs situés à certains endroits, établissant ainsi une carte des frictions politiques ancrées dans une réalité géographique. En somme, chacune des couches du cyberspace peut être appréhendée à la fois d'un point de vue technique et en termes de rivalité géopolitique.

Par conséquent, la concurrence émergente dans le cyberspace peut être attribuée à cette restructuration des capacités technologiques. En appliquant une censure politique à tous les niveaux de l'infrastructure réseau, la Chine a pu établir des frontières pour Internet et se positionner en challenger des États-Unis dans la bataille pour la domination du cyberspace.³⁰

Il devient de plus en plus difficile d'appliquer des normes internationales dans le cyberspace, car il n'existe désormais aucun traité contraignant pour le régir. Le monde semble évoluer vers deux blocs géopolitiques distincts, chacun soutenu par un écosystème technologique unique. D'un côté, le bloc occidental, dirigé par les États-Unis, et de l'autre, le bloc oriental, que la Chine tente d'établir.

Le cyberspace est donc devenu, à la fois un terrain de compétition de pouvoir entre différents acteurs, un lieu d'affrontements et un outil redoutable dans les conflits géopolitiques. A cet égard, la concurrence géopolitique entre les grandes puissances du cyberspace devrait s'intensifier.

Conclusion

Le cyberspace est une révolution technologique extrêmement puissante, rapide et surtout universelle. Il a contribué à l'affaiblissement des contrôles aux frontières en soutenant la mondialisation.

Aujourd'hui, de plus en plus de pays ont compris que cette nouvelle dimension immatérielle redéfinit profondément les équilibres géopolitiques traditionnels et transforme la nature même de la puissance entre les États. Outre l'offre de nouvelles possibilités d'action, le cyberspace est au cœur de la souveraineté. Souvent perçu comme un environnement virtuel et sans

frontières, le cyberspace est devenu l'objet de vives rivalités de pouvoir et de processus de territorialisation, impliquant une diversité d'acteurs.

Mobiliser le concept de géopolitique pour étudier le cyberspace est non seulement pertinent mais indispensable, le cyberspace, un lieu où se reconfigurent les rapports de force, est devenu un nouvel espace de confrontation dans les rivalités de pouvoir géopolitiques entre une multitude d'acteurs, et le nouveau théâtre d'une compétition géopolitique totale, où se mêlent les enjeux de sécurité nationale, de puissance économique, d'influence culturelle, et où se projettent et se recomposent les rivalités de pouvoir.

L'étudier sous cet angle, nous oblige à reconsidérer notre compréhension du territoire, de la souveraineté et des frontières, et à intégrer un large éventail d'acteurs jusqu'alors inexplorés, des Etats aux géants du numérique en passant par les hackers. Les conflits qui s'y déroulent sont indissociables des luttes de rivalités géopolitiques traditionnelles. Au contraire, ils en représentent à la fois l'expression et une nouvelle dimension qu'il convient de considérer dans une approche multiscalaire, présente à tous les niveaux d'analyse.

En définitive, la géopolitique du cyberspace, dont les enjeux sont intimement liés à des considérations politiques, économiques, sociales et culturelles, permet de dépasser une vision purement technique pour révéler les luttes de pouvoir, les rivalités stratégiques qui s'y déploient entre les Etats et les autres acteurs internationaux.

Références :

1 PECH Yannick (2019) « Vers une intelligence cyber ? Penser le renseignement augmenté dans la noosphère », in *Prospective et stratégie*, Vol. 1, N° 10, pages 73 à 102, p.73.

2 Mihan S. (2025), « Essai analytique sur la notion de cyberspace », in *Cahiers Droit, Sciences & Technologies*, 20, pp. 135-154, sur le site <http://journals.openedition.org/cdst/12510>, p.5.

3 D'argain Henri, « Géopolitique de l'espace numérique : quelles stratégies de sécurité ? », in *Futuribles*, N°451, Paris, novembre-décembre, 2022, p.23

4 Loiseau H.& Waldispuehul E. (2017), « cyberspace et sciences politiques, de la méthode au terrain, du virtuel au réel », Éd. Presse de l'Université du Québec, Canada, pp 76-78.

5 Douzet F., (2014), « la géopolitique pour comprendre le cyberspace », in *Hérodote*, 1-2, n°152-153, pp. 3-21.

6 ANSSI, (2011), « Défense et sécurité des systèmes d'information. Stratégie de la France », Paris, p. 21.

7 Nye Joseph S (2010). *Cyber Power*, Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge, May, p. 3.

- 8 Nocetti Julien, (2018), « géopolitique de la cyber-conflictualité », in *Politique étrangère*, n° 2, p. 17.
- 9 PECH Yannick (2019) *Ibid.* p.74.
- 10 Nye Joseph S (2010). *Ibid.* p. 19.
- 11 Centre d'études stratégiques aérospatiales (2015), « Réflexions du le cyber : quels enjeux ? », in *Pensez les ailes françaises*, N°32, 146 p. sur le site https://www.irsem.fr/storage/file_manager_files/2025/03/plaf-32.pdf.
- 12 Douzet, F. & Géry, A. (2020), « Le cyberspace, ça sert, d'abord, à faire la guerre. Prolifération, sécurité et stabilité du cyberspace », *Hérodote*, n°177-178, p 334.
- 13 Cattaruzza A. et Douzet F. (2013), « Le cyberspace au cœur de tensions géopolitiques internationales », in *Revue Défense et Sécurité Internationale*, hors-série n° 32, pp.16-18.
- 14 Nye Joseph S (2010). *Cyber Power*, Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge, May, p.16.
- 15 Nocetti Julien, (2018), « géopolitique de la cyber-conflictualité », in *Politique étrangère*, n° 2, p 17.
- 16 Rosière Stéphane (2001), « Géographie politique, géopolitique et géostratégie : distinctions opératoires ». In *L'information géographique*, volume 65, n° 1, p. 37, sur le site : <https://doi.org/10.3406/ingeo.2001.2732>.
- 17 Lacoste Y. (dir.) (1993), « La géopolitique traite des rivalités de pouvoir sur un territoire », *Dictionnaire de géopolitique*, Flammarion, Paris, p. 587.
- 18 Lacoste Y. (2003), « De la géopolitique aux paysages, dictionnaire de la géographie », Armand Colin, Paris.
- 19 Desforges A. (2013), « Les frontières du cyberspace », in DOUZET F. et GIBLIN B. (dir.), *Des frontières indépassables ?* Armand Colin, Paris. P 74.
- 20 Douzet F, (2014), « la géopolitique pour comprendre le cyberspace », in *Hérodote*, 1-2, n°152-153, p. 12.
- 21 Desforges, A. (2013), *Ibid.*, p 74.
- 22 Douzet F ,(2014) *Ibid.* p. 12.
- 23 Douzet F ,(2014) *Ibid.* p. 9.
- 24 Douzet F. (2007), « Les frontières chinoises de l'Internet », in *Hérodote*, La Découverte 2^{ème} trimestre, n° 125, p.130.
- 25 Département Of Defense Cyber (2018), « Cyber Strategy », sur le site <https://dodcio.defense.gov/Portals/0/Documents/Library/CyberStrategy2018.pdf>
- 26 Nye Joseph S (2010). *Ibid.* p. 22.
- 27 Douzet, F. & Géry, A. (2020), *Ibid.* p. 345.
- 28 D'argain Henri, *Ibid.* p.23.
- 29 Cattaruzza A. et Douzet F. (2013), *Ibid.*
- 30 Douzet F. (2007), *Ibid.* p. 131.