

**LA SOUVERAINETE DES ETATS FACE A LA PREEMINENCE DES
GEANTS DE LA TOILE.**

Bouchra EL Hafed

Doctorante en droit international, Université MOHAMMED V, FSJES SOUISSI,
RABAT.

Abstract :

De prime abord, la souveraineté comme concept central en droit international désigne l'autorité absolue et suprême d'un État sur son territoire reconnu internationalement et sur sa population avec ses différentes composantes¹. En d'autres termes, la souveraineté est le fondement de la notion de l'État de droit et de la légitimité de son gouvernement.

Garantie par le droit international et est reconnue par les autres États, la souveraineté signifie que chaque État a le droit de déterminer sa propre politique intérieure et extérieure et de mener ses affaires sans ingérence extérieure.

La notion de souveraineté – comme celle d'État – se situe à l'intersection entre les scènes interne et internationale.

Si on plonge dans le passé, le concept de souveraineté avait été évoquée par le philosophe et polymathe grec Aristote (384-322 av. J.C), avant qu'elle ne soit définie par le théoricien politique français Jean Bodin (1529-1596) dans son ouvrage « Les Six Livres de la République en 1583 et dans lequel il dégage une conception politique de la souveraineté de l'État, perpétuelle et absolue, indissociable de l'indépendance². Ce concept de souveraineté sera par la suite influencé notamment par les philosophes Thomas Hobbes, J. Jacques Rousseau, Friedrich Hegel et Karl Marx.

Citation:Bouchra EL Hafed,. LA SOUVERAINETE DES ETATS FACE A LA PREEMINENCE DES GEANTS DE LA TOILE, The International Journal of Advanced Research on Law and Governance, Vol.5, Issue 2, 2023.

© 2023 EL HAFED, B, licensee The Egyptian Knowledge Bank (EKB). This article is published under the terms of the EKB which permits non-commercial use, sharing, adaptation of the material, provided that the appropriate credit to the original author(s) and the original source is properly given.

¹ Nabli, Bélig. « Chapitre 8. Le statut de l'État en droit international », L'Etat. Droit et Politique, Armand Colin, 2017, p. 168-186.

² Coutau-Bégarie, Hervé. « Histoire et prospective de la souveraineté. Une relecture de Bertrand de Jouvenel et de Jacques Ellul », Prospective et stratégie, vol. 1, no. 1, 2010, p. 35-45.

D'après les idées avancées de Bodin, l'État ne se trouve pas en situation de dépendance envers d'autres entités et ne se plie qu'à sa propre détermination. Il exerce sa prééminence sur une population et une étendue géographique spécifique. Par conséquent, la notion de souveraineté sous-entend autonomie, aptitude à ne pas se soumettre aux désirs externes (principe de non-ingérence), et liberté en ce qui concerne la structuration interne. Cependant, dans les faits, les avancées du droit humanitaire ou des telles idées que le concept de « Responsabilité de protéger » transforme la souveraineté en un devoir tout autant qu'en un droit, en ce qui concerne la protection des individus.

En ce qui concerne la souveraineté extérieure, son fondement réside dans le principe d'équité entre les États, déterminant de leur puissance réelle, de leurs ressources ou de leur démographie. La Charte des Nations Unies mentionne ainsi le concept d'« égalité souveraine » (article 2 § 1) pour exprimer cette notion. Cette égalité implique également que les États ne se trouvent assujettis à aucune instance supérieure. Théoriquement, ils sont en position de subordination uniquement vis-à-vis des règles qu'ils ont établies par eux-mêmes ou auxquelles ils ont consenti.

De plus, les dynamiques des relations internationales modernes ont vu surgir des entités régionales, auxquelles il est possible de déléguer des compétences décisionnelles, telles que l'Union européenne ou autres. Cette évolution a conduit des chercheurs comme le politologue français spécialisé en relations internationales, Bertrand Badie, à évoquer un « univers dépourvu de souveraineté ». C'est ainsi qu'il a évoqué une « illusion de souveraineté »³, en se référant à la responsabilité partagée par divers acteurs face aux enjeux mondiaux contemporains, et non plus uniquement assumée par les États.

Telle que précédemment définie, la souveraineté découle étroitement de l'existence d'un domaine où elle s'exerce en réalité. Cet espace englobe les terrains terrestres, maritimes et atmosphériques qui tracent les contours des frontières étatiques. Cependant, cette explication ne couvre pas toutes les dimensions, en particulier avec l'émergence d'Internet qui a donné naissance à un nouvel espace nommé le « cyberspace ».

Le concept de cyberspace a reçu diverses définitions, mais il englobe généralement tout l'univers des échanges en ligne. Ceci englobe l'intégralité des réseaux informatiques, des dispositifs connectés et des services en ligne qui

³ Bertrand Badie. Un monde sans souveraineté. Les Etats entre ruse et responsabilité. In : Politique étrangère, n°2 - 1999 - 64^eannée. p. 410-411.

autorisent les individus et les entreprises à communiquer, partager des informations et interagir avec d'autres individus et organisations à travers la planète.

Le cyberspace est devenu un outil essentiel dans notre vie quotidienne, porté par la prolifération de l'utilisation d'Internet et des médias sociaux, ainsi que l'essor de l'usage des appareils connectés tels que les smartphones et les objets connectés.

Cependant, le cyberspace peut tout autant être un environnement risqué, avec des menaces de cyberattaques⁴. Une situation qui a incité les États à prendre des mesures pour sauvegarder leur sécurité ainsi que celle de leurs citoyens.

Néanmoins, il est erroné de considérer le cyberspace comme un espace sans régulation. Au contraire, il est soumis à la fois aux règles juridiques et à la souveraineté nationale des États. Ces derniers sont habilités à faire respecter leurs lois sur leur territoire et, par extension, sur les infrastructures matérielles, les individus et les entreprises exploitées sur leur sol. Cependant, la mise en pratique de cette souveraineté peut se révéler complexe. La mise en œuvre de cette souveraineté est compliquée par la capacité à opérer à distance, particulièrement avec l'utilisation de plateformes (Google, Weibo, Facebook, Twitter) établies à l'étranger, sur lesquelles l'État ne possède pas d'autorité.

En abordant la question de la conduite du cyberspace, diverses interprétations émergentes, englobant à la fois la gestion de l'internet (ses opérations, protocoles, structure, noms de domaine) et une supervision sur l'internet (contrôle des contenus, infractions, liberté d'expression).

La gouvernance du cyberspace se réfère aux règles, normes et mécanismes qui supervisent l'usage de l'internet et des réseaux informatiques. Cela concerne les aspects techniques, économiques et sociétaux de cette utilisation, dans le but de garantir une fonctionnalité stable, sécurisée et équitable de cet environnement⁵.

Englobant une multitude d'acteurs, comprenant des gouvernements, des entreprises, des organisations internationales et des utilisateurs individuels, la gouvernance du cyberspace se révèle être un sujet de plus en plus crucial. Cela

⁴La connaissance de vulnérabilité informatique n'ayant fait l'objet d'aucune publication ou n'ayant aucun correctif connu, (vulnérabilité du jour zéro « zero-day ») des systèmes d'exploitation, élaboration d'une ou plusieurs « charges utiles » permettant d'agir sur les systèmes de contrôle industriel et sur des automates programmables. Hacking par clé USB, le ver STUXNET qui a frappé les installations nucléaires iraniennes à l'été 2010 était conçu avec 4 « zero-day » et de 2 charges utiles, l'une déphasant les centrifugeuses, l'autre perturbant les systèmes de contrôle qui n'ont rien remarqué.

⁵ Douzet, Frédéric. « La géopolitique pour comprendre le cyberspace », Hérodote, vol. 152-153, no. 1-2, 2014, pp. 3-21.

s'explique par la prévalence croissante de l'internet et des réseaux informatiques de nos jours, qui jouent un rôle central même dans l'économie globale.

Les défis liés à la gouvernance du cyberspace sont divers, comprenant la résolution des conflits d'intérêts, la préservation de la vie privée et de la liberté d'expression, ainsi que la sécurisation des réseaux et la lutte contre la cybercriminalité⁶. Les initiatives pour répondre à ces problèmes sont complexes et en constante évolution.

La gouvernance opère de manière hautement décentralisée, se développant au sein de multiples enceintes et forums où participent tous les acteurs concernés (société civile, communauté technique, secteur privé, gouvernements). Ces réseaux sont largement gérés par des acteurs du secteur privé. Cependant, le cyberspace n'échappe pas aux lois des nations et au principe de souveraineté ; cela exige toutefois une reconsidération de leur application.

Le cyberspace se compose de réseaux d'entreprises partagés entre divers intervenants : individus, groupes politiques, hackers, militants, gouvernements, terroristes et forces militaires⁷. Ces entités sont omniprésentes dans toutes les facettes de notre vie quotidienne, de notre économie et de nos sociétés.

Cela engendre une série de problématiques et de vulnérabilités dans tous les domaines. Les nouveaux services en ligne perturbent les équilibres économiques et mettent en péril des secteurs entiers. Les attaques informatiques se multiplient, devenant de plus en plus sophistiquées et ciblées, mettant en danger la sécurité des infrastructures cruciales et des citoyens.

Même les entreprises ne sont pas à l'abri de ces risques, car leurs données peuvent être dérobées, divulguées, altérées ou leurs opérations perturbées à distance. De la même manière, les individus risquent que leurs données personnelles et leur intimité soient exploitées par des gouvernements ou des entreprises. En outre, les forces militaires peuvent voir leurs capacités opérationnelles compromises par des actes de sabotage, de manipulation de l'information ou d'influence.

Une chose est certaine : le cyberspace génère des interactions particulièrement complexes entre différents domaines. Les mesures prises pour faire face à un risque ou saisir une opportunité dans un domaine entraînent souvent des conséquences dans

⁶ Weber, Rolf , Principes de la gouvernance de l'Internet: analyse comparative UNESCO, 2015, p. 24-35.

⁷ Douzet, Frédéric. « La géopolitique pour comprendre le cyberspace », Hérodote, vol. 152-153, no. 1-2, 2014, pp. 3-21.

d'autres domaines. Les enjeux sont souvent interconnectés. Dans ce contexte, la souveraineté des États sur leurs territoires respectifs fait face à une nouvelle réalité incarnée par le cyberspace, un domaine caractérisé par l'incertitude. Ainsi, il est crucial d'envisager le passage de la souveraineté traditionnelle, limitée à un territoire physique, vers une souveraineté plus « virtuelle ». Cependant, il ne faut pas négliger les défis auxquels les États doivent répondre dans un contexte où les géants du numérique (GAFAM, BATX, etc.) prennent une place prépondérante sur la scène internationale. Cette évolution appelle à une réévaluation du concept de souveraineté étatique.

D'UN ESPACE LIMITE A UN ESPACE SANS FRONTIERES.

Le cyberspace est un terme qui fait référence à l'ensemble des activités et des interactions qui ont lieu dans l'univers numérique, notamment sur Internet⁸. Ce nouveau territoire immatériel sans corps ni frontières peut être considéré comme un espace virtuel ou une extension de ce monde réel, dans lequel les individus et les organisations peuvent communiquer et échanger des informations, ainsi que des biens et des services. Le cyberspace est en constante évolution et est influencé par les technologies et les pratiques qui y sont utilisées.

Étroitement lié à l'avènement de la mondialisation, le cyberspace joue un rôle central dans la virtualisation des échanges financiers, l'augmentation de la circulation d'informations et la rapidité des échanges de biens, de services et entre particuliers.

Le cyberspace possède une réalité complexe, s'étendant à la fois de manière tangible et matérielle, construite sur des bases d'infrastructures bien concrètes. Une analyse approfondie du cyberspace révèle qu'il se compose de trois strates majeures qui sont interconnectées : une strate physique englobant l'assise technologique et les infrastructures matérielles de support (câbles sous-marins et terrestres, satellites en orbite basse, serveurs, centres de données, terminaux, etc.), une stratégie logique et programmatique englobant les systèmes d'information, les programmes, les langages et les protocoles responsables de la transmission des données entre deux points du réseau (logiciels), et une troisième stratégie cognitive ou sémantique qui correspondent à la partie directement perceptible par les utilisateurs.

Cette dernière englobe l'ensemble des interfaces qui agrègent une pléthore de données, qu'elles soient personnelles, militaires ou industrielles, engendrées par les divers usages numériques. Elle concentre également les informations en circulation

⁸ Boulanger, Philippe. « 9. Le cyberspace, nouvel espace de rivalités », , Planète médias. Géopolitique des réseaux et de l'influence, sous la direction de Boulanger Philippe. Armand Colin, 2021, p. 325-370.

dans le cyberspace, comme les contenus, les échanges en temps réel et les interactions, ainsi que les comportements issus d'identités numériques uniques ou multiples.

Fondamentalement, le cyberspace englobe à la fois des infrastructures matérielles localisées sur des territoires géographiques et politiques spécifiques, mais il constitue également un domaine d'échanges intangibles formé par la prolifique production de données, collecté automatiquement par des applications logicielles. Ces applications rassemblent, stockent et traitent les flux d'informations capturées dans divers buts (commerciaux, industriels, politiques, militaires) à travers l'usage de protocoles (langages) communs.

À la croisée du physique et du virtuel, le cyberspace ne correspond pas à un territoire géographique au sens conventionnel, mais plutôt à un quatrième élément qui complète la structure de l'écosystème territorial (air, mer et terre).

LE CYBERESPACE, UNE NOUVELLE FORME HYBRIDE DU TERRITOIRE

Le cyberspace reste un territoire nouveau aux défis propres. C'est un espace aussi bien physique que virtuel. Physique de par ses spécificités matérielles consacrées par les infrastructures, la technologie et les outils informatiques pour accéder au cyberspace, et virtuel du fait qu'il n'a pas de forme physique ou de localisation géographique précise, mais qu'il est accessible via des appareils connectés, tels que des ordinateurs, des téléphones intelligents et des tablettes.

En cela, le cyberspace peut être considéré comme une extension de notre monde physique, qui a des impacts sur notre vie quotidienne et sur la société dans son ensemble. En tant que territoire hybride, le cyberspace pose de nombreux défis et opportunités. C'est un monde complexe et dynamique, qui regroupe de nombreuses activités et interactions différentes, telles que la communication, le commerce en ligne, l'éducation, le divertissement, etc.

En tant qu'espace virtuel, le cyberspace est souvent décrit comme étant "immatériel" ou "incorporel", mais il peut tout de même avoir un impact important sur notre vie quotidienne et sur la société dans son ensemble.

Inutile de rappeler que le territoire est un espace géographique sur lequel un projet politique est mis en place, ceci implique son appropriation, pour exercer une domination directe ou une influence indirecte. Paradoxalement, le cyberspace est un espace numérique sur lequel on peut également installer un projet politique. Or, la

maîtrise du cyberspace reste fortement ambiguë étant donné qu'Internet peut être contrôlé par tous types d'acteurs qu'il s'agisse d'individus, entreprises, organisations ou encore les États⁹.

Le cyberspace peut être considéré comme un espace de liberté et de communication, qui permet à de nombreuses personnes de s'exprimer et de se connecter, indépendamment de leur localisation géographique. Toutefois, le cyberspace peut également être utilisé à des fins malveillantes, telles que la diffusion de propagande, la cybercriminalité, le cyber espionnage, etc. En tant que territoire hybride, le cyberspace pose de nombreux défis et opportunités pour les acteurs politiques et les gouvernements, qui doivent trouver un équilibre entre la protection des droits et des libertés individuelles, et la sécurité et la stabilité internationales. Les enjeux géopolitiques du cyberspace sont complexes et en constante évolution, et nécessitent une réflexion approfondie et une collaboration internationale pour trouver des solutions adéquates.

Depuis les années 2000, le cyberspace est devenu un nouvel enjeu géopolitique pour les États ¹⁰. Il est même considéré comme un nouvel espace de bataille, avec ses méthodes, ses moyens et ses tactiques propres, parallèlement aux autres espaces physiques (terre, mer, air).

L'enjeu géopolitique du cyberspace lui a valu une place prépondérante dans les discours des gouvernements, en tant que territoire porteur de menaces et qui requiert un contrôle et une surveillance avec pour objectif de lui remettre des frontières et de le soumettre à sa souveraineté.

Les exemples sont légion, mais celui de l'Estonie¹¹ en 2007 est le plus marquant. En effet, le pays a été la cible d'attaques ayant mis hors service les serveurs des administrations publiques, banques, hôpitaux et autres services de l'Etat, ce qui a dévoilé les vulnérabilités que pouvait entraîner la dépendance aux réseaux informatiques pour les États.

⁹ JEAN-SÉBASTIEN DUPRAT, Le cyberspace et ses enjeux géopolitiques, <https://major-prepa.com/geopolitique/cyberspace-enjeux-geopolitiques/>, 2 janvier 2022, Dernière modification : 7 janvier 2022.

¹⁰ Boulanger, Philippe. « Chapitre 9 - Le cyberspace, nouvel espace de rivalités », , Géopolitique des médias. Acteurs, rivalités et conflits, sous la direction de Boulanger Philippe. Armand Colin, 2014, p. 263-294.

¹¹ Considérée comme le pays le plus connecté au monde, ce pays baltique surnommé « E-stonia » en raison de son appétit pour les nouvelles technologies, a fait encore un pas dans cette direction, en entamant l'utilisation des services internationaux en nuage pour sauvegarder les données de l'e-gouvernement.

D'un côté, les attaques perpétrées contre la Géorgie en 2008¹² ont clairement démontré que les cyberattaques pouvaient être un soutien aux forces militaires dans le cadre d'un conflit armé. Cette nouvelle donne a fait des cyberattaques, restées jusque-là essentiellement entre les mains d'experts et de techniciens, un procédé qui sert de tactique militaire¹³.

Le cyberspace est ainsi devenu une question géopolitique ; il est à la fois un enjeu de rivalités de pouvoirs, un théâtre d'affrontement et une arme redoutable dans les conflits géopolitiques.

Les États ne sont pas les seuls acteurs des conflits du cyberspace, bien au contraire. À l'exception de certains pays, comme les États-Unis, la Chine et la Russie, le développement de la technologie et le développement de stratégies cyber adaptées à ces défis sont à la traîne. Les entrepreneurs, les start-ups, les criminels et les hackers, pour le meilleur ou pour le pire, peuvent désormais tirer parti de ces nouveaux outils plus rapidement et plus efficacement¹⁴.

Avec désormais plus de 2,5 milliards d'Internautes, l'émergence des géants du web¹⁵, et la multiplication des attaques de plus en plus raffinées, Les Etats sont fortement incités à reconsidérer les menaces à leur souveraineté. Nombre d'entre eux reviennent en force dans le cyberspace, faisant de la cyberdéfense et de la cybersécurité une priorité stratégique, à commencer par les États-Unis. Ainsi, le cyberspace représente à la fois des risques et des opportunités. Effectivement, la croissance exponentielle des réseaux peut avoir à la fois des effets positifs et négatifs sur les États.

¹² Tarkhan-Mouravi, George. « Les conflits en Géorgie suite à la guerre de 2008. (Traduit de l'anglais) », Les Cahiers de l'Orient, vol. 101, no. 1, 2011, p. 59-71.

¹³ « En 2007, à la suite d'une décision du gouvernement estonien de déplacer un mémorial de guerre datant de l'époque soviétique dans la ville de Tallinn, des hackers russes avaient semé la panique en attaquant simultanément les sites des ministères du pays ainsi que ceux de nombreuses entreprises privées, paralysant les principales institutions financières et les systèmes de télécommunication de l'état balte. Les mêmes techniques avaient vraisemblablement été employées lors de la crise géorgienne en 2008 et au début de la crise actuelle en Ukraine. Les autorités russes n'ont jamais reconnu être à l'origine de ces attaques, affirmant qu'il s'agissait du fait de hackers isolés. Et l'OTAN, prise au dépourvu, s'est rendue compte qu'elle n'avait pas de ligne politique claire ni de réponse à apporter à ce genre d'agression » peut-on lire dans la Tribune (Sauné 2014).

¹⁴ Selon cette théorie, « les individus interagissant les uns avec les autres, auraient tendance à s'agréger autour de « nœuds », personnes (ou entreprises) possédant une influence (ou technologie) supérieure aux autres et qui auraient donc le pouvoir de rassembler autour d'eux une grande partie de leur auditoire (ou de leurs clients) », Banque transatlantique, Les nouvelles menaces : le monopole des GAFAM et l'effet réseau, août 2019, <https://www.banquetransatlantique.com/fr/actualites/le-monopole-des-gafam.html>.

¹⁵ O. FEIERTAG, « Entre la nation et le marché : une histoire mondiale des grands monopoles », *Questions internationales* sept.-oct. 2021, *Les GAFAM, une histoire américaine*, p. 12.

D'un côté, les réseaux peuvent être une source d'opportunités pour les États. Ils peuvent par exemple permettre de développer l'économie en facilitant les échanges commerciaux, en créant de nouvelles industries et en offrant de nouvelles possibilités de travail. Les réseaux peuvent également être une source d'innovation en permettant à des idées et des technologies de se diffuser rapidement et de manière large.

D'un autre côté, la croissance exponentielle des réseaux peut également être source de risques pour les États¹⁶. Par exemple, elle peut entraîner une concentration de la richesse et du pouvoir dans les mains de certaines entreprises ou individus, ce qui peut avoir des effets négatifs sur la distribution de la richesse et la démocratie. Les réseaux peuvent également être utilisés à des fins malveillantes, comme la diffusion de fausses informations ou la pratique du cyberharcèlement. Enfin, la dépendance croissante des États aux réseaux peut les rendre vulnérables aux cyberattaques et aux perturbations de ces réseaux.

Il est vrai que la course à la donnée et à la technologie a des enjeux importants pour la souveraineté des États et leur capacité à faire appliquer leur volonté politique. La puissance d'un État ne se mesure pas uniquement à sa capacité militaire, mais aussi à sa capacité à innover et à développer de nouvelles technologies. Les grandes entreprises technologiques, les "BigTech", ont un rôle important à jouer dans cet écosystème et peuvent avoir une influence considérable sur les politiques publiques et les normes technologiques. Cela peut poser des défis pour les États, qui doivent trouver un équilibre entre la nécessité de s'appuyer sur ces entreprises pour innover et la nécessité de maintenir leur souveraineté et leur capacité à définir leur propre politique.

Il est donc important pour les États de trouver un équilibre entre les avantages et les risques de la croissance exponentielle des réseaux, et de mettre en place des réglementations et des politiques adéquates pour en tirer le meilleur parti tout en protégeant leurs intérêts et leur sécurité.

La course à la donnée et au Data Monde a certainement créé de nouveaux attributs de puissance¹⁷. La possession et l'utilisation efficace des données peuvent donner un avantage concurrentiel considérable aux entreprises et aux gouvernements qui en disposent, en leur permettant de prendre des décisions éclairées, de développer de nouvelles technologies et de créer de nouveaux produits et services. Les États qui

¹⁶ Philippe Vidal, « Quelle prise au sérieux du cyberspace pour la défense et la sécurité nationale ? Compte-Rendu de la thèse d'Alix Desforges », Netcom, 2018, p.201-206.

¹⁷ Vasseur, Gauthier. « Chapitre 5. Maximiser le potentiel de la donnée », Devenez un data pionnier ! Comprendre et exploiter les données en entreprise, sous la direction de Vasseur Gauthier. Mardaga, 2021, pp. 125-223.

sont en mesure de collecter et de traiter de grandes quantités de données peuvent également avoir un avantage dans les négociations internationales et dans la définition de normes et de réglementations.

Il est indéniable que la "Data Economy" a un impact important sur de nombreux aspects de la société. La collection, l'analyse et l'utilisation de données ont de nombreuses applications pratiques qui peuvent entraîner des répercussions sur les politiques, la géopolitique et l'économie. Par exemple, l'analyse de données peut être utilisée pour améliorer l'efficacité des gouvernements, influencer les décisions politiques, et même pour aider à prédire les tendances économiques et les comportements de consommation. En même temps, la "Data Economy" soulève également des questions importantes sur la vie privée et la protection de la confidentialité, ainsi que sur les inégalités économiques qui peuvent être amplifiées par l'utilisation inégale de ces technologies. De ce fait, l'accès et la capacité à exploiter et comprendre les données peuvent être considérés comme une forme de pouvoir.

La capacité de rendre les données transparentes ou invisibles, de les effacer, de les manipuler ou de les revendiquer peut avoir un impact important sur les relations de pouvoir. Par exemple, une entreprise qui détient de grandes quantités de données sur ses clients peut utiliser ces données de manière à influencer leurs comportements de consommation, ou à leur fournir des services personnalisés.

De même, un gouvernement qui a accès à de grandes quantités de données sur ses citoyens peut les utiliser pour prendre des décisions politiques éclairées

De même, la "mise en donnée du monde" peut avoir un impact important sur les relations de pouvoir entre les géants technologiques et les États, ainsi que sur les relations entre les États.

Les entreprises technologiques qui détiennent de grandes quantités de données sur les individus et les organisations peuvent avoir un pouvoir considérable en termes de capacité à influencer les comportements et les décisions. Les États, de leur côté, peuvent essayer de réglementer l'utilisation de ces données pour protéger les droits des individus et assurer une utilisation responsable des données. Les relations entre les États peuvent également être influencées par les données, en particulier lorsqu'il y a des différences dans l'accès aux données ou aux technologies d'analyse de données.

Force est de constater que l'exploitation du cyberspace peut être liée à l'utilisation et l'accès aux données¹⁸, car les données sont un élément central de nombreuses activités en ligne. Cependant, l'exploitation du cyberspace ne se limite pas

¹⁸ Frédéric Douzet et Alix Desforges, « Du cyberspace à la datasphère. Le nouveau front pionnier de la géographie », Netcom, 2018, p.87-108.

uniquement à l'utilisation et l'accès aux données, mais comprend également d'autres aspects tels que la sécurité en ligne, la vie privée et la liberté d'expression.

Le cyberspace est souvent considéré comme une extension de l'espace physique et peut être utilisé comme un moyen de refléter et d'influencer les relations géopolitiques. Par exemple, les États peuvent utiliser le cyberspace pour mener des campagnes de désinformation ou pour cibler des infrastructures critiques dans d'autres pays, ce qui peut avoir un impact sur les relations internationales et la stabilité géopolitique. De même, le développement de technologies de l'information et de la communication peut influencer la distribution des pouvoirs et des ressources dans le monde, et ainsi affecter la géopolitique. En ce sens, le cyberspace peut être considéré comme une représentation géopolitique, car il reflète et influe sur les relations et les dynamiques géopolitiques dans le monde.

Alix Desforges a mis en évidence le cyberspace comme représentation géopolitique¹⁹. Le cyberspace vient donc se surajouter à toutes nos cartes du monde, comme une nouvelle dimension de notre espace géographique, c'est un nouveau territoire à conquérir et à contrôler.

C'est de cette façon que Walter Peretti, Responsable Majeure Informatique Objets connectés et Sécurité à l'ESILV, a décrit des nouveaux enjeux du cyber espace, un nouveau territoire dont les Etats sont dans une course freinée pour le conquérir. C'est un combat de longue haleine que les Etats mènent quasi quotidiennement pour dominer cet espace et le soumettre à leur souveraineté²⁰.

Le cyberspace est devenu un élément important de la géopolitique mondiale en raison de son impact croissant sur les affaires économiques, les relations internationales et la sécurité nationale. Les gouvernements du monde entier sont de plus en plus conscients de l'importance de la sécurité en ligne et de la nécessité de protéger leur pays et leurs intérêts contre les cybermenaces.

En tant que tel, le cyberspace est devenu un enjeu important dans les relations internationales et a un impact significatif sur la géopolitique mondiale. L'information est en effet l'une des principales ressources du cyberspace et a une valeur économique considérable. L'accès à l'information de qualité et à jour peut être crucial

¹⁹ Desforges, Alix. « Les représentations du cyberspace : un outil géopolitique », Hérodote, vol. 152-153, no. 1-2, 2014, p. 67-81.

²⁰ Walter Peretti : « Normal donc d'y entendre le bruit des bottes numériques des états. Le cyberspace s'invite dans la géopolitique mondiale, son or noir : l'information, ses axes d'exploitation : acquérir plus d'information pour soi, compromettre l'accès à l'information de l'autre, ou mieux, fausser l'information à laquelle il a accès ».

pour la prise de décision dans les affaires et pour la compétitivité économique d'une entreprise ou d'un pays.

En outre, l'information peut également avoir une valeur stratégique pour les gouvernements et les militaires, qui ont besoin d'accéder à des données sensibles pour assurer la sécurité nationale et la défense de leur pays²¹.

En raison de sa valeur, l'information est souvent protégée par des mesures de sécurité pour empêcher son accès par des tiers non autorisés. Cela peut inclure la mise en place de firewalls et de systèmes de cryptage pour protéger les données contre les cybermenaces, ainsi que l'adoption de mesures de gestion de l'information pour s'assurer que seules les personnes autorisées ont accès aux données sensibles. En effet, contrôler le cyberspace est désormais le fantasme de tout État.

²¹ Hérisson, Audrey. « Le cyberspace, cet espace de confrontation à part entière », *Stratégie*, vol. 117, no. 4, 2017, pp. 231-246.

Références :

- Bertrand Badie. Un monde sans souveraineté. Les Etats entre ruse et responsabilité. In : Politique étrangère, n°2 - 1999 - 64^eannée. p. 410-411.
- Boulanger, Philippe. « 9. Le cyberspace, nouvel espace de rivalités », Planète médias. Géopolitique des réseaux et de l'influence, sous la direction de Boulanger Philippe. Armand Colin, 2021, p. 325-370.
- Boulanger, Philippe. « Chapitre 9 - Le cyberspace, nouvel espace de rivalités », Géopolitique des médias. Acteurs, rivalités et conflits, sous la direction de Boulanger Philippe. Armand Colin, 2014, p. 263-294.
- Coutau-Bégarie, Hervé. « Histoire et prospective de la souveraineté. Une relecture de Bertrand de Jouvenel et de Jacques Ellul », Prospective et stratégie, vol. 1, no. 1, 2010, p. 35-45.
- Considérée comme le pays le plus connecté au monde, ce pays baltique surnommé « E-stonia » en raison de son appétit pour les nouvelles technologies, a fait encore un pas dans cette direction, en entamant l'utilisation des services internationaux en nuage pour sauvegarder les données de l'e-gouvernement.
- Douzet, Frédéric. « La géopolitique pour comprendre le cyberspace », Hérodote, vol. 152-153, no. 1-2, 2014, pp. 3-21.
- Douzet, Frédéric. « La géopolitique pour comprendre le cyberspace », Hérodote, vol. 152-153, no. 1-2, 2014, pp. 3-21.
- Desforges, Alix. « Les représentations du cyberspace : un outil géopolitique », Hérodote, vol. 152-153, no. 1-2, 2014, p. 67-81.
- Nabli, Bélig. « Chapitre 8. Le statut de l'État en droit international », L'Etat. Droit et Politique, Armand Colin, 2017, p. 168-186.
- La connaissance de vulnérabilité informatique n'ayant fait l'objet d'aucune publication ou n'ayant aucun correctif connu, (vulnérabilité du jour zéro « zéro-day ») des systèmes d'exploitation, élaboration d'une ou plusieurs « charges utiles » permettant d'agir sur les systèmes de contrôle industriel et sur des automates programmables. Hacking par clé USB, le ver STUXNET qui a frappé les installations nucléaires iraniennes à l'été 2010 était conçu avec 4 « zero-day » et de 2 charges utiles, l'une déphasant les centrifugeuses, l'autre perturbant les systèmes de contrôle qui n'ont rien remarqué.
- Weber, Rolf, Principes de la gouvernance de l'Internet : analyse comparative UNESCO, 2015, p. 24-35.
- JEAN-SÉBASTIEN DUPRAT, Le cyberspace et ses enjeux géopolitiques, <https://major-prepa.com/geopolitique/cyberspace-enjeux-geopolitiques/>, 2 janvier 2022, Dernière modification : 7 janvier 2022.
- Tarkhan-Mouravi, George. « Les conflits en Géorgie suite à la guerre de 2008. (Traduit de l'anglais) », Les Cahiers de l'Orient, vol. 101, no. 1, 2011, p. 59-71.
- « En 2007, à la suite d'une décision du gouvernement estonien de déplacer un mémorial de guerre datant de l'époque soviétique dans la ville de Tallinn, des hackers russes avaient semé la panique en attaquant simultanément les sites des ministères du pays ainsi que ceux de nombreuses entreprises privées, paralysant les principales institutions financières et les systèmes de télécommunication de l'état balte. Les mêmes techniques avaient vraisemblablement été employées lors de la crise géorgienne en 2008 et au début de la crise

actuelle en Ukraine. Les autorités russes n'ont jamais reconnu être à l'origine de ces attaques, affirmant qu'il s'agissait du fait de hackers isolés. Et l'OTAN, prise au dépourvu, s'est rendue compte qu'elle n'avait pas de ligne politique claire ni de réponse à apporter à ce genre d'agression » peut-on lire dans la Tribune (Sauné 2014).

- Selon cette théorie, « les individus interagissant les uns avec les autres, auraient tendance à s'agréger autour de « nœuds », personnes (ou entreprises) possédant une influence (ou technologie) supérieure aux autres et qui auraient donc le pouvoir de rassembler autour d'eux une grande partie de leur auditoire (ou de leurs clients) », Banque transatlantique, Les nouvelles menaces : le monopole des GAFAM et l'effet réseau, août 2019, <https://www.banquetransatlantique.com/fr/actualites/le-monopole-des-gafam.html>.
- O. FEIERTAG, « Entre la nation et le marché : une histoire mondiale des grands monopoles », Questions internationales sept.-oct. 2021, Les GAFAM, une histoire américaine, p. 12.
- Philippe Vidal, « Quelle prise au sérieux du cyberspace pour la défense et la sécurité nationale ? Compte-Rendu de la thèse d'Alix Desforges », Netcom, 2018, p.201-206.
- Vasseur, Gauthier. « Chapitre 5. Maximiser le potentiel de la donnée », Devenez un data pionnier ! Comprendre et exploiter les données en entreprise, sous la direction de Vasseur Gauthier. Mardaga, 2021, pp. 125-223.
- Frédéric Douzet et Alix Desforges, « Du cyberspace à la datasphère. Le nouveau front pionnier de la géographie », Netcom, 2018, p.87-108.
- Walter Peretti : « Normal donc d'y entendre le bruit des bottes numériques des états. Le cyberspace s'invite dans la géopolitique mondiale, son or noir : l'information, ses axes d'exploitation : acquérir plus d'information pour soi, compromettre l'accès à l'information de l'autre, ou mieux, fausser l'information à laquelle il a accès ».
- Hérisson, Audrey. « Le cyberspace, cet espace de confrontation à part entière », Stratégique, vol. 117, no. 4, 2017, pp. 231-246.