Géopolitique du cyberespace : « territoire », frontières et conflits

AUTEURS
Frédérick DOUZET, CRAG (France)
Alix DESFORGES, CRAG (France)
Kevin LIMONIER, CRAG (France)

RÉSUMÉ
Le cyberespace ne correspond pas à la définition classique d'un espace géographique et encore moins à celle d'un territoire. Les acteurs du cyberespace mettent pourtant en œuvre des stratégies spatialisées voire territorialisées. On observe ainsi que la représentation d'un cyberespace comme territoire domine chez ses acteurs qui se battent pour se l'approprier, le contrôler ou en défendre l'indépendance, voire pour le « militariser ». La démarche géopolitique, par l'analyse des représentations, permet de comprendre le processus de territorialisation dont le cyberespace fait l'objet et sa fonction dans les conflits relatifs aux enjeux de l'Internet. Elle permet en outre, d'analyser les enjeux de pouvoir et les rivalités qui se jouent pour ce territoire imaginé, à l'heure où les attaques informatiques se multiplient et que les États, soucieux de la défense de leurs pouvoirs régaliens, reviennent en force dans le cyberespace pour défendre leur souveraineté, protéger leurs valeurs ou affirmer leur puissance.

MOTS CLÉS
Géopolitique, cyberespace, territorialisation, conflits, Internet

ABSTRACT
The term "cyberspace" does not correspond to the classical definition of space in geography, let alone of territory. Yet, actors of cyberspace apply geographical strategies. The representation of cyberspace as a territory is widespread among these actors who fight for its appropriation, control, independence or even militarization. The geopolitical approach helps to understand the territorialisation process of cyberspace and its function within conflicts. It enables us to analyse the power games and struggles for this imagined territory, in a context of proliferation of cyberattacks and state policies. Concerned about the challenges to their powers and privileges, nation states strike back in cyberspace to defend their sovereignty, protect their values or assert their power.

KEYWORDS
Geopolitics, cyberspace, territorialisation, conflicts, Internet

INTRODUCTION

Alors même que le terme « cyberespace » ne possède pas de définition consensuelle, il est de plus en plus utilisé dans les médias et étudié dans les sciences humaines et sociales. S'il en a l'étymologie, le cyberespace ne constitue pas un espace géographique et moins encore un territoire tel que défini par Yves Lacoste, à savoir « une étendue sur laquelle vit un groupe humain qu'il considère comme sa propriété collective » (2003). Qualifié de « monde virtuel », le cyberespace est souvent identifié, y compris par les géographes, comme constitutif d'une nouvelle forme d'espace hors de

l'espace géographique dit classique mais qui viendrait s'y superposer ou fusionner avec lui (Rosière, 2009). Pour les acteurs qui se battent pour se l'approprier, le contrôler, en défendre l'indépendance ou le « militariser », il est largement perçu et imaginé comme un territoire. En d'autres mots, il est déjà au cœur de conflits géopolitiques qui sont loin de n'être que virtuels ; des conflits géopolitiques qui s'ancrent dans une réalité spatio-temporelle précise. Dans ce contexte, l'analyse géopolitique qui étudie les rivalités de pouvoir sur un territoire à différents niveaux d'analyse constitue un outil essentiel dans la compréhension de ces conflits (Douzet et Cattaruzza, 2013 ; Desforges, 2013). Nous prendrons ici l'exemple de la stratégie des États pour montrer comment les acteurs mobilisent cette représentation du cyberespace afin de défendre leurs intérêts et leur souveraineté. Nous montrerons comment cette représentation, en retour, influe sur leurs actions.

Nous verrons que s'il ne constitue pas un territoire à proprement parler, le cyberespace est soumis à un processus mental de territorialisation qui produit non pas une mais plusieurs représentations du cyberespace parfois antagonistes. Ces représentations sont par la suite mobilisées dans l'expression des conflits induits et véhiculés par le cyberespace qui est à la fois l'enjeu, le théâtre et l'outil de rivalités de pouvoir entre les acteurs qu'ils soient États, individus ou entreprises.

1. CYBERESPACE : LA REPRÉSENTATION D'UN TERRITOIRE

Une représentation est « une construction, un ensemble d'idées plus ou moins logiques et cohérentes » (Lacoste, 2003). Elle « décrit, exprime une partie de la réalité, de façon floue ou précise, déformée ou exacte ». Une représentation se nourrit de faits objectifs mais garde un caractère profondément subjectif. Dans le cadre d'un conflit, les représentations ne sont pas neutres, elles ont une fonction. Elles façonnent la stratégie des acteurs, ont le pouvoir de convaincre, de susciter l'adhésion à une stratégie, de provoquer l'inquiétude, voire la peur, ou encore d'entraîner la mobilisation d'acteurs ou d'électeurs.

Le terme « cyberespace » jouit d'un certain flou sémantique. Il n'existe en effet aucune définition consensuelle de ce terme issu de la littérature de science fiction (Gibson, 1982) et désormais utilisé dans les discours politiques et stratégiques des États mais aussi des organisations internationales, des entreprises et des médias. On notera cependant l'importance d'un lexique géographique, principalement emprunté à la mer : on *navigue* dans le cyberespace, on emprunte des *passerelles*, des *canaux*, des *ports*, etc. À travers la littérature relative au cyberespace, on observe que les acteurs des conflits se représentent le cyberespace comme un territoire et même un champ d'affrontement au même titre que la terre, la mer, l'air et l'espace.

Perçu principalement comme une entité supranationale, « sans frontière », qui viendrait se superposer au territoire des États pour l'anamorphoser (Musso, 2003), le cyberespace est parfois considéré comme une entité politique distincte des États. D'ailleurs, pour ceux qui en ont la conception la plus libertaire, comme les *Anonymous*, il aurait toutes les caractéristiques d'un territoire indépendant : une population (les internautes), un mode de gouvernance propre (la logique de réseau) qui produirait une nouvelle société, celle de l'information (Castells, 2002). Cette logique est empreinte d'idées et de valeurs positivement connotées (pas de centre, pas de contrôle) et reflète la culture contestataire des campus californiens des années 1960 et 1970 au sein desquels est né l'Internet. Ce

territoire serait en outre affranchi des règles du monde physique, abolissant le temps et la distance. Il s'ancre pourtant dans une réalité spatiale et politique indéniable, ne serait-ce que par l'infrastructure du réseau qui le génère, faite de routeurs, de nœuds et de câbles parfaitement localisables à un point précis du globe et qui relèvent de juridictions précises (Douzet, 2013 ; Betz et Stevens, 2011).

Historiquement, cette représentation territoriale du cyberespace est développée par les pionniers de l'Internet dans les années 1990. Elle apparaît au moment de la naissance du web (l'application qui allait démocratiser l'usage de l'Internet) pour défendre l'idée d'un territoire indépendant ; un territoire que les États ne devraient pas réguler. Une déclaration d'indépendance du cyberespace est d'ailleurs rédigée en ce sens par John Perry Barlow (co-fondateur de l'*Electronic Frontier Foundation*, puissant *lobby* américain militant pour les libertés numériques) en 1996 affirmant que les États ne possèdent aucune souveraineté pour intervenir dans le cyberespace. Ce texte fait référence de façon très marquée aux concepts de la construction politique des États-Unis. Et si son auteur a depuis modéré ses propos, ce texte demeure pour certains une référence. Si la formulation d'une représentation territoriale du cyberespace est relativement récente, le processus de territorialisation est antérieur à l'existence même de l'Internet et prend sa source dans l'émergence du concept de réseau (Musso, 2003).

Le terme « cyberespace » tombe par la suite en désuétude alors que les conflits commencent à se multiplier. Il faudra attendre le milieu des années 2000 pour assister à la remobilisation de cette représentation, cette fois dans une acception contradictoire. Elle est en effet fortement présente dans les discours des États qui doivent faire face à des attaques informatiques de plus en plus nombreuses et de plus en plus complexes et qui s'inquiètent de la possible remise en cause de leurs pouvoirs régaliens. Ils mobilisent alors cette représentation pour légitimer des velléités d'action et pour mieux affirmer leur souveraineté dans le cyberespace, en cherchant à y remettre des frontières. Les États mobilisent ainsi une représentation du cyberespace à l'opposée de celle des pionniers de l'Internet, celle d'un territoire à contrôler, sinon à maîtriser, voire à conquérir. Il s'agit avant tout de faire appliquer leurs lois et de défendre leurs valeurs au sein du cyberespace, garantir leur sécurité et assurer leur défense. Les États cherchent alors à définir leur parcelle de cyberespace national.

L'exemple de la Russie est à ce titre particulièrement pertinent. L'État russe n'utilise pas dans ses textes officiels le terme cyberespace et lui préfère, pour des questions de stratégie de contrôle de l'information, la notion plus large « d'espace informationnel ». Cependant, il développe la représentation d'un cyberespace propre à la Russie, le « *Runet* ». L'idée du *Runet* est bâtie sur celle d'altérité par rapport à l'Internet « mondialisé » d'inspiration occidentale. On trouve sur le web de nombreux textes écrits par des internautes russophones vantant les mérites de cet espace « alternatif », non pas dans ses caractéristiques techniques (il ne s'agit pas d'un *usenet* [1]), mais dans ses pratiques culturelles. Les vecteurs identitaires qui fondent cette altérité sont à trouver dans l'expérience de la transition post-soviétique et la disparition de l'URSS en tant qu'entité politique, qui demeure un fort vecteur d'identification dans tous les pays issus de son éclatement : il existe une véritable identité, communauté de langue, de culture qui relie les internautes

1 *Usenet* : ensemble de machines reliées à différents réseaux qui véhiculent des articles postés dans des groupes de discussions (Dictionnaire de l'informatique et de l'Internet).

de ces différentes républiques et leurs permet de recréer en ligne cette communauté qui serait inéluctablement destinée à vivre ensemble et partager une histoire commune, une communauté de destin. À l'échelle internationale, le gouvernement russe a dénoncé à l'Union internationale des Télécommunications, lors du Sommet de Dubaï en décembre 2012, la toute-puissance américaine en matière de contrôle du réseau. La position défendue par la Russie est assez proche de celle qui s'est développée sur le *Runet* : il faut donner des droits égaux aux États pour réguler l'Internet, afin de limiter la suprématie américaine et permettre l'émergence de « réseaux souverains », très attachés à leurs zones géopolitiques de prédilection.

La représentation d'un cyberespace comme territoire est ainsi mobilisée dans deux conceptions diamétralement opposées. D'une part, celle d'un territoire indépendant, sans frontières, qu'il faut préserver de tout contrôle et, d'autres part, pour les États, celle d'un territoire à conquérir et à contrôler, sur lequel il faut affirmer sa souveraineté, ses frontières et sa puissance. Ces deux visions de la territorialisation du cyberespace induisent des rivalités fortes qui s'expriment parfois de façon brutale, notamment par le biais d'attaques informatiques. Le cyberespace devient donc à la fois le vecteur et l'objet de rivalités de pouvoir entre acteurs pour son contrôle, sa domination et la régulation de ses activités.

2. CYBERESPACE : DES CONFLITS GÉOPOLITIQUES ENTRE DIFFÉRENTS ACTEURS

Pour les États, le cyberespace menace leurs pouvoirs régaliens (sécurité du territoire, défense, souveraineté financière et économique). Il présente autant de risques que d'opportunités pour l'affirmation de leur puissance économique, militaire ou politique (outils de renseignement, intelligence économique, influence culturelle et diplomatique, cybercapacités militaires). On constate ainsi une multiplication des conflits pour son contrôle et sa régulation. Les États non démocratiques défendent l'idée d'un contrôle étatique d'un Internet « souverain » et sont particulièrement actifs en matière de censure et de filtrage. Mais les États démocratiques ne sont pas en reste.

Au niveau militaire, les conflits dans le cyberespace se jouent en marge des champs traditionnels des conflits géopolitiques. L'attaque des centrifugeuses iraniennes de Natanz par le virus Stuxnet, élaboré par les services américains et israéliens, constitue une nouvelle forme d'action. Le cyberespace devient alors un théâtre d'opération au même titre que la terre, la mer, l'air et l'espace et leur est complémentaire dans l'action militaire. Il existe cependant une différence majeure : le cyberespace n'est pas un milieu naturel, il est entièrement construit, régi et pensé par l'homme. On observe pourtant que les doctrines militaires appliquées au cyberespace sont conçues par analogie à des champs militaires connus, comme la dissuasion nucléaire par exemple. Or le cyberespace pose un défi à un certain nombre de concepts stratégiques ou de normes dans les conflits géopolitiques en raison de ses spécificités (caractère intangible, faible régulation, forte accessibilité, vitesse des échanges). Les attaques menées via les réseaux entraînent des difficultés d'appréhension, d'anticipation, d'attribution, de riposte et donc de planification stratégique.

Pour autant, les conflits du cyberespace ne peuvent être dissociés des conflits réels et des autres moyens d'action. Ainsi, l'étude de ces conflits nécessite une

compréhension des enjeux géopolitiques, des rapports de force et des stratégies de contrôle et de pouvoir dans le cyberespace, mais également en dehors. Les conflits du cyberespace s'ancrent dans des rivalités géopolitiques classiques qui peuvent dégénérer en cas d'attaque sérieuse. Certains États, dont la France, ont d'ailleurs déclaré qu'une attaque informatique de grande ampleur pourrait être à l'origine d'une action militaire.

Mais le cyberespace n'est pas l'apanage des États et de nombreux acteurs non étatiques cherchent également à profiter de la puissance du réseau pour servir leurs intérêts (forces politiques, groupes terroristes, militants, criminels, etc.), y compris au sein d'un même État. Des moyens d'actions moins coûteux et une logistique moindre permettent à ces petits acteurs non étatiques de lancer une attaque informatique qui pourrait déstabiliser un État alors qu'ils n'ont pas les moyens de monter une armée ou même une arme nucléaire.

Parmi les acteurs des conflits du cyberespace, les acteurs privés, comme les entreprises, jouent un rôle grandissant. Les géants du web comme Google, Facebook ou Amazon amassent des quantités de données sur les citoyens et les États eux-mêmes. Certains chercheurs estiment que Google connaîtrait mieux les Français que l'INSEE (Grumbach et Frénot, 2013). Ces données font l'objet de fortes rivalités pour leur contrôle, tant pour les questions relatives à la protection des libertés individuelles et de la vie privée que pour leur exploitation économique, politique et stratégique. Leur statut et leur exploitation dépendent de la législation du pays d'origine de ces entreprises ; des entreprises qui sont aujourd'hui très majoritairement américaines. Au-delà des enjeux économiques, ces données sont aussi stratégiques, d'autant que ces entreprises peuvent également exercer une forme de souveraineté des États dans le cyberespace, prolongeant leur zone d'influence ou collaborant à leur effort de renseignement. En 2009, le Département d'État américain avait expressément demandé à Twitter de repousser une opération de maintenance qui devait avoir lieu sur la zone iranienne alors que les manifestants opposés à la réélection d'Ahmadinejad utilisaient le service de *microblogging* pour s'organiser. Face à ces puissances numériques, certains pays, comme la Russie, développent leurs propres plateformes. Les Facebook et Google y ont leurs équivalents, respectivement Vkontakte et Yandex en Russie ou Renren et Weibo en Chine. Ces États s'appuient sur le succès de ces géants nationaux pour se préserver de l'influence occidentale.

CONCLUSION

La représentation d'un cyberespace comme territoire est particulièrement forte et pose de nombreux défis, pour les États mais également pour les chercheurs, dans l'appréhension de cet objet qui a émergé depuis une vingtaine d'années. Le cyberespace ne constitue pourtant pas un territoire géographique, ni un monde à part, virtuel et hors du temps et de l'espace. Il n'existe que par l'action de l'homme. Ainsi les conflits relatifs au cyberespace ne peuvent se comprendre en dehors de tout contexte géopolitique. Leur étude nécessite ainsi de tenir compte des représentations fortes qu'il véhicule et qui sont elles-mêmes porteuses de conflits. Leur analyse doit faire également l'objet d'une approche pluridisciplinaire, notamment avec des informaticiens, pour en saisir les enjeux, y compris ceux qui se cachent derrière des standards techniques qui peuvent pourtant avoir des impacts politiques.

RÉFÉRENCES

Betz D., Stevens T., 2011, *Cyberspace and the State, Toward a strategy for cyber-power*, London, Routledge.

Castells M., 2002, *La galaxie Internet*, Paris, Fayard.

Cattaruzza A., Douzet F., 2013, « Le cyberespace au cœur des tensions géopolitiques internationales », *DSI Magazine* Hors Série, n° 32, pp. 16-18.

Desforges A., 2013, « Les frontières du cyberspace », *in* Douzet F., Giblin B. (dir.), *Des frontières indépassables*, Paris, Armand Colin, pp. 101-12.

Gibson W., 1982, “Burning Chrome”, *Omni Magazine*.

Grumbach S., Frénot S., 2013, « Les données puissance du futur », *Le Monde* du 7 janvier 2013 [en ligne http://www.lemonde.fr/idees/article/2013/01/07/les-donnees-puissance-du-futur_1813693_3232.html].

Kramer F. *et al*., 2009, *Cyberpower and National Security*, Dulles, National Defense University Press–Potomac Books.

Lacoste Y. (dir.), 2003, *Dictionnaire de géographie*, Paris, Armand Colin.

Musso P., 2003, *Critique des réseaux*, Paris, PUF.

Rosière S., Cox K. *et al*., 2009, *Penser l’espace politique*, Paris, Ellipses.

LES AUTEURS

Frédérick Douzet
CRAG
Université Paris 8
Chaire Castex de cyberstratégie
fdouzet@gmail.com

Alix Desforges
CRAG
Université Paris 8
Chaire Castex de cyberstratégie
alix.desforges@gmail.com

Kevin Limonier
CRAG
Université Paris 8
kevin.limonier@gmail.com