



L'Espace Politique

Revue en ligne de géographie politique et de géopolitique

40 | 2020-1

Pensées émergentes en géographie politique et géopolitique + Varia

Le rôle de la topologie d'Internet dans les territoires en conflit en Ukraine, une approche géopolitique du routage des données

A Geopolitical Approach to Routing, The Impact of Internet Topology in Disputed Territories in Ukraine

Louis Pétoniaud et Loqman Salamatian



Édition électronique

URL : <https://journals.openedition.org/espacepolitique/8031>

DOI : 10.4000/espacepolitique.8031

ISSN : 1958-5500

Éditeur

Université de Reims Champagne-Ardenne

Ce document vous est fourni par Columbia University Libraries

[COLUMBIA UNIVERSITY LIBRARIES](#)

Référence électronique

Louis Pétoniaud et Loqman Salamatian, « Le rôle de la topologie d'Internet dans les territoires en conflit en Ukraine, une approche géopolitique du routage des données », *L'Espace Politique* [En ligne], 40 | 2020-1, mis en ligne le 21 octobre 2020, consulté le 02 octobre 2025. URL : <http://journals.openedition.org/espacepolitique/8031> ; DOI : <https://doi.org/10.4000/espacepolitique.8031>

Ce document a été généré automatiquement le 16 février 2023.



Le texte seul est utilisable sous licence CC BY-NC-ND 4.0. Les autres éléments (illustrations, fichiers annexes importés) sont susceptibles d'être soumis à des autorisations d'usage spécifiques.

Le rôle de la topologie d'Internet dans les territoires en conflit en Ukraine, une approche géopolitique du routage des données

A Geopolitical Approach to Routing, The Impact of Internet Topology in Disputed Territories in Ukraine

Louis Pétoniaud et Loqman Salamatian

Introduction

La numérisation des champs sociaux

- 1 Le développement d'Internet dans un nombre toujours plus important de champs sociaux a bousculé la pensée géographique traditionnelle. La mise en place de ce réseau mondial, permettant des échanges de données, d'informations et de communications d'une rapidité inédite, a contribué à repenser notre rapport au temps et à l'espace. Ces transformations sont dans le prolongement des progrès technologiques effectués dans les communications et les transports depuis le milieu du XV^e siècle et particulièrement depuis le XIX^e. Internet se démarque cependant la rapidité de sa mise en place, son caractère de plus en plus incontournable et enfin par ses caractéristiques d'adaptabilité. Internet permet en effet la « datafication du monde » (Cattaruzza, 2019), c'est-à-dire la transformation de larges pans de tous les champs sociaux en données numériques, Internet est devenu un socle utile, parfois nécessaire (Szozkiewicz, 2018), à une très grande diversité d'activités humaines, qu'elles soient économiques, sociales, politiques. Autrement résumé par Henry Bakis (2013), « le monde est devenu tellement dépendant des réseaux de la communication électronique que l'on n'ose plus penser le fonctionnement économique, social, culturel sans eux » (Bakis, 2013, p.296). L'accès à Internet s'accroît exponentiellement dans le monde : aujourd'hui, environ la moitié de

la population globale, et plus de 80 % de celle des pays les plus développés¹, peuvent se connecter. L'adaptabilité d'Internet fait en conséquence augmenter toujours le nombre et la diversité des activités humaines qui en dépendent. La numérisation apparaît progressivement dans l'ensemble des champs sociaux et politiques : circuits bancaires et financiers, gestion des ressources ; gouvernance et gouvernement ; gestion de la santé ; communication au sens large ; « plateformes » ou « uberisation » de pratiques de déplacements ou de loisirs ; éducation etc. Toutes ces activités, dont une partie répond à des besoins fondamentaux, se fondent désormais sur la capacité du réseau à échanger des données à grande vitesse sur des distances importantes.

- 2 En retour, l'augmentation de ces pratiques accroît la nécessité de relier au réseau le plus possible l'ensemble de la population, dans certains États en particulier, comme en Estonie (Margetts, Naumann, 2017)². Progressivement, l'idée de faire de l'accès à Internet un droit fondamental s'impose dans les organisations internationales et les gouvernements. Les progrès constants de la connectivité et des objets connectés amènent par ailleurs à imaginer un futur où Internet n'est plus seulement un instrument utile, mais un système de grande adaptabilité, bientôt indispensable à la plupart des activités économiques, à l'exercice de la citoyenneté, et plus généralement, à la fabrique du tissu social. Par sa progressive ubiquité et ses caractéristiques intrinsèques de rapidité et d'apparente immatérialité, Internet a amené à repenser la place des réseaux de données numériques dans l'espace et dans les rivalités de pouvoir qui s'y jouent.

Penser la géographie d'Internet

- 3 Les questions géographiques qui ont d'abord accompagné l'avènement d'Internet ont souvent produit des approches attribuant à ce réseau une prévalence sur la topographie et le territoire. Nombre d'auteurs ont imaginé comment Internet pourrait provoquer une « fin » – du moins une forme d'obsolescence – de la géographie (O'Brien, 1992 ; Virilio, 1997, 1998), de la souveraineté (Camilleri et Falk, 1992), ou encore, dans une approche plus mesurée, son dépassement partiel par l'émergence d'ensembles spatiaux nouveaux, telle la ligue hanséatique numérique décrite par Jacques Lévy (1997), une « cyberhanse », échappant aux contrôles étatiques. Ces formes d'extraterritorialité apposées à Internet se sont par exemple incarnées dans l'usage répandu du vocable mal défini de « cyberspace » (Desforges, 2018). La revendication politique d'un tel espace est alors symbolisée par la populaire *Déclaration d'indépendance du cyberspace* de John Perry Barlow³, adressée aux gouvernements des pays industriels : « Vos concepts de propriété, d'expression, d'identité, de mouvement et de contexte ne s'appliquent pas à nous. Ils sont fondés sur la matière, et il n'en est aucune ici ». Le milieu des années 1990 est marqué aussi par la popularisation de l'expression « village global » (MacLuhan, 1962) pour désigner l'apparition, grâce à Internet ou le World Wide Web, d'une forme de civilisation mondiale.
- 4 En parallèle et en réponse, sont apparus au tournant des années 2000 des critiques de ces mythes liés au cyberspace (Moisy, 1997 ; Van Alstyne et Brynjolfsson, 1997), et des études, souvent axées sur des parties spécifiques du réseau, de l'ancrage topographique d'Internet. Frédéric Lasserre (2000) insiste en économie sur le côté illusoire de la fin de la géographie, et des géographes rappellent l'existence des infrastructures physiques (câbles, serveurs, centres de données, etc.), qui demeurent sous juridictions étatiques,

ou soumis à des turbulences géomorphologiques, climatiques, ou humaines⁴ (Kitchin et Dodge, 2001).

- 5 Emmanuel Eveno (2004) retrace ainsi les nombreuses approches – en géographie mais aussi en science des télécommunications, sociologie, philosophie etc. – qui font se rencontrer TIC (technologies de l'information et de la communication), espace, et société. Ce faisant, il met ainsi en exergue la nécessité d'une « controverse », et propose une approche transversale, dans laquelle « ces Techniques prennent sens dans les dimensions socio-spatiales, [...] elles en sont une composante parmi d'autres. » (Eveno, 2004, p.129)
- 6 Les approches géographiques d'Internet évoluent au cours des années 2000 avec la multiplication de ses usages, et en particulier avec l'avènement du « web 2.0 » qui permet l'émergence des réseaux sociaux. Dès lors, Internet peut être conçu comme un outil servant à la production d'espace, ou de « lieux » spécifiques. Boris Beaudé (2012) qualifie ce processus de synchronisation, c'est-à-dire la possibilité de « se donner un espace commun pour être et pour agir, [...] le pendant spatial de la synchronisation » (Beaudé, 2012, p.66-67), favorisant des formes d'auto-organisation (Loveluck, 2015).
- 7 La géographie des réseaux au niveau des infrastructures physiques et protocolaires est resté un sujet d'étude relativement peu exploité. L'interaction entre le territoire et ces réseaux de données pose question. Si les définitions les plus classiques du territoire se rapportent à « un espace à métrique topographique » (Lévy et Lussault, 2013), un ensemble de définitions topologiques (réticulaires, archipélagiques) inscrivent Internet, ressource à la fois matérielle et symbolique, dans la production du territoire. Il est ainsi cohérent que la méthode géopolitique, qui étudie les rivalités de pouvoir sur des territoires, se soit rapidement saisie d'Internet.
- 8 En géopolitique, l'appropriation de cet objet à partir de la fin des années 1990 questionne également l'existence d'un espace créé par Internet dans ou *via* lequel se développent des rivalités de pouvoir, notamment entre Etats souverains (Douzet, 1997). La multiplication d'importantes cyberattaques à la fin des années 2000⁵ mettent au jour l'émergence d'une « menace systémique » sur un monde de plus en plus numérisé, dépendant d'un grand nombre d'infrastructures ancrés dans la topographie (Bakis, 2013).
- 9 L'émergence d'acteurs économiques puissants issus du « web 2.0 » tels que les « GAFAM » – Google, Amazon, Facebook, Apple et Microsoft – a par ailleurs amené à reconsidérer les rapports de force entre Etats ou entre Etats et entreprises, avec semble-t-il plus d'acuité que dans les époques précédentes (Douzet, 2014). C'est notamment la question de la superpuissance américaine dans le domaine numérique qui a été et reste posée, par la question des organismes régulateurs d'Internet (Lacroix, 2014), ou par celles posées par les révélations d'Edward Snowden en 2013 (Pétiniaud, 2014). Ce sont aussi et enfin les enjeux de maîtrise des données – production, transit, stockage – qui ont nourri des questionnements sur la territorialisation du réseau et de ses produits (Cattaruzza, 2019).
- 10 Les interactions croissantes du réseau et du politique amènent cependant à poser plus directement encore la question du rôle d'Internet dans des conflits territoriaux. A l'inverse d'un Internet dématérialisé, l'évolution du réseau et des acteurs politiques concernés indique un « tournant vers l'infrastructure » (Musiani, 2016), y compris dans les questions géopolitiques. L'infrastructure, définie au sens large, comprend autant les câbles sous-marins, les centres de données et les serveurs que les nombreux protocoles

qui façonnent Internet. De manière croissante, la compréhension et la maîtrise des infrastructures sont au centre d'enjeux politiques et territoriaux majeurs. Au niveau protocolaire notamment, les « couches basses »⁶ d'Internet contiennent et produisent des informations géographiques qui, tout en présentant des difficultés de récolte, de traitement et d'analyse, n'en demeurent pas moins de précieuses ressources pour créer des méthodes de recherche nouvelles. Cet article vise ainsi à proposer une approche empirique de l'analyse de données numériques issues d'un des protocoles majeurs d'Internet : le *Border Gateway Protocol* (BGP). Il propose également de renouveler les questionnements sur la notion d'espace numérique portés par l'avènement d'Internet, en dépassant la dualité entre topologie et topographie. La description du fonctionnement du cœur du réseau Internet, au niveau BGP, montre que cette dualité n'est pas exclusive. Au contraire, son fonctionnement peut s'analyser simultanément de manière topographique dans un espace géographique et de manière topologique dans un espace appartenant à « une famille d'espace particulière, définie par une métrique à dominante topologique » (Lévy, 1997). Cette ambivalence a des implications en termes géopolitiques : ces deux espaces, bien qu'en interaction, présentent des anomalies lors du transfert des données. Ces anomalies renseignent sur des rivalités de pouvoir dans le réseau qui rejaillissent sur les territoires observés. Le cas d'étude des conflits territoriaux en Ukraine, en Crimée et dans les régions du Donbass, montre comment le niveau protocolaire d'Internet s'intègre à des rivalités territoriales et contribue ainsi à des logiques de puissance traditionnelles.

Le cœur topologique d'Internet

Les systèmes autonomes : unité de base du réseau

- ¹¹ Internet est caractérisé par son absence de centralité. Son fonctionnement résulte de l'interconnexion d'environ 60 000 réseaux⁷ nommés les Systèmes Autonomes (*Autonomous System*, AS). Un AS est lui-même un plus petit réseau, qui a plusieurs fonctions principales. D'abord, il décide de son routage interne, donc de comment les données transitent à l'intérieur de celui-ci. Ensuite, il distribue des adresses IP, en général à ses clients : une adresse IP constitue l'identifiant d'une machine (modem de particulier, page web, etc.) sur le réseau, qui est compréhensible par les autres machines. Enfin et surtout, un AS définit ses politiques d'accessibilité, c'est-à-dire lesquels des autres systèmes autonomes peuvent accéder à lui pour faire transiter des données jusqu'à une adresse IP. Ainsi deux AS se connectent par l'intermédiaire de câbles physiques qui relient leurs réseaux et d'accords signés au préalable visant à définir les modalités de l'échange. Ces accords, appelés *accords BGP*, sont généralement de deux natures : (1) client-fournisseur lorsqu'un AS de taille moindre paie pour accéder au réseau d'un autre AS plus conséquent et (2) *peering* lorsque deux AS de taille équivalente acceptent d'échanger du trafic gratuitement.
- ¹² Il existe une grande diversité de systèmes autonomes, notamment par leur taille et leur importance. La taxonomie la plus simple les divise en trois catégories : niveaux-1, 2 et 3 : ils forment dans cette logique une structure en réseau hyperbolique (Krioukov *et al.*, 2010), c'est-à-dire ayant tendance à prendre une forme arborescente, avec de nombreuses extrémités et assez peu de nœuds centraux dans leur fonction de transmission de données d'un point à l'autre. Le Center for Applied Research Data

Analysis (CAIDA) a établi (Luckie *et al.*, 2013) une méthode de classification des systèmes autonomes en termes d'importance commerciale. Les résultats de cette méthode conduisent à une taxonomie hiérarchique des systèmes autonomes. Cette hiérarchie ne divise pas les AS selon leur valeur financière, ni selon le volume de données qui transite par eux, mais plutôt par leur degré d'importance au sein de l'ensemble de l'écosystème. Elle se fonde sur le concept de *customer cone*, ou « cône de consommateurs », qui dépend de la quantité d'autres AS, et d'adresses IP accessibles via un AS donné, uniquement par des liens de client-fournisseur. Cette taxonomie divise les AS en trois groupes nommés *Tier 1* (de premier rang), *Tier 2*, et *Tier 3*. Les AS de *Tier 1* sont ainsi en général des gestionnaires de câbles sous-marins internationaux, par lesquels passent la majorité du trafic Internet⁸ : Level 3, Telia etc. Les *Tier 1* ont comme propriété spécifique de n'avoir aucun fournisseur. Ils ont soit des liens de *peering* avec les autres *Tier 1*, soit des clients qui ont besoin d'accéder au reste d'Internet. Les AS de niveau 2 sont des fournisseurs de transit ou grand fournisseurs d'accès Internet (FAI). On peut distinguer fournisseurs de transit et fournisseurs d'accès en ce que les premiers fournissent aux seconds leur accès au reste du réseau. En revanche, les fournisseurs d'accès Internet ne fournissent qu'à des clients à l'extrémité du réseau, entreprises ou particuliers. Enfin les AS de niveau 3, aussi nommés « domaines d'extrémité » sont en général de plus petits réseaux gérés par une entreprise, une université etc.

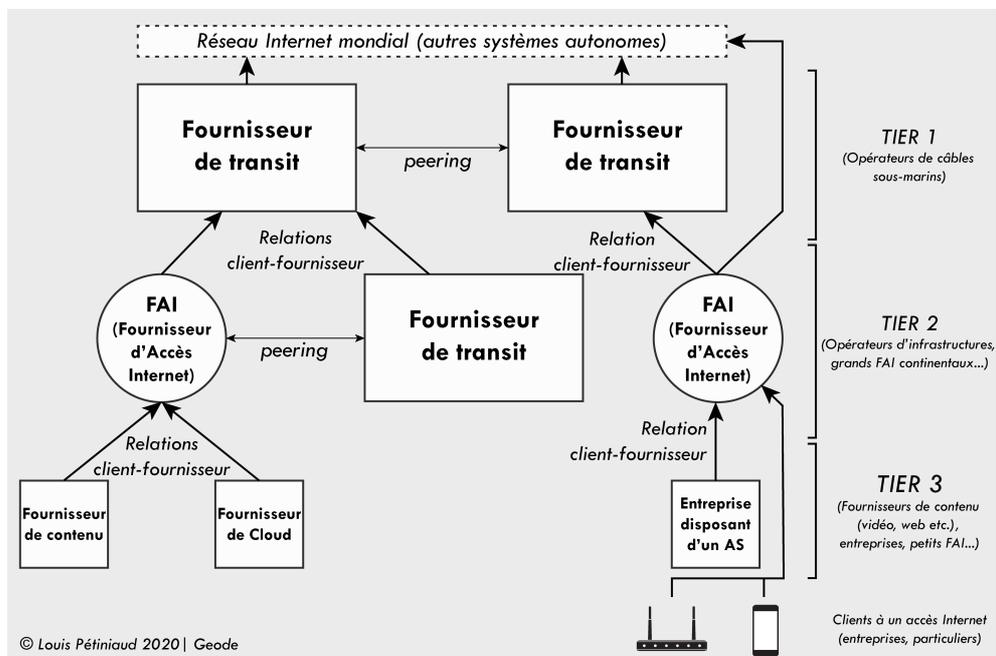
- 13 Un AS est donc un niveau d'abstraction du réseau : il s'agit d'une dénomination administrative et juridique qui recouvre des réalités différentes. Ces AS ont un numéro unique alloué par des organismes de régulation d'Internet, en l'occurrence les Registres Internet régionaux (RIR). Chaque AS est géré par une autorité administrative, publique ou privée, qui détermine sa politique de routage. En résumé, l'administrateur d'un AS décide avec quels autres systèmes autonomes il va établir des connexions, ainsi que le comportement de ses routeurs externes lorsqu'il reçoit des données à faire transiter plus loin dans le réseau. Le protocole utilisé pour établir une connexion entre deux systèmes est nommé *Border Gateway Protocol* ou BGP : il constitue de fait l'unique protocole de routage « inter-domaine », c'est-à-dire utilisé entre AS.

Le réseau des AS est politique

- 14 Le fonctionnement interne d'un AS et son comportement dans le réseau peuvent être politiques pour deux raisons principales. D'une part, lorsqu'un système autonome souhaite se connecter au reste du réseau, il doit établir une connexion BGP avec d'autres AS, en client-fournisseur ou en *peering*. Lors du choix d'un fournisseur, un AS choisit donc selon un certain nombre de critères : infrastructurels (la connexion nécessite une base physique), économiques et commerciaux, mais aussi sécuritaires, politiques, voire géostratégiques. Un fournisseur de contenus ou un nouvel opérateur sur le marché devra composer avec les offres possibles pour essayer de mettre en place une connexion la plus pérenne, la plus sécurisée, et la moins chère possible. Des recherches sur les critères déterminant les probabilités (ou le type) d'interconnexions entre AS ont décrit certains des paramètres favorisant les chances d'accords BGP. Par exemple, alors que des AS concurrents ont moins de probabilité de mettre en place un accord, des paramètres comme la taille de deux AS ou leur proximité géographique résulte en une plus grande probabilité de mise en place d'un accord (Colombier *et al.*, 2010).

- 15 D'autre part, les administrateurs d'AS mettent en place des algorithmes de routage qui déterminent quels chemins prennent les données pour arriver à destination. Les mécanismes de routage dépendent d'abord de critères commerciaux et de sécurité, mais peuvent également être déterminés par des considérations politiques. Lorsqu'un AS reçoit une information sur un nouveau chemin pour rejoindre une adresse IP spécifique, il choisit s'il change de chemin ou s'il garde l'existant. Le choix d'un chemin plutôt qu'un autre est déterminé par un certain nombre de critères complexes, qui constituent dans leur ensemble ce que les ingénieurs réseaux appellent justement une « politique de routage ». Ces politiques intègrent à la fois les règles de base de BGP (Rexford *et al.*, 2010), et des attributs que les administrateurs de réseaux mettent en place pour créer de complexes algorithmes (Habibi, 2000).
- 16 Ainsi, un moyen simplifié de représenter Internet est un ensemble de trois différents types de systèmes autonomes, certains ayant des connexions avec d'autres. Sur cette représentation simplifiée du réseau (fig. 1), pour qu'un client (en bas à droite) accède à une vidéo stockée par un fournisseur de contenu (en bas à gauche), différents chemins sont possibles, selon des accords passés entre les différents acteurs du routage.

Figure 1 : Représentation schématique d'une partie du réseau des AS



- 17 Il est possible de concrètement visualiser le trajet que peuvent prendre des données. Par exemple, depuis Paris pour atteindre le site de l'équivalent russe de Facebook, Vkontatkte, <https://vk.com/> à Moscou, on constate (fig. 2) que les paquets de données⁹ suivent un chemin spécifique détaillé ci-dessous.

Figure 2 : Traceroute ICMP entre un ordinateur particulier connecté à Paris et le site Internet russe <https://vk.com/>

```
Détermination de l'itinéraire vers vk.com [87.240.129.72]
avec un maximum de 30 sauts :

 1   1 ms   1 ms   1 ms   box [192.168.1.1]
 2   8 ms   8 ms  10 ms  1.139.21.109.rev.sfr.net [109.21.139.1]
 3   9 ms   9 ms   8 ms  161.65.24.109.rev.sfr.net [109.24.65.161]
 4  17 ms  11 ms  12 ms  133.129.96.84.rev.sfr.net [84.96.129.133]
 5  13 ms  12 ms  10 ms  v4087.bou1-co-3.n9uf.net [62.39.148.30]
 6   8 ms  11 ms  14 ms  102.244.5.109.rev.sfr.net [109.5.244.102]
 7  14 ms   9 ms   9 ms  lag-5.ear3.Paris1.Level3.net [4.68.72.253]
 8  45 ms  47 ms 263 ms ae-113-3503.bar1.Stockholm1.Level3.net [4.69.158.249]
 9  45 ms  45 ms  67 ms ae-113-3503.bar1.Stockholm1.Level3.net [4.69.158.249]
10  59 ms  60 ms  60 ms  213.242.69.70
11  *      *      *      Délai d'attente de la demande dépassé.
12  *      *      *      Délai d'attente de la demande dépassé.
13  80 ms  64 ms  63 ms  srv72-129-240-87.vk.com [87.240.129.72]

Itinéraire déterminé.
```

- 18 Trois paquets ont été envoyés en décembre 2017 depuis Paris (XVIII^e arrondissement) jusqu'au site Internet de Vkontatke dont les serveurs sont probablement situés dans la région de Saint-Petersbourg¹⁰. Ils effectuent de nombreux *hops* (sauts), qui sont les points, et plus précisément des routeurs, par lesquels les données transitent, et pour lesquels une ligne numérotée est attribuée, de 1 à 13. Dans ce cas précis, ces points de passage sont au nombre de 11 (les lignes 1 et 13 étant celles des points de départ et d'arrivée).
- 19 Voici l'itinéraire de ces trois paquets de données :
- Ils partent depuis un ordinateur jusqu'à un routeur (une « box ») via un protocole Wi-Fi (ondes électromagnétiques). Ce premier passage n'est pas renseigné par le *traceroute*, qui ne prend en compte que le trajet sur le réseau externe.
 - La ligne 1 de la « box » renseigne l'adresse IP publique de l'émetteur : [192.168.1.1].
 - Les lignes 2, 3 et 4 présentent les sauts effectués à l'intérieur des réseaux de l'opérateur de télécommunications SFR (Société Française du Radiotéléphone), dont une des activités est d'être Fournisseur d'Accès Internet (FAI). Ces trois points se situent probablement à ou autour de Paris¹¹.
 - Le saut 5 est également à Paris, mais l'administrateur change : il s'agit désormais de l'entreprise N9UF, auparavant un grand FAI également, racheté par SFR en 2008.
 - Le saut 6 reste dans les réseaux de SFR, mais les sources de localisation des adresses IP divergent davantage : certaines sources le placent à Paris, d'autres en Franche-Comté.
 - Les sauts 7, 8 et 9 et 10 montrent un passage des données à un autre niveau d'Internet : celui des câbles. Les paquets passent en effet sous gestion de Level 3, un des opérateurs de télécommunications les plus importants, qui administre notamment des câbles terrestres et maritimes. Les paquets transitent donc par Stockholm, puis possiblement par un autre point de passage suédois (saut 10).
 - Les sauts 11 et 12 ne sont pas renseignés, avec la précision « délai d'attente dépassé », ce qui peut signifier différentes choses, notamment que le routeur filtre les réponses aux paquets ICMP.
 - Enfin, le saut 13 correspond à l'adresse du serveur de Vkontatke.
- 20 Durant le trajet, ces paquets de données subissent des transformations physiques et protocolaires diverses. Dans les câbles par exemple, ces paquets deviennent des impulsions lumineuses qui transmettent un langage binaire (en 0 et 1), base technologique de la fibre optique. Jusqu'à aboutir aux serveurs de Vkontatke, ces

paquets transitent donc *via* des installations, principalement des câbles et des routeurs, permettant leur transfert de proche en proche. Le voyage des données est donc linéaire au niveau infrastructurel : elles ne disparaissent pas en un point du monde pour réapparaître ailleurs. Sous le prisme protocolaire en revanche, la progression des données est topologique : elle marque des sauts bien identifiables, qui correspondent à autant de machines au niveau desquelles les données ont emprunté un chemin, souvent en en « choisissant » un parmi plusieurs. Or, ce prisme protocolaire est essentiel : les nœuds du réseau où émerge la donnée sont les endroits du territoire où se façonne la réelle structure du réseau. Si l'existence des infrastructures physiques est nécessaire, ce sont les AS et les accords BGP entre eux qui structurent le transit des données. Les infrastructures comme les câbles génèrent des chemins possibles d'un point A à un point B. C'est le routage qui permet la concrétisation de ce déplacement, et qui conditionne le chemin réellement emprunté.

Les AS : un réseau qui façonne le territoire et les rivalités de pouvoir

- 21 Les AS sont territorialisés, quoique différemment selon les cas : un grand fournisseur de transit intercontinental et une université occupent l'espace à des échelles très différentes. En dépit de la difficulté de localiser précisément la plupart d'entre eux, ils constituent des éléments se déployant sur l'espace terrestre. En ce sens, ils incarnent justement la dualité spatiale d'Internet : un réseau topologique, ancré et utilisé dans un espace topographique. Les systèmes autonomes définissent la forme et les chemins d'Internet. Ils sont les pourvoyeurs d'Internet aux populations, aux services de l'économie et des Etats, et définissent donc leur possibilité d'accéder au reste du réseau. A ce titre, leur maîtrise est cruciale. A l'échelle mondiale, les AS ne risquent pas sérieusement de faillir à la fluidité des flux de données. A d'autres échelles, diverses problématiques territoriales se posent. A l'échelle des Etats, deux questions fréquentes émergent : celle de la résilience du réseau des AS¹², mais aussi celle de son contrôle comme c'est le cas en Chine ou en Iran (Salamatian *et al.*, 2019). A des échelles territoriales inter- et infra-étatiques, la structure des AS peut impliquer des logiques de puissance spatiale spécifiques, en particulier une forme de « puissance topologique ». John Allen définit ce concept dans un article sur les « tournants topologiques » de la géographie de la puissance (Allen, 2011). La puissance topologique est conçue comme une capacité d'agir sur un réseau pour « faire ressentir sa présence » : « ces puissances de longue portée [...] sont souvent mieux compréhensibles, non comme des entités s'étendant à travers les frontières et les réseaux, mais plutôt comme un agencement qui permet à des acteurs distants de faire ressentir leur présence, plus ou moins directement, en traversant le fossé entre "ici et là-bas" » (Allen, 2011, p.290)
- 22 L'interconnexion des AS d'Etats différents permet de comprendre comment des pays peuvent être « influents » vis-à-vis du réseau d'autres Etats, c'est-à-dire dans quelle mesure ils disposent d'une certaine puissance. En particulier, sur des espaces plus restreints, les systèmes autonomes peuvent être considérés comme *de facto* partie prenante de la fabrique des territoires (Painter, 2010). Dans ces espaces réduits et éloignés des hubs de connectivités, les AS sont des fournisseurs d'accès essentiels car moins nombreux. Alors que la topologie d'Internet est en constant changement, et ce à une fréquence très élevée, cette propension à fluctuer décroît dans ce type de zones du réseau. Pour ces zones, les AS en amont constituent donc des rouages stratégiques, qui permettent à de nombreux services de fonctionner normalement et en sécurité. A cette

échelle, on peut utiliser une comparaison limitée mais évocatrice : un AS est pour les données numériques et l'accès à Internet, l'équivalent d'une gare ferroviaire, qui permet à des populations éloignées de se connecter à un nœud plus important, d'où ils peuvent ensuite accéder plus rapidement à des espaces éloignés (via des aéroports par exemple, ou des câbles sous-marins pour Internet). L'extrapolation pousse à proposer l'existence de territoires définis par le réseau, enchâssés dans sa topologie. Ces territoires de connectivité sont caractérisés par la dépendance des populations de celui-ci à un ou quelques AS spécifiques pour accéder à une connexion au réseau mondial. Ces entités portent comme caractéristique d'être circonscrites par des frontières difficiles à appréhender parce que changeantes, et parfois superposées. Néanmoins, en conjuguant différents types de données, nous proposons dans cet article des méthodes de visualisation et de cartographie qui permettent d'identifier de tels ensembles, en particulier dans des zones relativement périphériques du réseau des AS.

- 23 La structure du réseau des AS induit nécessairement une dépendance pour ce types de territoires de connectivités, mais aussi, pour le ou les AS en amont, une puissance qui s'incarne de différentes manières. D'abord, cette dépendance implique des détours géographiques et matériels dans le transit des données. L'absence de multipolarité dans la connexion d'un territoire rend nécessaire le passage par un seul AS externe non choisi, qui peut décider du chemin des données. Ces détours impliquent une baisse de la stabilité, de la fiabilité, et de la rapidité du réseau pour ces zones (Chiu *et al.*, 2015). La puissance de ces AS se matérialise aussi par la capacité de surveillance acquise par leur situation topologique stratégique. Les transferts de paquets de données via les systèmes autonomes permettent théoriquement aux nœuds du chemin d'identifier la source de la donnée et, le cas échéant, de retransformer les paquets reçus en information d'origine. Ensuite, elle permet une potentialité de déconnexion. Cette faculté à briser le circuit des données peut être cruciale, et est amenée à le devenir davantage à mesure de la numérisation de champs sociaux toujours plus nombreux. Enfin, elle permet de manière plus générale une mainmise plus forte sur le réseau et ses voisins. La maîtrise de BGP permet des manœuvres de plus grande portée sur le réseau, en facilitant par exemple l'obfuscation, c'est-à-dire la possibilité de dissimuler l'auteur d'attaques, en utilisant des AS dépendants¹³.

Les enjeux de puissance topologique en Ukraine

L'Ukraine : un cas d'étude fécond

- 24 Pour appréhender l'analyse des données du réseau des AS dans des conflits, l'Ukraine présente un cas d'étude intéressant à plusieurs égards. En premier lieu, parce que l'affrontement avec la Russie, dans les domaines économiques, diplomatiques et territoriaux constitue un cas récent et unique de conflit territorial majeur en Europe. A ce titre, les deux républiques autoproclamées de Donetsk et de Luhansk à l'est du pays, ainsi que la Crimée au sud, constituent des entités spatiales à la souveraineté disputée et impliquant à des degrés différents l'acteur russe. En cela, elles sont un laboratoire pour l'étude des intersections entre rivalités territoriales et réseaux Internet. Ensuite, la construction progressive d'Internet dans les années 1980 et 1990 dans ces deux Etats a mené à une profusion des systèmes autonomes. Il existe aujourd'hui plus de 6200 AS en Russie, et plus de 2200 en Ukraine¹⁴. Cette profusion permet d'obtenir des quantités de données plus importantes, et plus précises. En effet, les données des interconnexions

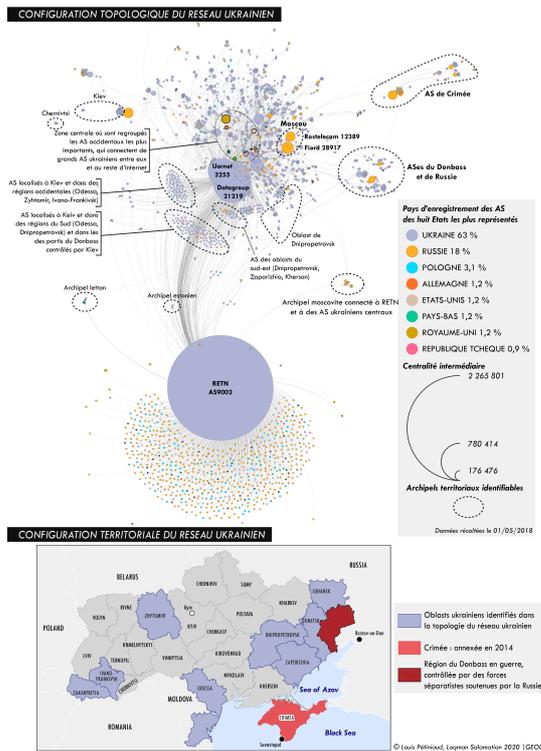
entre AS proviennent de points d'observation à travers le réseau (Petiniaud, Salamatian, 2019), qui récoltent de manière continue des informations sur le routage mondial. Ces données ne peuvent être exhaustives, et ont tendance à être plus parcellaires aux extrémités du réseau. Dans ces extrémités, une profusion de systèmes autonomes comme celle de l'Ukraine donne à voir davantage d'informations que sur des territoires pauvres en AS.

- 25 Enfin, la Russie, en tant que puissance régionale, occupe une place à part dans la géopolitique d'Internet. Le pouvoir russe opère en effet depuis quelques années une politique de « souverainisation » (Limonier, 2019) de son réseau, en particulier de son infrastructure¹⁵. À l'inverse d'Etats comme la Chine dont le réseau a été conçu comme un Internet plus fermé, l'écosystème russe des AS est très riche et diversifié. Ses acteurs sont par ailleurs souvent attachés à la culture libertaire des débuts d'Internet (Ermoshina, Musiani, 2017). Le pouvoir russe développe ainsi différentes méthodes pour rendre le réseau national plus facilement maîtrisable par l'Etat. Le gouvernement de la Fédération a lancé depuis les années 2010 des politiques originales de re-nationalisation des réseaux de données, comme l'obligation depuis 2015 d'héberger les données de ses citoyens sur le territoire national. Plus récemment, Moscou est allé plus loin en affirmant la nécessité d'organiser le Runet – le « segment russe » d'Internet – de manière la plus autonome possible. En pratique, cela impliquerait de pouvoir, si nécessaire, déconnecter la Russie du réseau mondial tout en préservant le réseau national¹⁶. La pensée d'Internet en Russie est déjà une pensée territoriale, et les dynamiques du réseau dans des territoires conflictuels où la Russie occupe une place importante permettent de questionner dans quelle mesure cette pensée peut être appliquée à ces cas extérieurs.

Visualiser la connectivité en Ukraine

- 26 Pour analyser la connectivité des territoires en Ukraine, on utilise ici une méthode empirique, qui consiste à observer des graphes (fig. 3) issus de données de connexion entre systèmes autonomes afin d'identifier l'interpénétration des enjeux géopolitiques régionaux et de la construction du réseau. Ces données proviennent de plusieurs points d'observation du réseau BGP selon une méthode développée par l'université de Savoie (Salamatian *et al.*, 2018). Un graphe est un objet mathématique constitué de nœuds, ici les AS, reliés par des arêtes, ici l'existence d'accord BGP entre deux AS. Pour des raisons techniques, ces graphes ne sont pas exhaustifs, mais ils permettent d'avoir à ce jour le meilleur aperçu possible du réseau (Petiniaud et Salamatian, 2019). Les graphes obtenus par la récolte de ces données sont uniquement une somme de points et d'arêtes sans direction dans un espace indéterminé. L'espace géographique ne permet pas de les visualiser correctement. Nous appliquons à ces graphes divers algorithmes de visualisation. Suite à l'utilisation d'un algorithme de visualisation, chaque sommet est matérialisé par un point, et les arêtes par des lignes reliant les points à leur extrémité. Le premier algorithme que nous utilisons est nommé Force Atlas 2, qui permet une représentation graphique du réseau. Cet algorithme est fondé sur les principes d'attraction et de répulsion et repose sur la simulation de la dynamique d'un système physique afin de spatialiser le réseau (Jacomy *et al.*, 2013). Les nœuds se repoussent comme des particules chargées, tandis que les arêtes attirent leurs nœuds, comme des ressorts. Ces forces créent un mouvement qui converge vers un état stable après un certain moment.

Figure 3 : Structure topologique et territoriale des réseaux en Ukraine



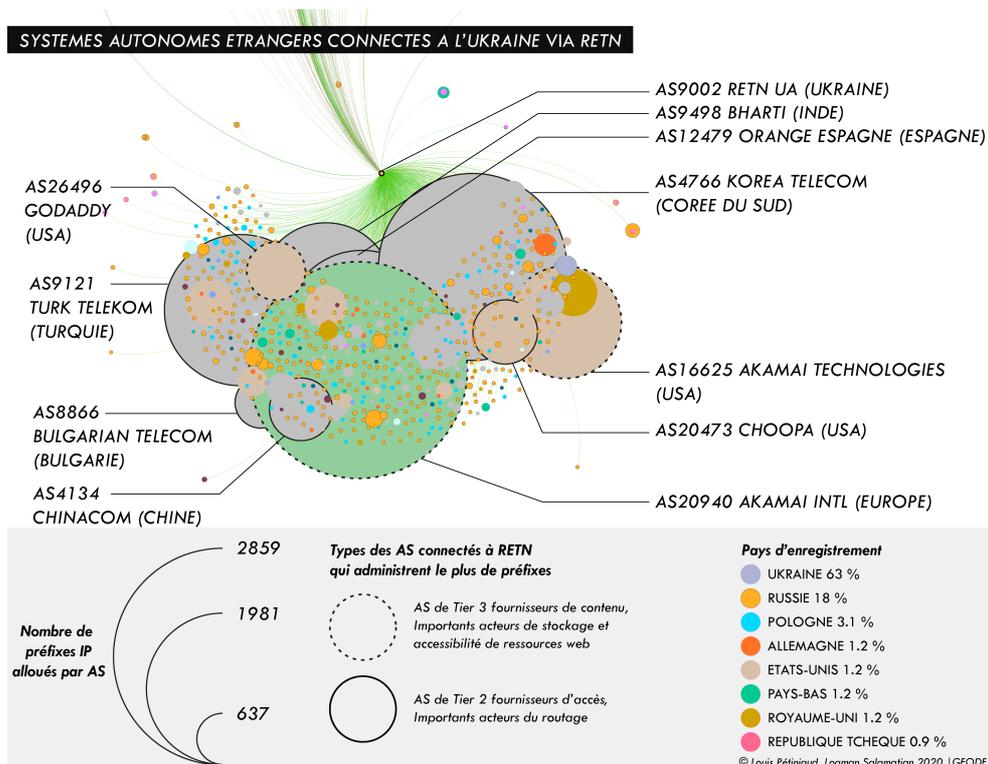
- 27 Ce graphe représente, pour la date du 5 janvier 2018, les AS ukrainiens et leurs voisins immédiats, c'est-à-dire des AS avec lesquels ils peuvent échanger directement des données, ainsi que leurs connexions, figurées par des arêtes. Les nœuds sont colorés par pays d'enregistrement auprès des autorités de régulation¹⁷. Ces données sont fiables, mais ne représentent qu'une partie de la réalité. Un exemple ici crucial est le grand AS 9002 en bas, déclaré ukrainien. Il est cependant administré par la branche ukrainienne de RETN, une grande entreprise de Télécommunications basée à Saint-Petersbourg, mais possédant des antennes et un réseau d'envergure mondiale¹⁸. Il est ainsi important de noter que dans notre analyse, la notion de territorialité n'est pas systématiquement corrélée à une emprise spatiale précise. Nous utilisons ainsi l'adresse déclarée aux autorités régulatrices par les gestionnaires des AS. Dans le cas d'AS de niveau 1, cette adresse ne correspond pas à une localisation fiable. Pour de plus petits systèmes autonomes, elle constitue une information plus précise. Enfin, la taille des systèmes autonomes dépend de leur centralité intermédiaire¹⁹, qui constitue une métrique de son importance pour la transmission de données dans le réseau ukrainien de manière globale.

Un profil de connectivité cohérent

- 28 L'analyse de ce graphe nous amène à un certain nombre d'observations qui permettent de développer une analyse géographique de graphes visualisés par algorithme, c'est-à-dire dont la représentation en deux dimensions est élaborée par un algorithme spécifique. A l'échelle du graphe, le premier constat est ce foisonnement d'AS, caractéristique de l'Ukraine comme de la Russie : les deux pays agrègent proportionnellement à leur population connectée un nombre très élevé d'AS (environ

20 000 usagers par AS en moyenne pour l'Ukraine et 23 000 en Russie, tandis qu'on constate environ 110 000 usagers par AS en moyenne pour les autres pays européens²⁰). Dans cet écosystème, on constate une bipolarité très forte. En effet, l'AS 9002 constitue un point d'accès très important entre le réseau ukrainien et de nombreux AS extérieurs, dont une grande partie sont des AS éloignés qui sont peu importants pour le réseau ukrainien mais sont des nœuds très importants du réseau mondial. Si on agrandit cette zone (fig. 4), et qu'on adapte la taille des AS au nombre d'adresses IP qu'ils gèrent, on voit que l'AS 9002, bien plus petit, est connecté à de grands opérateurs de Corée du Sud, d'Inde, de Turquie ou encore des Etats-Unis.

Figure 4 : Réseaux connectés aux AS d'Ukraine via RETN (AS 9002)



- 29 On observe plus généralement dans la topologie ukrainienne (fig. 3) l'existence d'une cohérence entre géopolitique et topologie. L'importance de la Russie dans le réseau ukrainien est considérable. Les AS russes constituent 18 % des AS du réseau élargi ukrainien (c'est-à-dire la somme des AS d'un pays, et leurs voisins directs). Outre l'AS 9002, un certain nombre d'entre eux montre qu'une proportion importante sert de passerelle vers le réseau global. Les Russes ne sont cependant pas les seuls acteurs étrangers ici. Au centre du réseau ukrainien, on observe effectivement un groupe d'AS étrangers aux contours noirs épais, relativement importants. Ils connectent les plus gros AS ukrainiens avec de nombreux autres AS d'Ukraine et de l'étranger de centralité moyenne. La Grande-Bretagne, l'Allemagne, les Etats-Unis, les Pays-Bas et quelques autres pays constituent ainsi des points de passage importants, bien que non essentiels au réseau, pour la plupart.
- 30 L'Ukraine présente un profil de connectivité relativement cohérent avec sa position géopolitique. Sa dépendance au réseau russe, issue d'une histoire commune, apparaît avec clarté, mais on constate également la présence d'AS occidentaux importants au

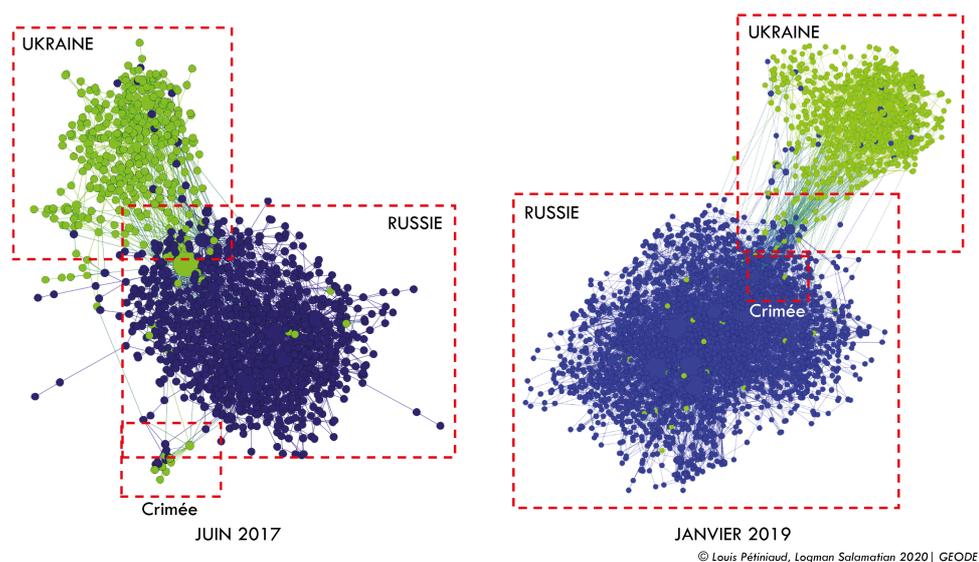
cœur du réseau. Cette corrélation entre topologie et géopolitique apparaît de manière bien plus significative dans les extrémités du réseau. Plusieurs archipels de réseau correspondent concrètement à des territoires plus ou moins bien circonscrits. L'existence de certains d'entre eux semble assez cohérente, les Etats de Lettonie et Estonie par exemple qui forment des amas de faible importance. Certaines villes et oblasts (équivalent administratif d'une région) d'Ukraine sont également identifiables, comme Dnipro (anciennement Dnipropetrovsk), capitale industrielle de la partie orientale du pays. Kiev, en tant que cœur économique de l'Ukraine, se retrouve à de nombreux endroits du graphe car les AS qui y sont présents servent de portail pour de nombreuses régions.

Puissance topologique en territoires disputés

- 31 Le graphe présente surtout des incohérences géographiques significatives. Dans le quart haut-droit de l'image, on observe la formation d'un sous-réseau nettement séparé, qui témoigne visuellement de l'évolution des politiques de routage des territoires en conflit de l'Ukraine : la Crimée et le Donbass.
- 32 Pour la Crimée, la séparation de la péninsule de l'Ukraine et son rattachement à la Russie se sont fait progressivement, mais sont désormais effectifs notamment via les télécommunications²¹. Ce rattachement des télécommunications a été progressif, mais débute avec l'arrivée des premiers soldats russes en février-mars 2014. Ces soldats occupent alors rapidement les stations des chaînes de télévision, mais aussi le point d'échange Internet²² de Crimée, Crimea-IX²³. Il s'agit d'une des premières occurrences d'un tel intérêt pour l'infrastructure d'Internet lors d'un conflit territorial. Il est donc cohérent que cette partie du réseau soit la plus éloignée du centre du graphe, et qu'il soit connecté par relativement peu d'accords BGP via un seul AS en Crimée, celui de Crimea-IX. On remarque cependant la proximité d'AS moscovites dans cette portion du graphe, ce qui dépasse la cohérence géographique de l'îlot. Une analyse temporelle de la position du réseau criméen révèle le changement du paysage de connectivité de la Crimée au fur et à mesure des événements géopolitiques. En effet, les villes commerciales majeures abondent dans le Sud de la Russie, et l'on aurait pu, compte tenu de la connectivité régionale, s'attendre à observer des AS régionaux (à Rostov-sur-le-Don, Krasnodar etc.) ou même d'autres Etats (Istanbul par exemple). Cela indique probablement la faiblesse du réseau criméen, mais montre également le relatif verrouillage du réseau de la péninsule, encore sujette à des tensions importantes et officiellement revendiquée par l'Ukraine.
- 33 Pour représenter l'évolution de la connectivité de la Crimée, nous faisons usage d'un algorithme spectral (fig. 5). L'algorithme spectral est initialement un algorithme de clustering, c'est-à-dire visant à séparer le graphe en différentes communautés cohérentes. Dans ce cas précis, nous focalisons notre attention uniquement sur l'Ukraine et la Russie pour observer l'évolution de l'îlot criméen. En juin 2017, une analyse du nombre optimal de communautés montre que le graphe est constitué de trois communautés ; la Crimée est en effet toujours un territoire contesté se situant à la jonction du réseau russe et ukrainien, ce qui en fait une communauté à part entière. Une capture en janvier 2019 montre comment la Crimée est alors complètement assimilée au réseau russe. Nous observons aussi une modification dans

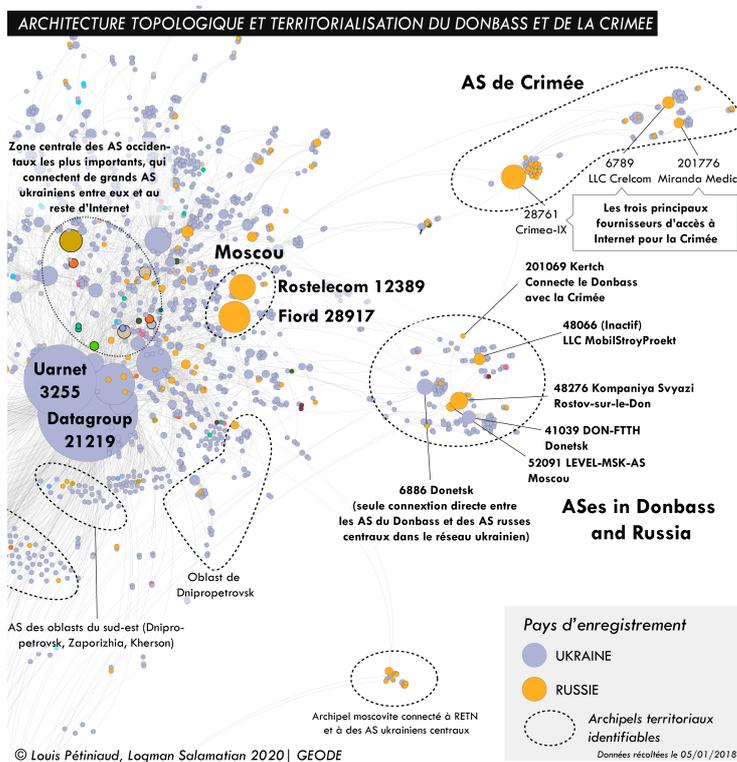
l'enchevêtrement des réseaux avec l'Ukraine qui s'est nettement scindé de la Russie entre 2017 et 2019.

Figure 5 : Représentation spectrale de la Crimée dans les réseaux ukrainien et russe, 2017-2019



- 34 Cette transformation topologique revêt une signification très concrète dans le territoire criméen. Ce changement de connectivité fonctionne dans ce cas comme un phénomène d'auto-entraînement. La connectivité accrue vers la Russie implique une modification des latences, c'est-à-dire du temps que mettent les données à aller d'un point à un autre. Dans le cas de la Crimée, il est notable que cette modification topologique entraîne un « rapprochement » en temps avec la Russie et un « éloignement » de l'Ukraine. Le fait que les données circulent plus vite vers la Russie – non seulement vers le cœur politique et économique de Moscou – Saint-Pétersbourg mais aussi vers des zones plus éloignées – peut entraîner un intérêt croissant des acteurs économiques à se rapprocher de la Russie, en particulier dans les secteurs nécessitant des performances de vitesse plus importantes²⁴. Cette tendance implique à moyen terme une demande accrue de connectivité vers la Russie et, à plus long terme, contribue à l'intégration de la Crimée dans la Fédération de Russie.

Figure 6 : Zoom (fig. 3) : Connectivité des archipels de Crimée et du Donbass



- 35 L'archipel de réseau du Donbass (fig. 6) présente également un profil intéressant. Il confirme comment l'observation du réseau permet de mettre au jour des logiques de puissance territoriale via l'infrastructure Internet. L'existence bien plus foisonnante de connexions avec le centre du graphe reflète bien la proximité territoriale de ces territoires avec le reste de l'Ukraine, mais leur éloignement distinct et leur cohérence en tant que groupe externe expose clairement leur aspect « hybride », voire leur qualité d'Etats *de facto*. Dans ce cas-là, la présence de Rostov a du sens, de même que celle de Moscou, et encore davantage celle de Kertch, qui fait office de « pont » entre les deux zones les plus conflictuelles du territoire ukrainien. Qui plus est, dans le Donbass, les changements de connectivité récents montrent une dépendance de plus en plus forte vis-à-vis des réseaux du sud de la Russie, qui constituent depuis peu la source de connexion principale des réseaux des républiques populaires autoproclamées de Donetsk et Luhansk. Il est difficile, sinon impossible de savoir si dans ce cas, le réseau participe pleinement de stratégies territoriales russes ou séparatistes pensées comme telles. La situation de dépendance constatée dans les graphes est probablement la conséquence de choix de routage autonomes des différents opérateurs du Donbass. Autrement dit, différents fournisseurs d'accès des territoires séparatistes peuvent tout-à-fait avoir choisi sans concertation de préférer des fournisseurs Internet russes plutôt qu'ukrainiens, pour diverses raisons (risques de contrôle par Kiev de la connexion, crainte d'une surveillance, risques de sanctions commerciales pesant sur les fournisseurs ukrainiens etc.) Pour paraphraser Yochai Benkler, la connectivité des régions conflictuelles décrite ici est un « effet coordonné d'actions non coordonnées »²⁵ (Benkler, 2006, p.6). Malgré cette absence d'intentionnalité avérée, l'architecture topologique régionale montre clairement l'existence d'une forme de puissance topologique de l'Etat russe vis-à-vis de réseaux Internet hors de ses frontières. Plus directement, les réseaux Internet participent directement à des mécanismes de

transferts de souveraineté, en favorisant l'éloignement entre des zones séparatistes ou annexées, et l'Etat ukrainien. Dans cette dynamique, et dans un contexte où l'Etat russe montre régulièrement sa volonté d'accroître son contrôle sur les acteurs russes du routage, c'est *in fine* le pouvoir exécutif de Moscou qui renforce sa puissance sur les réseaux des deux républiques auto-proclamées.

Conclusion

- 36 Le réseau des AS au cœur de l'architecture d'Internet, constitue un objet d'étude géopolitique récent. Dans cet article, nous proposons une approche nouvelle des enjeux d'Internet, que l'on considère sous l'angle de la couche protocolaire du réseau. Nous développons une méthode en partant du constat qu'Internet est un objet spatial dual mêlant topographie et topologie. Le protocole BGP est à cet égard un prisme intéressant et encore peu étudié en sciences sociales. Les AS forment une structure résiliente qui permet le bon fonctionnement d'Internet, mais leur gestion et leur fonctionnement sont profondément géopolitiques. Les modalités de leurs interconnexions dépendent d'acteurs aux préoccupations à la fois économiques, commerciales, sécuritaires et politiques, et le savoir technique permet à ces acteurs de jouer un rôle important dans certains territoires. Plus encore, le réseau BGP peut être directement vecteur d'une forme de puissance topologique sur des territoires dont il contribue à la production. L'étude du conflit russo-ukrainien permet de montrer comment ces rivalités de pouvoir sur des territoires s'incarnent pleinement à travers et par le réseau. En Crimée, les réseaux Internet ont été et demeurent partie prenante d'une politique d'incorporation, dès le début de l'annexion par les soldats russes. Dans cette péninsule, mais aussi dans le Donbass, depuis 2014, on constate une évolution de plus en plus ferme vers une dépendance aux acteurs russes des télécommunications. Par-là, c'est également le pouvoir russe qui dispose d'un effet de levier important envers des territoires disputés. Nous notons ainsi que la notion de territorialité dans le routage se traduit dans ces territoires en une influence extérieure, et une division d'Internet en îlots, cette dernière est aux antipodes de l'idéal de « gouvernance distribuée » (Mathew, 2014), qui précédait l'avènement de BGP comme unique protocole de routage. Cet article est le résultat de recherches nouvelles, et préfigure notre volonté de développer une véritable grille de lecture transdisciplinaire visant à appréhender le caractère géopolitique du routage.

BIBLIOGRAPHIE

ALLEN, J., 2011, « Topological twists: Power's shifting geographies », *Dialogues in Human Geography*, vol. 1, n° 3, p. 283-298

Agence Nationale pour la sécurité des systèmes d'information, 2017, Résilience de l'Internet français 2016, [En ligne], <https://www.ssi.gouv.fr/uploads/2016/06/resilience-de-linternet-rapport-2016.pdf>, mis en ligne le 13 juillet 2017, consulté le 16 septembre 2020

- BEAUDE, B., 2012, *Internet, changer l'espace, changer la société*, Limoges, FYP éditions
- BENKLER, Y., 2006, *The Wealth of Networks - How Social Production Transforms Markets and Freedom*, New York, Yale University Press
- CAMILLERI, J., FALK, J., 1993, *The End of Sovereignty?: The Politics of a Shrinking and Fragmenting World*, Aldershot, Edward Elgar Publishing Limited
- CATTARUZZA, A., 2019, *Géopolitique des données numériques. Pouvoir et conflits à l'heure du Big Data*, Paris, Le cavalier bleu
- CHIKHI N., 2010, Calcul de centralité et identification de structures de communautés dans les graphes de documents, Thèse de Doctorat, Université Toulouse 3, [En ligne], <https://tel.archives-ouvertes.fr/tel-00619177/document>, mis en ligne le 5 septembre 2011, consulté le 2 juin 2020
- CHIU, Y. C., SCHLINKER, B., RADHAKRISHNAN, A.B., KATZ-BASSETT, E., GOVINDAN, R., 2015, « Are we one hop away from a better internet? », in *Proceedings of the 2015 Internet Measurement Conference*, p. 523-529
- COLOMBIER, N., M'CHIRGUI, Z. et PENARD, T., 2010, « Une analyse empirique des stratégies d'interconnexion des opérateurs internet », *Revue d'économie industrielle*, vol. 131, n° 3, p. 25-50
- DOUZET, F., 1997, « Les enjeux géopolitiques du cyberspace », *Netcom*, vol.11, n° 1, p. 181-216
- DOUZET, F., 2014, « La géopolitique pour comprendre le cyberspace », *Hérodote*, vol. 152-153, n° 1, p. 3-21
- DOUZET, F. et DESFORGES, A., 2018, « Du cyberspace à la datasphère. Le nouveau front pionnier de la géographie », *Netcom*, vol. 32, n°1-2, p. 87-108
- ERMOSHINA, K., MUSIANI, F., 2017, « Migrating Servers, Elusive Users: Reconfigurations of the Russian Internet in the Post-Snowden Era », *Media and Communication*, vol. 5, n°1, p. 42-53
- EVENO, E., 2004, « Le paradigme territorial de la Société de l'Information », *Netcom*, vol. 18, n°1-2, p. 89-132
- JACOMY, M., VENTURINI, T., HEYMANN, S., BASTIAN, M., 2014, « ForceAtlas2, a Continuous Graph Layout Algorithm for Handy Network Visualization Designed for the Gephi Software », *PLOS ONE*, vol. 9, n° 6, [en ligne], <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0098679>, mis en ligne le 10 juin 2014, consulté le 16 septembre 2020
- KITCHIN, R., DODGE, M., 2001, *Atlas of Cyberspace*, Edimbourg, Pearson Education
- KRIOUKOV, D., PAPADOPOULOS, F., KITSAK, M., VAHDAT, A., BOGUNA, M., 2010, « Hyperbolic Geometry of Complex Networks », *Physical Review*, vol. 82, n°3
- LACROIX, D., 2014 « Ranger la Terre. Le nommage des domaines est-il l'expression d'une stratégie des Etats-Unis de domination des réseaux ? », *Hérodote*, vol. 152-153, n° 1, p. 185-200
- LASSERRE, F., 2000, « Internet : La fin de la géographie ? Internet : The end of geography ? », *Cybergeo : European Journal of Geography* [En ligne], <https://journals.openedition.org/cybergeo/4467>, mis en ligne le 31 octobre 2000, consulté le 27 septembre 2019
- LEVY, J., 1997, « De territoires et de réseaux », *Quaderni*, n° 31, p. 135-139
- LEVY, J., LUSSAULT, M., COLLECTIF, 2013, *Dictionnaire de la Géographie et de l'espace des sociétés*, Paris, Belin

- LOVELUCK, B., 2015, « Internet, une société contre l'état ? Libéralisme informationnel et économies politiques de l'auto-organisation en régime numérique », *Réseaux*, vol. 192, n°4, p. 235-270
- LUCKIE, M., HUFFAKER, B., CLAFFY, K., DHAMDHERE, A., GIOTSAS, V., 2013, « AS Relationships, Customer Cones, and Validation », in *IMC '13: Proceedings of the 2013 conference on Internet measurement conference*, p. 243-256
- MACLUHAN, M., 1962, *The Gutenberg Galaxy: The Making of Typographic Man*, Toronto, University of Toronto Press
- MARGETTS, H., NAUMANN, A., 2017, « Government as a Platform: What Can Estonia Show the World », *Oxford Internet Institute*, Research Paper, [En ligne], <https://www.politics.ox.ac.uk/publications/government-as-a-platform-what-can-estonia-show-the-world.html>, mis en ligne le 28 février 2017, consulté le 2 juin 2020
- MATHEW, A., 2014, *Where in the world is the internet? Locating political power in internet infrastructure*, Thèse de doctorat, UC Berkeley [en ligne], <https://www.ischool.berkeley.edu/research/publications/2014/where-world-internet-locating-political-power-internet-infrastructure>, mis en ligne le 20 septembre 2016, consulté le 16 septembre 2020
- MOISY, C., 1997, « Myths of the Global Information Village », *Foreign Policy*, n° 107, p. 78-87
- MUSIANI, F., COGBURN, D.L., DENARDIS, L., LEVINSON N.S., 2016, *The Turn to Infrastructure in Internet Governance*, Houndmills, Palgrave Macmillan
- O'BRIEN, R., 1992, *Global Financial Integration: The End of Geography*, Londres, Pinter for Royal Institute of International Affairs
- PAINTER, J., 2010, « Rethinking Territory », *Antipode*, vol. 42, n° 5, p. 1090-1118
- PETINIAUD, L., 2014, « Cartographie de l'affaire Snowden », *Hérodote*, vol. 152-153, n° 1, p. 35-42
- SALAMATIAN, L., DOUZET, F., LIMONIER, K., SALAMATIAN, K., 2019, « The geopolitics behind the routes data travels: a case study of Iran », [En ligne], <http://arxiv.org/abs/1911.07723>, mis en ligne le 19 novembre 2019, consulté le 16 septembre 2020
- SALAMATIAN, L., KAAFAR, D., SALAMATIAN, K., 2018, « A Geometric Approach for Real-time Monitoring of Dynamic Large Scale Graphs: AS-level graphs illustrated » [En ligne] <http://arxiv.org/abs/1806.00676>, mis en ligne le 2 juin 2018, consulté le 16 septembre 2020
- SZOSZKIEWICZ, L., 2018 « Internet Access as a New Human Right? State of the Art on the Threshold of 2020 », *Przełąd Prawniczy Uniwersytetu im. Adama Mickiewicza*, n°8, p. 49-62
- POESE, I., KAAFAR, M., DONNET, B., GUEYE, B., UHLIG, S., 2011, « IP geolocation databases: Unreliable? » *ACM SIGCOMM Computer Communication Review*, vol. 41, n°2, p. 53-56
- VAN ALSTYNE, M., BRYNJOLFSSON, E., 1996, « Electronic Communities: Global Village or Cyberbalkans? », in *Proceedings of the 17th International Conference on Information Systems*, p. 80-98
- VIRILIO, P., 1997, « Fin de l'histoire, ou fin de la géographie ? Un monde surexposé », *Le Monde diplomatique*, n° 521, p. 17
- VIRILIO, P., 1998, *La Bombe informatique : essai sur les conséquences du développement de l'informatique*, Paris, Galilée

NOTES

1. <https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx>, consulté le 02/06/2020
2. L'Estonie, qui a numérisé une grande partie de ses services publics, fait même figure de pionnier en la matière.
3. <https://www.eff.org/fr/cyberspace-independence>, consulté le 01/06/2020
4. De nombreux incidents ont par ailleurs contribué à rappeler la fragilité de certaines infrastructures et, par-là, leur ancrage topographique. On peut noter par exemple des incidents importants en janvier 2008 sur des câbles sous-marins ayant provoqué des troubles de connexion pour des millions de personnes au Moyen Orient et en Inde, ou rappeler qu'en Arménie (et dans des zones de Géorgie et d'Azerbaïdjan), le coup de bêche malheureux d'une Géorgienne septuagénaire avait coupé totalement l'accès à Internet pendant plusieurs heures en 2011. <https://webdoc.rfi.fr/ocean-cables-sous-marins-internet/chapitre-2.html>, consulté le 01/06/2020 ; <https://www.theguardian.com/world/2011/apr/06/georgian-woman-cuts-web-access>, consulté le 01/06/2020
5. Citons en particulier l'attaque par déni de service (DDoS) contre des sites gouvernementaux estoniens en 2007 puis géorgiens en 2008 attribués à la Russie, ou le ver Stuxnet découvert en 2010 visant à infiltrer les centrifugeuses d'enrichissement d'uranium en Iran.
6. Internet peut être considéré comme divisé en plusieurs couches superposées, en général au nombre de trois ou quatre en sciences sociales (Douzet, 2014). On distingue alors la première couche comme l'infrastructure physique implantée topographiquement, la deuxième couche l'infrastructure logique qui regroupe les protocoles qui permettent la transmission des données, la troisième comprend les applications et programme qui permettent à l'utilisateur d'interagir avec la machine, et la quatrième, définie par l'ensemble des interactions humaines ayant lieu sur ou grâce au réseau.
7. <http://ressources.potaroo.net>, consulté le 29 août 2019
8. https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.20-2019-PDF-E.pdf, consulté le 16/09/2020
9. Un « paquet de données » est un moyen utilisé pour envoyer des données à travers un réseau. Une somme de données (par exemple, une page Web à afficher sur un navigateur), est trop massive pour de nombreux protocoles, qui ont une taille maximale de transport. Il faut donc les sectionner en paquets, de taille souvent fixe.
10. D'après le site IpLocation, et selon les bases de données des services IP2Location et DB-IP. D'autres services ont été incapables de localiser l'adresse. (<https://www.iplocation.net/>, consulté le 31/08/2018).
Il est difficile, parfois impossible, d'identifier une localisation précise pour une adresse IP donnée (Poese, Kaafar, Donnet, Gueye, Uhlig, 2011).
11. *Idem.*
12. En France, par exemple, l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), publie annuellement un document sur la résilience de l'Internet français visant à « étudier[r] les technologies critiques au bon fonctionnement d'Internet », en l'occurrence BGP, DNS, et TLS, ainsi que les attaques DDoS. En ce qui concerne BGP, les auteurs évoquent la sécurité globale du protocole en France, mais aussi des aspects géopolitiques, sur la présence d'AS étrangers dans le réseau français par exemple. (ANSSI, 2017, p.15-17)
13. Par exemple, l'augmentation superflue d'AS par lesquels transitent des données rendent plus difficile la surveillance ou l'identification d'AS ou d'adresses IP prenant part à une attaque, et participe à établir un écran de fumée autour d'une ou de plusieurs sources d'attaque.
14. https://www-public.imtbs-tsp.eu/~maigron/RIR_Stats/RIR_Delegations/RIPENCC/ASN-ByNb.html, données mises à jour le 23 septembre 2019, d'après RIPE NCC, consulté le 02/06/2020

15. La Chine, exemple classique d'un « Internet fermé », a conçu et développé son réseau ainsi dès sa création. A l'inverse un Etat comme la Russie dispose d'un écosystème Internet très riche, divers, et souvent attaché à la culture libertaire des débuts d'Internet. Le pouvoir russe, comme le pouvoir iranien, développe ainsi différentes méthodes pour rendre leur réseau plus facilement maîtrisable par l'Etat.

16. https://www.rbc.ru/technology_and_media/28/11/2017/5a1c1db99a794783ba546aca, consulté le 02/06/2020

17. Il s'agit ici de RIPE NCC. Tous les systèmes autonomes sont identifiés par un numéro unique. Des plages de numéros sont allouées par l'*Internet Assigned Number Authority* (Autorité d'assignement des Numéros Internet, IANA), qui dépend de l'*Internet Corporation for Assigned Names and Numbers* (Société pour l'attribution des noms de domaine et des numéros sur Internet, ICANN), à des sous-entités administratives géographiques, les Registres Internet régionaux (RIR). Il en existe cinq, répartis sur autant de régions du monde. RIPE NCC est le RIR qui occupe cette fonction pour l'Eurasie, le Proche Orient et le Golfe Persique. <https://www.ripe.net/participate/member-support/list-of-members/list-of-country-codes-and-rirs>, consulté le 01/06/2020

18. <https://retn.net/networkmap/>, consulté le 01/06/2020

19. La centralité intermédiaire est une mesure définie, pour un nœud donné, par le nombre de fois où le chemin le plus court entre deux autres nœuds du graphe passe par celui-ci. Elle peut ainsi être considérée comme « la probabilité qu'une information transmise entre deux nœuds passe par ce nœud intermédiaire. » (Chikhi, 2010, p.22)

20. <https://bgp.potaroo.net>, consulté le 01/06/2020

21. Voir à ce sujet la vidéo de Ksenia Ermoshina captée au Chao Computer Club Congress en 2018, « A Routing Interregnum: Internet infrastructure transition in Crimea after Russian annexation » https://media.ccc.de/v/35c3-9864-a_routing_interregnum_internet_infrastructure_transition_in_crimea_after_russian_annexation, consulté le 01/06/2020

22. Un point d'échange Internet (*Internet exchange point*, IXP) est une infrastructure physique où s'interconnectent par câbles des systèmes autonomes, souvent des fournisseurs d'accès Internet (FAI) ou des réseaux de diffusion de contenu.

23. <https://foreignpolicy.com/2014/03/03/hack-attack/>, consulté le 01/06/2020

24. Différents secteurs ont besoin de vitesses optimales. Les activités financières, comme le *trading*, mais aussi des activités bancaires plus classiques nécessitent une grande rapidité. Mais de très nombreuses activités professionnelles et de loisir peuvent être sensibles à de faibles différences (quelques millisecondes) de latence, qui est la mesure standard de la vitesse des données. C'est le cas de certains types de communications (voix sur IP, visioconférence), ou la consultation de contenu (vidéo, jeux vidéo, *cloud computing* etc.).

25. Dans son ouvrage, Yochai Benkler fait de cet élément la caractéristique centrale de l'économie de l'information en réseau.

RÉSUMÉS

Les systèmes autonomes (AS) sont les unités de base du routage des données : ils sont les réseaux (fournisseurs d'accès Internet, fournisseurs de contenu, entreprises etc.) qui, par leurs interconnexions, constituent l'Internet. En établissant entre eux des accords de connexion via le

protocole BGP, les AS permettent de faire circuler les données d'un point à l'autre du globe. Dans cet article, nous montrons comment le réseau des AS est à la fois révélateur et partie prenante de luttes de pouvoir sur des territoires en conflit. Le comportement de ces systèmes, et en particulier leur connexion avec le reste du réseau, répond à des contraintes géopolitiques : il dépend de choix commerciaux, politiques, géographiques, juridiques. Le territoire et les rivalités de pouvoir qui s'y appliquent se trouvent transformés par cette topologie. En déterminant les chemins par lesquels passent les données, les administrateurs des systèmes autonomes font émerger des territoires et des formes de « puissance-topologie » (Allen, 2011). Notre méthodologie combine géopolitique et sciences techniques (informatique, géométrie), et se fonde sur des récoltes de données des interconnexions entre systèmes autonomes. Nous utilisons une approche empirique de lecture de graphes issus de ces données sur une étude de cas : les territoires conflictuels en Ukraine. Nous montrons comment l'infrastructure technique de BGP met au jour un nouveau vecteur de la puissance russe en Crimée et dans le Donbass, mais aussi comment le réseau Internet s'intègre directement dans des dynamiques de transfert de souveraineté.

Autonomous systems (AS) are the basic units of Internet global routing. They are group of routers interconnected by the same administrative control (Internet Service Providers, Content Providers, companies, public services etc.) that interconnect to each other to form the Internet as a whole. By establishing connection agreements between themselves via the Border Gateway Protocol (BGP), ASes allow data to flow from one point to another around the globe. In this article, we aim to understand how the aspect of the routing of data can be decisive in how we consider both the relationship between Internet and territory, and the impact of the structure of the Internet on territorial conflicts. Much literature has addressed the relationship between space and the Internet, both in geography and geopolitics. The increasing digitization of various aspects of society (Bakis, 2013 ; Cattaruzza, 2019) was first accompanied by comments about a paradigm shift of the concepts of geography (Virilio, 1997) or sovereignty (Camilleri, Falk, 1992). The relationship between space and Information and Communications Technologies (ICT) has also been considered under the angle of infrastructures and their territorial integration (Lasserre, 2000) More recently, Beaudé (2012) and Loveluck (2015) have shown how the complex interactions between Internet and society, produced alternative forms of space. Increasingly, the many dimensions of the Internet and of digitization are considered a salient feature of the social construction of territories, and therefore of geopolitical conflicts (Douzet, 2014). We draw from this literature to illustrate how the network of Autonomous Systems is linked to territorial conflicts. The behavior of autonomous systems, and in particular their integration within the rest of the network, responds to geopolitical constraints. The choice of an AS's administrators to connect to some ASes and not others, or the way they design and implement routing policies are subject to commercial, political, geographical and legal decisions. The construction of this topology then alters territories, especially disputed ones, and the power rivalries that apply to it. We show that this network is emblematic of the duality of the Internet between topography and topology. This study aims at understanding the role AS topology can play in the traditional power struggle. By selecting the paths through which data flows, administrators of AS bring out territories and new forms of « power-topology » (Allen, 2011). Our methodology combines elements of geopolitics and technical sciences (Internet measurements, network theory) and is based on quantitative approaches. We use data of interdomain connectivity gathered through BGP monitors that allow us to create graphs showing the interconnections between autonomous systems. We use an empirical approach to read the output graphs on a specific case study: disputed territories in Ukraine. The territories of Donbass and Crimea are ideal case studies in that the dispute over them is rather new, which allow us to observe with detail the changes in the topology of their networks over time. They also represent two different types of disputed

territories. While Crimea was annexed by the Russian Federation in March 2014, the Donbass region is home to the two self-proclaimed People's Republics of Donetsk and Luhansk, and is actively fighting against the central government of Ukraine with the help of Russia. By looking at the stakeholders of connectivity in these territories and their evolution, we show how the Internet is embedded into dynamics of changing sovereignty. In fact, the technical infrastructures of the Internet highlight a new vector of Russian power. The evolution of the routing topology indicates that Crimea is now fully dependent on Russia to connect to the Internet, and Donbass is following the same path.

INDEX

Mots-clés : géopolitique, Internet, réseaux de données, topologie, routage, Ukraine, BGP, système autonome

Keywords : geopolitics, Internet, data networks, topology, routing, Ukraine, BGP, autonomous system

AUTEURS

LOUIS PÉTINIAUD

Doctorant

GEODE, Institut Français de Géopolitique, université Paris 8

l.petiniaud@gmail.com

LOQMAN SALAMATIAN

Doctorant

Columbia University

salamatianloqman@gmail.com