Éditorial. Menace sur les infrastructures numériques : un enjeu géopolitique central pour le XXIe siècle

Frédérick Douzet[1] *et Stéphane Taillat*[2]

Le 28 avril 2025, en quelques secondes, l'Espagne et le Portugal basculent dans le noir. Une panne de courant de grande ampleur prive des dizaines de millions de personnes d'électricité, paralyse les transports, interrompt les communications, révèle la vulnérabilité de sociétés hyperconnectées à l'arrêt brutal d'un réseau que l'on ne voit, d'ordinaire, jamais. Quelques mois plus tôt, en mer Rouge, les attaques des rebelles houthistes contre le trafic commercial provoquent le naufrage d'un navire britannique, le *Rubymar*, qui sombre au fond de l'eau. Son ancre sectionne alors quatre câbles sous-marins qui transportaient environ 25 % du trafic de données entre l'Europe, l'Asie et le Moyen-Orient, provoquant des perturbations majeures et des ralentissements conséquents[3]. En Ukraine, depuis février 2022, les frappes russes visent méthodiquement les centrales électriques, les antennes-relais, les centres de données et les points d'atterrissement des câbles, comme si la guerre se jouait désormais autant dans les couches basses

1. Professeure à l'Institut français de géopolitique de l'université Paris 8, directrice de GEODE, PI de l'ERC DATAROUTES. « Cofinancé par l'Union européenne [ERC DATAROUTES nº 101098032]. Les points de vue et opinions exprimés n'engagent toutefois que leurs auteurs et ne reflètent pas nécessairement ceux de l'Union européenne ou du Conseil européen de la recherche (CER). Ni l'Union européenne ni l'autorité chargée de l'octroi de la subvention ne peuvent en être tenues responsables. »

2. Maître de conférences HDR en histoire contemporaine, Institut français de géopolitique (université Paris 8) et Académie militaire de Saint-Cyr Coëtquidan.

3. <https://geocables.com/research/red-sea-cable-cuts-2024>.

Herodote202_CC2021_PC.indd 5 11/09/2026 13:19:50

de l'Internet que sur le champ de bataille. Trois scènes, trois échelles, un même enseignement : les infrastructures – et tout particulièrement les infrastructures numériques – n'apparaissent jamais aussi nettement que lorsqu'elles cessent, un instant, de fonctionner.

Or, ces infrastructures sont aussi vulnérables qu'elles sont devenues indispensables. Elles sont sous la menace croissante de multiples risques, qu'il s'agisse d'opérations de manipulation ou de sabotages stratégiques, dans un contexte d'exacerbation des conflits géopolitiques ou d'incidents liés à l'accélération du changement climatique. Et ce alors même qu'avec la transition numérique et écologique nous concentrons toujours davantage nos activités sur les infrastructures numériques et électriques dont nos sociétés dépendent désormais pour leur fonctionnement.

C'est de cette centralité paradoxale, car visible seulement dans la panne, la coupure ou encore l'attaque, que ce numéro d'*Hérodote* entend rendre compte, en prolongeant la réflexion collective engagée lors du colloque « Infrastructures et données : leviers de pouvoir et instruments de puissance » organisé à Rennes les 10 et 11 juin 2025 et dont est issue cette introduction.

Trois affirmations en organisent l'architecture. En premier lieu, la notion d'infrastructure, bien qu'ancienne et d'apparence banale, constitue un outil heuristique précieux pour penser les rapports de pouvoir contemporains. Dès 1972, le géographe Yves Lacoste (1929-2026) démontrait que le bombardement des digues du fleuve Rouge au Vietnam mené par l'aviation américaine était délibéré. Le sabotage de ces infrastructures critiques, essentielles à la protection du delta contre les inondations, s'inscrivait dans une stratégie visant à affaiblir la capacité de résistance du Nord-Vietnam en provoquant une catastrophe susceptible de déstabiliser durablement le pays. En second lieu, les infrastructures numériques et les données qu'elles font circuler occupent, au sein de cet ensemble, une position singulièrement centrale, puisqu'elles soutiennent, permettent et façonnent désormais la plupart des autres infrastructures. Enfin, ces objets se prêtent pleinement à une lecture géopolitique, au sens que *Hérodote* a contribué à donner à ce terme depuis un demi-siècle, à condition d'étendre la notion de territoire aux dispositifs eux-mêmes et de se doter des outils cartographiques capables de rendre visibles des rivalités qui, par construction, se dérobent au regard.

La centralité des infrastructures numériques et des données

Cette centralité mérite d'être précisée. Les trois scènes évoquées en ouverture ne sont pas de simples illustrations juxtaposées d'un même phénomène. Elles rappellent, chacune à sa manière, que les infrastructures numériques ne se

Hérodote, n° 202, La Découverte, 3e trimestres 2026.

Herodote202_CC2021_PC.indd 6 11/09/2026 13:19:50

contentent plus de véhiculer de l'information, mais conditionnent désormais le fonctionnement des réseaux d'énergie, de transport, de finance ou de défense qui, à leur tour, rendent la vie numérique possible. Cette interdépendance circulaire et cette imbrication des infrastructures expliquent le caractère essentiel de ces objets et, en même temps, leur vulnérabilité à une multitude de risques, des catastrophes naturelles aux défaillances accidentelles en passant par les sabotages, les cyberattaques, ou les conséquences de la coercition étatique.

On peut analyser cette centralité selon trois configurations. La première concerne les infrastructures propres aux données numériques elles-mêmes, c'est-à-dire les câbles sous-marins, les points d'échange internet, les centres de données, les constellations satellitaires, les systèmes de routage. Ce sont autant de dispositifs matériels et protocolaires sans lesquels aucune donnée ne circule. La deuxième porte sur les infrastructures en tant qu'elles produisent des données. Il ne s'agit pas uniquement des objets connectés ou des plateformes d'intermédiation mais aussi d'une conséquence de la numérisation de toutes les infrastructures. Les dispositifs matériels, les protocoles de circulation, de stockage ou de traitement des données, les acteurs privés et publics qui les exploitent ou les maintiennent assurent ainsi de très nombreuses fonctions (transport, énergie, santé, commerce, administration, finance) et génèrent en creux des masses de données devenues elles-mêmes stratégiques. La troisième, enfin, s'intéresse aux données comme leviers et instruments de pouvoir et de contrôle, dans, sur et par des infrastructures qui ne sont pas nécessairement numériques. Dans cette configuration, la donnée devient alors un moyen d'action sur des réseaux d'énergie, de transport ou de communication, voire sur l'appareil administratif des États contemporains.

À travers ces trois entrées émergent des questions convergentes qu'explorent les articles de ce numéro : comment les dispositifs infrastructurels résultent-ils de jeux de pouvoir antérieurs, et comment deviennent-ils à leur tour des leviers de pouvoir pour ceux qui les contrôlent ou qui en dépendent ? Quels risques et quelles opportunités ouvrent-ils pour les acteurs en présence ? Que nous apprend l'étude de la concentration du pouvoir au sein des écosystèmes numériques, entendus comme systèmes de relations plus ou moins denses et plus ou moins intégrées entre acteurs publics et privés ? Selon quelles modalités ces infrastructures contribuent-elles au déploiement, ou au contraire à la remise en cause, des instances politiques souveraines, qu'elles soient territoriales ou étatiques ? Comment, enfin, s'articulent dans la politique internationale contemporaine rivalités infrastructurelles et instrumentalisation de l'interdépendance qu'elles engendrent ?

Hérodote, n° 202, La Découverte, 3e trimestres 2026.

Herodote202_CC2021_PC.indd 7 11/09/2026 13:19:50

Une lecture géopolitique des infrastructures

Depuis la fondation d'*Hérodote*, la géopolitique s'y définit comme l'étude des rivalités de pouvoir et d'influence sur des territoires, rivalités qui opposent des acteurs mobilisant des représentations différentes, voire contradictoires, de ces mêmes territoires. Cette définition, pensée d'abord pour les espaces terrestres ou maritimes, garde toute sa pertinence en élargissant la notion de territoire, Ainsi, les territoires en question sont à la fois les territoires classiques de la géopolitique (États, régions, villes, mers et détroits) et les infrastructures numériques elles-mêmes, ou les autres infrastructures qui en dépendent désormais étroitement.

Un câble sous-marin, un point d'échange internet, un centre de données ou un système d'adressage sont donc des territoires au sens plein du terme, dont l'appartenance, le contrôle, la localisation ou les règles de fonctionnement font l'objet de représentations concurrentes. Pour certains acteurs, l'infrastructure numérique relève d'un bien commun mondial, dont la neutralité et l'ouverture doivent être préservées contre toute tentative de fragmentation. Pour d'autres, elle relève d'un patrimoine national ou d'un attribut de souveraineté qu'il convient de contrôler, y compris en la reconfigurant physiquement. C'est tout le sens des stratégies russes de réorientation du routage de la Crimée après 2014, ou de la déconnexion volontaire par les régimes à des fins de censure ou de contrôle de l'espace informationnel en Iran. Pour d'autres encore, elle constitue avant tout un actif économique, propriété d'opérateurs privés dont les intérêts ne coïncident pas nécessairement avec ceux des États sur le territoire desquels ils opèrent. Ces représentations concurrentes engendrent des rivalités bien réelles : autour des normes techniques et des standards, autour de la localisation physique des équipements, autour des règles de gouvernance de l'Internet, autour des capacités de surveillance ou de coupure que ces infrastructures rendent possibles. Une lecture géopolitique des infrastructures, et tout particulièrement des infrastructures numériques, permet aussi d'articuler ces représentations à la matérialité des dispositifs, qu'il s'agisse des boitiers de filtrage que doivent mettre en place les fournisseurs d'accès internet en Russie, des chaînes d'approvisionnement en semi-conducteurs ou des outils de messagerie de l'administration fédérale étatsunienne.

Cette lecture exige des outils et une méthode permettant de rendre visibles des dispositifs qui, par construction, échappent au regard ordinaire, qu'il s'agisse du regard du géographe habitué aux territoires terrestres ou de celui du citoyen qui ne perçoit l'infrastructure numérique qu'à travers l'écran de son terminal. C'est tout l'enjeu des travaux conduits depuis plusieurs années au sein de l'IFG Lab et du centre Géopolitique de la datasphère (GEODE) qui appliquent la démarche géopolitique classique, fondée sur l'analyse spatiale, l'étude des stratégies d'acteurs et la cartographie, à ce nouvel espace de rivalités qu'est la datasphère. Cette

Hérodote, n° 202, La Découverte, 3e trimestres 2026.

Herodote202_CC2021_PC.indd 8 11/09/2026 13:19:50

approche distingue les couches basses de la datasphère (câbles, routeurs, protocoles qui aiguillent les données à travers le réseau) et ses couches hautes, celles des données elles-mêmes et de l'information qu'elles portent. Sur les couches basses, l'exploitation des données de routage, notamment les annonces de routes du protocole BGP (Border Gateway Protocol), permet d'inférer et de représenter cartographiquement la structure de connectivité d'un État ou d'un acteur donné, et donc de mettre au jour des dépendances, des points de passage obligés et des marges de manœuvre stratégique qu'aucune source ouverte classique ne permettrait de documenter.

Cartographier le routage, documenter les points d'échange, localiser les centres de données ou le tracé des câbles sous-marins : ce travail empirique, loin d'être un simple appui technique à l'analyse géopolitique, en est aujourd'hui une composante à part entière. Il prolonge, dans le champ numérique, l'attention qu'*Hérodote* a toujours portée à la carte comme outil de connaissance et comme enjeu de pouvoir, la carte n'étant jamais un décalque neutre du territoire, mais l'expression d'une représentation parmi d'autres, potentiellement concurrente de celles que portent d'autres acteurs. Appliquée aux infrastructures numériques, cette exigence cartographique permet de sortir d'un discours souvent incantatoire sur la souveraineté numérique ou la guerre du routage, pour lui substituer une analyse fondée sur des données vérifiables, des méthodes reproductibles et des résultats discutables, donc contestables, donc scientifiques.

Ce numéro suppose ainsi parfois d'accepter un détour par la technique. Cet effort de lecture est toutefois la condition d'une compréhension éclairée des enjeux géopolitiques qui se cristallisent autour des infrastructures numériques. Conscients de cette exigence, les auteurs comme l'équipe éditoriale ont veillé à accompagner le lecteur dans la découverte de ces contributions en recherchant un équilibre entre précision technique, clarté de l'exposé et fluidité de la lecture.

Le numéro s'ouvre sur l'analyse d'un véritable coup d'État administratif qui a suscité une prise conscience à l'échelle mondiale : l'action du Department of Government Efficiency (Département de l'efficacité du gouvernement, DOGE) au sein de l'administration fédérale américaine début 2025. Cet épisode démontre la brutalité et la rapidité avec lesquelles une infrastructure numérique peut être mobilisée à des fins politiques en raison de leur imbrication avec les infrastructures administratives, ce que Stéphane Taillat nomme « la capture de l'État fédéral par ses infrastructures ». Il constitue surtout un point de bascule dans les relations transatlantiques : les dépendances stratégiques aux infrastructures numériques étatsuniennes, jusqu'alors largement tolérées, deviennent désormais un enjeu géopolitique majeur.

L'ampleur de ces dépendances aux infrastructures numériques étatsuniennes s'est accélérée avec l'adoption du cloud, une infrastructure qui permet de stocker

Herodote202_CC2021_PC.indd 9 11/09/2026 13:19:50

des données et d'utiliser des services informatiques sur des serveurs distants, et aujourd'hui de l'intelligence artificielle générative. Laurent Carroué démontre que « les stratégies de localisation dans l'espace géographique du cyberespace – équipements, centres de données, réseaux de fibres optiques, CDN – posent d'immenses jeux de pouvoirs et enjeux de puissance et de souveraineté, à la fois aux échelles locale, régionale, nationale et mondiale ». Dès les débuts de l'Internet, les États-Unis ont cherché à tirer parti de l'interdépendance offerte par un Internet libre et ouvert, grâce à leur suprématie sur les infrastructures numériques. Jonathan Guiffard démontre ainsi la « subversion intime » des infrastructures numériques par la National Security Agency (NSA), l'agence de renseignement américaine en charge de la cyberdéfense et de l'interception des signaux et données numériques. Cette subversion, régulièrement dénoncée par la Chine, repose sur des stratégies territoriales que l'auteur met en lumière.

L'instrumentalisation des infrastructures numériques à des fins de puissance ne se limite pas au domaine du renseignement. Benjamin Bürbaumer montre au contraire que les États-Unis et la Chine se livrent une concurrence féroce pour le contrôle des infrastructures numériques de l'économie mondiale. Il propose le concept d'infrastructure technologique du numérique pour saisir le pouvoir politique à portée extraterritoriale associé aux technologies de l'information et de la communication. Les rivalités de pouvoir et d'influence sur les territoires entre grandes puissances se jouent également au niveau des infrastructures de connectivité, qui permettent aux usagers d'accéder à l'Internet et donc aux services numériques. Célestine Rabouam analyse les stratégies de déploiement de l'opérateur Starlink, l'entreprise d'Elon Musk, dans le Grand Nord canadien, et les logiques de dépendances et de contrôle qui en découlent et dont le Canada aura du mal à s'émanciper. L'Australie, en revanche, cherche justement à éviter que les îles du Pacifique s'installent dans une dépendance aux infrastructures de connectivité de la Chine. Sophie Hamel démontre comment l'Australie et ses partenaires, notamment les États-Unis, mobilisent l'aide au développement comme un levier stratégique pour le déploiement des câbles sous-marins desservant les États insulaires du Pacifique.

L'enjeu du contrôle des infrastructures numériques est aussi celui du contrôle de l'information. Et de la désinformation. Saïd Haddad aborde les notions de violence infrastructurelle et de violence symbolique pour qualifier les manipulations de l'information en ligne. Là encore, la question des dépendances stratégiques contraint fortement la capacité à étudier ces menaces, et plus encore à lutter contre, pour les pays qui n'ont pas le contrôle sur les données et sur les infrastructures. Or, les champs d'affrontement se multiplient et se diversifient. Les manipulations de l'information et les stratégies d'influence ont migré vers les métavers. Didier Danet analyse ainsi les stratégies d'influence des mouvements

Hérodote, n° 202, La Découverte, 3e trimestres 2026.

Herodote202_CC2021_PC.indd 10 11/09/2026 13:19:50

extrémistes dans les univers immersifs des jeux en ligne massivement multijoueurs et en démonte les mécanismes tels que l'informatique affective, capable d'exploiter en temps réel les états émotionnels des utilisateurs.

Enfin, Ksenia Ermoshina démontre la « colonisation par les infrastructures » exercée par la Fédération de Russie sur les « républiques autochtones », en se plaçant du point de vue de l'utilisateur. Elle documente ainsi les coupures internet, les dénis d'accès, le filtrage de l'information grâce à un terrain numérique appuyé sur des mesures depuis les zones contrôlées. Au-delà de ses résultats, elle démontre aussi la complémentarité des approches de la géopolitique et des sciences, techniques et société (STS) pour comprendre dans toute leur finesse et leur complexité les dynamiques de contrôle et de pouvoir par les infrastructures.

Les contributions rassemblées ici déclinent ainsi, chacune à sa manière, les trois configurations identifiées plus haut, à savoir les infrastructures propres aux données, les infrastructures comme productrices de données et les données comme instruments de pouvoir, en les articulant aux enjeux qui leur sont attachés : dispositifs techniques comme résultats et comme leviers de jeux de pouvoir, risques et opportunités pour des acteurs aux capacités inégales, concentration du pouvoir au sein d'écosystèmes numériques de moins en moins lisibles, remise en cause ou redéploiement des instances politiques souveraines, instrumentalisation enfin de l'interdépendance dans la compétition entre puissances. Puisse ce numéro contribuer à rendre plus visible ce qui, d'ordinaire, ne l'est pas. Jusqu'à la prochaine panne.

Hérodote, n° 202, La Découverte, 3e trimestres 2026.

Herodote202_CC2021_PC.indd 11 11/09/2026 13:19:50