



HAL
open science

**Militants face à la “ souverainisation ” numérique.
Réactions et nouvelles mobilisations dans l’ex-bloc
socialiste (Russie, Ukraine, Cuba)**

Olga Bronnikova, Bella Ostromooukhova, Perrine Poupin, Anna Zaytseva

► **To cite this version:**

Olga Bronnikova, Bella Ostromooukhova, Perrine Poupin, Anna Zaytseva. Militants face à la “ souverainisation ” numérique. Réactions et nouvelles mobilisations dans l’ex-bloc socialiste (Russie, Ukraine, Cuba). Terminal. Technologie de l’information, culture & société, 2022, 134-135, 10.4000/terminal.8498 . hal-03900652

HAL Id: hal-03900652

<https://hal.science/hal-03900652>

Submitted on 27 Dec 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Terminal

Technologie de l'information, culture & société

134-135 | 2022

Militants face à la « souverainisation » numérique.

Militants face à la "souverainisation" numérique

Militants face à la « souverainisation » numérique

Réactions et nouvelles mobilisations dans l'ex-bloc socialiste
(Russie, Ukraine, Cuba)

OLGA BRONNIKOVA, BELLA OSTROMOOUKHOVA, PERRINE POUPIN ET ANNA
ZAYTSEVA

<https://doi.org/10.4000/terminal.8498>

Texte intégral

« Nous sommes accrochés au cordon ombilical primaire des USA. Actuellement, nous sommes en train de sortir une cisaille pour le couper et rendre notre Internet souverain »

Denis Davydov, co-dirigeant de la Ligue pour l'Internet sûr,
Forum pour l'Internet sûr, avril 2019

« Lorsqu'une loi se donne pour but la protection contre des menaces extérieures, et qu'ensuite, il s'avère que la défense vise certaines choses de l'intérieur du périmètre, un déséquilibre est inévitable [...] Mais dans cette guerre, l'appareil bureaucratique sera toujours plus lent que le Réseau. » (Mikhaïl Klimarev, dirigeant de la Société de la protection d'Internet, OZI, article dans Novaya Gazeta, le 1er octobre 2019).

1 Ces propos de personnes engagées dans diverses formes de militantisme en ligne en Russie donnaient à voir la variété des réactions face aux tentatives de souverainisation de l'Internet russe dont la loi dite « de l'Internet souverain », entrée en vigueur en novembre 2019, a été le point d'orgue. Qu'elles soient positives ou critiques, ces réactions illustrent les enjeux stratégiques et les conflits d'intérêts attachés à cette évolution récente de l'Internet, que l'on peut observer ailleurs qu'en Russie.

2 Nous avons conçu ce dossier avant le 24 février 2022, date à laquelle l'invasion russe a débuté en Ukraine et a bouleversé les équilibres nationaux et internationaux, y compris en ce qui concerne les souverainetés numériques. Ce dossier ne tend pas à identifier d'éventuelles continuités entre l'avant-guerre et le conflit, et encore moins à faire croire que nous avons anticipé dans nos observations et analyses cette guerre abominable, qui nous a surpris comme elle a surpris nos interlocuteurs. Il nous paraît néanmoins clair que la guerre accélère et fait aboutir des tendances à la « souverainisation » d'Internet qui sont analysées dans ce numéro et qui ont permis, notamment, la mise en place rapide d'une censure martiale et la liquidation



de nombreux médias indépendants en Russie dès le début de mars 2022. L'objectif que nous nous fixons est de documenter les différentes étapes de la souverainisation de l'Internet à l'œuvre dans l'ex-bloc socialiste à travers l'analyse des formes de critique et de résistance que celles-ci ont suscitées dans les milieux militants avant la guerre. Ce faisant, nous espérons que ces témoignages et enquêtes pourront alimenter les recherches, en cours et à venir, quant à la circulation et les transferts des techniques de contrôle des infrastructures et réseaux au sein des pays post-socialistes et au-delà. Définie comme le droit absolu d'exercer une autorité sur un territoire et un peuple, la souveraineté est inhérente à l'ordre juridique étatique en perpétuelle mutation (Hammarlund, 2005 ; Chevallier, 2017) et permet de penser la relation de l'État par rapport aux autres (Bigo, 2011 ; Pellet, 2014). Or, depuis la fin de la Seconde Guerre mondiale, de nouveaux régimes de souveraineté se mettent en place autour d'entités supranationales (Union européenne, organisations internationales), modifiant les prérogatives des États. Par ailleurs, de nombreux travaux décrivent la montée en puissance, ces dernières décennies, d'acteurs transnationaux (firmes multinationales, opérateurs financiers, ONG, etc.) qui transforme la compréhension de la souveraineté. Cette notion est parfois mobilisée également pour légitimer des revendications d'autonomie infra-nationales de la part de communautés ethno-territoriales rattachées à des régions (Tiller, 2008 ; Laffaille, 2009). En Russie et dans les pays post-soviétiques, la notion de souveraineté a subi des mutations à la suite du démantèlement de l'URSS. Depuis l'avènement de Vladimir Poutine au pouvoir en Russie en 2000, on assiste à une présidentialisation accrue et à un renforcement du pouvoir central, qualifiés parfois de processus de souverainisation, contrariant les velléités d'autonomie de certaines régions et visant à recréer une sphère d'influence russe sur les ex-républiques soviétiques. C'est aussi en prétextant de la nécessité de défendre sa propre souveraineté contre l'extension de l'Otan vers les pays de l'espace post-soviétique que la Russie a justifié l'invasion de l'Ukraine le 24 février 2022.

3 L'espace numérique, initialement administré en dehors des modèles classiques de régulation nationale, est lui aussi concerné par un mouvement de souverainisation. La notion de « souveraineté numérique » fait désormais partie des discours de divers acteurs publics et privés impliqués dans le développement du numérique. Face aux différentes formes de domination s'exerçant sur l'Internet, les États cherchent depuis plusieurs années à renforcer leur influence dans ce domaine, à étendre leur souveraineté dans et à travers ce champ, à y légiférer, à imposer des contraintes ou à garantir des libertés (Benyekhlef, 2002 ; Bellanger, 2012 ; Bonnet et Türk, 2017 ; Mueller, 2017 ; Deibert, 2008 ; Deibert et Crete-Nishihata, 2012). Ils sont concurrencés par de grands acteurs économiques (Gafam) et d'autres institutions transnationales (Icann, RIPE NCC, IETF, W3C) qui détiennent le contrôle de l'infrastructure numérique susceptible d'affecter la souveraineté de par son caractère extraterritorial. Les initiatives de l'État en la matière rencontrent de la part de différents acteurs des résistances multiformes, y trouvent des appuis et suscitent des controverses (Nocetti, 2015 ; Daucé, Ermoshina, Loveluck et Musiani, 2019).

4 Les révélations de Edward Snowden en 2013, mettant en évidence la surveillance de masse effectuée par la NSA (*National Security Agency*) depuis les États-Unis à travers le monde, ont apporté une nouvelle pièce à l'argumentaire des autorités de différents États visant à maîtriser leurs espaces Internet nationaux et à les protéger contre les menaces extérieures. La revendication d'une autorité étatique ou intergouvernementale sur le cyberspace semble faire désormais partie d'un cadre d'interprétation global de la cybersécurité ou sécurité d'information, affichant une nette tendance à une militarisation des méthodes allant parfois jusqu'à annoncer une course aux cyberarmements (Ristolainen, 2017 ; Limnell, 2016). Par exemple, en Russie, la « *sécurité d'information* » est considérée comme un enjeu majeur dans le contexte d'une « *confrontation informationnelle* » (Doktrina, 2000 ; Doktrina, 2016) qui opposerait notamment les États membres de l'Otan et la Russie. Cet argumentaire s'inspire de « *l'autoritarisme digital* » chinois, à la faveur des accords de coopération bilatéraux et déclarations conjointes Russie-Chine pour promouvoir l'idée de la « *souveraineté numérique* » au sein de la gouvernance globale d'Internet et faire reconnaître cette souveraineté « *comme une continuation et un élargissement de la souveraineté étatique dans le cyberspace* » (Kovachich, 2019 ; Budnitsky et Jia, 2018). La cybersécurité devient en outre l'un des objets majeurs de différents forums, stratégies et programmes de coopération au sein de la CEI, de l'Organisation du traité de sécurité collective entre Russie, Bélarus, Arménie, Kazakhstan, Kirghizstan, Tadjikistan, ainsi que de l'Organisation de Shanghai. Le discours officiel des États membres de diverses alliances en dehors du bloc euro-atlantique au sujet de la souveraineté numérique se consolide ainsi et prend une tournure plus ouvertement

sécuritaire, l'Internet global sous la houlette des multinationales américaines étant conceptualisé comme une menace à l'ordre et à la stabilité politique intérieure.

- 5 La Russie, l'Ukraine et le Cuba, loin de représenter l'ensemble de l'ex-bloc socialiste (ce qui n'était pas l'ambition du dossier), ont néanmoins l'avantage de donner à voir trois cas de figure contrastés, quant aux dynamiques de souveraineté numérique. Dans le premier, la souverainisation de l'Internet signe une accélération de la prise de contrôle étatique sur l'ensemble des communications et des infrastructures de l'Internet domestique, une fermeture vis-à-vis des flux extérieurs, accompagnées des dispositifs punitifs toujours plus puissants. Dans le deuxième, la souverainisation prend corps comme une arme défensive vis-à-vis de l'agresseur voisin, sans revêtir de caractère absolu ni centralisé, car les acteurs privés disposent toujours d'une marge de liberté. Enfin, le troisième cas de figure offre peut-être un exemple unique d'un bricolage, orchestré à la fois par des acteurs privés, des militants ordinaires et des organismes d'État, qui conduit à une réouverture partielle et détournée du cyberspace vers l'extérieur.
- 6 Dans ce numéro, nous proposons donc de brosser un tableau de la question de la souveraineté numérique dans trois pays de l'ex-bloc socialiste, et notamment d'explorer les façons dont certains militants réagissent aux dynamiques engendrées par cette souverainisation. Tout d'abord, Valéry Kossov fait le point sur la souveraineté numérique à partir des discours et des politiques du gouvernement russe à ce sujet depuis le début des années 2010. Il a aussi pour objet l'étude de la jurisprudence en la matière. Ensuite, Françoise Daucé analyse, dans ce contexte de contrôle de plus en plus fort de l'espace numérique, les trajectoires de lutte de militants des libertés numériques, comme le Parti Pirate en Russie. Olga Bronnikova et Anna Zaytseva, pour leur part, se penchent sur les formes de résistance et d'adaptation des militants des ONG de défense des droits humains et des journalistes indépendants à la progressive souverainisation de l'Internet en Russie, notamment concernant leurs pratiques de sécurité numérique. Enfin, Perrine Poupin consacre son texte à la notion de souveraineté numérique à partir de l'analyse d'une mobilisation d'habitants contre un projet de décharge dans le nord de la Russie, à la frontière de la région d'Arkhangelsk et de la République des Komis.
- 7 En contrepoint des contributions portant sur la Russie, celle de Natalia Calderón interroge les politiques de souveraineté numérique à Cuba depuis le début du Blocus de l'île menant à la déconnexion d'Internet. Diverses tactiques de "technocontestations" populaires émergent dès lors, entretenant un dialogue complexe et ambivalent avec les politiques volontaristes de souveraineté numérique (un « hacking d'État »).
- 8 La rubrique *Libres propos* offre un autre contrepoint aux terrains russes, à la fois plus proche que Cuba et plus ouvert. Les chercheurs du *think tank* ukrainien NN étudiant les politiques numériques en Europe et dans le monde, Sergey Zhdanov, Nastya Travkina et Anton Tarasyuk, nous livrent une réflexion sur la cybersouveraineté qui est à la fois théorique, comparative (entre différents modèles de souveraineté numérique) et nourrie de leurs pratiques de défense de l'Internet en Ukraine dont la résistance à l'agresseur russe se déroule aussi dans le cyberspace.
- 9 Le reste de cette même rubrique est nourri par les matériaux du colloque final du projet ANR ResisTIC *Critiques et contournements des contrôles et de la surveillance sur Internet* (31 mars-1^{er} avril 2022, EHESS, Paris). D'abord, l'entretien avec Mikhaïl Klimarev, l'un des intervenants à ce colloque et militant de l'ONG russe Société de protection d'Internet, prolonge et approfondit son propos tenu à l'occasion de cet événement : il propose un classement d'États selon le degré de liberté de leur Internet, allant d'un Internet totalement dépourvu de toute contrainte étatique (exemple de la Finlande) à un « Splinternet » (Corée du Nord), en passant par des pays soumis à des coupures temporaires partielles ou totales d'Internet (Russie, Bélarus, Kazakhstan). Enfin, le dossier se termine par la transcription de la table ronde conclusive du colloque, avec la participation de l'équipe du projet ANR (Olga Bronnikova, Françoise Daucé, Benjamin Loveluck, Francesca Musiani, Bella Ostromoukhova, Perrine Poupin, Anna Zaytseva). Passant en revue les données recueillies lors de leurs enquêtes de terrain, les chercheurs nous offrent tant un bilan scientifique du projet ANR (2018-2022) que des ouvertures et interrogations, quant à de multiples défis se posant devant celles et ceux qui étudient et défendent un Internet libre dans un monde où émergent de nouvelles frontières de souverainetés, mouvantes et contestées.

- BELLANGER, P. (2012). « De la souveraineté numérique ». *Le Débat*, 3/170, p. 149-159
DOI : 10.3917/deba.170.0149
- BENYEKHLIF, K. (2002). « L'Internet : un reflet de la concurrence des souverainetés ». *Lex Electronica*, 8.
https://www.lex-electronica.org/files/sites/103/8-1_benyekhlef.pdf
- BIGO, D. (2011). « Frontières, territoire, sécurité, souveraineté ». *CERISCOPE Frontières*.
<http://ceriscope.sciences-po.fr/content/part1/frontieres-territoire-securite-souverainete>
- BONNET, J. ET TÜRK, P. (2017). « Le numérique : un défi pour le droit constitutionnel ». *Les Nouveaux Cahiers du Conseil constitutionnel*, 4/ 57, p. 13-24
DOI : 10.3917/nccc1.057.0013
- BUDNITSKY, S., JIA, L. (2018), « Branding Internet sovereignty : Digital media and the Chinese–Russian cyberalliance ». *European Journal of Cultural Studies*, 21, p. 594–613.
- CHEVALLIER, J. (2017). *L'État post-moderne*, Paris, LGDJ.
- DEIBERT, R. J. (2008). « The geopolitics of internet control : Censorship, sovereignty, and cyberspace ». Dans A. Chadwick et P. N. Howard (dir.), *Routledge handbook of Internet politics* (p. 339-352). Routledge
- DEIBERT, R. J. ET CRETE-NISHIHATA, M. (2012). « Global governance and the spread of cyberspace controls ». *Global Governance*, 18, p. 339–361
DOI : 10.1163/19426720-01803006
- DAUCÉ, F., ERMOSHINA K., LOVELÜCK, B. ET MUSIANI, F. (2019, 18 mars). « Souveraineté numérique : l'Internet russe peut-il se couper du reste du monde ? » *The Conversation*.
<https://theconversation.com/souverainete-numerique-linternet-russe-peut-il-se-couper-du-reste-du-monde-113516>
- DOKTRINA 2000 (9 septembre), *Doktrina informatsionnoi bezopasnosti Rossiiskoi Federatsii* (doctrine de la sécurité d'information de la Fédération de Russie). <http://base.garant.ru/182535/>
- DOKTRINA 2016 (5 décembre), *Doktrina informatsionnoi bezopasnosti Rossiiskoi Federatsii* (doctrine de la sécurité d'information de la Fédération de Russie).
<http://static.kremlin.ru/media/acts/files/0001201612060002.pdf>
- HAMMARLUND, P. (2005). *Liberal Internationalism and the Decline of the State, The Thought of Richard Cobden, David Mitrany, and Kenichi Ohmae*, The Palgrave Macmillan
DOI : 10.1057/9781403980366
- KOVACHICH, L. (2019, 1 février). « Russia Flirts With Internet Sovereignty ». *The Moscow Times*.
<https://www.themoscowtimes.com/2019/02/01/russia-flirts-with-internet-sovereignty-op-ed-a64369>
- LIMNÉLL, J. (2016). « The cyber arms race is accelerating—what are the consequences ? » *Journal of Cyber Policy*, 1 :1, p. 50-60.
- LAFFAILLE, F. (2009). « La souveraineté régionale, entre oxymoron et hendiadys constitutionnels. À propos de l'État « régional-fédéraliste » italien et de la sémantique en droit constitutionnel ». *Revue internationale de droit comparé*, 61-2/1, p. 315-355
- MUELLER, M. (2017). *Will the Internet Fragment ? Sovereignty, globalization and cyberspace*, Cambridge, Polity Press
- NOCETTI, J. (2015). « Contest and conquest : Russia and global internet governance ». *International Affairs*, 91, p. 111–130. <https://doi.org/10.1111/1468-2346.12189>
DOI : 10.1111/1468-2346.12189
- PELLET, A. (2014). *Le droit international entre souveraineté et communauté*, Paris, Pedone
- RISTOLAINEN, M. (2017). « Should 'RuNet 2020' Be Taken Seriously ? Contradictory Views about Cyber Security between Russia and the West ». *Journal of Information Warfare*, 16-4, p. 113-131
- TILLER, V. (2008). « La souveraineté tribale des Indiens des États-Unis et le système fédéral américain ». *Nuevo Mundo Mundos Nuevos*. <https://doi.org/10.4000/nuevomundo.46193>
DOI : 10.4000/nuevomundo.46193

Pour citer cet article

Référence électronique

Olga Bronnikova, Bella Ostromooukhova, Perrine Poupin et Anna Zaytseva, « Militants face à la « souverainisation » numérique », *Terminal* [En ligne], 134-135 | 2022, mis en ligne le 12 octobre 2022, consulté le 27 décembre 2022. URL : <http://journals.openedition.org/terminal/8498> ; DOI : <https://doi.org/10.4000/terminal.8498>

Auteurs

Olga Bronnikova
MCF, Université Grenoble Alpes

Articles du même auteur

« **Se protéger ou périr** » [Texte intégral]

Transformations des savoir-faire en sécurité numérique des militants et journalistes russes indépendants (2017-2022)

Paru dans *Terminal*, 134-135 | 2022

Bella Ostromoukhova
MCF, Sorbonne Université

Articles du même auteur

Entretien avec Mikhaïl Klimarev, président de la Société de protection d'Internet en Russie

[Texte intégral]

Effectué le 16 septembre 2022 en ligne

Paru dans *Terminal*, 134-135 | 2022

Perrine Poupin

Chargée de recherche CNRS, Université Grenoble Alpes, CNRS, ENSAG, AAU-CRESSON

Articles du même auteur

Conflit contre un projet de méga-décharge à Shies [Texte intégral]

Enjeux de souveraineté dans le nord-ouest russe à l'ère d'Internet

Paru dans *Terminal*, 134-135 | 2022

Anna Zaytseva

MCF, Université Toulouse Jean Jaurès

Articles du même auteur

« **Se protéger ou périr** » [Texte intégral]

Transformations des savoir-faire en sécurité numérique des militants et journalistes russes indépendants (2017-2022)

Paru dans *Terminal*, 134-135 | 2022

Droits d'auteur

Tous droits réservés