mercredi 18 mai 2022

NUMÉRIQUE

Internet, technologie de puissance dans un monde déchiré par la (cyber-)guerre

Par **Ksenia Ermoshina** et **Francesca Musiani**

SOCIO-ÉCONOMISTE, SOCIO-ÉCONOMISTE

Le conflit russo-ukrainien soulève à nouveaux frais un nombre important de questions quant au contrôle et à la surveillance d'Internet. Entre sécurisation des données, « besoin de connectivité » et recherche d'outils numériques alternatifs, des résistances numériques similaires se dessinent en Ukraine et en Russie pour se protéger d'un arsenal législatif et technique imposant.

Nous étudions depuis plusieurs années les architectures et les infrastructures d'Internet comme instruments de gouvernance, c'est-à-dire comment les technologies qui facilitent les interactions en ligne et la connexion à un réseau global peuvent être utilisées, voir cooptées, par des acteurs étatiques et du secteur privé pour une variété d'objectifs politiques.

Depuis quelques années, notamment dans le cadre du projet ResisTIC, la Russie offre un cas d'étude particulièrement stimulant, à la fois du fait de ses spécificités et parce qu'il permet d'identifier et d'analyser certaines tendances plus larges qui concernent la souveraineté numérique, la surveillance ou la gouvernance d'Internet.

Cet article fera le point sur l'arsenal technique et législatif mis en place par la Russie au cours de la dernière décennie pour renforcer sa souveraineté et son indépendance numérique, et reliera ces enjeux au contexte actuel de la guerre en Ukraine.

Un arsenal législatif et technique toujours plus imposant

Au cours de la première décennie du XXIe siècle, caractérisée par des niveaux relativement élevés de liberté dans l'innovation numérique, les contraintes techniques de la construction de l'Internet russe (RuNet) sont restées pour la plupart invisibles pour ses utilisateurs. Cependant, depuis le début des années 2010, les réglementations de plus en plus strictes imposées par le gouvernement ont rendu ces contraintes plus manifestes. En particulier, Roskomnadzor (RKN), l'organisme du gouvernement fédéral de contrôle des communications, a vu sa compétence et sa portée rapidement étendues à des domaines aussi variés que le contrôle du contenu en ligne, le droit de bloquer des sites Web et l'enregistrement dans une « liste noire » de sites Web bloqués, avec un pouvoir accru de censure. Le contrôle de RKN repose sur son important réseau de relations et de collaborations avec les acteurs qui assurent le fonctionnement d'Internet et proposent des solutions de connectivité aux utilisateurs (fournisseurs d'accès, points d'échange de trafic ou IXP, hébergeurs, propriétaires d'entreprises numériques…).

Ce scénario a conduit à une instanciation particulière et spécifique à la Russie de l'étiquette de « souveraineté numérique », qui s'est imposée au cours de la dernière décennie : en effet, les autorités russes poursuivent activement une stratégie de souveraineté numérique qui se concentre sur une autonomisation et une « souverainisation » du RuNet par l'adoption de nouvelles lois pour contrer les influences et agents étrangers, ainsi que leurs dispositifs et applications.

Deux textes en particulier offrent des exemples de cette tendance : la loi dite sur « l'Internet souverain » (officiellement 90 FZ), adoptée en 2019, et la loi dite « contre Apple » (officiellement 425 FZ), adoptée en 2020. La première loi charge le gouvernement d'assurer le fonctionnement stable de son infrastructure critique en prenant le contrôle des points d'échange de trafic, de tous les systèmes autonomes et du système des domaines nationaux ru. et рф. La loi prévoit également la mise en place d'un contrôle étatique sur le trafic Internet qui circule au-delà des frontières russes, par le biais d'une infrastructure (solution de type Deep Packet Inspection) qui assurera l'acheminement des paquets de données en cas d'impossibilité de connexion à des serveurs étrangers. La deuxième loi oblige les fabricants de matériel étrangers à préinstaller des logiciels « made in Russia » sur les appareils électroniques vendus en Russie à partir du 1er avril 2021, et a rencontré une réponse défavorable de la part de grandes marques de terminaux numériques, dont Microsoft et Intel, ainsi qu'Apple.

Ukraine, l'invasion qui chamboule le monde (numérique)

Le 24 février 2022, les forces armées de la Fédération de Russie ont envahi l'Ukraine et la guerre fait rage sur le territoire ukrainien depuis lors. Au milieu de profondes inquiétudes pour la sécurité des proches et des collègues directement touchés par les événements, ainsi que plus largement pour l'avenir des peuples d'Ukraine, de Russie, d'Europe et du monde, nos « esprits académiques » sont toujours au travail. Au fur et à mesure de la guerre, nous observons les multiples champs de bataille autour de la désinformation en ligne, de la cybersécurité et des infrastructures de communication qui sont une partie cruciale du conflit et qui sont liés de longue date à des « préoccupations numériques ».

Par exemple, des débats ont lieu depuis longtemps dans les arènes de la gouvernance d'Internet sur le droit à la vie privée en lien avec notre dépendance toujours croissante aux technologies numériques, qui s'est particulièrement politisée à la suite des révélations de Snowden. Un accent particulier est mis sur les technologies de chiffrement. Ces technologies encodent l'information en convertissant sa représentation originale en formes alternatives que les ordinateurs modernes sont incapables de casser, assurant la sécurité des communications. Ces technologies sont également au cœur d'une controverse publique, dans laquelle les défenseurs de la vie privée s'opposent à ceux qui prétendent que le chiffrement est une menace pour la sécurité générale car il permet le terrorisme et d'autres formes d'action subversive.

La guerre en Ukraine rend encore plus pressant le besoin de répondre aux questions qui sont depuis longtemps soulevées par les technologies de chiffrement « en société » : en temps de guerre, quel est le rôle des technologies de cryptage et de protection de la vie privée ? Comment le conflit armé remet-il en question les modèles de menace existants ? Quels sont les nouveaux risques pour la société civile ? Et le chiffrement peut-il vraiment sauver des vies ?

L'invasion russe en cours de l'Ukraine est également une « cyberguerre ». Elle a eu un impact considérable sur le cyberespace russe et ukrainien à de nombreux niveaux, des modifications drastiques de la législation sur Internet et des sanctions internationales aux infrastructures physiques fortement endommagées par les opérations militaires ; des cyberattaques massives contre les services gouvernementaux aux campagnes de désinformation menées par l'État prenant le contrôle des réseaux sociaux russes.

Suite à la loi de 2019 visant à approfondir un « Internet souverain » en Russie, le gendarme RKN a maintenant entre les mains un déclencheur qui permet de ralentir considérablement et de bloquer partiellement Twitter, YouTube et Facebook (le système dit « TSPU » : Tehnicheskiye Sredstva Protivostoyaniya Ugrozam, ou « moyens techniques pour contrer les menaces »). De nouveaux systèmes de Deep Packet Inspection, installés sur la majorité des réseaux russes, sont utilisés pour ralentir et/ou bloquer Facebook, Instagram et Twitter ainsi que des médias indépendants, afin de prendre le contrôle du récit du conflit en cours que l'État russe refuse encore d'appeler une guerre. En raison de ce système, les résidents russes ont été officiellement coupés des principales sources et services d'information étrangers.

Les sanctions internationales, elles aussi, ont fortement impacté le cyberespace russe. Une conséquence inattendue de ces sanctions, qui est, elle, plutôt bénéfique pour la société civile russe, concerne les instruments techniques de censure et surveillance. Notamment, avec le départ du marché russe des grands fabricants comme Cisco, Mikrotik, Huawei ou Nokia, les fournisseurs d'accès à Internet (FAI) russes ne sont pas en mesure de respecter les lois en vigueur sur le stockage ou l'inspection de trafic utilisateur. Le projet de RuNet souverain est ainsi remis en question, car les sanctions ont révélé des dépendances profondes des systèmes de contrôle de l'information dits « russes » aux fabricants internationaux.

Mais la deuxième grande conséquence des sanctions numériques contre la Russie fait actuellement débat au sein des communautés des défenseurs des droits et libertés numériques (des ONG locales russes telles que Roscomsvoboda ou OZI, aux ONG de renommée internationale, telles que AccessNow). En effet, les décisions de certaines entreprises numériques (comme les grands opérateurs Cogent ou Lumen) de ne plus offrir de services aux Russes ont un impact plutôt négatif car elles rendent encore plus difficile l'accès du peuple russe à des informations plus ou moins objectives.

Des résistances numériques plurielles

En temps de guerre, le besoin de *connectivité* prime sur la sécurité. Nos terrains en cours montrent que, dans le contexte où les infrastructures matérielles d'Internet sont instables, les usagers ont recours aux modes plus anciens (et qui paraissent plus robustes), dont les SMS et les appels vocaux non-chiffrés.

En Russie, le bon fonctionnement des services de communication est menacé non pas par les bombes mais par les nouvelles mesures législatives adoptées dans le cadre de la « censure de guerre » : blocage de Facebook et Instagram ; menaces de blocage des services de Google et YouTube. De plus, toute activité de propagande anti-guerre est sévèrement réprimée, et les militants sont surveillés et poursuivis en justice. Le recours au chiffrement est ainsi en train d'augmenter, de même que le recours aux solutions de contournement et anonymisation de type réseau privé virtuel (VPN) et Tor.

Ces nouvelles habitudes d'auto-défense numérique se répandent bien au-delà des cercles militants. Comme nous l'avons démontré dans nos travaux antérieurs, le risque est relationnel ; des familles entières commencent à utiliser des messageries chiffrées telles que Telegram, ou un réseau VPN pour rester en communication, lorsqu'un membre de la famille s'engage dans des activités militantes anti-guerre.

Malgré sa réputation ambiguë et ses procédures de cryptage douteuses, la plateforme de messagerie Telegram est devenue le principal outil de communication pour les Russes et les Ukrainiens. Parfois dit « imblocable », Telegram est utilisé non seulement pour diffuser des informations plus ou moins indépendantes et de la documentation vidéo et photo de première main sur la guerre, mais sert également d'outil principal pour les Ukrainiens pour se coordonner dans les situations d'urgence, et pour certains Russes afin d'organiser des actions contre la guerre et coordonner le soutien aux militants arrêtés.

Or, Telegram sert également d'outil de dénonciation et de « cyber-vigilantisme » : plusieurs chaînes anonymes publient les photos et données personnelles de prétendus « nationaux-traîtres » (militants anti-guerre russes). D'autres chaînes, au contraire, sont créées pour dénoncer les « ruscistes » (qui partagent des opinions pro-guerre).

La dynamique de la guerre introduit de nouveaux risques qui affectent le choix des outils de communication par les utilisateurs. Les citoyens ukrainiens et les militants anti-guerre russes, malgré leurs différences évidentes, partagent le même modèle de menace (c'est-à-dire l'identification d'adversaires ou d'hostilités potentiels, et d'éventuelles stratégies d'atténuation), très spécifique à la situation de guerre : la partielle ou totale coupure d'Internet. En Ukraine, ces perturbations de la connectivité sont principalement provoquées par des dommages physiques causés par des opérations militaires aux câbles optiques ou aux antennes relais. En Russie, ces coupures sont orchestrées du haut vers le bas, notamment par le biais du système TSPU.

Ce nouveau contexte a conduit les Russes et les Ukrainiens à rechercher des outils alternatifs qui peuvent être fiables même lorsque « l'Internet normal » est en panne. La perspective d'être totalement ou partiellement hors ligne signifie que les utilisateurs se tournent vers des protocoles et des outils plus anciens, tels que les SMS et les appels téléphoniques réguliers, ainsi que le courrier électronique. Les Ukrainiens appellent et envoient des SMS à leurs proches qui sont confinés dans des abris anti-bombes pendant de nombreux jours sans Internet, tandis que les FAI ukrainiens travaillent courageusement pour réparer et maintenir leurs infrastructures et amener Internet jusque dans les bunkers. Les médias d'opposition en Russie reviennent aux « bonnes vieilles » listes de diffusion pour partager des informations sur la guerre, car leurs sites Web sont officiellement bloqués. Pour la majorité des personnes vivant dans un contexte de guerre, la connectivité devient souvent plus une priorité que la sécurité (il est préférable d'avoir une communication non protégée que pas de communication du tout).

Des utilisateurs plus compétents sur le plan technique ont cependant initié un *exode numérique*, préconisant l'utilisation de différents systèmes de messagerie cryptés décentralisés ou fédérés – Briar, Matrix ou Delta Chat, par exemple. En effet, les architectures techniques des services Internet sont désormais au cœur des débats liés au numérique, notamment avec la critique des GAFAM et de leur modèle d'affaires basé sur l'extraction des données des usagers. Pour les Russes surtout, la dépendance des solutions centralisées est indésirable, car elles s'avèrent être plus facilement blocables et offrent moins de protection en termes de métadonnées.

En quête d'une plus grande autonomie informationnelle, d'une meilleure connectivité et d'un plus ample contrôle sur leurs données, certains internautes cherchent des alternatives aux plateformes centralisées et optent pour des solutions décentralisées, auto-hébergées ou maintenues par des collectifs d'hébergeurs indépendants, qui tiennent à la transparence algorithmique et à la protection des données de leurs utilisateurs. Les dispositifs fédérés ou décentralisés proposent une solution possible au problème du *silo effect* (c'est-à-dire l'impossibilité d'interagir entre des outils de messagerie différents ou de migrer d'une application vers une autre) en permettant une communication entre une multitude d'instances ou de serveurs différents, sans forcer les utilisateurs à converger vers un serveur unique.

Des systèmes comme Briar, Matrix ou Delta Chat proposent d'utiliser des solutions fédérées ou décentralisées en y intégrant le chiffrement et les caractéristiques de sécurité les plus récentes, pour ainsi garantir non seulement la protection du contenu des messages, mais aussi la liberté de choix des serveurs, la résistance aux éventuels blocages, la meilleure protection de l'anonymat et des métadonnées. Dans un contexte de contrôle centralisé comme celui adopté par l'État russe, ces systèmes constituent un moyen important de « résistance par l'infrastructure ».

Ainsi, deux solutions proposant des services de communication « d'urgence » ont été mises en place par l'ONG canadienne eQualit.ie et les techno-enthousiastes locaux : une en Ukraine (appelée dComms, proposant des serveurs sécurisés dans huit villes, dont Kyiv, Lviv, Kharkiv, et Odessa) et une en Russie (appelée Chatv3, offrant des serveurs dans huit villes également, dont Moscou, Saint-Pétersbourg, Ekaterinbourg, et Samara). Les serveurs proposant des messageries préinstallées comme Matrix et Delta Chat et offrant des applications de contournement de censure (telles que le navigateur CENO) sont configurés de sorte qu'ils permettent de rester en contact avec les usagers de la même ville même si l'Internet est coupé.

Des symétries transfrontalières, une vision de liberté

L'observation des vies numériques des Russes et des Ukrainiens montre des symétries qui, lues à la lumière de la guerre, peuvent sembler surprenantes. Des entretiens que nous avons effectués par le passé avec des journalistes et des militants de l'opposition russe, ainsi qu'avec des formateurs ukrainiens en sécurité numérique, révèlent des visions du monde très similaires, ces groupes utilisant souvent les mêmes technologies pour se protéger d'adversaires très similaires.

Ils partagent également des méthodes, telles que l'élaboration d'un « modèle de menace » : des instruments tels que la modélisation des menaces et l'évaluation des risques sont déployés notamment lors du développement ou du choix de systèmes de messagerie chiffrée, afin d'identifier par rapport à qui un utilisateur doit se protéger, ou afin d'analyser la possibilité qu'une menace se produise. Enfin, ces groupes partagent également une vision : celle d'un monde où l'indépendance des pays est respectée, où la liberté d'information est garantie et où le droit à la vie privée est protégé. Cela peut paraître surprenant, mais des échanges d'expérience continuent entre les experts en sécurité numérique ukrainiens et russes, car les deux communautés partagent le même objectif : sauver des vies, mettre fin à la guerre et contrer le régime autoritaire russe qui est à son origine.

Alors que – et cela vaut la peine d'être rappelé – le conflit russo-ukrainien dure déjà depuis huit ans, la phase ouverte et certainement encore plus violente dans laquelle il est désormais entré pose de nouveaux défis à la société et aux technologues qui œuvrent à la défense de nos droits et libertés numériques. Le rapport des personnes à leurs outils numériques est plus que jamais non seulement une question de liberté, mais une question qui relève de la préservation des vies humaines.

NDLR : Ksenia Ermoshina et Francesca Musiani ont récemment publié Concealing for Freedom : The Making of Encryption, Secure Messaging and Digital Liberties*, chez Mattering Press.*

Ksenia Ermoshina

SOCIO-ÉCONOMISTE, CHARGÉE DE RECHERCHE AU CNRS

Francesca Musiani

SOCIO-ÉCONOMISTE, DIRECTRICE ADJOINTE DU CENTRE INTERNET ET SOCIÉTÉ DU CNRS

Partager : copier le lien sur Twitter sur Facebook sur Linkedin par Mail

RAYONNAGES

International Europe Russie Ukraine

Médias et numérique Internet Réseaux sociaux Technologie

à lire aussi dans l'édition du mercredi 18 mai 2022

Opinion

Éternité ou inévitabilité, une dangereuse alternative politique

Par Fabrice Flückiger

En 2022 comme en 2017, l'élection présidentielle semble s'être réduite à un choix entre « politique d'éternité » et « politique d'inévitabilité », binarité exposée par Timothy Snyder dans The… lire plus

Critique

Pédagogie de la répugnance – à propos de *Pétrole* de Pier Paolo Pasolini

Par Federico Luisetti

Pier Paolo Pasolini aurait eu 100 ans le 5 mars dernier. Son assassinat peut, tout comme notre présent – guerre en Ukraine et crise énergétique subséquente –, être pensé à la lumière de Pétrole, son roman… lire plus