Networked Craftiness : How Internet Service Providers Resist “By Infrastructure” in Russia

Ksenia Ermoshina, Francesca Musiani

Ruser sur les réseaux : Résistances « par l'infrastructure » des fournisseurs d'accès Internet en Russie

Ksenia Ermoshina et Francesca Musiani
Centre Internet et Société, CNRS

Table des matières

Introduction

Le marché des fournisseurs de services Internet (FAI) s'est développé de façon décentralisée en Russie, à l'initiative d'ingénieurs-entrepreneurs qui travaillaient au sein d'institutions scientifiques et étaient en relation étroite avec les pays de l'aire occidentale, dans un contexte presque « anarchique » (Kuznetsov, 2004), c'est à dire sans leaders prédominants, contrôle centralisé ou primauté des intérêts marchands. En effet, la Russie n'a pas connu un projet de développement centralisé des infrastructures informationnelles au niveau national, malgré le projet d'un réseau à l'échelle de l'URSS (intitulé OGAS) dans les années

1960-1970s ; les réseaux numériques en Russie ont le plus souvent pris la forme d'un "patchwork" de réseaux locaux, ou de communications à des fins purement militaires, plutôt que d'un réseau global interconnecté ouvert aux civils (Peters, 2016). Les premières années du RuNet se sont ainsi déroulées sous la bannière de l'auto-régulation, avec notamment un accord sur l'administration de la zone ".ru" signé en 1993 par les FAI les plus importants.

A ce stade, l'État n'est intervenu dans le développement et la régulation du marché des services Internet que de façon très limitée. Les tentatives de réguler les activités des FAI dans les années 1990-2000 ont été cantonnées à des aspects tels que la distribution des licences, l'attribution des noms de domaine. Lorsqu'en décembre 1999 Vladimir Poutine, alors Premier Ministre, convoque une réunion avec des "experts d'Internet" afin de discuter d'un projet de loi pour déléguer l'administration et la régulation du RuNet au gouvernement, la proposition est vivement critiquée par les "élites d'Internet" (Asmolov & Kolozaridi, 2017) ingénieurs, propriétaires des premières grandes plateformes numériques russes et journalistes, et elle est rejetée.

Le marché des services Internet se développait alors dans une optique d'autorégulation et de ce qu'on pourrait appeler un « multi-parties-prenantes sauvage »[1], avec une concurrence dynamique et une grande diversité d'acteurs mais sans institutions de régulation formelles. Cette décentralisation, ainsi que la topologie des réseaux russes, très connectés à et dépendants de l'étranger, rendaient le contrôle de l'Internet russe compliqué. Un ensemble de lois marquant un tournant autoritaire et centralisateur pour le RuNet, et sous-tendant une vision d'"Internet souverain" (Nocetti, 2015 ; Freiberg, 2014), n'est arrivé qu'au début des années 2010. Cette gouvernance de plus en plus centralisée s'incarne en deux niveaux principaux : la censure et la surveillance (Ermoshina et Musiani, 2017). Une liste noire répertorie désormais les pages web dont l'accès doit être restreint ; le système d'interception légale dit "SORM-3" oblige les fournisseurs d'accès à conserver le trafic de leurs clients pendant au moins 30 jours, et les métadonnées pendant 1 an ; des boîtiers d'analyse de trafic sophistiqués sont développés, et une copie de la structure du Domain Name System (DNS), qui devrait permettre de "boucler" le trafic à l'intérieur du réseau national, est également envisagée.

L'application de ces mesures nécessite l'intégration d'équipements très coûteux chez les FAI, qui doivent assurer les coûts d'achat, d'installation et de maintenance de ces dispositifs, aussi appelés « boîtiers intermédiaires ». Des dizaines de fabricants sont apparus sur ce marché ces dernières années, laissant les FAI perplexes face à une offre de solutions non-certifiées : en effet, les standards, spécifications et prescriptions techniques précises pour ces dispositifs n'apparaissent que très tard, ouvrant la voie à des longues périodes d'incertitude techno-juridique. En réponse à cette gouvernance à la fois floue et de plus en plus centralisée, et face à des risques économiques importants, les FAI développent de nombreuses techniques de résistance afin d'éviter les amendes ou de minimiser les dépenses associées à l'installation des boîtiers. On appelle ces résistances, ensemble de techniques et de pratiques, « ruses sur les réseaux », nous appuyant sur la conceptualisation de ruse développée par Détienne et Vernant (1974) : un ensemble

[1] Les expressions « multi-partisme » ou « multi-parties-prenantes » traduisent l'anglais *multi-stakeholderism*, vocable indiquant le principe selon lequel l'Internet est objet d'intérêt et d'action pour de nombreux acteurs aux alliances multiples et mouvantes. Ce principe a été identifié comme fondateur pour plusieurs institutions de gouvernance d'Internet, notamment l'Internet Governance Forum (IGF).

de stratagèmes ancrés dans la pratique quotidienne qui mêlent l'expertise au sens de l'opportunité et de la débrouillardise.

Ces ruses se déploient selon différents répertoires d'action (Tilly, 2002) – des moyens d'agir sur la base d'intérêts partagés afin de « se faire entendre » sur des problématiques spécifiques – et peuvent se dérouler à des niveaux très différents. Certains de ces répertoires sont d'ordre juridique – notamment entre les "très petits FAIs" et les agents du FSB (Bureau Fédéral de Sécurité) locaux – ou économiques, tels que les arrangements entre FAIs afin de partager les coûts de l'équipement SORM nécessaire à la surveillance. D'autres ruses se concentrent sur les usages créatifs de la technique, véritables bricolages (Akrich, 1998), tels que des scripts artisanaux, permettant d'économiser sur les solutions extérieures, et des actions directes relevant de l'hacking voir du « hacktivisme », telles que les usages détournés du système de noms de domaine qu'on a pu qualifier de « guérilla DNS » (selon l'expression employée par les acteurs).

Cet article propose de se concentrer sur ce dernier type de stratégie, relevant du bricolage numérique[2]. On cherchera à souligner en quoi le hacking et le hacktivisme , ainsi que d'autres ruses comme la mise en place de sous-réseaux dédiés au contrôle, font partie intégrante de l'action des FAI, et à montrer comment les pratiques de ces acteurs relèvent de la « ruse » au sens de Détienne et Vernant (1974). Si les nombreuses études de l'histoire du RuNet se focalisent le plus souvent sur le rôle des "élites culturelles" ou économiques, on se concentre ici sur les acteurs techniques et leurs résistances au quotidien, ancrées dans la technique, aux dispositifs techno-juridiques d'administration des réseaux. Les petits et moyens FAI sont donc les principaux protagonistes de cette étude.

Cette enquête est menée depuis 2018 dans le cadre du projet ANR ResisTIC et en collaboration avec le Citizen Lab (Université de Toronto). Elle s'appuie sur les entretiens effectués avec des fournisseurs d'accès Internet russes, des fabricants de boîtiers intermédiaires, des juristes spécialisés en droit du numérique, des militants pour les "libertés d'Internet", mais aussi sur des observations lors des réunions informelles de FAIs et lors des conférences spécialisées à Saint-Pétersbourg. Notre terrain nous a amené à participer à plusieurs rencontres intitulées "Les Jeudis du Beering" en 2019 où des représentants des petits et moyens FAIs et des Internet Exchange Points (entre douze et quinze en moyenne) se réunissent pour discuter de façon semi-informelle les évolutions et péripéties de l'industrie. Les récits du quotidien des ingénieurs réseau ont été au centre de ces rencontres fermées, y compris le partage des savoir-faire et ruses face aux contraintes de la régulation. Nous avons également mené une analyse des forums spécialisés et des chats des FAIs sur Telegram, la messagerie la plus utilisée par les experts techniques russes. L'étude est ancrée dans une perspective qui puise à la fois dans la sociologie pragmatiste et les *science and technology studies*, ainsi que dans la sociologie des mouvements sociaux, de la participation et de l'activisme numérique (e.g. Milan, 2013).

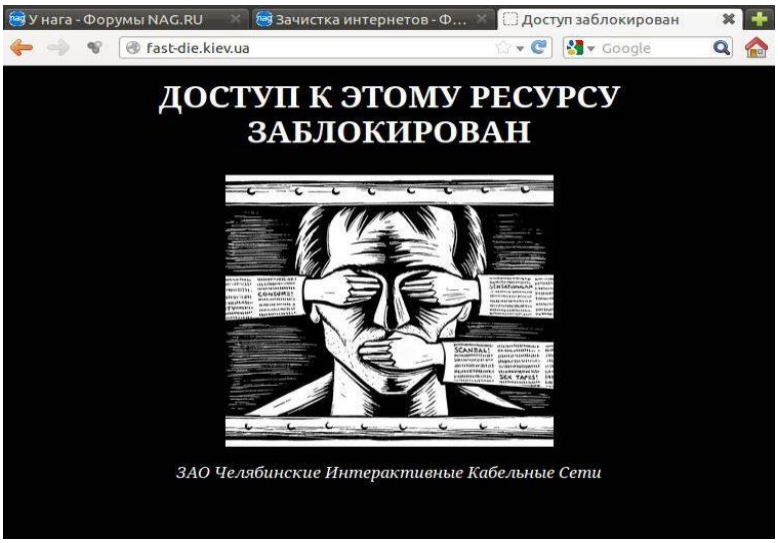
[2] On rappellera ici la définition que Claude Lévi-Strauss (1962) fait de la « pensée sauvage » comme « bricoleuse » dans la mesure où elle est une science « du concret » qui construit du sens à partir de l'assemblage de parties de la matière sensible.

La pomme de discorde : surveillance et censure “par l’infrastructure” dans le RuNet

Avant l’introduction, en 2012, de la liste noire par RosKomNadzor (RKN, l’entité fédérale russe responsable des actions de restriction et censure sur les technologies de communication), l’échange entre les FAI et les régulateurs était sporadique : en juillet 2007, la « liste des ressources extrémistes » contenant alors 14 documents (livres, tractes, vidéos classifiées surtout de l’idéologie nationaliste ou islamiste) fut créée par le Ministère de la Justice. En mars 2008 le Procureur Général délégua la responsabilité de restreindre l’accès à ces sites aux hébergeurs et aux FAIs. A partir de 2008, les opérateurs ont effectivement commencé à recevoir, de temps en temps, des demandes de blocage de certains contenus numériques, et ils disposaient d’un délai de plusieurs jours pour leur donner suite. À cette période-là, les FAI avaient également une possibilité de contester ce genre de demandes en justice[3].

Pendant les premières années qui ont suivi la création de cette “liste noire”, les fournisseurs d’accès n’ont pas été très nombreux à manifester leur mécontentement, selon nos différents entretiens. Les premières actions contestataires ont été entreprises surtout par les acteurs que Asmolov et Kolozaridi appellent les “élites culturelles” (2017), bien que par des moyens déjà ancrés dans la technique : ainsi, par exemple, le fondateur de la plus grande bibliothèque russe en ligne, Maksim Moshkov, répondit au blocage de son site par un « hack », en bloquant en retour le site du Ministère de Justice. Pour cela, il utilisa la méthode désormais connue sous le nom de « DNS guérilla » : il modifia les adresses IP associées au DNS de son site en adresses IP du site du Ministère[4].

Certains FAI avaient déjà riposté à l’introduction des listes noires en utilisant leurs pages de blocage en tant qu’espace d’expression critique (Ermoshina et Musiani, 2017) (Figure 1).



3 Entretien avec un FAI de la ville de Tambov, 2019.

4 https://tjournal.ru/46700-moshkov-minjust

Figure 1. Page conçue par le FAI "Tchélyabinskie Interaktivnye Kabelnye Seti". Le site "fast-die.kiev.ua", dédié au suicide et figurant sur la liste noire du RKN, renvoie l'usager sur une page de blocage avec la fameuse illustration issue du livre de George Orwell "1984"

Or, le mécontentement des FAI a grandi au fur et à mesure que les lois se sont multipliées, et que les modalités de contrôle de leurs activités se sont durcies et se sont concrétisées. Il faut préciser que, dans le cas russe, les rapports entre la "loi" et le "code" (au sens de Lessig, 1999) prennent une forme intéressante : notamment, les solutions techniques s'avèrent souvent être "en retard" par rapport à la régulation. Par exemple, même si les lois qui ordonnent le blocage du contenu web existent depuis 2012, les prescriptions précises quant aux modalités et formes de ce blocage n'ont été publiées qu'en mars 2018. Ainsi, pendant six ans, un certain "vide techno-juridique" a laissé les FAI dans le flou quant aux outils et méthodes nécessaires pour appliquer correctement la loi.

De la même façon, l'industrie russe n'est toujours pas en mesure de proposer une solution suffisamment efficace pour mettre en œuvre la loi Yarovaya, qui oblige les FAIs à stocker les métadonnées pendant 3 ans, et le trafic pendant 30 jours. La loi a même été modifiée à cause des difficultés techniques liées à sa mise en application. La certification des boîtiers pour interception légale "SORM" est également lente. SORM étant un objet techno-juridique distribué, qui se compose de commutateurs, serveurs, logiciels, de systèmes de stockage et d'un terminal d'accès à distance (situé au bureau local du FSB), son architecture même rend sa certification complexe puisqu'elle engage des acteurs nombreux et variés.

Ce vide techno-juridique produit à la fois des contraintes et des opportunités : il laisse des marges de manœuvre aux FAI pour mettre en œuvre des bricolages et des contournements. Il favorise l'apparition d'un marché florissant des fabricants de « boîtiers intermédiaires » pour la censure et la surveillance du trafic, mais place les FAI en situation de flou par rapport à la régulation, dans la mesure où ils risquent d'être pénalisés pour les usages incorrects des installations techniques. En l'absence de méthodes précises prescrites pour les blocages, de nombreux FAIs ont utilisé, pendant presque six ans, des scripts « faits maison » ; ou encore, ils ont adapté leurs installations existantes.

Cela a entraîné à son tour une réponse des régulateurs, qui ont cherché à contrôler l'efficacité de blocage des sites web de façon centralisée et automatisée, en introduisant en 2016 le système automatique Revizor. Cette solution, existant à la fois comme boîtier et logiciel, "imite" un utilisateur d'Internet en envoyant des requêtes vers des sites de la liste noire. Si les pages consultées ne s'avèrent pas être bloquées, les FAIs reçoivent un avertissement ou une amende qui peut varier entre 50 et 100 mille roubles. La responsabilité juridique pour un cas de non-blocage est cependant souvent difficile à établir, vu les arrangements entre des FAI de taille différente, et les pratiques de « filtrage *upstream* », c'est-à-dire, un pré-filtrage par l'opérateur qui revend le trafic à un plus petit FAI. Notre entretien avec le directeur de la Société de Défense d'Internet, ainsi que l'analyse du forum Nag.ru et du tchat homonyme sur Telegram, montrent que les plus petits fournisseurs d'accès perdent le plus souvent et sont les acteurs qui se trouvent le plus fréquemment à faire face aux amendes.

L'automatisation du contrôle des FAI par RKN, ainsi que l'introduction de nouvelles lois qui, à leur tour, augmentent la taille de la liste noire des URL à bloquer, mettent les FAI dans une situation où il devient de plus en plus compliqué d'éviter l'installation d'une solution spécialisée (boîtier ou logiciel) pour le

filtrage de trafic. En effet, la façon dont le blocage des sites web est implémenté en Russie comprend une liste noire centralisée compilée toutes les heures par RKN à partir de plusieurs sous-listes proposées par un ensemble d'institutions[5]. Chaque acteur peut, à son niveau, introduire des erreurs dans la liste. Un des cas les plus connus est représenté par lesdites « barres obliques inversées » ou « antislash », devenu, pour la communauté des petits et moyens FAIs, un qualificatif ironique de l'activité même de tout le RKN[6]. RKN avait introduit dans la liste noire plusieurs URL erronées contenant ces caractères, ce qui avait conduit à la pénalisation de certains FAI pour le non-blocage[7]. Un FAI de la région de Moscou (40 000+ abonnés) nous a parlé à ce propos du niveau de complication très élevé que représente désormais la gestion manuelle d'une liste noire de plus en plus longue et « bruyante ».

Les FAI sont alors obligés d'assumer le coût d'installation de solutions techniques de plus en plus chères, ou bien de payer les amendes. L'analyse des achats publics entre 2016 et 2018 a montré que le coût des solutions pour interception légale (SORM) varient entre 105 mille roubles (RGGU[8]) et 91 383 000 roubles (Rostelecom)[9]. Pour les boîtiers ou solutions logicielles de filtrage de trafic, les prix peuvent aller jusqu'à 1 million de roubles. Tous les FAI interviewés remarquent alors des conséquences économiques très lourdes de cette régulation sur le marché, et certains parlent même de dépenses égales aux recettes annuelles[10]. Cela conduit à la diminution du nombre des FAI, à l'absorption des petits par les grands (par exemple Dom.ru, qui a racheté de nombreux petits FAI) et par conséquent à la centralisation du marché et à la consolidation de ses acteurs. Le directeur de SkyDNS parle des FAI qui comptent quelques milliers d'abonnés comme étant « candidat[s] à l'acquisition », ne pouvant pas couvrir la très importante augmentation de leurs dépenses.

Une autre conséquence concerne le prix des services pour les abonnés, en augmentation chez tous les FAI. Selon les données d'un sondage mené par la revue TelecomDaily auprès de 100 FAIs dans quinze villes russes (21 novembre 2018), 52 % prévoient une augmentation du prix des services Internet pour l'utilisateur final ; 29 % des FAIs envisagent une augmentation de plus de 10%[11]. Tous les FAI interviewés voient la centralisation du marché comme un facteur négatif, tout d'abord pour des raisons

---

5 Aussi variées que le Service Fédéral des Taxes, le Procureur Général, le Ministère de l'Intérieur, le Service Fédéral de Contrôle des Drogues et autres.

6 L'analyse des tchats professionnels montre l'usage de l'expression « barres obliques inversées » dans des contextes où les FAIs parlent des nouvelles mesures de régulation, comme métaphore de solution technique inefficace, voire, destructrice introduite par les agents du gouvernement.

7 Les exemples cités par les FAI incluent des urls comme http://vse-soski.ru/category\\kurganskaya-obl/vargashi/, http://ximikstyle.com/katalog\\metan/metanabol-ot-british-dragon/, http://www.alcomas.ru/katalog\\nujnoe.html, http://pro100farma.net\\stanozolol\\ et autres.

8 RGGU signifie Université d'Etat des Sciences Humaines de Russie. Selon la législation, les universités publiques peuvent avoir l'obligation de passer par la procédure des achats publics afin de se procurer et d'installer l'équipement SORM.

9 Notre analyse est basée sur les données ouvertes de « goszakupki.ru », un site Web qui publie des procédures d'appel d'offres et des résultats pour les marchés publics. En utilisant le mot clé « SORM », nous avons analysé les achats entre 2016 et 2018.

10 Les coûts pour tout le secteur sont évalués à 4,5 trillions de roubles selon FSB et Ministère de Communication, et à 17,5 trillions selon l'Union des Industriels et Entrepreneurs de Russie [https://www.rbc.ru/newspaper/2017/11/09/5a03187e9a7947d88f988f53]

11 L'augmentation a déjà commencé en 2018 (Rostelecom) ; https://telecomdaily.ru/news/2018/11/22/telecomdaily-operatory-obosnovali-povyshenie-tarifov-na-svyaz-na-10-i-bolee

économiques, mais également pour des raisons techniques. Un FAI de la région de Saint-Pétersbourg remarque que « *lorsqu'il y a beaucoup de petits FAI, c'est mieux pour la qualité de la connectivité. […] Puis c'est aussi bien pour les abonnés, car les plus gros FAI ne peuvent pas offrir de la bonne qualité de service technique aux abonnés. Le client doit toujours pouvoir choisir* ».

Bricolages techniques, hacktivisme et ruses numériques

Face à cette situation, inédite jusqu'à il y a quelques années, la majorité des FAI reste « silencieuse » politiquement. Les formes de participation tenant du répertoire militant traditionnel, comme les manifestations de rue, ou même les débats avec les représentants du gouvernement (Ermoshina, 2016), sont considérées comme beaucoup moins efficaces que des outils techniques offrant une possibilité d'agir sur un cas précis. Les « petites choses » qui ne marchent pas deviennent la base sur laquelle ces acteurs techniques se regroupent, et parviennent à dialoguer, à se mettre d'accord au cas par cas, à partager et construire, petit à petit, des répertoires de ruses techniques et des connaissances tacites leur permettant d'alléger leur sort et défendre leurs intérêts économiques.

C'est donc par la technique que prennent forme les « politisations » particulières des technologues et ingénieurs russes. En effet, les acteurs techniques, les FAI en tout premier lieu, introduisent des éléments de ruse et résistance dans leurs pratiques quotidiennes, dans l'architecture de leurs installations et réseaux mêmes. C'est leur expérience ordinaire en tant qu'opérateurs de télécommunications qui se voit modifiée en réponse à la régulation de plus en plus stricte, et face à cette situation, même les FAI les moins « politisés » sont amenés à se lancer dans des bricolages techniques souvent très ingénieux, afin de pouvoir contourner au quotidien les contraintes posées par les régulateurs. La résistance la plus créative et active ne se déploie donc pas tant dans les tribunaux, ni dans la rue : elle se déplace au niveau des agencements techniques des installations réseau ou même des bricolages au niveau des protocoles. La partie suivante du papier explore ce répertoire d'action et met en lumière son potentiel de « ruse numérique ».

Revizor et son « bac à sable »

En analysant les différentes formes de contournement des contraintes techniques (installation des boîtiers SORM et application de la censure), on a pu constater que les FAI appliquent leur « intelligence rusée » à ces endroits physiques et virtuels où le régulateur n'a pas tout prévu, en se fabriquant des marges de manœuvre et d'action. Ce qui est considéré comme un manque d'expertise chez les régulateurs devient alors une source d'inspiration pour les opérateurs. Les résistances techniques se dessinent alors en fonction des caractéristiques techniques des dispositifs de contrôle. Par exemple, de nombreux opérateurs témoignent (dans les entretiens mais aussi dans les groupes de discussion spécialisés) d'une pratique répandue qui consiste à développer un réseau parallèle où se branche le système automatique de contrôle « Revizor » :

« Certains opérateurs appliquent la censure seulement dans un sous-réseau séparé, où ils installent le boîtier Revizor. Revizor consulte des pages web et pense que tout est bloqué, alors que pour leurs utilisateurs finaux il existe un autre réseau où il n'y a pas de censure, ou il y en a mais beaucoup moins » [Entretien avec le directeur de SkyDNS]

Ce sous-réseau est également appelé de façon ironique un « bac à sable »[12] (*pesotchnitsa*). Revizor devient lui-même objet de nombreuses blagues. Le système est critiqué pour sa « stupidité », ses dysfonctionnements fréquents et erreurs récurrentes qui conduisent à des amendes injustifiées. Un groupe de discussion dédié, « J'aime l'AS Revizor » , a été créé dans Telegram (615 membres en mai 2019) où les FAI partagent leurs problèmes avec cet instrument. De plus, juste après son introduction en 2016, un ingénieur a fait une étude poussée de « *reverse engineering* » afin de montrer de quoi se compose cette « boîte noire » qui s'est avérée être un simple routeur TP-Link avec un logiciel. Cette analyse technique[13] avait comme objectif la critique à la fois technique et économique du marché des solutions régulatrices, le coût de cette solution très simple et peu efficace étant de 80 millions de roubles.

Une autre façon de contourner la censure au quotidien consiste à utiliser le protocole IPv6, faiblement adopté en Russie et où la censure ne s'applique pas encore de la même façon :

> *Utilisateur 1 : EN 2019 ipv6 peut vous protéger contre les blocages. Pas à 100 pour cent bien sûr, mais ça peut aider. Le "Ministère de la Vérité"[14] n'a pas encore entendu parler de ipv6 et pense qu'il n'existe pas.*
>
> *Utilisateur 2 : Tous les FAI doivent implémenter ipv6 mais ne dire à Revizor que les adresses ipv4" (source : tchat Nag.Ru, 5 mai 2019).*

Guérilla DNS

Les failles dans le système de blocage des sites web implémenté par RKN ont été explorées et exploitées dans le cadre de ce qui a été appelé « Guérilla DNS », pour la première fois en 2012 par Maksim Moshkov, puis en 2017 et 2018. Ce mode d'action exploite le mécanisme d'envoi automatisé de la "liste noire" aux opérateurs. La *blacklist* compilée par le RKN, qui compte à ce jour 32 267 URLs[15] est mise à jour de façon automatique presque toutes les 10 minutes. Seul le « delta » (la différence entre l'ancienne et la nouvelle liste) est envoyée aux opérateurs ; les FAI doivent alors appliquer la nouvelle liste. Les noms de domaines de la liste noire sont associés à des adresses IP, parfois plusieurs adresses IP sont

---

[12] Un « bac à sable » (*sandbox* en anglais), en sécurité informatique, est un terme qui désigne un mécanisme utilisé pour améliorer la sécurité d'un logiciel et de pages web, d'habitude en créant un environnement isolé du reste du système. Pour un système d'exploitation, il diminue les risques lors de l'exécution d'un logiciel.

[13] https://habr.com/ru/post/282087

[14] "Ministère de la Vérité" - surnom ironique du RosKomNadzor inventé par les FAI, en référence au livre 1984 de George Orwell.

[15] Données du 29 avril 2021, selon https://usher2.club/, le site dédié au monitoring et analyse de la *blacklist*, administré par Phil Kuline, un des résistants les plus actifs du RuNet.

associées au même DNS. Toutes ces adresses sont automatiquement communiquées aux FAI qui doivent alors les bloquer. Il faut noter que de nombreux sites de la liste noire sont abandonnés depuis des années.

La « Guérilla DNS » consiste alors à racheter les noms de domaine "orphelins" et à modifier les adresses IP associées à ces noms de domaine, ce qui permet alors de bloquer des sites web stratégiques (comme les sites des banques ou ministères), voire, le site du RKN lui-même. Cette faille fut exploitée en 2017 : Revizor fut bloqué le 15 mai et entre le 4 et le 9 juin, une véritable campagne menée par plusieurs ingénieurs conduisit au blocage de ressources numériques importantes telles que OK.ru, VK.com, Rostelecom, RZD, RBC, Microsoft Office 365, AS Revizor, COMODO, badoo.com, booking.com, facebook.com, mail.ru, nic.ru, ntv.ru, pikabu.ru, reg.ru, nag.ru, sipnet.ru, skbkontur.ru, vasexperts.ru[16], des serveurs racine DNS et d'autres sites.

Le RKN et le Ministère de la Communication ont alors réagi en urgence, en imposant aux opérateurs d'arrêter de bloquer quoi que ce soit, et en introduisant des "listes blanches" de ressources à ne jamais bloquer. À la veille de l'émission « Ligne Directe avec Vladimir Poutine » (un événement médiatique majeur de « rencontre en direct » entre le président et le peuple russes, qui s'est tenu en mai 2017), les régulateurs ont craint que les adresses IP utilisées par les installations de la transmission de la ligne ne soient-bloquées de la même manière. Les auteurs de la « guérilla DNS » ont alors fui la Russie par précaution et se sont cachés pendant plusieurs semaines en Europe. Cette action a mené à un changement dans la régulation du RuNet, car elle a forcé RKN à changer les normes de fonctionnement de la liste noire et à prescrire des méthodes de blocage plus précises aux opérateurs.

La « performance hacktiviste » comme ruse : le code Morse de Leonid Evdokimov

Cependant, la faille a persisté. Et un an plus tard, le 6 mai 2018, Léonid Evdokimov – développeur, mathématicien et hacker – l'exploita de nouveau afin d'organiser ce qui fut par la suite qualifié de performance hacktiviste, et qui était également une ruse de contournement très efficace. Evdokimov racheta plusieurs noms de domaine orphelins qui figuraient toujours dans la liste noire, et écrivit un script en Python qui lui permit de modifier de façon automatique les adresses IP associées à ces noms de domaine. Il parvint ainsi à écrire en code Morse la phrase "Digital Resistance 5, 4, 3, 2, 1, 0" sur le graphique des IP bloquées maintenu par le site Usher.Club dédié au monitoring et à l'analyse de la liste noire (Figure 2).

[16] Il est intéressant de remarquer que Vasexpert est un des fabricants les plus connus des boîtiers DPI et des solutions pour le filtrage de trafic et censure. Le choix du site de ce fabricant placé dans la même liste avec les sites du gouvernement et des institutions financières témoigne de l'intention des organisateurs de la guérilla DNS de critiquer les acteurs de l'industrie de censure et surveillance.

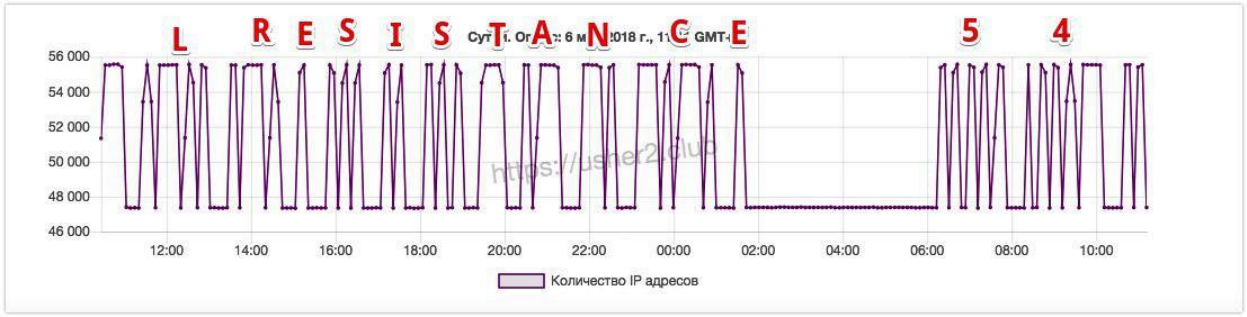


Figure 2. Une capture d'écran du Usher.Club. Action de Evdokimov "Digital Resistance", 6 mai 2018

Dans notre entretien, Evdokimov commente ainsi le sens de son action :

« C'était tout d'abord pour rigoler, de façon dadaïste. J'ai été un peu inspiré par les trucs que j'ai vus sur le site Beautiful Trouble, qui répertorie des actions un peu créatives, artistiques. Et puis surtout c'était pour attirer l'attention sur le problème potentiel de ce système des listes noires énormes. J'ai déjà évoqué ça pendant mon intervention à la Douma ».

En effet, les failles qui permettent de saturer la liste noire par des milliers d'adresses IP peuvent conduire à des incidents majeurs sur les réseaux, car les boîtiers de filtrage de trafic (même les installations coûteuses de DPI) ont des limites de traitement. Le 14 mars 2018 un inconnu exploita cette même faille en produisant une panne des réseaux de l'un des plus gros opérateurs de Russie, TTK (Figure 3).

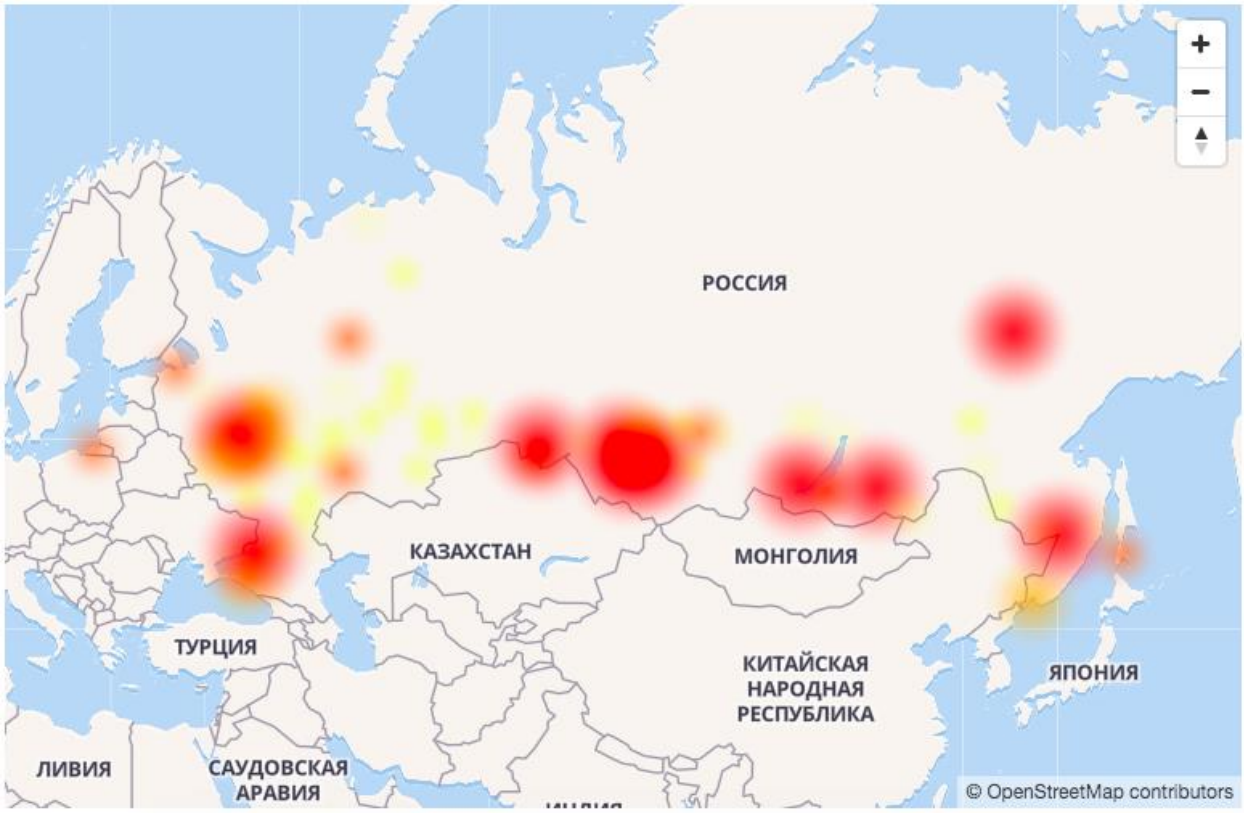


Figure 3. En rouge : pannes sur les réseaux TTK. Source : https://usher2.club/articles/ttk-strike/

Ce qui est particulièrement intéressant dans le cas de la « guérilla DNS », au-delà des façons créatives d'exploiter les failles dans les infrastructures de contrôle, c'est l'intention des acteurs, leur positionnement spécifique par rapport aux régulateurs. Il s'agit pour eux d'utiliser ces attaques non pas pour s'opposer au gouvernement, mais plutôt afin de provoquer des changements dans les façons de gouverner : attirer l'attention, *de facto*, sur la nécessité de revoir et affiner les lois et les mécanismes techniques en œuvre. Si le RuNet doit être gouverné, il doit être gouverné par des experts – et sans risque d'abîmer les réseaux : ainsi pourrait-on résumer la thèse que ces stratégies, mêlant à la fois prouesse technique et sens du spectacle, essaient de transmettre.

L'affaire Telegram et ses ruses

D'autres types de ruses techniques se sont développées en réponse à la décision de bloquer Telegram, la messagerie la plus populaire parmi les opposants, journalistes et ingénieurs russes. Lorsque, le 16 avril 2018, le RKN ordonne le blocage de cet outil, une course-poursuite commença entre le régulateur et les résistants : l'équipe technique qui développait l'outil, les FAI qui s'opposaient au blocage, les nombreux administrateurs des services Proxy et VPN et autres enthousiastes techniques, qui déployèrent alors de nombreux protocoles et applications permettant de contourner les blocages. Une campagne fut lancée par le créateur de Telegram Pavel Durov, soutenue dans tout le pays, sous le nom de « Digital Resistance ». Celle-ci comprenait une variété d'actions hors ligne, des *flashmobs* ironiques (jeter en même temps dans toutes les villes de la Russie un avion en papier par la fenêtre en signe de contestation) aux manifestations de rue (la plus grande comptant douze mille personnes à Moscou), et incluait également un large volet de ruses techniques.

Par exemple, l'équipe Telegram intègre des solutions de contournement dans son code, comme le *IP-hopping*[17], qui consiste à changer d'IP toutes les x minutes et à le communiquer par des notifications push aux clients mobiles. Une autre technique largement employée fut le *domain fronting*, un mécanisme de contournement de la censure qui dissimule la véritable destination d'une connexion ; le mécanisme permet à un utilisateur de se connecter par HTTPS à un site interdit tout en paraissant communiquer avec un site différent, par exemple les serveurs cloud de google.com, software-download.microsoft.com, amazon.com et autres. Enfin, les mobilisations utilisaient des protocoles comme Obfuscated2[18] qui permettent de camoufler le protocole MTProto utilisé par Telegram.

L'usage des services intermédiaires, comme les plateformes des géants du Net – Google, Amazon, Microsoft – par Telegram eut un effet collatéral sur le fonctionnement du RuNet, connu maintenant sous le nom des « blocage en tapis de bombes » (*kovrovaya bombardirovka*). Ainsi, en une semaine seulement, 18 millions d'adresses IP furent bloquées ; parmi elles, des centaines de milliers d'adresses associées à des services tels que Google, AWS, Microsoft, Digital Ocean, et même le serveur NTP (Network Time

17 http://telegra.ph/telegram-blocks-wtf-05-26

18 https://blog.susanka.eu/how-telegram-obfuscates-its-mtproto-traffic

Protocol). Cela a impliqué des dysfonctionnements chez de nombreux utilisateurs des services en ligne hébergés sur les mêmes IP.

Les « blocages en tapis de bombes » pendant l'affaire Telegram ont eu des effets, probablement inattendus, sur la société civile, dans la mesure où ils ont aidé à faire apparaître le problème de censure Internet en tant que problème public, qui touche non seulement les experts, ingénieurs, ou FAI, mais également des acteurs qui ne se sentaient pas concernés auparavant. Les blocages collatéraux ont produit des « nouveaux résistants », notamment parmi les petits entrepreneurs dont les entreprises en ligne étaient hébergées sur des serveurs cloud touchés accidentellement par les blocages Telegram. Thème auparavant réservé aux tchats des experts, les activités des régulateurs du RuNet sont devenues alors un sujet médiatique à destination de la société civile engagée. En ce sens, l'étude des effets de la régulation du RuNet sur la société civile russe permet de comprendre comment « certaines situations, qui ne sont pas d'emblée perçues comme 'politiques', sont susceptibles d'être recadrées dans ce sens » (Berger et al., 2011) grâce à un ensemble de stratégies guidées par l' « intelligence rusée » : des stratagèmes qui puisent dans la longue expérience d'un environnement à haute technicité, guidés par la curiosité et la volonté de subvertir par la technique propres du hacking, afin de maintenir ou reprendre la maîtrise sur un système auquel on tient et qu'on perçoit comme menacé.

Conclusion

Ainsi que le démontre Ermoshina (2019) dans le cas des « civic hackers » qui ont développé des plateformes pour signaler les défaillances voire la corruption des autorités locales (travaux de voirie), le mouvement d'hacking russe n'est pas homogène, et ne s'identifie pas seulement avec ses aspects plus « révolutionnaires » qui consistent à coder des systèmes complexes, à inventer de nouveaux langages de programmation ou à commettre des cyber-crimes. Alors que la figure de l'hacker russe est bien connue à l'international en lien avec des cyber-attaques, infiltrations et manipulations, d'autres formes d'hacking ont fait l'objet de cette enquête. Nos interlocuteurs se démarquent par ailleurs de la réputation des « Russian hackers » et, par ailleurs, de leurs collègues-ingénieurs qui travaillent pour le gouvernement.

Les pratiques d'hacking présentées dans cet article sont synonyme d'expérimentation, dans un sens proche de celui du mot français « bricolage » ; le terme russe *smekalka* le saisit également. Dérivé d'un ancien verbe, *smekat'* (« comprendre » ou, familièrement, « y arriver »), le *smekalka* est une qualité que les Russes revendiquent pour eux-mêmes, déjà présent dans les contes de fées comme pouvoir surnaturel pour trouver une solution rapidement, dans des endroits très contraints, lorsqu'on n'a pas d'outils ou de moyens adéquats et qu'on ne peut utiliser que ce qui est disponible. Les hackers sont ceux qui ont les compétences et l'inventivité – l'« intelligence rusée » – de rapidement concevoir un nouveau moyen intelligent et peu coûteux pour mettre en lumière et contourner des formes de contrôle au moyen des technologies informatiques.

Les stratégies, ruses, *smekalka* qu'on a vues se déployer au cours de cet article s'inscrivent dans cette acception de « hacking » et de « hacktivisme », deux mots aux significations variées, comme le montrent

bien les coordinateurs de ce numéro dans leur introduction. En réponse à une gouvernance du RuNet qui comporte de nombreuses zones grises mais qui est en même temps de plus en plus centralisée, les FAIs russes réagissent en développant des techniques de résistance. Cette étude s'est donnée pour objectif d'analyser ce répertoire de ruses, en se focalisant sur la dimension des bricolages techniques. En proposant une description analytique de ces nombreuses pratiques de contournement, nous avons cherché à comprendre comment les ingénieurs et les informaticiens russes deviennent acteurs, parfois malgré eux, de la gouvernance et d'une « contre-gouvernance » du RuNet. Suite à cette enquête, il est possible d'identifier un certain nombre d'éléments qui contribuent à tracer le portrait des acteurs techniques de l'Internet russe face aux évolutions de sa gouvernance.

En premier lieu, une grande majorité des FAI, notamment ceux qui sont actifs dans des associations et à l'occasion des débats en ligne, ne croient pas que la finalité politique est prédominante dans les lois les plus récentes qui visent à « brider » le RuNet. Pour ces FAI, c'est la finalité économique qui prime : il s'agit de reconfigurer les équilibres de marché du RuNet et avec eux, les équilibres de pouvoir (voir Ermoshina, Loveluck et Musiani, 2021). Par leurs stratégies de résistance et de ruse, les FAI se battent pour leur survie en tant qu'acteurs dans ce marché ; hormis les intérêts économiques, certains visent également à défendre une certaine vision nostalgique de l'âge d'or d'un RuNet libre et décentralisé.

Deuxièmement, on peut reconnaître une certaine logique du « *care* » (qu'on retrouve notamment dans les travaux STS concernant d'autres types d'infrastructures ; voir par exemple Denis et Pontille, 2015) : par leurs ruses, les acteurs techniques du RuNet souhaitent défendre la qualité de la connectivité, et l'état des réseaux en général. Les régulateurs sont souvent appréhendés comme des entités qui, par incompétence, « abîment » l'Internet que les ingénieurs doivent alors « protéger ». Comme le dit le directeur de la Société de Protection de l'Internet, « l'incompétence, la corruption et l'inefficacité des régulateurs protègent le RuNet de la dégradation » au sens où, malgré le discours fort de la « souverainisation » du RuNet, et une panoplie de lois visant à le réguler, très peu est mis en application.

Enfin, l'analyse de ces ruses numériques et du contexte dans lequel elles se déploient amène à y voir plus clair sur les formes de politisation particulière de ces « publics experts » que sont les ingénieurs et les acteurs techniques de l'internet russe. Celles-ci incluent l'évitement de ce qui est explicitement politique (Eliasoph, 2010), en faveur de la préoccupation et de l'investissement dans des cas concrets ; une opposition du politique « traditionnel » et du technologique, par des visions du type « on était bien avant que l'Etat n'intervienne… » ; et enfin, une vision du marché comme protecteur naturel de l'internet, estimant que les intérêts économiques des acteurs, y compris ceux des acteurs internationaux, peuvent défendre le RuNet mieux qu'une mobilisation de masse.

Les ruses quotidiennes sur l'internet russe – mises en œuvre par des techniciens face à une gouvernance d'internet qui ressemble de plus en plus à du gouvernement – ont leur fondement dans tous ces éléments. Les intermédiaires techniques du RuNet préfèrent mettre en œuvre leurs luttes pour les libertés en ligne via des pratiques de résistance invisible (De Certeau, 1990), plutôt que par le biais d'une confrontation ouverte. La clé pour une « guerre de la gouvernance d'Internet » (DeNardis, 2014) efficace réside, pour ces acteurs, dans des pratiques cachées, partagées, distribuées – dans le *tacit knowledge* que permet la ruse et le contournement. Notre terrain révèle ainsi peut-être une nouvelle facette de l'hacking comme ruse. Si d'un côté il aide les acteurs techniques à continuer à exister sur le plan économique – en se

cachant, en épargnant de l'argent, en fabriquant des réseaux parallèles… – d'un autre côté il est aussi, plus largement, une métaphore de l'état actuel du RuNet : un « bac à sable » de la gouvernance où les apparences sont celles d'une domination par une grande machine autoritaire, centralisée et efficace, mais où, dans la pratique, des alternatives sont possibles.

Références

Akrich, M. (1998). Les utilisateurs, acteurs de l'innovation, *Education permanente*, 134 : 78-89.

Asmolov, G., Kolozaridi, P. (2017). "The imaginaries of RuNet: the change of the elites and the construction of online space", *Russian Politics*, 2(1): 54-79.

De Certeau, M. (1990). *L'Invention du quotidien, 1. : Arts de faire*. Paris, Gallimard

DeNardis, L. (2014). *The global war for internet governance*. New Haven, CT: Yale University Press.

Denis, J., & Pontille, D. (2015). "Material ordering and the care of things". *Science, Technology, & Human Values*, 40(3), 338-367.

Détienne, M. & Vernant, J.-P. (1974). *Les Ruses de l'intelligence. La mètis des Grecs*, Paris, Flammarion.

Eliasoph, N. (2010). *L'évitement du politique. Comment les Américains produisent l'apathie dans la vie quotidienne*. Lectures. Économica, coll. « Etudes Sociologiques »

Ermoshina, K. (2016). *Au code, citoyens : la mise en technologies des problèmes publics*, thèse de doctorat sous la direction de Cécile Méadel. Paris Sciences et Lettres. https://pastel.archives-ouvertes.fr/tel-01712465/document

Ermoshina, K. (2019). For Code and Country: Civic Hackers in Contemporary Russia. In M. Biagioli & V.-A. Lépinay (eds.), *From Russia With Code: Programming Migrations in Post-Soviet Times*, Duke University Press, pp. 87-109.

Ermoshina, K., Loveluck, B. et Musiani, F. (2021). "A Market of Black Boxes: The Political Economy of Internet Surveillance and Censorship in Russia", *Journal of Information Technology & Politics*, DOI: 10.1080/19331681.2021.1905972.

Ermoshina, K. et 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.

Freiberg, P. (2014). "Putin's Russia - on a path to cyber sovereignty?" *Capstone project for the Master of Arts in Media Communications Program for Webster University*, http://www.academia.edu/10762446/Future_of_Internet_Freedom_in_Russia

Klyueva, A. (2016). “Taming Online Political Engagement in Russia: Disempowered Publics, Empowered State and Challenges of the Fully Functioning Society”, *International Journal of Communication*, 10: 4661-4680.

Kuznetsov, S. (2004). *Oshchupyvaia slona. Zametki po istorii russkogo internet*. Moscou: Novoe literaturnoe obozrenie.

Lévi-Strauss, C. (1962). *La Pensée sauvage*. Paris : Presses Pocket.

Lessig, L. (1999). *Code: And Other Laws of Cyberspace*. New York: Basic Books.

Milan, S. (2013). *Social movements and their technologies: Wiring social change*. Springer.

Nocetti, J. (2015). “Russia’s ‘dictatorship-of-the-law’ approach to internet policy”, *Internet Policy Review*, 4 (4), DOI: 10.14763/2015.4.380

Peters, B. (2016). *How Not to Network a Nation: The Uneasy History of the Soviet Internet*. Cambridge, MA: The MIT Press.

Tilly, C. (2002). *Stories, Identities, and Political Change*. New York: Rowman & Littlefield.