The Telegram ban: How censorship “made in Russia” faces a global Internet

Ksenia Ermoshina and Francesca Musiani

Paper presented at the 2021 Annual Symposium of the Global Internet Governance Academic Network (GigaNet), virtual conference, December 6, 2021

Published after peer review in *First Monday*, Volume 26, Number 5, 3 May 2021, https://firstmonday.org/ojs/index.php/fm/article/download/11704/10130,
doi: https://dx.doi.org/10.5210/fm.v26i5.11704

Abstract

When, in April 2018, the Russian Internet watchdog Roskomnadzor orders to block Telegram — the country’s most popular messenger — Internet users in the country respond with a diverse set of digital resistance tactics, including obfuscation and circumvention protocols, proxies, virtual private networks, and full-fledged hacks. This article analyzes the “Telegram ban” and its ramifications, understanding it as a socio-technical controversy that unveils the tensions between the governmental narrative of a “sovereign Internet” and multiple infrastructure-based battles of resistance, critique and circumvention. We show how, in the context of a Russian Internet which is heavily entwined with and dependent from foreign and global infrastructures, a number of bottom-up, infrastructure-based digital resistances are able to emerge and thrive despite the strategy of effective centralised management that the Russian government seeks to present to the world as its own.

Introduction

April 2018: the Russian Internet (RuNet) watchdog Roskomnadzor (RKN) orders to block Telegram, the country's most popular messaging tool. RuNet users respond with a diverse and lively wave of actions, ranging from satirical memes to flashmobs and rallies (Asmolov and Kolozaridi, 2017). The movement for the defense of Telegram, quickly baptized "digital resistance", soon starts displaying, alongside more "classical" repertoires of street manifestations, a rich "e-repertoire of contention" (Costanza-Chock, 2003; Rolfe, 2005). This burst of technical creativity would go on to include dozens of new obfuscation and circumvention protocols, proxies and VPNs designed by tech-savvy users — and by the Telegram team itself — in order to help bypass governmental censorship.

This article analyzes the case of the "Telegram ban" in Russia, understanding it as a socio-technical controversy that unveils the tensions between the governmental narrative of a "sovereign Internet" (Nocetti, 2015; Freiberg, 2014), based on Russian-made censorship and filtering technologies, and the transnational character of global Internet infrastructures. Our analysis pays particular attention to the infrastructure-based "war for Internet governance" (DeNardis, 2014) between Telegram and RKN, and tracks the "cat-and-mouse" dynamics between protocols aimed at filtering and circumvention. It shows how the main Telegram circumvention technique, also known as IP-hopping [1], depends on the willingness of Internet giants such as Google and Amazon to keep on allowing Telegram to access their platforms and allowing them to change IP addresses without limits, and makes the targeted blocking of Telegram very complex without also provoking collateral damage. The article shows how this overblocking results in the creation of new "concerned publics" (Geiger, *et al.*, 2014) including entrepreneurs, tech experts, previously depoliticized users. Finally, the official decision to "unblock" Telegram in June 2020 raises doubts *vis-à-vis* the technical and infrastructural capacity of regulators to effectively control the Russian Internet, and partly confirms the hypothesis of the Russian style of Internet governance being first and foremost a "theater of security" (see Schneier, 2003) rather than an effective centralised management.

Ultimately, our article shows, the Telegram case is yet another arena where the "turn to infrastructure" (Musiani, *et al.*, 2016) in Internet governance can be observed, fostering a number of bottom-up, infrastructure-based digital resistances challenging the approach to Internet governance currently adopted by RKN. However, the paper also questions the role of Telegram as a "training ground" for RKN, towards a more efficient global control over the Russian Internet. Indeed, the most recent developments of the "Battle for Telegram" show that new technical and legal tools deployed by the regulator can be further applied to other online services — while simultaneously demonstrating the shortcomings of the centralized, top-down strategy applied to the Russian Internet by its current authorities.

The "Telegram ban"?

The encrypted messenger Telegram was founded by the Russian entrepreneurs, brothers Pavel and Nikolai Durov, in 2013. According to popular belief, Telegram was created as a tool to protect their communication in the context of political persecutions Pavel Durov was subject to after he had refused to collaborate with the Russian government and had to cede his first famous project, the social network VKontakte. Telegram is, in 2020, the third most popular messenger in Russia with its 30 million users [2]. Beyond its initial status of "messenger" application,

Telegram has become the pre-eminent circumvention tool for hundreds of censored media resources and political activists whose Web sites were blocked by RKN. Popular liberal media such as Grani or Meduza, or opposition politicians Alexey Navalny, Leonid Volkov and many more, have been actively using Telegram's broadcasting function to continue delivering news content to their audiences regardless of the blocking of their main Web sites and blogs.

Telegram fell under scrutiny of the Russian political police in the space of a few years: on 14 July 2017, the Russian Federal Security Service (FSB) requested decryption keys for all messages sent and received via Telegram, in accordance with the 2016-approved Yarovaya Law [3]. This request concurred with another important event: a criminal case initiated against Durov in Iran, where Telegram had allegedly been used by terrorists. Telegram did not satisfy the FSB's request, and after a second request to provide the keys in March 2018, Telegram's lawyers explained that it was cryptographically impossible because of the way in which encryption works in Telegram: "Taking into account the architecture of this messenger, the administrator has absolutely no possibility to access information necessary to decrypt messages that are sent, transmitted or received using Telegram" [4]. To illustrate the technical absurdity of the FSB's demand to hand out "decryption keys from Telegram", a photo was published on the channel of Telegram's lawyer Pavel hikov featuring a letter from Durov to the FSB Director Bortnikov and two metal keys (Figure 1).

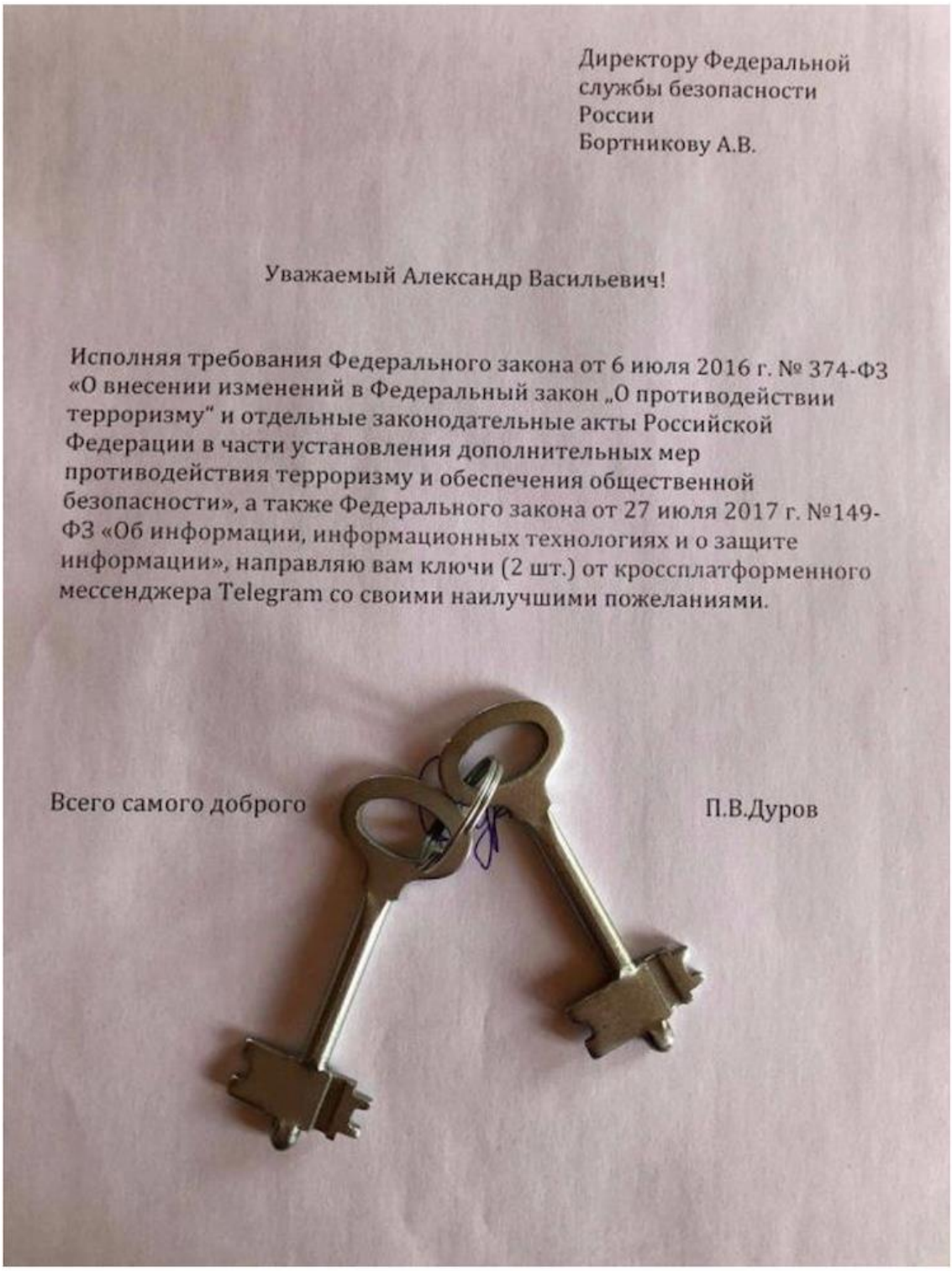

Figure 1: A satirical letter from Pavel Durov to the FSB Director Alexander Bortnikov, and two accompanying metal keys. Published by the director of Agora, Pavel Chikov, on his personal Telegram channel on 10 April 2018, at https://t.me/pchikov/929.

Six days after publishing this satirical response, on 16 April 2018, Telegram was officially blocked by RKN, within the context of Vladimir Putin's re-election as President of Russia in March. The Runet users responded to the blocking with a variety of actions — from satirical memes to flashmobs and "in-the-flesh" rallies — that rapidly became known as the "battle for Telegram" [5].

Besides collective action, the Telegram ban led to a burst of technical creativity, with dozens of new obfuscation and circumvention protocols, proxies and virtual private networks (VPNs) [6] designed by tech-savvy users — and by the Telegram team itself — in order to help bypassing governmental censorship. Indeed, Telegram was never completely blocked on the territory of the Russian Federation, and users could access all of its services rather easily, sometimes even without any circumvention tools, as small and medium ISPs did not always comply with RKN's requirements. This inability of governmental agencies to successfully block Telegram raised concerns as for the efficiency of RKN and its technical expertise.

In June 2020, the government issued the official decision to unban Telegram, and on 12 July, Telegram's Vice-President gave a talk at a meeting of IT industry representatives with the Russian Prime Minister Mikhail Mishustin. These events have affected Telegram's reputation among activists who have started to harbor doubts about Durov and his team's loyalty to the opposition. However, while this article will later briefly discuss the reasons for the Telegram unban, as both a conclusion and overture towards future research, the scope of its interest concerns the period of blocking of Telegram, as it presents a challenging use-case for science and technology studies (STS), in particular infrastructure studies, as well as for the studies of new forms of social mobilization and for surveillance studies.

Methodology and theoretical framing

Our research draws from perspectives in STS, and in particular on infrastructure studies (Bowker and Star, 1999; DeNardis, 2012; Musiani, 2013). Through an STS-inspired "thick description" (Ponterotto, 2006) of the Telegram case, this paper aims to deconstruct the representation — ever-present in governmental discourses — of RuNet governance as a set of highly centralized, efficient and automated processes. Instead, we try to articulate our actors' definition [7] of Russia's Internet regulation style as a "theater of security" — an expression introduced in the scholarly literature by Schneier (2003) but to be found "on the field" as well, meaning, for the actors uttering it, that the political discourse on Internet sovereignty is largely in excess of the actual technical capacities and expertise necessary to execute these ambitions. Not only did the unsuccessful attempts to block Telegram make visible the lack of technical expertise of the authorities; interestingly enough, Telegram has been continuously used by the authorities themselves even during the official ban. This controversial relationship of the authorities with the messenger helps to understand how the Telegram ban has been mobilized as an argument and an instrument in the context of the official discourse on Internet sovereignty.

Beyond STS, this paper borrows from pragmatist sociology and from the sociology of social movements, as it aims to foster understanding of new forms of politicization and resistance practices in contemporary Russia. The Battle for Telegram brings to the spotlight profiles such as "engaged" engineers and technologists and "civic hackers" (Ermoshina, 2019) and crystallizes formations of new "concerned publics" (Geiger, *et al.*, 2014), such as Internet service providers, small IT entrepreneurs and communities of developers directly or indirectly

affected by the blocking of Telegram. The ban has led to new forms of expert mobilization around a number of initiatives created to "measure" RuNet's freedoms and monitor the "health" of the RuNet. Through these projects — aimed at producing collective expertise and independent network measurements and monitoring, relationships of engineers with code — networks and infrastructures are redefined. From "avoiding politics" (Eliasoph, 1998) to "caring about plumbing" (Musiani, 2012), the Telegram ban has initiated an important shift in Russian technologists' attitude towards RuNet infrastructures and services, as something that needs "care" and "protection" from state actors.

From a methodological standpoint, we rely on a qualitative, mixed-methods approach. The core of our work has been a series of 23 in-depth interviews with Russian technical experts, ISPs, journalists and Internet freedom activists. These respondents started to be recruited during our previous research on Russian "Internet freedom" activists (see Ermoshina and Musiani, 2017) and following multi-year participant observations at professional conferences of Russian telecommunication and IT industry experts, and international Internet Freedom gatherings such as RightsCon or Internet Freedom Festival. Furthermore, we were able to interview middle and small-size ISPs (between 5,000 and 500,000 clients), mostly critical towards RKN and state-centered Internet governance. We were unable to interview representatives of large telecommunication companies such as Rostelecom or Dom.Ru.

Our methods also include qualitative controversy mapping, *i.e.*, analyzing reports, documents and research produced by actors, such as engineers, governmental agencies, media, and establishing a cartography of alliances, conflicts and their shifts over time (see Venturini and Munk, forthcoming). We also conducted an analysis of a number of Telegram chats and channels (see Appendix), which allowed us to unveil the technical tools of 'information control' deployed in the Telegram case. Our fieldwork started in early 2018 and continues to this day, to keep abreast of the most recent developments in Telegram's relationship with the authorities.

The Telegram ban as a use-case

Within the vibrant field of end-to-end encrypted messengers (Ermoshina, *et al.*, 2016), Telegram stands out as the epitome of several important socio-technical controversies, notably those that oppose two visions of encryption, as a protecting mechanism for Internet rights and a facilitator of terrorist or extremist activities. This debate has been accompanying the messenger throughout its short history, from accusations by several governments of "favoring" subversion and crime (for the Iranian case, see Newman, 2018) to the very recent statement by Durov himself suggesting that the "struggle against terrorism and right to privacy are not excluding each other" [8].

Due to its status of emblematic case that "presents the ongoing clashes between non-democratic states and users who struggle to access free flows of information but also highlights important issues about platform independence, alternative commercial models of platform development, and the future of platform surveillance across various political contexts" (Akbari and Gabdulhakov, 2019), Telegram has enjoyed substantial attention from researchers in recent years. Computer scientists have engaged in analyses of its security and information spreading mechanisms, pointing out its potential flaws (see Saribekyan and Margvelashvili, 2017, and Nobari, *et al.*, 2021, respectively), and scholars from various disciplines have examined different uses of the Telegram messenger, including as a social networking service for libraries

(Asnafi, *et al.*, 2017, in Iran; Manna and Ghosh, 2018, in India) and even as a supporting system for tele-dentistry (Chaple-Gil and Afrashtefar, 2020). Other contributions examine how Telegram's affordances of anonymity and group formation are being leveraged by particular groups to conduct activities strongly connotated as socially and politically undesirable (see Semenzin and Bainotti, 2020, on the use of Telegram as an arena for non-consensual dissemination of intimate images, or Urman and Katz, 2020, on radicalized far-right groups), and even by terrorist networks such as ISIS (Yayla and Speckhard, 2017).

Of particular interest in setting the stage for this article is how literature has addressed the role of Telegram (and of its ban in different countries) in co-shaping Internet censorship and resistances. Nathalie Maréchal provides a substantial political history of Telegram that examines how the messenger has emerged in the context of Russia's progressively stronger digital authoritarianism, and concludes that "(r)ather than earning user trust through transparency and accountability, Telegram's value proposition hinges on blind trust on Pavel Durov's good intentions and his team's stated credentials" (Maréchal, 2018). Azadeh Akbari and Rashid Gabdulhakov focus on the "platform surveillance" aspects of Telegram adoption and subsequent bans in Iran and Russia, and propose a comparative analysis of the role they play in "totalitarian" and "strategic" surveillance respectively in the two countries (Akbari and Gabdulhakov, 2019). Telegram bans in Russia and in Iran are the subject of more detailed case studies by Glukhova (2018), focusing on the blend of "modern authoritarianism and authoritarian informationalism" that the Telegram case unveils in the Russian digital strategies, and Kargar and McManamen (2018), addressing the strategy of the Iranian government in facilitating migration to state-sanctioned "alternative" applications as well as circumvention strategies by Iranians and their migration to independent alternatives of their own choice, such as Psiphon.

The success of Telegram in Russia helps understand the variety of motivations beyond Internet users' choice of a particular encrypted messenger. Beyond technical features and design choices, extra-cryptographic and extra-security features may become arguments for the adoption of a specific tool. In the case of Telegram, it is interesting to observe how the actual cryptographic protocol and security and privacy properties diminish in importance for users, compared to other aspects, such as the reputation of the app's creator. The trust in Telegram, according to our interviews (see also Maréchal, 2018), lies not with the technology, but with the main developer and his political position. Here is an excerpt from an online discussion in a group chat called *Soprotivlenie* [сопротивление, *Resistance*], posted on 11 June 2017:

> User 1: Maybe you shouldn't discuss that over Telegram?
> User 2: Why not? Pashka Durov will never give away any of our data, he doesn't care about the Russian police.

Ironically enough, it is the ban of Telegram in Russia that has helped bolster its reputation as a "trusted" messenger for the opposition activists. As we will see again at the conclusion of this article, the unban, on the contrary, raised a wave of suspicion among the most active audiences, and launched a process of migration to decentralized alternatives, such as Riot (now Element) [9] or Delta.Chat [10]. Indeed, even during the ban years, Telegram became so influential in Russia that governmental institutions kept maintaining their own official Telegram channels, probably so as to maintain some kind of influence within this platform. As the official Telegram statistics show, Telegram's Russian audience has doubled since 2018 and the ban did not impact this growth [11].

The blocking of Telegram has unveiled the close dependencies and interconnections of RuNet *vis-à-vis* global Internet infrastructures, such as Amazon and Google Web servers, used to evade censorship. The "battle for Telegram" therefore questions both technical and geopolitical boundaries as it opposes the strong government-originated discourse on the Russian "Sovereign Internet" (Nocetti, 2015; Freiberg, 2014) and the transnational character of material Internet infrastructures. This use-case favors a better understanding of both the threat of balkanisation of the Internet and the "turn to infrastructure" (Musiani, *et al.*, 2016) in Russian Internet governance, as it unveils and makes visible the ensemble of socio-technical and legal mechanisms used to exercise control over RuNet.

The rise of Telegram in Russia also helps to shed light on processes of "digital migration", as we call the dynamics of users moving from one platform to another, usually following a critical event. This migration may be caused by a discovery of a security vulnerability, a public scandal involving platform developers, a politically-marked decision made by the technical team or the acquisition of the platform by another corporation, sometimes linked to the government.

Histories and framings of the Telegram ban

The success of Telegram within the Russian context needs to be understood in relation to Vkontakte, or Vk.com, Pavel Durov's first project. Following its acquisition by the Mail.Ru Group — a corporation heavily criticized by tech experts and activists for its poor data protection policies and direct collaboration with authorities — Vk.com was essentially deserted by these audiences. Our fieldwork shows a deep change of attitude towards Vk.com, a decline of trust and a shift in the ways it is used: users still use it primarily for the multimedia content (Vk.com is internationally known for its pirated content) and to keep in touch with individuals in other users' social graphs who are connected to some of their own, usually with less technical expertise (*e.g.*, relatives or school friends; see however Perrine Poupin's article in this issue on Vk's increased usage in local mobilizations). Telegram, however, has always been somewhat connected to Vk, via Durov's presence and influence, but also due to its Application Programming Interface (API), which makes it easy for developers to build bridges between the two tools, by creating bots to download multimedia from Vk to Telegram.

Precisely because of its modularity and the opportunities offered by its API, Telegram has attracted tech user communities that have chosen it as their primary messenger, not only for daily one-to-one communication but also for professional chats. Some of our respondents compared Telegram to the pioneer Internet Relay Chat (IRC; see Latzko-Toth, 2008). Telegram's API has engendered a dynamic development of the bot ecosystem which made Telegram something "bigger than just a messenger, a new kind of social network" — as one of our respondents puts it [12]. The tech chats that we have observed were very creative in their use of various bots and bridges that connect Telegram to other platforms — from Matrix.org to Delta.Chat. Thus, Telegram has evolved into a hybrid network with multiple functions and purposes, offering shelter to censored media (such as Grani or Krym.Realii, and many others that use Telegram as a circumvention tool to deliver content to their audiences), allowing public group chats or "rooms", and proposing tools to promote cultural and political events and gatherings, organize surveys, create and distribute cultural and artistic content, generate stickers.

Partly because of its success in Russia, there is no single history of the Telegram ban, but several ways to tell this story, competing chronologies and narratives that trace it back to different moments in the history of the RuNet — itself a rather controversial one.

The story of the Telegram ban was recollected many times in recent years during tech conferences and gatherings of the "Internet Freedom" community, such as local events held by the Society for Protection of the Internet, or by Roskomsvoboda, but also during larger international hacker gatherings, such as the Chaos Communication Congress (CCC). The talk given by Russian engineer and hacker Leonid Evdokimov at the 35th CCC in 2018 attracted a lot of attention from the hacker community, as it framed the Telegram ban as a use-case to effectively unbox and explain the ways in which Internet censorship is applied in Russia. Evdokimov's speech included several revelations addressing the complex network of surveillance and filtering equipment used to enforce the ban. The talk unveiled many side controversies, including incorrect configurations of SORM boxes, and the inequalities between larger and smaller ISPs, the latter being much more vulnerable to state regulation and sanctions). Furthermore, the Telegram ban was frequently cited at international gatherings such as RightsCon or Internet Freedom Festival, as a "proof" of the tightening control over the RuNet. Indeed, the Telegram ban became the ground for comparison between Russia and other more repressive countries, such as Iran, where Telegram was also partly banned.

On the other hand, Russian regulatory actors and government officials elaborated their own ways of telling the history of Telegram ban at the meetings with representatives of the IT sector, through their official media channels and through government-loyal press. The difference in framing strategies unveils how an instant messenger becomes in itself an instrument used to build and distribute concurrent political narratives about what RuNet has been and how it should function in the future. We understand the Telegram ban as a powerful moment that crystallizes two competing paradigms: the one mourning RuNet's "Golden Age", based on free competition and cooperation between tech professionals, absence of censorship and centralized regulation, transnational circulation of tools, services and people; and the other which affirms the necessity of stronger, infrastructure-driven control of RuNet's "borders" and content production and circulation. Both paradigms include a third party: the complex network of foreign, mostly U.S.-made, services such as Google or Amazon Web Servers, that actually become crucial for the functioning and well-being of RuNet. While the Telegram ban unveils these fundamental dependencies on foreign infrastructures, it paradoxically becomes the trigger for faster "sovereignisation" — the relocalisation of servers and services — of the Russian segment of the global network.

Our interviews with tech experts show that some ISPs trace the history of Telegram ban back to 2007, when the first Web sites were blocked [13]. The ban was, for them, the culmination of a longer attack on the Internet:

> "Telegram is just the mushroom cap, it is what everyone sees and talks about. But I would say, the background process was unfolding for many years and it has gradually led us to the point where we are now. We (the ISPs) were ignoring it for many years (...) we did not take it seriously enough, there was almost no overt resistance to it. And when Telegram was banned I understood it was too late to react." (ISP from Saint-

Petersburg, member of the Thursday Beering gathering, interview)

This comparison with mushrooms helps us to understand Russian technologists' vision of how governance and resistance "by infrastructure" unfold in today's RuNet. Other respondents use militarized vocabulary, describing the Telegram ban as a "civil cyberwar", which had an "open phase" (with street protests, legal campaigns) and a "cold phase" after the beginning of blocking, when technical resistance went "underground" and the cat and mouse game started between circumvention protocols and blocking techniques. This "militarized" vocabulary was abundantly used by the defenders of Telegram to describe the actions of RKN. A patriotic framing of the "battle for Telegram" used by Durov is particularly curious: one day before the Russian "Victory Day" (9 May, the most important patriotic holiday of the year, celebrating the surrender of Germany in 1945) Durov claimed on his page on Vk.com that the Telegram team "will continue the battle for Telegram, because our ancestors have taught us to fight until the end" [14].

A recurring expression was "carpet blocking", in reference to carpet bombing, a large-area bombardment conducted in gradually so as to inflict damage to every part of a selected area of land. The phrase evokes the image of explosions completely covering an area, in the same way that a *carpet* covers a floor. Thus, "carpet blocking" consisted of a technique for blocking wide ranges of unrelated IP addresses, instead of successfully targeting the servers where Telegram was located. The militarized metaphors were dominating the imagery related to the controversy as well; the following are examples of illustrations used by Telegram defenders in their campaigns, representing the RuNet watchdog as the heavily armed enemy, equipped with powerful tools such as tanks or airplanes (Figures 2 and 3), whereas the protesters were represented with the "peaceful" and "innocent" paper planes.

Figure 2: A tank with logos of RKN. Published on 6 April 2018, at https://roskomsvoboda.org/37807/.

Figure 3: The "carpet blocking" operation — Nazi Germany planes with the logo of RKN. Source: https://roskomsvoboda.org/38315/, published 24 April 2020.

In general, the defenders of Telegram do not interpret the ban as an isolated case but analyze it in a broader context of Internet censorship comparing it to other apps, such as Zello, a peer-to-peer walkie-talkie app banned in Russia, together with 15 million IPs of subnets [15] of Amazon and other international Web services. The Telegram case is also framed within a larger discussion about the force of the law, the relative importance of different legal documents, and of their interpretations: for instance, by comparing the anti-terrorist legislation and the right to privacy guaranteed by Article 23 of the Constitution of Russian Federation [16].

Pro-governmental media, on their end, frame the Telegram ban as "the war on terrorism". The campaign against Telegram started in Spring 2017, one year before its official ban, and federal TV channels have been actively communicating about the controversial messenger since then. For instance, the most influential pro-governmental journalist, Dmitry Kiselev, first criticized Telegram in his evening program [17] "Vesti Nedeli" (Weekly News) on "Rossia 24" channel (25 June 2017). In that instance, Telegram was alleged to be the tool used to prepare the infamous terrorist attack in the subway of Saint-Petersburg on 3 April 2017, and it was stated

that “Telegram has become the main tool of communication and enrollment for terrorists”. On the same day, Anton Vernitskiy of First Channel described Telegram as “the tool for creating dormant terrorist cells” [18], and Irina Zeynalova of NTV said that “Pavel Durov tolerates terrorists in his messenger” [19]. Usage of Telegram was also directly linked to the Paris attacks of 2015, and other cases involving acts of terrorism. Another official, though less popular, narrative justified Telegram blocking in the context of the “war on drugs”, as Telegram was said to host channels promoting drug culture or bots used to buy drugs.

Telegram agreed to delete group chats and channels allegedly run by terrorist groups (almost 5,000 chats and channels deleted by June 2017), while the FSB demanded access to the content of secret chats and account information of the six suspected organizers of the Saint-Petersburg terrorist attack. Durov explained that it was “technically impossible” because of the “Perfect Forward Secrecy”, a property of the MTProto cryptographic protocol used in Telegram for key exchange [20]; furthermore, it could “violate the right to privacy” [21]. A public dispute ensued between Durov (supported by RuNet freedom NGOs and tech experts), FSB and Roskomnadzor [22], which could be briefly summarized, quoting one of our respondents, as the “fight between mathematics and bureaucracy”. Because Telegram uses end-to-end encryption for secret chats, unique keys are generated on the users’ device. FSB, on the contrary, requested “universal decryption keys”, implying that either Telegram had to redesign all of its encryption, or send secret chat keys on a server which, according to Durov’s estimations, would require extra four petabytes of storage every month on every Telegram channel.

After receiving a fine of 800,000 rubles, Telegram partnered with the Inter-regional Association of Human Rights Organization Agora to represent it in court battles. The choice of this organization was commented upon in specialized Telegram chats that we were observing; for many users this choice has been a proof that Telegram case was “getting really political”, while encryption was promoted as a technology that enables “human rights”, such as privacy. Telegram’s court suit against FSB was, however, rejected on 20 March 2018 and the messenger was given 15 days to provide requested information to security services. On 13 April 2018 the Moscow Tagansky District Court ruled, with immediate effect, on restricting access to Telegram in Russia.

Collateral damage or fight against IT giants?

Even before the official ban, Telegram started to prepare for blocking and launched its cat-and-mouse game with RKN. Durov promised to introduce circumvention mechanisms without additional efforts on users’ side, including IP hopping, domain fronting and embedded proxy servers [23]. MTProto Proxy, the official circumvention protocol, was in constant development and improvement throughout the whole ban. On the users’ side, the demand for VPNs, proxies and other circumvention tools grew exponentially. According to Combot analytics [24], Telegram Socks5 Bot (proxy) was downloaded 900,000 times in less than four days between 12 and 16 April 2018.

The very circumvention mechanisms used by Telegram (such as IP hopping) involved a third-party actor in this game: Amazon and Google Web servers were used to temporarily host the elusive messenger. The court decision, however, did not limit its reach to Russian ISPs; access restrictions to Telegram were extended to all third parties providing infrastructural support for

the infamous messenger. Therefore, between 16 April and 26 April 2018, when the first attempts to block Telegram were experienced by users, collateral damages turned out to be quite important.

Eighteen million IP addresses were blocked, including hundreds of IPs of Amazon, Google and other major Web services. Users had trouble accessing YouTube, Doubleclick, Google Translate, Google push notification and other major services [25]. Fifty-three subdomains of Google (from Google Play and Google Fonts to Google APIs) were blocked. Consequently, Russian Web services also suffered, including Yandex, Vk.com and MSK-IX, which were totally or partly blocked or down between 26 April and 27 April.

On 25 April 2018 the vice-head of RKN, V.A. Subbotin, explicitly stated that RKN was not (only) blocking Telegram but was meeting with "overt opposition" from the largest global IT giants, including Google, Amazon and Microsoft [26]. Subbotin stated that "Amazon and Google know exactly which IP range has been distributed to Telegram and which subnetworks they were using, and how they can technically isolate these IP-addresses to make it possible for Russian ISPs to block them". The foreign Internet giants were described as driven by "political, not economic interests". The fight against Telegram had become, at its core, a campaign for infrastructural sovereignty of RuNet.

As previously mentioned, this period was portrayed as "carpet blocking" by major RuNet Freedom activists and tech enthusiasts, unveiling the close dependency of crucial Russian Web services from foreign infrastructures. Independent tech experts started to actively monitor "the health of RuNet", introducing various instruments such as the "graph of blocked IPs" [27] (Figure 4) and a number of dedicated Telegram channels and bots to monitor blockings (such as https://t.me/rkn_block_check; https://t.me/rkn_blockflood, RKN Dump Check, and others).

Figure 4: Graph of blocked IP addresses as of 20 April 2018. Source: https://usher2.club.

The “carpet blocking” method turned out to be quite inefficient: according to Leonid Evdokimov’s analysis, only 18 IP addresses out of three million blocked Amazon addresses were actually used by Telegram. As he described it in the interview we conducted with him [28], “*RKN used terrorist methods while combating the so-called terrorist Telegram, by taking those networks as hostages*”. Telegram was still accessible, while many unrelated, though important, services were down. The reputation of Roskomnadzor suffered greatly, even within the government (as another respondent, engineer Phil Kulin [29], said,“*RKN does not really know what it is doing*”) and the agency became labeled as “Roskompozor”, that could be translated as Russian Communication Shame. Kulin conveyed the critical image of the watchdog using a quote [30] from Korney Chukovsky’s children’s poem “Confusion”: “for many hours did the crocodile try to cool down the fire on the sea, he used some pierogi, some pancakes and dry mushrooms” (see Figure 5 for the illustration).

Figure 5: Illustration inspired by K. Chukovsky’s children’s poem “Confusion”, used to depict RKN’s unfruitful, messy and even dangerous measures used to block Telegram.

By 25 April 2018, the emergency hotline of the Regional Social Organization “Center of Internet Technologies” (ROCIT) [31] had received 3,439 [32] complaints from individuals and businesses related to blocking of various services, 70 percent of which complained about

inaccessibility of Google services, and 17 percent were concerned about the lack of access to Amazon; RKN's hotline received more than 46,000 complaints [33]. Furthermore, the Russian Association for Electronic Communications (RAEC) [34] recognized that "the problem ha(d) gone beyond technical circles", and the media largely agreed on the vast scale of side-effects of Telegram blocking for entrepreneurs and start-ups (Daucé, 2019). An emergency gathering [35], with more than 30 representatives of the private sector and governmental agencies and RKN representatives was held on 25 April 2018 on request of RAEC and ROCIT where RKN activities were widely criticized.

The criticism was accepted even by the ROCIT Director, who acknowledged that "The resistance formed by active Internet users and IT businesses is a legitimate reaction to destructive measures of the regulators (...) Businesses admit that Russian equivalents of those services simply do not exist or their quality is much worse". Following the emergency meeting, lawyers from Agora launched a court suit against RKN for collateral damages to small businesses [36]. The first case was opened on 27 April 2018 by the CEO of a real estate company, Investori, who estimated his losses around five million rubles after 10 days of blocking of their Web site [37]. According to Agora [38], a total of 150 organizations filed complaints against RKN for collateral damage. Some of these cases have come as far as the European Human Rights Court and are still under consideration.

"Concerned publics" and resistance strategies

Collateral damages to small businesses, or to people's favorite online services, had an important effect on the politicization of particular segments of RuNet users, creating new "concerned publics" (Geiger, *et al.*, 2014), involving them into collective action or cultivating their understanding of circumvention technologies:

> "In fact, small entrepreneurs who have never really been concerned by politics ... they have felt the immediate effect of RKN's actions. I have friends who were running family businesses on the net, selling stuff for kids online, they were super angry when their site was just blocked. The following week they were already reading everything about VPNs and stuff, and trying to reach out to lawyers, wanted to organize something, subscribed to technical channels on Telegram to understand what was actually happening." (interview, ISP, our translation)

Researchers have observed wider adoption of privacy-enhancing technologies and circumvention tools such as VPN and Tor, especially by journalists (Daucé, 2019) whose activities were largely relying on Telegram. A vibrant market of proxies for Telegram developed, while popular opposition media helped raise user awareness about Internet censorship generally, and more specifically, by developing games (Figure 6) or infographics to explain the methods of blocking used by RKN, the functioning of a proxy or a VPN, the principles of IP hopping and other technical solutions used by Telegram to circumvent blocking.

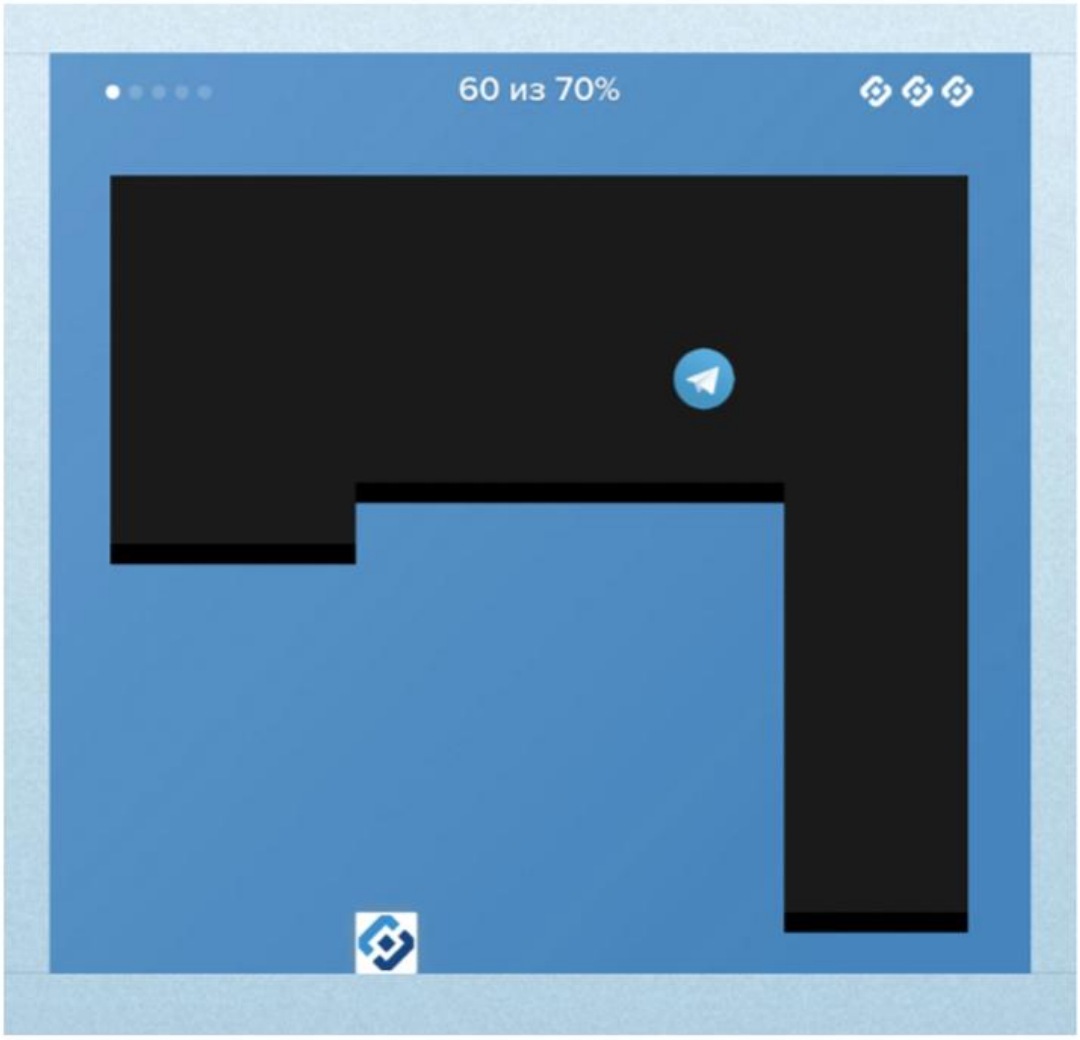

Figure 6: A game on Meduza.io about the Telegram ban.

By mid-April 2018, we observed a steady increase in the creation of a new kind of Telegram channels, focused on quantifying and analyzing the consequences of the Telegram ban on the connectivity and functioning of the RuNet, namely, on its connectedness with foreign infrastructures. Experts started to produce regular monitoring and to alert on any new serious cases of collateral blocking. Although, after one year of unsuccessful blocking of Telegram, many of these channels were discontinued, some projects are still active and participate in maintaining what we could describe as “expert-led vigilance”. The Telegram ban ultimately contributed to fostering a novel culture of RuNet “health monitoring”. A new hybrid public emerged, at the crossroads between developers, network engineers, journalists, Internet

freedom lawyers and opposition activists, involved in producing collective data and analytics of RuNet's functioning and connectedness with the "outside world".

During the first months of Telegram ban, tech activists developed a new repertoire of contention (Tilly, 2002), leveraging the very same vulnerabilities that caused collateral damages in order to organize resistance or awareness campaigns. What subsequently became known as the most famous action in this field, led on 18 May 2018 by Leonid Evdokimov, used the graph of blocked IP addresses to write a statement in Morse code with an automated Python script (Figure 7).

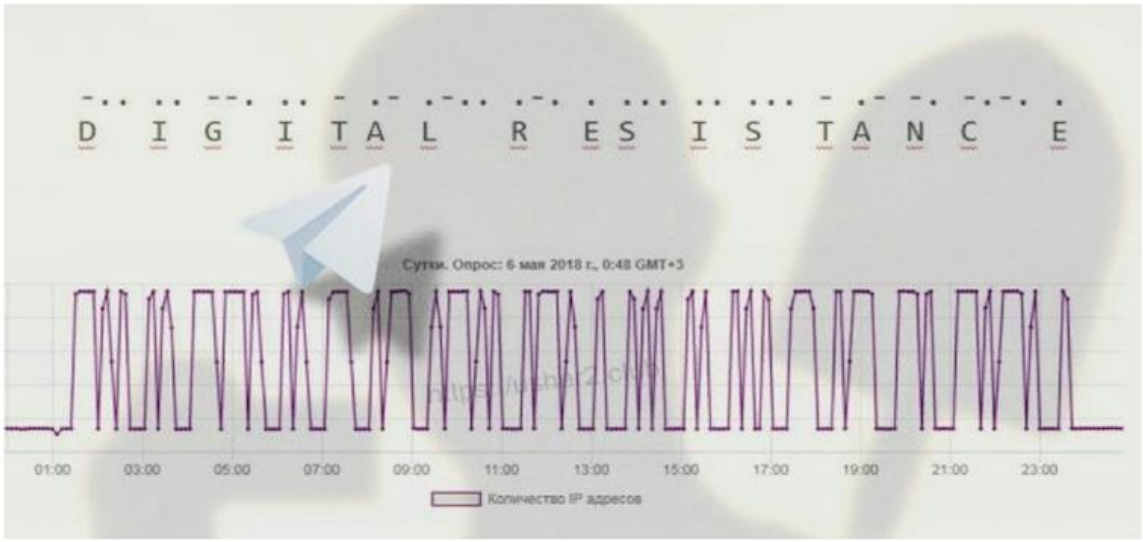

Figure 7: Leonid Evdokimov wrote "Digital Resistance" in Morse code on the graph of blocked IP addresses.

As Leonid Evdokimov, the author of the Morse code prank, explained in our interview with him [39], the hack's purpose was to attract media attention to the "holes and bugs in the system of blocking". Besides media interest in this action, the Morse prank had a direct influence on the domain blacklist, which was cleaned up from expired domains (from 15M to 11M banned IP addresses). Thus, paradoxically, tech activists had an active role in reshaping governance infrastructures, by helping to clean, restructure and maintain the blacklist, urging RKN to standardize blocking methods, certify blocking and filtering equipment, rewrite and improve documentation for the ISPs.

Analyzing Telegram chats of ISPs during this intense period, we observed that many ISPs simply refused to block the popular messenger. As we describe in detail in a dedicated paper (Ermoshina, *et al.*, 2021), they have deployed technical strategies to simulate blocking, such as the so-called "sandbox" [40], or even overtly refused to block Telegram. Moreover, vendors of equipment for traffic filtering, such as Carbon Reductor, offered special solutions for small

ISPs to minimize effects of carpet blocking and guarantee access to popular services (Instagram, Youtube, Facebook and so on) to their clients, regardless of the carpet blocking. This special offer was overtly described as “make Roskomnadzor believe you block things, while actually you don’t” [41].

In addition to these underground resistances “by infrastructure”, the Telegram ban led to a rise of off-line activism focused on Internet freedom. A wave of demonstrations “For Telegram” took place across the country (Figure 8), producing quite peculiar hybrid publics: indeed, Telegram rallied political groups from different sides of the spectrum, from anarchists protesting against state surveillance to libertarians and right-wing activists defending “free speech” [42]. Other actions included flashmobs (throwing paper planes from the window, Figure 9) or artistic interventions in public space (Figure 10). The instant messenger became, at least for Spring and Summer 2018, a contextual point of unity for various anti-governmental movements.

While some “concerned publics” identified in the wake of the Telegram ban controversy may have a shorter life span — across-the-spectrum political groups are likely not about to become stabilized entities in the panorama of Internet freedom activists — the Telegram ban case may indicate that emerging types of actors and resistance strategies could have a more durable impact in the field of Internet infrastructural battles. For example, this case has revealed a number of circumvention practices that are close to hacking in the sense described by Ermoshina (2019): not as a “revolution” in programming or coding, but as a set of ongoing experimentations or *bricolages*. Hacking is about having the competencies and the inventiveness to rapidly invent an inexpensive and intelligent way to solve (or at least raise awareness about) a societal problem, by leveraging specific technical features — preferably the very same features in authorities’ strategies that are causing collateral damages and vulnerabilities. Engineers and developers in Russia have become, often in spite of themselves, concerned actors of the governance and counter-governance of RuNet; this “concerned public” is very likely to stay and even institutionalize its existence through a set of tools and practices that are now becoming, to some extent, standardized. For example, crowdsourced censorship monitoring or traffic measurement is now widely used beyond the Telegram case, during mass protests or other events where state-driven shutdowns or blocking are expected.

Figure 8: The biggest rally “for Telegram”, held in Moscow on Sakharov avenue on 30 April 2018, with around 12,500 participants.

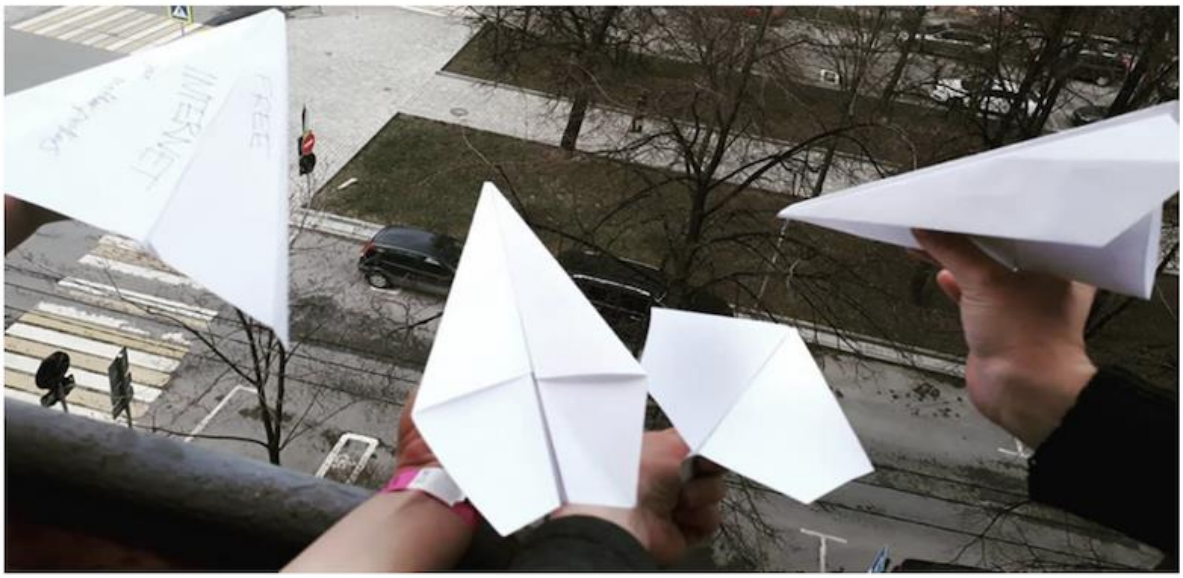

Figure 9: Flashmob was held on 22 April 2018 at 7 pm Moscow time across the country. Source: https://www.rbc.ru/photoreport/13/04/2019/5c99d9b49a7947ac099feafd.

Figure 10: Artistic intervention on Dvortsovaya Square, historical center of Saint-Petersburg, made by Russian contemporary artist Hiroshi. The installation is named “paper

hits the rock", making a reference to the famous game "Rock-paper-scissors", where the paper plane symbolizes Telegram while RKN's style of Internet governance is qualified by the artist as "coming from the stone age". As the artist himself explains: "I have always wondered how paper can win over the rock. But looking at the Telegram case I got how it works: the paper plane simply brings down and destroys RKN's reputation" [43].

Conclusion: Telegram's reputation challenged by the ban

Telegram was officially unbanned in June 2020, for two main reasons explained by the Ministry of Communication: first, the "technical impossibility" to effectively block it, and second, because Telegram has agreed to block specific channels related to drug sale or terrorism [44]. This decision raised a few concerns in terms of the collaboration between Telegram's founder, Pavel Durov, and the Russian government. A few communities, which we have been observing since 2017, left Telegram after its unban; for instance, the "Mesh and CryptoAnarchy" community, dedicated to discussions about decentralization and security, moved their discussions to Matrix. After the unban, we conducted a survey [45] targeting tech-savvy users and activists: the survey eventually showed that the majority of users did not lose trust in Telegram. Users believed that the unban was used by the government to improve its reputation in the wake of the general vote for amendments to the Constitution in July 2020.

On 9 July 2020, the vice-president of Telegram spoke with Russian Prime Minister Mishustin at a meeting of IT-industry leaders [46]. In his speech, he focused on the role of transnational IT giants, including those who once helped Telegram to avoid blocking. He criticized the influence of Apple and Google on small and medium software startups. Besides the influence of IT giants on the market, Durov's critical attitude towards Apple can be partly explained by Apple's refusal to push Telegrams updates to the App Store during the "open phase" of the battle for Telegram. Following this roundtable, Pavel Durov published an official statement [47] on his Telegram channel, suggesting that Russian government must take steps to restrain the impact of Silicon Valley giants on RuNet. Telegram's reputation as an "independent" messenger was largely questioned, and a second wave of "migrations" from Telegram to other messengers started.

However, our second survey showed that while more politically active and tech-savvy users slightly changed their usage patterns on Telegram (*e.g.*, applying self-censorship, using secret chats with disappearing messages more often, not sharing their phone numbers or using two-step authentication), the majority of respondents did not modify their habits and did not consider moving away from Telegram. Moreover, recently Durov refused [48] to satisfy Apple's request to block three Belarusian channels focused on documenting police violence in Belarus against protesters triggering a regain of trust among the activist user communities. Indeed, Telegram still remains the most popular and actively developing messenger in Russia, and is now considered both as a hybrid social network, a circumvention tool for many censored media, and a favorite chat app for tech-savvy audiences and main source of news for millions of Russians. This article has sought to demonstrate how the Telegram ban made visible several vulnerabilities of technical and legal blocking mechanisms implemented by RKN, and unveiled the fundamental dependencies of Runet on foreign Internet infrastructures. We have shown how resistances to the Telegram ban, primarily those conducted "by infrastructure", have conducted to partial modification of legislation, cleaning of blacklists, unblocking of millions of IP

addresses; and eventually, led to the birth and development of new initiatives for Internet measurement and monitoring of RuNet's "health", creating a new culture of tech vigilance.

The Telegram case helps deconstructing a simplistic vision of RuNet governance as highly efficient and strictly centralized, to tell instead multiple stories of discordance and dissonance: between the proclaimed ambitions of the Russian government and its willingness, capacity and resources to commit to the task; between the official narrative of "war against terror" and paradoxical popularity of Telegram among governmental officials; between the levels of security declared by Durov and the cryptographic "realities" actually offered by the Telegram messenger; and between particular users' technical knowledge (allowing them to understand that Telegram has in fact never been completely secure) and their allegiance and fidelity to the messenger despite all odds. In fact, as we have seen, governmental actors fail to control the multitude of ISPs and the strategies they implement, and lag behind the "protocol creativity" of the Telegram team. The race between blocking mechanisms and circumvention tools in this particular case shows the inefficiency of the infrastructural apparatus and of the censorship methods used by RKN. The unsuccessful attempt to block Telegram, and its recent unban, have both impacted the reputation of RKN as the Russian Internet watchdog, and undermined the overall capacity of the government to effectively control RuNet in the centralized, homogeneous and top-down manner it claims as its own. As one of our respondents phrased it, it is likely that "corruption, laziness and lack of expertise will save RuNet better than any kind of protest".

However, there are indications that the Russian authorities, RKN in particular, may also have learned some lessons from the case, in terms of how they could adapt their "sovereignisation" strategies. An investigation by the journalists of *Proekt*, released in November 2018 [49], concluded that Russian authorities understood that the main focus of their tactics should shift from attempts to block the messenger to attempts to undermine it from within, by buying popular Telegram channels and sponsoring ideological content by their means. Besides, several government representatives have created their own official Telegram channels, some of them during the official "ban". Another "lesson learned" for authorities consisted in devising a rather successful tactic to report specific Telegram channels (*e.g.*, on drug markets, or some of the Islamist-labelled channels) and request their local ban. While this article focuses on the level of infrastructure and on the technical battles around Telegram, it is interesting to highlight that one of the core lessons the Russian authorities may have learned from the Telegram case is the necessity to be more "hybrid" in their digital sovereignty strategies, acting at both the infrastructure and content governance levels.

However, recent speeches by Telegram's vice-president, and Pavel Durov's subsequent publication [50], makes it clear that the battle for Telegram has crossed the path of yet another kind of discourse, focused on technical/infrastructural sovereignty and on the opposition to Western IT giants. While Durov, according to one of our respondents, is acting as a "politician, not a mere CEO of a tech company", Telegram users are left in a state of uncertainty when it comes to the future of the controversial messenger, and its choice of independence from, or loyalty to, the Russian government. At the very moment while we finish this paper, a new fieldwork should be engaged, in order to study the most recent processes of "digital migration" of Russian users from Telegram to new — and likely decentralized — alternative messaging and social networking platforms. The present study of the Telegram case and its ramifications, current and future, is both a reminder that, to paraphrase Bruno Latour (1993), "we have never been secure", and a sketch of an anthropology of the "theaters of security" of our time, framed by our information and communication infrastructures.

About the authors

Ksenia Ermoshina is Associate Research Professor at the French National Centre for Scientific Research (CNRS) at the Centre for Internet and Society.
E-mail: ksenia [dot] ermoshina [at] cnrs [dot] fr

Francesca Musiani is Associate Research Professor at the French National Centre for Scientific Research (CNRS) and Deputy Director of its Centre for Internet and Society.
E-mail: francesca [dot] musiani [at] cnrs [dot] fr

Notes

1. The practice of using one particular IP address for a period of time and then changing it to another one, with the purpose of avoiding flags and bans (see Keenan, 2020). Pavel Durov, Telegram's creator, repeatedly praised Google and Amazon for continuing to allow Telegram access to their platforms, and so did other actors such as the American Civil Liberties Union (ACLU); see *e.g.*, https://twitter.com/ACLU/status/986702628334768128, accessed 12 March 2021.

2. According to Pavel Durov's official Telegram channel, at https://t.me/durov_russia/22, accessed 12 March 2021.

3. The Yarovaya law (or 'package') refers to two Russian federal bills, 374-FZ and 375-FZ, passed in 2016, mandating the expansion of authority for law enforcement agencies, establishing new requirements for data collection, and providing for mandatory deciphering in the telecommunications industry. Since the passing of the bill, its implementation in Russian Internet infrastructure has been deemed as extremely difficult from a practical standpoint, as well as extremely expensive for Internet operators.

4. According to Dmitry Dinze, ex-lawyer of Telegram. https://www.rbc.ru/technology_and_media/02/04/2018/5ac1f2f89a79471b98083b34, accessed 12 March 2021.

5. The expression was first mentioned by Roskomsvoboda on 21 December 2017.

6. A VPN is an encrypted connection that enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

7. During our observations and interviews with the "engaged" engineers and technologists operating the RuNet, we observed the emergence of a very specific attitude towards the RuNet watchdog RKN as highly incompetent, and often described as a "monkey with a grenade".

8. Posted on Durov's official Telegram channel on 4 June 2020, at https://t.me/durov_russia/22, accessed 12 March 2021.

9. https://riot.im/app/#/welcome, accessed 12 March 2021.

10. https://delta.chat/en/, accessed 12 March 2021.

11. By May 2020 at least 30 million active users of Telegram were identified as Russian. Source: Durov's official channel, https://t.me/durov/117, accessed 12 March 2021.

12. Interview with the CEO of a middle-size ISP, Saint-Petersburg, 20 August 2019.

13. Evdokimov's talk also refers to this chronology, see https://darkk.net.ru/35c3/, accessed 12 March 2021.

14. Durov's official page on Vk.com: https://m.vk.com/wall1_2442097, accessed 12 March 2021.

15. A subnet is a "network inside a network", a smaller network within a broader one. The practice of subnetting makes Internet routing more effective.

16. "If the FSB limited itself to asking for data of a few terrorists, it would be a request that does not violate the Constitution. But since they reclaim universal decryption keys to have an unlimited access to users communications, this goes against Article 23, the right to private communications" — Durov's post on his Vk page, 8 May 2018 (our translation), at https://m.vk.com/wall1_2442097.

17. https://www.youtube.com/watch?v=crB0GqKFDPQ, accessed 12 March 2021.

18. https://www.youtube.com/watch?v=qPIN6nB8If8&feature=emb_err_woyt, accessed 12 March 2021.

19. *Ibid.*

20. https://core.telegram.org/api/pfs, accessed 12 March 2021.

21. https://www.forbes.ru/tehnologii/358701-obraz-geroya-pochemu-durov-ne-otdaet-fsb-klyuchi-k-perepiske-v-telegram, accessed 12 March 2021.

22. https://www.interfax.ru/russia/567771, accessed 12 March 2021.

23. IP hopping: see note 1 above. Domain fronting is also a technique for circumventing Internet censorship, consisting of using different domain names in different communication layers of an HTTPS connection, in order to connect to a different target domain than those detectable by monitoring third parties. A proxy server is a machine that acts as an intermediary for requests from clients seeking a resource. Thus, a proxy server potentially masks the true origin of the request to the resource server.

24. https://www.vedomosti.ru/technology/articles/2018/04/12/766567-blokirovka-telegram, accessed 12 March 2021.

25. https://vc.ru/flood/36798-neskolko-ip-adresov-google-popali-pod-blokirovki-roskomnadzora, accessed 12 March 2021.

26. https://tass.ru/obschestvo/5158814, accessed 12 March 2021.

27. https://usher2.club/, accessed 12 March 2021.

28. Interview with Leonid Evdokimov, 4 June 2019.

29. CTO of Deep Forest hosting services, Internet Freedom activist and author of the Usher Club project.

30. See Phil Kulin's project Usher2 and his analysis of collateral blocking of Google, which starts with quoting the poem: https://usher2.club/articles/google-ban/, accessed 12 March 2021.

31. A civil society organization created in 1996 to "create a friendly digital environment and spread IT education" that hosts an "emergency Runet hotline" — an online feedback form for complaints related to violation of digital rights and freedoms (https://rocit.ru/; https://rocit.ru/hotline).

32. https://rocit.ru/news/2250-complaints-about-blocking, accessed 12 March 2021.

33. https://roskomsvoboda.org/38434/, accessed 12 March 2021.

34. A business-oriented organization created in 2006 in order to "support the development of a civilized market of IT services and products, assist relevant projects and develop efficient legal norms and standards to support the industry," https://raec.ru/about/, accessed 12 March 2021.

35. https://raec.ru/live/raec-news/10316/, accessed 12 March 2021.

36. https://republic.ru/posts/90583?code=794b3ee0e9ffec9c65088b6039a85aca, accessed 12 March 2021.

37. https://www.rbc.ru/society/27/04/2018/5ae315de9a794771d19b1604, accessed 12 March 2021.

38. https://t.me/pchikov/1065, accessed 12 March 2021.

39. Interview with Leonid Evdokimov, 4 June 2019.

40. Sandbox is a kind of subnetwork configured within a bigger network of an ISP, that would simulate specific behaviors by sending necessary responses to the requests of the RKN's monitoring device called Revizor. When Revizor probes if a Web site is successfully blocked, the system would respond with the relevant code, whereas the Web site is in fact accessible for end users.

41. Source: Web site of Carbonsoft, https://www.carbonsoft.ru/google-youtube-telegram/, accessed 12 March 2021.

42. It should be noted, however, that two different meetings took place in Moscow: the first one organized by libertarians, with the support of Durov (30 April), the second one by liberals and democrats (13 May). So, while the battle for Telegram did gather diverse publics, we cannot go as far as arguing that they did so in a unified manner.

43. https://forpost-sz.ru/a/2018-05-10/khudozhnik-hioshi-ustanovil-polutorametrovyj-samolyotik-u-dvorcovoj-ploshchadi, accessed 12 March 2021.

44. https://novayagazeta.ru/news/2020/06/22/162498-v-minkomsvyazi-ob-yasnili-razblokirovku-telegram-nevozmozhnostyu-ego-zablokirovat, accessed 12 March 2021.

45. https://t.me/parisburns/9125.The survey was published on Ksenia Ermoshina's Telegram blog (3,855 followers) targeting a mixed audience of tech-savvy journalists, activists and technologists and shared on other channels, such as ZaTelecom (27,930 followers) focused on technical audiences. In total, 1,188 people took part in the survey.

46. https://profile.ru/news/society/vice-prezident-telegram-rassmeshil-mishustina-shutkoj-pro-zolotuyu-ordu-368756/, accessed 12 March 2021.

47. https://te.legra.ph/Kak-Apple-unichtozhaet-startapy-po-vsemu-miru--i-kak-ehto-mozhno-ostanovit-07-09, accessed 12 March 2021.

48. Official statement was published on 8 October 2020 by Durov in his channel: https://t.me/durov/135, accessed 12 March 2021.

49. https://www.proekt.media/narrative/telegram-kanaly/, accessed 12 March 2021.

50. https://te.legra.ph/Kak-Apple-unichtozhaet-startapy-po-vsemu-miru--i-kak-ehto-mozhno-ostanovit-07-09, accessed 12 March 2021.

References

Azadeh Akbari and Rashid Gabdulhakov, 2019. "Platform surveillance and resistance in Iran and Russia: The case of Telegram," *Surveillance & Society*, volume 17, numbers 1–2, pp. 223–231.
doi: https://doi.org/10.24908/ss.v17i1/2.12928, accessed 20 April 2021.

Gregory Asmolov and Polina Kolozaridi, 2017. "The imaginaries of RuNet: The change of the elites and the construction of online space," *Russian Politics*, volume 2, number 1, pp. 54–79.
doi: https://doi.org/10.1163/2451-8921-00201004, accessed 20 April 2021.

Amir Reza Asnafi, Shima Moradi, Mohasedeh Dokhtesmati and Maryam Pakdaman Naeini, 2017. "Using mobile-based social networks by Iranian libraries: The case of Telegram messenger," *Library Philosophy and Practice*, at https://digitalcommons.unl.edu/libphilprac/1539/, accessed 20 April 2021.

Geoffrey C. Bowker and Susan Leigh Star, 1999. *Sorting things out: Classification and its consequences*. Cambridge, Mass.: MIT Press.
doi: https://doi.org/10.7551/mitpress/6352.001.0001, accessed 20 April 2021.

Alain Manuel Chaple-Gil and Kelvin Ian Afrashtefar, 2020. "Telegram messenger: A suitable tool for teledentistry," *Journal of Oral Research*, volume 9, number 1, pp. 4–6.
doi: https://doi.org/10.17126/joralres.2020.001, accessed 20 April 2021.

Sasha Costanza-Chock, 2003. “Mapping the repertoire of electronic contention,” In: Andy Opel and Donnalyn Pompper (editors). *Representing resistance: Media, civil disobedience, and the global justice movement*. London: Praeger, pp. 173–191.

Françoise Daucé, 2019. “Épreuves professionnelles et engagement collectif dans la presse en ligne à Moscou (2012–2019),” *Le mouvement social*, numéro 268, pp. 101–116.

Laura DeNardis, 2014. *The global war for Internet governance*. New Haven, Conn.: Yale University Press.

Laura DeNardis, 2012. “Hidden levers of Internet control: An infrastructure-based theory of Internet governance,” *Information, Communication & Society*, volume 15, number 5, pp. 720–738.
doi: https://doi.org/10.1080/1369118X.2012.659199, accessed 20 April 2021.

Nina Eliasoph, 1998. *Avoiding politics: How Americans produce apathy in everyday life*. Cambridge: Cambridge University Press.

Ksenia Ermoshina, 2019. “For code and country: Civic hackers in contemporary Russia,” In: Mario Biagioli and Vincent-Antonin Lépinay (editors). *From Russia with code: Programming migrations in post-Soviet times*. Durham, N.C.: Duke University Press, pp. 87–109. doi: https://doi.org/10.1215/9781478003342-004, accessed 20 April 2021.

Ksenia Ermoshina and Francesca Musiani, 2017. “Migrating servers, elusive users: Reconfigurations of the Russian Internet in the post-Snowden era,” *Media and Communication*, volume 5, number 1, pp. 42–53.
doi: http://dx.doi.org/10.17645/mac.v5i1.816, accessed 20 April 2021.

Ksenia Ermoshina, Benjamin Loveluck and Francesca Musiani, 2021. “A market of black boxes: The political economy of Internet surveillance and censorship in Russia,” *Journal of Information Technology & Politics* (1 April).
doi: https://doi.org/10.1080/19331681.2021.1905972, accessed 20 April 2021.

Ksenia Ermoshina, Francesca Musiani and Harry Halpin, 2016. “End-to-end encrypted messaging protocols: An overview,” In: Franco Bagnoli, Anna Satsiou, Ioannis Stavrakakis, Paolo Nesi, Giovanna Pacini, Yanina Welp, Thanassis Tiropanis and Dominic DiFranzo (editors). *Internet science: Third international conference, INSCI 2016, Florence, Italy, September 12–14, 2016, proceedings. Lecture Notes in Computer Science*, volume 9934. Cham, Switzerland: Springer, pp. 244–254.
doi: http://dx.doi.org/10.1007/978-3-319-45982-0_22, accessed 20 April 2021.

Phillip Y. Freiberg, 2014. “Putin’s Russia — On a path to cyber sovereignty?” capstone project for the Master of Arts in Media Communications Program for Webster University, at http://www.academia.edu/10762446/Future_of_Internet_Freedom_in_Russia, accessed 20 April 2020.

Susi Geiger, Debbie Harrison, Hans Kjellberg and Alexandre Mallard (editors), 2014. *Concerned markets: Economic ordering for multiple values*. Cheltenham: Edward Elgar.

Daria Glukhova, 2018. “Telegram ban in Russia and the theoretical framework of modern authoritarianism,” Bachelor thesis, Masaryk University, Czech Republic, at https://is.muni.cz/th/ir563/BCP_telegram_final.pdf, accessed 20 April 2020.

Simin Kargar and Keith McManamen, 2018. “Censorship and collateral damage: Analyzing the Telegram ban in Iran,” Berkman-Klein Center for Internet & Society, Harvard University, at https://cyber.harvard.edu/publication/2018/censorship-and-collateral-damage, accessed 20 April 2020.

James Keenan, 2020. “How IP hopping can help you bounce your IP address,” *SmartProxy*, at https://smartproxy.com/blog/how-ip-hopping-can-help-you-bounce-your-ip-address, accessed 20 April 2020.

Bruno Latour, 1993. *We have never been modern*. Translated by Catherine Porter. Cambridge, Mass.: Harvard University Press.

Guillaume Latzko-Toth, 2008. “L’Internet Relay Chat: un cas exemplaire de dispositif sociotechnique,” *COMMposite*, volume 4, number 1, pp. 52–73, and at http://www.commposite.org/index.php/revue/article/view/39, accessed 20 April 2020.

Rubi Manna and Shyamal Ghosh, 2018. “A comparative study between Telegram and WhatsApp in respect of library services,” *International Journal of Library and Information Science*, volume 7, number 2, pp. 1–5, and at http://www.iaeme.com/MasterAdmin/UploadFolder/IJLIS_07_02_001/IJLIS_07_02_001.pdf, accessed 20 April 2020.

Nathalie Maréchal, 2018. “From Russia with crypto: A political history of Telegram,” paper presented at the Eighth USENIX Workshop on Free and Open Communications on the Internet, at https://www.usenix.org/conference/foci18/presentation/marechal, accessed 3 February 2020.

Francesca Musiani, 2013. *Nains sans géants. Architecture décentralisée et services Internet*. Paris: Presses des Mines. doi: http://dx.doi.org/10.4000/books.pressesmines.1853, accessed 20 April 2021.

Francesca Musiani, 2012. “Caring about the plumbing: On the importance of architectures in social studies of (peer-to-peer) technology,” *Journal of Peer Production*, number 1, at http://peerproduction.net/issues/issue-1/peer-reviewed-papers/caring-about-the-plumbing/, accessed 29 October 2020.

Francesca Musiani, Derrick L. Cogburn, Laura DeNardis and Nanette S. Levinson (editors), 2016. *The turn to infrastructure in Internet governance*. New York: Palgrave Macmillan. doi: http://dx.doi.org/10.1057/9781137483591, accessed 20 April 2021.

Lily Hay Newman, 2018. “The unexpected fallout of Iran’s Telegram ban,” *Wired* (19 June), at https://www.wired.com/story/iran-telegram-ban/, accessed 29 October 2020.

Arash Dargahi Nobari, Malikeh Haj Khan Mirzaye Sarraf, Mahmood Neshati and Farnaz Daneshvar, 2021. “Characteristics of viral messages on Telegram: The world’s largest hybrid

public and private messenger," *Expert Systems and Applications*, volume 168, 114303. doi: https://doi.org/10.1016/j.eswa.2020.114303, accessed 20 April 2021.

Julien Nocetti, 2015. "Russia's 'dictatorship-of-the-law' approach to Internet policy," *Internet Policy Review*, volume 4, number 4. doi: https://doi.org/10.14763/2015.4.380, accessed 29 October 2020.

Joseph G. Ponterotto, 2006. "Brief note on the origins, evolution, and meaning of the qualitative research concept thick description," *The Qualitative Report*, volume 11, number 3, pp. 538–549. doi: https://doi.org/10.46743/2160-3715/2006.1666, accessed 29 October 2020.

Brett Rolfe, 2005. "Building an electronic repertoire of contention," *Social Movement Studies*, volume 4, number 1, pp. 65–74. doi: https://doi.org/10.1080/14742830500051945, accessed 20 April 2021.

Hayk Saribekyan and Akaki Margvelashvili, 2017. "Security analysis of Telegram" (18 May), at https://archive.shadowwarfare.info/Security%20Analysis%20of%20Telegram.pdf, accessed 3 February 2021.

Silvia Semenzin and Lucia Bainotti, 2020. "The use of Telegram for non-consensual dissemination of intimate images: Gendered affordances and the construction of masculinities," *Social Media + Society* (20 December). doi: https://doi.org/10.1080/14742830500051945, accessed 3 February 2021.

Bruce Schneier, 2003. *Beyond fear: Thinking sensibly about security in an uncertain world*. New York: Copernicus Books.

Charles Tilly, 2002. *Stories, identities, and political change*. Lanham, Md.: Rowman & Littlefield.

Aleksandra Urman and Stefan Katz, 2020. "What they do in the shadows: Examining the far-right networks on Telegram," *Information, Communication & Society* (20 August). doi: https://doi.org/10.1080/1369118X.2020.1803946, accessed 20 April 2021.

Tommaso Venturini and Anders Munk, forthcoming. *Controversy mapping: A field guide through actor-network theory and digital methods*. Cambridge: Polity Press.

Ahmet S. Yayla and Anne Speckhard, 2017. "Telegram: The mighty application that ISIS loves," *International Center for the Study of Violent Extremism* (9 May), at https://www.icsve.org/telegram-the-mighty-application-that-isis-loves/, accessed 3 February 2021.

Appendix: List of observed Telegram channels and public chats

Name	URL	Type	Author(s)	Description
Nag.ru	https://t.me/nag_public	Public chat	Nag.ru	Largest Telegram chat of Internet service providers
Nag News	https://t.me/NagNews	Channel	Nag.ru	Official Telegram channel of the Nag.ru Web site (ISP community)
Order Com	https://t.me/ordercomru	Channel	Dmitry Galoushko, telecom lawyer	Official Telegram channel of OrderCom, legal agency specialized in telecommunication law; helps ISPs in court
Za Telecom	https://t.me/zatelecom	Channel	Mikhail Klimarev, director of the Society for Protection of the Internet (OZI.ru)	Channel focused on telecom industry; professional news; analytics, research; “insider” information about censorship or surveillance equipment, Internet regulation etc.
Enog	https://t.me/enogtalk	Public chat	ENOG	Official chat of the ENOG community (Eurasia Network Operator Group of RIPE NCC)
RKNSHOWTIME	https://t.me/rknshowtime	Channel	Alex Rudenko; Usher2	Channel showing the amount of blocked IP during the “war against Telegram”. Discontinued since 30 July 2019
RKNshowtime support	https://t.me/rknshowtime_support	Public chat	Alex Rudenko; Usher2	Chat of the channel RKNSHOWTIME. Discontinued since December 2019
RKN block check	https://t.me/rkn_block_check	Channel	Dmitry Miroskin (engineer, member of the OZI expert community)	Automated data on new IP adresses added to the RKN blocklist
Pirate Party Russia	https://t.me/chatppru	Public chat	Pirate Party Russia	General chat of the Russia Pirate Party

Meshnet and Cryptoanarchy	https://t.me/meshnet	Public chat	Meshnet enthousiasts	A chat focused on decentralized protocols and alternative communication platforms
Distributed	https://t.me/distributed	Chat	FoxCool (IT expert, advocating for decentralization and “cryptoanarchy”)	Chat focused on p2p technologies, alternative routing protocols (type CJ DNS)
Decentralize!	https://t.me/dcntr	Channel	A group of developers	News about decentralized and distributed software, encryption and digital security
“The Ministry of Truth”	https://t.me/i_love_auditor	Public chat	Vladislav Minakov	The chat for ISPs dedicated to the automatic system Revizor, its technical implementation, bugs and other related questions. Also used to discuss court cases (ISP vs Roscomnadzor)
IT and SORM	https://t.me/unkn0wnerror	Channel	Vladislav Zdolnikov, IT consultant for Navalny’s Foundation Against Corruption; the founder and CEO of TgVPN; developer of free Telegram proxies	Channel dedicated to news and controversies around censorship mechanisms and circumvention tools (VPN, proxies); surveillance and anti-surveillance; RuNet governance regulation etc.
Politota	https://t.me/NR_Politota	Chat	Nag.ru	Chat of the Nag.ru members (ISPs) created for political discussions
NoNameClub	https://t.me/nnmclub_official	Channel	NoNameClub	Digital security, censorship, data protection, circumvention tools

Zablokiruy Eto! (Block this!)	https://t.me/blokiruy	Channel	Unknown	Censorship in Russia and abroad
RosKomSvoboda	https://t.me/roskomsvoboda	Channel	RosKomSvoboda	Official channel of Russian Internet freedom NGO Roskomsvoboda
Digital Rights Center	https://t.me/DigitalRightsCenter	Channel	Sarkis Darbinyan, lawyer	Channel of Roskomsvoboda's lawyer and their side-project Digital Rights Center
Leonid Volkov	https://t.me/leonid_volkov	Channel	Leonid Volkov, CTO of the Foundation Against Corruption	RuNet regulation and politics; Navalny's campaign news
Cybersecurity et Co	https://t.me/alexlitreev_channel	Channel	Alex Litreev (libertarian activist and developer)	Alex Litreev's channel: tech news and Russian Internet regulation
Novosti Teplitsy (Teplitsa's News)	https://t.me/teplitsa	Channel	Teplitsa Sotsialnyh Technologiy ("Greenhouse for Social technologies")	Official channel of the "Greenhouse for Social Technologies", Russian NGO specialized in social innovation and "tech for good"
FreeRuNet	https://t.me/freeRUnet	Channel	Several oppositional movements and parties	Organizing of rallies and demos "for Free RuNet" news of tech and politics
Tsifrovaya Ten (Digital Shadow)	https://t.me/digitshadow	Channel	Atanasov Vitaliy (Ukrainian journalist)	Platform economy, Internet censorship and circumvention tools; Internet freedom
Telegram Dozorniy (Telegram Watcher)	https://t.me/tlgdozor	Channel	Unknown	Telegram reachability data
Kak Telegram?	https://t.me/kak_telegram	Channel	Unknown	Telegram reachability; tech memes and humor

(“How’s Telegram”?)				
Usher Club	https://t.me/usher2	Channel	Phil Kulin; Internet measurements expert, hoster, author of the usher2.club project	Channel of Phil Kulin (blocking methods and tools, analysis of blacklists, legislation)
Telecom-review	https://t.me/gip_24	Channel	Unknown	News of telecom governance in Russia
Ivan Begtin	https://t.me/begtin	Channel	Ivan Begtin	“I write about Open Data, Procurement, e-Government, Open Government, Budgets, Privacy and other govtech stuff”
Proekty Normativov v Oblasti Svyazi (Projects of Laws and Norms in Telecom Industry)	https://t.me/ru_comreg	Channel	Phil Kulin	Bridge between Telegram and the governmental platform https://regulation.gov.ru/ (automated newsfeed generated by a Telegram bot @FeedRetranslatorBot)
LinkMeUp	https://t.me/linkmeup_podcast	Channel	LinkMeUp project	Professional news and specialized video podcasts on telecom industry