Measuring Internet Censorship in Disputed Areas: An examination of online media filtering in Russia and Crimea during the 2018 Russian presidential elections

by Igor Valentovitch and Ksenia Ermoshina

Table of Contents

I. Introduction

In March 2018, Russian citizens went to the polls to elect a president. For social scientists like us,[1] these elections presented an ideal opportunity to measure Internet censorship in Russia and in the disputed Crimean Peninsula. Accordingly, we set forth to assess whether processes unfolding in the political domain would influence freedom of access to critical content online, and whether strategically important territories such as Crimea would be subject to different information controls than those in mainland Russia.

The goal of our study was to provide more profound investigation of the filtering practices in the country by supplementing the research on blocking online resources with investigation how this blocking is executed and whether it is consistent across Russia and Crimea. We used the following three questions to guide our research. First, will critical platforms in Russia and Crimea be blocked during the presidential elections? Second, is the filtering of liberal platforms consistent or exclusive across the board? And third, if there are differences in the filtering approaches, what are the factors that account for them?

Back in 2010, researchers from the OpenNet Initiative determined that critical content on the Internet was blocked in certain countries of the Commonwealth of Independent States (CIS) during important political junctions (e.g., elections, social unrest, economic turmoil) as part of the so-called "second-generation" information controls.[2] Given this, we hypothesized that the 2018 elections would have an effect on information controls in the region. We discovered, however, that this significant political event did not have a substantial impact on the practices of Internet censorship in the area. Our research, however, identified that Internet censorship is not consistent across the examined territories and that it is experienced differently in Russia and Crimea. Although our initial expectations were not met, the elections nonetheless played an important role as an instrument to mobilize a network of volunteers and researchers to conduct a large-scale measurement experiment from which several lessons were learned.

Notably, we encountered many unexpected difficulties while conducting this experiment—several of which forced us to modify our analytical strategies in order to maintain a reflexive position with

[1] The authors of this paper, Igor Valentovitch and Ksenia Ermoshina, are social scientists in the fields of political science and science and technology studies (STS). They both held Open Technology Fund (OTF) fellowships focused on Internet freedom research projects in the Commonwealth of Independent States (CIS) region.

[2] "Second-generation" information controls involve the adoption of laws that provide for technical monitoring and blocking of access to information. They also include covert filtering during critical events (e.g., elections, mass protests, and economic turmoil) by extending requests to ISPs to block objectionable content, temporal shutdowns of communications, government instigated DDoS attacks and others. *See* Deibert, Ronald, eds. 2010. *Access controlled: The shaping of power, rights, and rule in cyberspace*. Cambridge: MIT Press.

regards to our research methodologies. In this study, we provide a summary of our major findings and key observations. Full results from this research will be published in a forthcoming academic article. Below, we reflect on our research experience and share lessons we hope will be useful to fellow researchers working on information controls and network measurements as well as tool developers.

II. Methodology

Forging a new methodology

Although our shared background is in social science, with a special focus on investigating information controls in the post-Soviet space, we both were interested in developing a mixed methods approach to this research that combined social science and network measurement techniques and approaches. This new methodology, which can be replicated in the future in different geographical contexts, is described below.

First, to answer the research questions posed by this project, we conducted a comparative study of Internet filtering in Russia and Crimea during the presidential elections held on March 18, 2018. To examine the accessibility of various critical and liberal platforms in both territories, we conducted extensive network measurements with the help of OONI Probes (network measurement tool developed by the OONI Project). These probes can collect a variety of measurements depending on user preference. We chose to conduct *web connectivity* tests which help to determine if websites are accessible and, if they are not, how access to them is being blocked (e.g., through DNS tampering, TCP connection blocking, or by a transparent HTTP proxy).

Second, to collect more information about how censorship is experienced on the ground, we employed qualitative methods. Using in-depth, semi-guided interviews with relevant actors, we combined a larger political science analysis with micro-sociology and empirical ethnographic data. As part of a separate research project under the Information Control Fellowship program[3], focusing on information operations in Crimea, 45 interviews were conducted between December 2017 and May 2018 with the following groups of professionals: journalists working in Crimea and Ukraine on Crimean topics, NGO activists working in Crimea and Ukraine on human rights and freedom of expression issues, Internet service providers (ISPs) working in Crimea and Ukraine with knowledge

[3] The Information Controls Fellowship Program (ICFP) supports examination into how governments in countries, regions, or areas of Open Technology Fund's core focus are restricting the free flow of information, cutting access to the open Internet, and implementing censorship mechanisms.

of the Crimean context, politicians working on Crimean information politics, and digital security trainers working with Crimean activists and journalists. In addition to these interviews, we employed web-ethnography to analyze the main forums in which Crimean users discuss issues of Internet service market, censorship, and circumvention. Together, the interviews, web-ethnography, and other qualitative methods (such as local media content analysis) helped us improve and prepare the custom list of URLs we ultimately used to probe for Internet censorship in mainland Russia and Crimea. In collaboration with the Internet Health Report Project, we also analyzed RIPE NCC data to assess routing changes across Crimean ASNs.

Preparing test lists

Far in advance of the 2018 elections, we prepared for our study by creating a custom test list of URLs of critical websites that were either already blocked by Roskomnadzor, the Russian telecommunications authority, or had a high probability of being blocked during the elections. These websites related to independent media and human rights projects, political dissidents and opposition parties, international broadcasters, minority content, and others.

We used three different methods to identify the URLs for our test list. First, we conducted content analysis of primary and secondary resources (e.g., media accounts, analytical reports, government documents, platforms of local Internet freedom organizations, social media posts) that discussed the blocking of critical websites in Russia over the past four years. Second, we conducted semi-structured interviews with journalists and activists in Crimea to determine firsthand what type of content was being blocked in the disputed peninsula. Third, we analyzed the platform of Roskomsvoboda, a renowned Russian digital rights organization, to identify critical platforms of interest to our research. We did so by using keywords and searching for blocked Ukrainian and Russian liberal online media and political websites.

Virtual feedback loop

Our connections with Ukrainian and Russian Internet Freedom communities enabled us to ask them to review our custom test list and provide feedback. The net result of this overall process was a list

of 110 URLs for our study. With the help of OONI Run,[4] this list was re-organized for easy distribution and then disseminated to volunteer testers throughout Russia and Crimea.

Notably, it was challenging to distribute the OONI Run link to certain local testers because not all messengers are capable of properly handling long links without breaking them. After unsuccessfully experimenting with WhatsApp and Signal, we ended up using Telegra.ph and Medium to achieve dissemination. As we found out from our testers, however, Telegra.ph was blocked in Crimea after April 2018, as part of Roskomnadzor's efforts to globally block Telegram and its various services. Given this development, we believe OONI Probe users will greatly benefit from creating a dedicated method for distribution of OONI Run links to testers, as mainstream tools may be censored in areas of interest to researchers.

Engaging testers on the ground

As a first step to making contact, we wrote several blog posts in Russian and English to help identify volunteer testers on the ground. In addition, we conducted online campaigns on various social media channels (mainly Telegram and Facebook) and sought the support of local Internet freedom and human rights organizations, such as Roskomsvoboda. Despite these efforts, it still proved challenging for us to find testers in conflict areas such as Crimea. Ksenia Ermoshina ended up identifying testers on the ground following her fieldwork in the region.

Next, knowing that the usage of OONI probes carries a certain degree of risk, we deployed a security protocol when working with our Crimean testers.[5] Accordingly, we had contact with only one tester on the ground, who then coordinated a group of local testers to conduct measurements on specific days and networks. This tester used WhatsApp to communicate the AS number of OONI probes and the relevant times for conducting tests. Except for the local coordinator, we never knew any personal details of any of our testers.

Testing period and key numbers

[4] OONI Run is an application that allows for inputting multiple URLs and outputting a single link that can be then distributed to testers on the ground. Upon clicking on the link, OONI Probe launches automatically and begins to test the accessibility of preselected URLs.

[5] Consult OONI's website for an explanation of the potential risks involved in using their tool in censorship hot spots.

Our goal was to collect measurements daily before, during, and after the elections. Web connectivity tests were conducted as planned in February, March, and April. Depending on the availability of testers on the ground, the measurements in mainland Russia were collected daily on the networks of 50 to 70 ISPs, including all major providers in the market. In Crimea, data was collected on the networks of 8 local providers out of 114 in existence. In March alone, more than 200,000 measurements were collected.

III. Data processing and analysis

The data processing and analysis phase proved to be the most challenging part of our study, as many measurements were collected over a prolonged period of time on multiple networks. Therefore, we decided to examine a representative sample of data collected on days when network probes were run simultaneously in Russia and Crimea. Igor Valentinovitch took the lead on this part of the study, starting by manually extracting and processing the collected data from OONI Explorer (a platform where measurements collected by all OONI probes around the world are published for researchers to use). This method, however, proved to be useful only when looking at small number of tests, so the OONI team ended up helping us automate the process of measurements extraction from their database.

After extraction, the data were organized in a comparative format using this methodology:

- Measurements were arranged chronologically in the following fields: tested URLs, network identifiers (ASN), timing of tests, test results, and types of filtering detected (if any).

- To investigate the consistency of blocking across Russia, we first had to determine what resources (e.g., domain names, or individual pages) were supposed to be blocked by local ISPs as per the regulations of the Russian telecommunications authority.[6] To do so, we cross-referenced the URLs from our custom test list with Roskomnadzor's registry of blocked resources. At the end, our test list represented a balanced mix of critical platforms, of which some were blacklisted and others were not (meaning they were supposed to be accessible).

[6] According to the Russian legislation, blocking of online content can be determined extra-judicially or following decisions of courts. The URLs that need to be blocked are entered in Roskomnadzor's registry. Next, the owners of the platforms are contacted by their respective hosting companies and asked to remove the questionable content immediately. If they fail to do so, the hosting providers must block access to the platforms (or pages on them) within 24 hours. Roskomnadzor maintains several registries of blacklisted resources. The URLs that need to be blocked are distributed electronically to all ISPs in the country. The ISPs are ultimately responsible for carrying out the blocking. Roskomnadzor uses a system called "Revizor" to monitor the process and see if blacklisted content is properly blocked by individual ISPs.

- To determine the type of content Russian censors seek to block, we organized the URLs from our list into the following categories: online media (distinguishing between Russian, Ukrainian, and Tatar media), human rights projects, political criticism, social media, international broadcasters, and foreign foundations. These thematic clusters were then validated by our expert interviewees on the ground. For example, Crimean Tatar media represents a special subset of resources which are highly monitored and frequently censored by Roskomnadzor and the new Crimean authorities.

- To make the data manageable for analysis, we worked with a data sample. For the sample, we included all measurements collected when probes were simultaneously run in mainland Russia and Crimea.

- Results for each tested URL were compared to determine whether individual ISPs in both territories were complying with Roskomnadzor's directives. If the ISPs were blocking the URLs per the agency's registry, it was then determined what methods were being used to do so. This comparative approach gave us the opportunity to examine whether the blocking of critical resources is consistent across the board and whether over-blocking is present.

The data extraction process from OONI Explorer proved to be quite challenging and time-consuming. Based on our experience with the platform, we were pleased to learn OONI has been working on revamping the Explorer. As part of that process, we recommend OONI put together a comprehensive and user-friendly guide for OONI data processing. Ideally, this guide should be geared toward researchers with limited technical skills (e.g., social scientists or journalists) and be tested iteratively with interested parties. Although the OONI team provided incredibly timely and useful assistance to our team, we believe there still should be a method and tool for researchers who are using OONI Probes to quickly and easily access datasets they have gathered. We recommend OONI take into account these considerations based on our firsthand experience with their platform's capabilities.

IV. Key findings: Accessibility of liberal and critical platforms in Russia and Crimea

Our analysis determined that online censorship is experienced differently within—and between—mainland Russia and Crimea. In particular, we detected the tendency to over-block resources is more pronounced in Crimea. Although we believe the over-blocking of liberal and critical content on the disputed peninsula is, in most cases, likely related to technical limitations experienced by local providers, certain cases we encountered suggested that over-blocking is also a consequence of the deliberate actions of select ISPs that have been pressured by Crimean authorities to restrict access to certain content. Table 6 in the Appendix demonstrates over-blocking incidents

that occurred in both territories.[7] Below, we summarize our key findings as organized by the following content categories: websites of political opponents, human rights organizations and foundations, social media, Russian media, Ukrainian media, Tartar minority media, and international broadcasters.

Websites of political opponents

We detected no recorded incidents of temporal blocking of opposition websites during the 2018 presidential elections. In general, we found the majority of the ISPs in the country carried out the blocking of critical content in Russia per the instructions of Roskomnadzor—yet this was not uniform across all ISPs. We found blacklisted platforms of certain dissident figures to be still accessible on select providers in both Russia and Crimea, suggesting that filtering is inconsistent across the board and dependent on the blocking capabilities of individual ISPs.

For example, the website of Garry Kasparov, an opponent of Russian President Vladimir Putin, was blacklisted and effectively blocked on the networks of all the Russian and Crimean ISPs we tested. But the website and social media channels of Alexei Navalny, a prominent anti-corruption blogger and main opposition figure, were not blacklisted and thus accessible during the elections in both Russia and Crimea. The platform of Mikhail Khodorkovsky, another major opponent of President Putin, was blacklisted and effectively blocked by 80% of Crimean ISPs and 91% of Russian ISPs we tested. It remained accessible, however, on the networks of five Russian providers and one Crimean provider. In each of these cases, the filtering was executed on the ISP level, primarily by HTTP (81%) and DNS (11%) blocking.[8] The social media channels of the above political dissidents were not blacklisted and remained accessible throughout. This was the case for both Russian platforms (e.g., VK, Odnoklassniki, Live Journal) and foreign platforms (e.g., Facebook, Twitter, Instagram).

Human rights organizations and foundations

We found access to platforms of human rights organizations to be inconsistent, providing further evidence that the Internet filtering in Russia is not strictly endorsed at the ISP level. For example, Khodorkovsky's social project for democracy, Open Russia, has been banned as "undesirable" by the authorities and its domains have been entered in Roskomnadzor's registry (meaning access to

[7] A more detailed analysis on this subject matter will be available in our forthcoming paper.
[8] An explanation of the different types of filtering determined by the "Web Connectivity" test executed by the OONI probes can be found at: https://ooni.torproject.org/nettest/web-connectivity/.

Open Russia should be blocked). The data we collected, however, revealed this platform was accessible on the networks of 18% of the Russian ISPs we tested. The other ISPs effectively restricted access to Open Russia's domain via HTTP and DNS blocking. As for influential foundations from the United States (e.g., Open Society, the National Endowment for Democracy, the U.S. Russia Foundation, and the National Democratic Institute), access to their websites was restricted by Roskomnadzor after these foundations were declared "undesirable" by the Russian authorities.[9] We detected no access to their websites from Crimea and most of mainland Russia.[10]

The website of Crimea SOS, a local human rights initiative whose mission is to aid internally displaced people in Crimea and Donbass and restore Ukrainian authority on the peninsula, was not blacklisted or filtered by any of the Russian ISPs we tested, nor by most (6 out of 7) of the Crimean ISPs. Despite these findings, members of Crimea SOS who were interviewed claim that their website was nonetheless rendered inaccessible at other times. Their claim has been confirmed by a survey conducted by Digital Security Lab Ukraine in partnership with Crimean Human Rights group, which identified at least one Crimean ISP that was restricting access to Crimea SOS's website. Notably, this ISP was identified in our tests as one that was also blocking access to Ukrainian and Crimean platforms that were not blacklisted by Roskomnadzor. This interesting discovery demonstrates the autonomy that some Crimean ISPs enjoy in the institution of filtering.

Our tests revealed that the same ISPs who fail to block the *https* addresses of American foundations also fail to restrict access to the secure protocols of other blacklisted resources from our test list (see Table 1 in the Appendix). This finding suggests the inconsistent blocking of blacklisted platforms by some ISPs is probably not intentional, but rather may be a result of their technical inability to filter traffic to secure protocols (a process which requires investment in expensive DPI equipment that smaller providers often cannot afford).

Social media

The 2014 Russian data localization law requires all domestic and foreign companies storing the user data and metadata of Russian citizens to do so in data centers based in Russia. Companies must keep this information for six months and make it available to security services upon request. Mail

[9] In 2015, the National Endowment for Democracy was the first organization to be labelled "undesirable" under Russian legislation. In December of that same year, Open Society Foundation was added to the list and its activities were banned. Russians who maintain ties with "undesirables" face penalties ranging from fines to six years imprisonment.

[10] NDI's website was blocked by 95% of Russian ISPs tested, OSF's by 90%, and USRF's by 81% (mostly by HTTP filtering).

services and social networks are also asked to place the personal data of Russian citizens on servers located in Russia.

In January 2017, LinkedIn became the first social network to be blocked in Russia for failing to comply with the localization law. As a result, its *http* and *https* addresses were effectively blocked by most of the ISPs we tested—yet we found a few exceptions. Select Russian and Crimean ISPs blocked only LinkedIn's secure protocol, while other providers did not block either of LinkedIn's protocols. This case provides another example of the inconsistent blocking practices in place across the country.

Interestingly, all social media channels of the liberal platforms we examined (including popular Russian ones like VKontakte and Odnoklassniki) remained accessible in both territories. This is an important discovery given that various types of social media have become the major content delivery platforms of liberal organizations in the CIS over the past five years.

Finally, it is worth noting that in April 2018, Roskomnadzor blocked access to the more popular in the country Telegram messaging service, causing mass Internet disruption across Russia. Unfortunately, this platform was not included in our tests because Telegram was not targeted at the time of our testing, meaning we did not gather any data which would allow us to assess how this blocking was ultimately carried out.

Russian Media

We found the blocking of Russian liberal news media to be selective throughout. Of the seven portals we tested, four were blacklisted by Roskomnadzor. Certain popular media projects that are known to be critical of Kremlin (e.g., *TV Rain, Zona Media, Meduza*) are not blacklisted and remain accessible throughout the country. Yet the websites of other less popular opposition media (e.g., *Grani*, *Kasparov*, and *Everyday Journal*) have been blacklisted since 2014. In theory, therefore, these websites should be inaccessible throughout the country. In reality, however, we found there to be only inconsistent blocking of these platforms.[11] The domains of *Grany* and *Everyday Journal* were blocked by the majority of the ISPs in Russia and Crimea. Yet these domains remained accessible on the networks of few providers in both territories. In a similar vein, although the blacklisted *Morning News* was fully blocked in Crimea, we found it to be accessible on the networks of 21% of providers in mainland Russia. The tendency to over-block in Crimea can be

[11] See Table 2 in the Appendix section for comparative numerical estimates of the porous blocking in Russia and Crimea.

seen by the treatment of the Sevastopol-based information portal *Meridian*. The portal does not appear in Roskomnadzor's registry, yet some Crimean ISPs still restrict access to it. These empirical findings are supported by interviews we conducted with individuals working at local ISPs, one of whom explained:

> General blocklists come from Roskomnadzor, but some URLs are communicated in emails or letters from the Ministry of Transportation and Communications [of Crimea]. We can try to argue with them and not block. [But] from the point of view of our business, there's no sense to argue with them. [...] Locals [authorities] want us to block. But it's not a question of desire, it's a question whether we want to make money. Some ISPs are still blocking only as per Roskomnadzor's official blocklists.[12]

This statement reveals that the inconsistent filtering across Crimea may not be just a result of technical limitations experienced by some providers but could also be due to administrative pressure imposed on Crimean ISPs by local officials. Notably, the activists we interviewed also confirmed the over-blocking tendencies we discovered in our tests and mentioned that the methods and block pages used for filtering vary across Crimean ISPs.[13]

Finally, we observed that in cases when Roskomnadzor demands restricting access only to select pages of select platforms, several Crimean and Russian ISPs tend block their entire domains by DNS. Given this approach, we believe that another reason for the over-blocking we detected in both territories may be the lack of proper filtering equipment by individual ISPs, or improper equipment set-up.

Ukrainian Media

Under Ukrainian rule, Crimea hosted a flawed but relatively pluralistic media environment.[14] Following Russia's annexation of Crimea in March 2014, however, popular Ukrainian channels were progressively substituted out for Russian broadcasters.[15] Attacks on local media dramatically

[12] This quote is from an April 20, 2018 interview of an employee of a Crimean Internet Service Provider who still works in the Crimean territory. For security reasons, the identity of this interviewee cannot be disclosed.

[13] See Table 6 in Appendix for comparison of over-blocking tendencies in Russia and Crimea.

[14] This was the case even though some of our interviews revealed that the Ukrainian media experienced some degree of influence from the oligarchy and there were a few attacks against independent media resources, before Maidan in 2013.

[15] Broadcasts from six Ukrainian TV stations were replaced with broadcasts from Russian channels ahead of the upcoming referendum in March 2014. Two months later, cable providers stopped airing most leading

increased and the independent Crimean media experienced pressure from the new authorities in an attempt to stifle pro-Ukraine media on the peninsula. Most journalists critical of the Kremlin left Crimea for mainland Ukraine, and those who remained often found themselves unable to work safely.

Just five months after the annexation, the Russian telecommunications monopolist Rostelecom started to provide traffic to the peninsula using a newly built submarine cable under the Kerch Strait. Following a short "transition period" given to Crimean ISPs to adapt to the new legislation and infrastructure, the Russian blocklist became mandatory on the peninsula and Roskomnadzor began monitoring if the 114+ local ISPs abide by the new regulations. Independent media, human rights groups, and anti-Russia movements were among the first resources to be blocked.

Similar to our findings on blacklisted Russian media outlets, we found the blocking of Ukrainian media to be inconsistent throughout Russia and Crimea. Online Ukrainian media that provided the Ukrainian point of view on issues such as the conflict with Russia, life in Crimea after the annexation, or the war in the pro-Russian separatist territories in the East (Donbass) were found to be blocked on an inconsistent basis.

Overall, our analysis revealed that the treatment of Ukrainian media by the Russian telecommunications authority is rather nuanced and varies from case to case. In terms of regulating access to Ukrainian content, we distinguished four categories of online resources (each of which is treated in a distinct manner). The first category consists of the group of popular Ukrainian TV channels (e.g., 1+1, 5TV, 112, 24 TV, and Ukrinform) that are not on Roskomnadzor's blocklist and are readily accessible in both Crimea and Russia. The second consists of Ukrainian news portals critical of the Kremlin (e.g., hromadske.ua), including those reporting on the events in Donbass (i.e. Donbass TV, Donbass News), for which access is not blocked by Roskomnadzor, nor restricted by local ISPs. The third category consists of Ukrainian media portals that are critical of the Kremlin (e.g., RBK Ukraine, Nova Rada, and Censor Net) and whose domains are listed in Roskomnadzor's registry of blocked resources. The fourth category consists of the group of independent media (e.g., Obozrevatel, Pravda.com.ua., and Segodnya.ua) for whom Roskomnadzor requires only select pages on their platforms to be blocked.

Of the 39 Ukrainian media portals on our test list, Roskomnadzor blocked access to the entire domains of 7 of them and restricted access to select pages for 17 others. The network measurements we collected from mainland Russia and Crimea, however, suggest that the actual availability of

Ukrainian-language channels. These acts significantly reduced the amount of televised Ukrainian-language content on the peninsula.

these resources is somewhat different on the ground. We also identified certain regional differences, with Crimean ISPs being more likely than their Russian counterparts to over-block Ukrainian media resources.

Table 4: Over-blocking of Crimean media by local ISPs

Crimean media	Roskomnadzor registry	Russian ISPs	Crimean ISPs
http://www.sobytiya.info/	blocked pages	domain accessible	14% block domain
http://www.blackseanews.net	blocked pages	10% block domain	57% block domain
http://meridian.in.ua/	not restricted	domain accessible	17% block domain

As shown in Table 4, we found Crimean ISPs tended to over-block also access to local Crimean media portals (e.g., Events of Crimea, Black sea news, and Meridian) and resources reporting on the conflict in Donbass. Although these platforms were blocked by certain Crimean ISPs (including the major ISP for the peninsula), they remained accessible in mainland Russia. In a few cases, blacklisted media platforms (e.g., Glavnoe UA) appeared to be accessible on many networks in both Russia and Crimea. Finally, as instructed by Roskomnadzor, certain news websites (e.g., Nova Rada, Censor Net, and RBK Ukraine) and investigative journalism projects (e.g., sled.net.ua) were uniformly blocked in both territories.

Tatar Minority Media

Crimean Tatars, indigenous to the peninsula since the 13th century, made up the majority of the population until the end of 19th century. Today, however, they constitute just 12% of the area's population. The media outlets of this minority served as an interesting case for our blocking analysis because most of them are vocal critics of the Kremlin's policies in the region, defenders of the rights of the Tatar minority and supporters of restoration of Ukrainian authority on the peninsula. Given these views, Russian authorities tried to silence critical Tatar media after the annexation of Crimea. This occurred through various means, including administrative hurdles, such as re-licensing procedures, and online censorship.

To test access to Tatar media in Russia and Crimea, we included the URLs of four major Tatar media platforms (*QHA, ATR, 15 Minutes, Meydan FM*) and their social media channels in our test list. Per Roskomnadzor's directives, ISPs are supposed to block the domain of just one popular Tatar news website (*15 Minutes*) and restrict access to certain pages of two others (*ATR* and *QHA*). Consistent with these orders, *15 Minutes* was not accessible on any of the Crimean ISPs we tested,

nor on 89% of the networks in Russia. However, instead of restricting access only to single pages on *QHA* and *ATR*, we found two Crimean ISPs chose to block their entire domains by DNS. These ISPs also blocked access to the Tatar news platform *Meydan FM* without any instruction to do so from Roskomnadzor. At the same time, the examined Tatar resources continued to be accessible in mainland Russia. These findings suggest that some Crimean ISPs tend to over-block Tatar resources on the peninsula.[16]

Table 6 in the Appendix summarizes the over-blocking incidents we detected in Crimea and Russia on days when measurements were collected simultaneously in both territories. Comparative analysis of the collected data reveals that over-blocking is more pronounced in Crimea than mainland Russia. Our qualitative survey determined that in some cases the over-blocking of liberal and critical content on the peninsula is most likely a result of technical limitations experienced by local providers. In other cases, however, it is a consequence of the deliberate actions of select ISPs after being asked by local authorities to block specific platforms.

In the meantime, we found the social media channels and video hosting resources of Tatar minority media to be freely accessible in both Russia and Crimea. This level of accessibility explains the tendency of targeted media in the region to migrate to foreign social media channels as their main content delivery platforms. Our interviews with Crimean Tatar journalists in exile revealed that they have developed strategies to bypass blocking by delivering content on popular platforms like Facebook or promoting usage of VPN technology among their Crimean audiences.

Finally, a new organization called "Crimean Solidarity" was created as a natural outcome of the blocking policies in place on the peninsula. The group regularly livestreams Crimean Tatar events (such as court hearings, rallies, gatherings, and celebrations), and organizes live reporting using social media (mainly Facebook). This amateur organization has become the main source of direct, on-the-ground information from Crimea for media outlets working from the Ukrainian mainland. Notably, because Crimean Tatars are among the most active critical content creators, they also run risks and are repeatedly arrested or subjected to device seizures for their "civic journalism" practices.

International Broadcasters

In April 2016, the Prosecutor General of Crimea sought to block Radio Liberty's *Krym Realii* website for publishing "extremist" posts and targeting the territorial integrity of the Russian Federation. In response, *Krym Realii* posted instructions on their website and Facebook page

[16] *See* Appendix, Table 5: Over-blocking of Tatar media by Crimean ISPs.

informing readers how to circumvent online censorship. The organization also put up information billboards near the border checkpoint between Ukraine and Crimea.

Access to *Krym Realii* was temporarily blocked several times in Crimea. During our tests, Roskomnadzor did not instruct access to *Krym Realii* or *Radio Free Europe/Radio Liberty*[17] to be restricted, and their platforms were found to be generally accessible on the networks of Russian and Crimean ISPs. We did, however, find one Crimean ISP that blocked *Krym Realii* by DNS, and one Russian ISP that blocked *Krym Realii* and *Radio Freedom* by http and tcp/ip.

Notably, even though *Krym Realii* has been removed from the block list and no court decision has been issued to block access to its website, some of our Crimean interviewees confirmed that their access to *Krym Realii* has been blocked. We came across other similar cases when specific resources were added and subsequently removed from Roskomnadzor's registry but still remain blocked on some networks. Our tests revealed that some ISPs implement Roskomnadzor's directives to block websites, but then fail to unblock access to those platforms upon their removal from the registry. This indicates that certain ISPs have the ability to implement filtering measures but may lack the necessary mechanisms to lift such measures after they are no longer required by Roskomnadzor.

VI. Conclusion

Our study set out to investigate whether the Russian presidential elections would affect Internet freedom in mainland Russia and Crimea, and whether Internet censorship is administered and experienced differently in the two territories. We found no empirical evidence to suggest that the elections caused filtering of critical or liberal resources in the examined regions. Platforms that were blocked before the elections remained inaccessible during and after them, and no other critical websites of the ones we tested were blocked specifically for this political event.

Notably, however, our research identified that Internet censorship is experienced differently in Russia and Crimea. The empirical evidence we collected during our study suggests that the blocking of critical content in both territories is not carried out in a uniform manner by all ISPs. By probing the accessibility of blacklisted platforms for political dissidents, critical media, minority groups, and human rights organizations, we determined that they may remain accessible on select

[17] Radio Free Europe/Radio Liberty (RFE/RL) is a United States government-funded organization that broadcasts and reports news, information and analysis to countries in Eastern Europe, Central Asia and the Middle East where it says that "the free flow of information is either banned by government authorities or not fully developed" (Wikipedia)

networks in both regions, resulting in under-blocking. In other instances, however, we determined that certain ISPs in Russia and Crimea tend to over-block access to critical platforms, as well as websites that are not blacklisted by Roskomnadzor. Comparative analysis of the collected data revealed this over-blocking to be more pronounced in Crimea where local ISPs, allegedly put under pressure from the local authorities, may restrict access to critical platforms - mainly Ukrainian and Tatar information websites.

Drawing upon the collected empirical and qualitative evidence, we conclude that Internet filtering is inconsistent across Russia and Crimea. This inconsistency of censorship practices in both territories has common and context specific explanatory factors. In mainland Russia, these are mainly the technical challenges experienced by a minority of operators who lack proper filtering equipment, may have misconfigured the latter or may refuse to block certain websites for ideological reasons. Such technical limitations are usually experienced by smaller providers who cannot afford the expensive technology for granular blocking (DPI). ISPs use various filtering systems and sometimes rely on custom-made installations, which may result in under-blocking or over-blocking, as indicated by our network measurements. Moreover, smaller ISPs in Russia may show critical attitude towards Internet censorship-related legislation for reasons that may be economic (due to high costs of filtering equipment) or technical (due to speed and quality loss associated with the filtering technology and the complexity of its maintenance) (Ermoshina, Musiani: 2017).

The over-blocking of critical resources in Crimea has additional factors that are unique for this territory. First, administrative pressure imposed by local authorities on ISPs can result in access to critical platforms being restricted beyond the specific requirements of Roskomnadzor. Our research revealed that the inconsistent blocking practices within Crimea can be attributed in part to some ISPs choosing to comply with these localized requests, and others choosing to disregard them. Second, the unavailability of some platforms and services on the peninsula has been found to be a consequence of the geo-blocking imposed by American and European companies as part of the sanctions against Russia for annexing Crimea. These sanctions have had a detrimental effect on both local ISPs and civil society groups who rely on Western services to pursue their liberal agendas. Following a new wave of sanctions, Google suspended its services in Crimea in January 2015. In September 2017, the distribution of Fedora Linux was banned on the peninsula because the program's developer (Fedora Project) is a U.S. legal entity whose products are subject to the export ban imposed under the U.S. trade embargo. According to recent research on CDN Geo-blocking (MC Donald et al., 2018), Crimea experiences particularly high rates of geo-blocking for finance and banking sites, as well as services like AirBNB, as a result of U.S. and E.U. economic sanctions.

These findings were confirmed by our interviewees and web-ethnography research.[18] From a digital security point of view, these sanctions have made it more difficult for users to access updates for privacy-enhancing technologies such as VPNs or secure messaging applications.[19]

As a type of international sanction, geo-blocking has had an impact on local IT markets (with important technical tools and platforms being rendered less accessible) as well as civil society (with activists experiencing a number of difficulties in attempting to receive regular software updates, download privacy-enhancing applications, and use other web-services important for their work). At times, the side effects of these sanctions seem to outweigh their actual economic impact on local Russian authorities, who continue to successfully operate in the area by creating "grey" ISPs and offshore IT companies. In such situations, Google sanctions are counter-productive in Crimea.

Finally, the specific censorship patterns in Crimea have been found to be affected by the distinctive Internet routing and infrastructure configuration on the peninsula. Interestingly, even though there is only one upstream provider that delivers Internet traffic to Crimea (Miranda-Media), the blocking that occurs in the region does so inconsistently across providers — suggesting that some of the blocking decisions are being made by local ISPs. The findings of our empirical research, backed by an independent study of our colleagues from the Digital Security Lab Ukraine and Crimean Human Rights Group, confirm that blocking in Crimea continues to be inconsistent today and varied across local ISPs. On some occasions, local ISPs fail to block access to online resources listed on Roskomnadzor's registry. On others, they restrict access to platforms that are not listed on the official blocklist. These findings suggest that either Miranda Media's upstream traffic is not arriving pre-filtered in Crimea, or that technical modifications of the filtering are being implemented at the local ISP level. Another survey needs to be conducted to determine the precise cause of these discrepancies. Such a survey should include additional measurements collected from the networks of multiple Crimean ISPs using a test list that includes "official" URLs blacklisted by Roskomnadzor, as well as "unofficial" URLs from the local Crimean blacklist.

Recommendations

The conflict between Russia and Ukraine over Crimea has transitioned into the Internet domain, resulting in a "censorship war" between both countries. The blocking of Ukrainian resources in Crimea and Russia has provoked the Ukrainian authorities to introduce a new list of Crimean media

[18] Several local ISPs admitted using sophisticated circumvention tricks in order to avoid the geo-blocking.
[19] For example, to carry out our network tests, we had to conduct a set of workarounds in order to distribute OONI probes to our testers or teach them how to use F-Droid.

with pro-Russian orientation which will be blocked on the Ukrainian mainland (President's Order #126/2018). According to our analysis of available OONI Probe data and additional tests run in Kyiv in January and April 2018, websites listed in Presidential Order 133[20] are inaccessible on the majority of Ukrainian networks we tested, with the exception of few providers. Another two blocklists proposed by the Ukrainian Security Service (including Russian TV channels and websites of pro-Russian governmental institutions in Crimea and Eastern Ukraine) have also been blocked inconsistently by Ukrainian ISPs.

We believe this "censorship war" may not be an adequate answer to the informational bubble in Crimea. Instead of copying the Russian approach to censorship, Ukraine could instead develop new approaches to reach out to Crimeans and support minority groups (e.g., Tatars), develop satellite Internet and local networks, promote censorship-resilient applications,[21] and encourage use of decentralized messaging solutions that are harder to block (such as Riot.im).

Accordingly, we offer the following recommendations:

1. More thorough controls should be administered on Crimean ISPs in relation to implementing online filtering. No arbitrary or extra-judicial blocking of content should be permitted. RIPE NCC and other expert organizations should collaborate to conduct a more thorough investigation of the traffic exchange and routing trajectories between the peninsula and the "outer world." Cases of collaboration between providers from Eastern Ukraine and those from Crimea should be investigated technically and legally.

2. The effectiveness of U.S. and E.U. sanctions with regards to online platform access should be reconsidered. By limiting Crimean citizen access to important services such as Google Play, Appstore, and others, these sanctions only raise the barrier of access to updates and privacy-enhancing technologies for civil populations, including activists and journalists (with ultimately little to no impact on Russian decision-makers and politicians).

3. To help citizens access censored content, more educational materials should be made available that promote the use of circumvention technologies. Social networks such as Facebook could be used to promote these materials (e.g., videos, gifs, illustrations, user-friendly guides). A white list of well-functioning VPNs in Crimea should be built. In addition, a digital security guide tailored to the Crimean context should be developed and enhanced by feedback from local testers regarding working aps on the peninsula.

4. Ukrainians from the mainland are getting little information about the life in Crimea. The volume of reporting related to Crimea on Ukrainian print and electronic media should be increased to maintain the connection between the Ukrainian mainland and the peninsula.

[20] Such as Vk.com, mail.ru, Ok.ru, Yandex.ru and its subdomains, drweb.ru, kinopoisk.ru, auto.ru.

[21] For example, the local RFE program "Krym.Realii" has implemented the libraries of Psiphon into the application to avoid potential blocking of service (Psiphon is a censorship circumvention tool that is popular in the region).

5. Ukrainian and Russian NGOs working on “Internet freedom” projects (e.g., Digital Security Lab in Ukraine, Roskomsvoboda in Russia) should collaborate to create a task force to monitor censorship, shutdowns, and surveillance cases on the peninsula. Such collaboration is necessary given the geopolitical and legal context in Crimea, where Russian citizens are able to gain easier access to the territory and encounter fewer obstacles when interacting with local institutions (e.g., observing court hearings, writing to the local administration, or defending Crimeans in court).

6. The procedures to gain access to Crimea from the Ukrainian mainland should be reviewed for potential modifications that would make it easier for international observers, journalists, human rights defenders, and researchers to visit the peninsula. The current procedure is overly complex and requires individuals to share important personal data with the Ukrainian immigration services and the Ministry of Occupied Territories, making it impossible to visit Crimea anonymously. The current procedure can also take considerable time (requiring, at times, more than a month for access to be granted), making it impractical for emergency situations.

7. Additional long-term research should be conducted on Internet traffic manipulation in the area, using OONI, RIPE atlas probes, IODA, and other tools. Given the recent modifications in Russian legislation in relation to promoting DPI as the main method for blocking, it would be interesting to check if any of these technical changes are already in use on Crimean networks.

Appendix

Table 1: ISPs failing to block *https* addresses

Input	Date	ISP 1	ISP 2	ISP 3	ISP 4	ISP 5	ISP 6	ISP 7	ISP 8
https://15minut.org/	18-03-18				accessible	accessible	accessible	accessible	accessible
https://glavnoe.ua/	18-03-18				accessible	accessible	accessible	accessible	accessible
https://graniru.org/	18-03-18				accessible	accessible	accessible	accessible	accessible
https://myrotvorets.center/	18-03-18		accessible		accessible	accessible	accessible	http-failur	accessible
https://or.team/	18-03-18				accessible	accessible	accessible	accessible	accessible
https://www.linkedin.com/	15-03-18	accessible		accessible					
https://www.linkedin.com/	21-03-18	accessible		accessible					
https://www.linkedin.com/	22-03-18	accessible		accessible					
https://www.ndi.org/	27-02-18	accessible	accessible						
https://www.ndi.org/	03-03-18		accessible						
https://www.ndi.org/	06-03-18	accessible	accessible						
https://www.ndi.org/	15-03-18	accessible		accessible					
https://www.ndi.org/	18-03-18	accessible			accessible	accessible	accessible	accessible	accessible
https://www.ndi.org/	21-03-18	accessible		accessible					
https://www.ndi.org/	22-03-18	accessible		accessible					
https://www.opensocietyfoundations.org/	27-02-18	accessible	accessible						
https://www.opensocietyfoundations.org/	03-03-18		accessible						
https://www.opensocietyfoundations.org/	06-03-18	accessible	accessible						
https://www.opensocietyfoundations.org/	15-03-18	accessible		accessible					
https://www.opensocietyfoundations.org/	18-03-18	accessible			accessible	accessible	accessible	accessible	accessible
https://www.opensocietyfoundations.org/	21-03-18	accessible		accessible					
https://www.opensocietyfoundations.org/	22-03-18	accessible		accessible					

Table 2: Consistency of blocking Russian online media in Russia and Crimea

URLs	Category	Roskomnadzor's Registry	Russian ISPs	Crimean ISPs
https://toneto.net/	Media Russia	not restricted	accessible	accessible
http://www.grani.ru	Media Russia	blocked	blocked 92%	blocked 80%
https://graniru.org/	Media Russia	blocked	blocked 90%	blocked
http://www.ej.ru/	Media Russia	blocked	blocked 88%	blocked 80%
http://ej.ru	Media Russia	blocked	blocked 86%	blocked 86%
http://utronews.org	Media Russia	blocked	blocked 79%	blocked
https://zona.media/	Media Russia	not restricted	accessible	accessible
https://tvrain.ru/live/	Media Russia	not restricted	accessible	accessible
http://www.ostro.org/general/world/news	Media Russia	blocked	blocked	blocked 80%
http://www.linkedin.com	Social Media	blocked	blocked 91%	blocked 83%
https://www.linkedin.com/	Social Media	blocked	blocked 95%	blocked
https://twitter.com/GraniTweet	Social media - Grani	not restricted	accessible	accessible
https://vk.com/grani_ru	Social Media - Grani	not restricted	accessible	accessible
https://www.facebook.com/GraniRu/	Social Media - Grani	not restricted	accessible	accessible
https://twitter.com/kasparovru	Social media - Kasparov	not restricted	accessible	accessible
https://www.facebook.com/Kasparov.Ru	Social Media - Kasparov	not restricted	accessible	accessible

Table 3: Over-blocking of Ukrainian media by Crimean ISPs

Ukrainian media	Roskomnadzor's registry	Crimean ISP N1	Crimean ISP N2	Crimean ISP N3	Crimean ISP N4
http://espreso.tv/	blocked page	domain accessible	blocks domain http-diff	blocks domain by DNS	blocks domain by DNS
http://glavcom.ua/	blocked pages	blocks domain by DNS	blocks domain http-failure	blocks domain by DNS	blocks domain by DNS
http://maidanua.org/	blocked page	domain accessible	domain accessible	blocks domain by DNS	blocks domain by DNS
http://uainfo.org/	blocked pages	domain accessible	blocks domain http-diff	no data	no data
http://www.sobytiya.info/	blocked pages	domain accessible	blocks domain http-diff	domain accessible	domain accessible
https://hromadskeradio.org/	blocked page	blocks domain by DNS	blocks domain http-failure	blocks domain by DNS	blocks domain by DNS
https://www.pravda.com.ua/	blocked pages	domain accessible	blocks domain http-failure	blocks domain by DNS	blocks domain by DNS
https://www.segodnya.ua/	blocked pages	domain accessible	domain accessible	blocks domain by DNS	no data

Table 5: Over-blocking of Tatar media by Crimean ISPs

Tatar minority media	Roskomnadzor's registry	Russian ISPs	Crimean ISPs
http://qha.com.ua/	blocked page	domain accessible 90%	domain accessible 71%
http://atr.ua/	blocked page	domain accessible 96%	domain accessible 83%
https://atr.ua/	not restricted	domain accessible 88%	domain accessible 71%
https://15minut.org/	blocked domain	domain accessible 11%	domain accessible 0%
http://meydan.fm/ua	not restricted	domain accessible 92%	domain accessible 71%
https://www.youtube.com/c/ATRChannel2015	not restricted	accessible	accessible
https://twitter.com/ATR__Official	not restricted	accessible	accessible
https://www.facebook.com/15minut.kiev/	not restricted	accessible	accessible
https://twitter.com/15_minut	not restricted	accessible	accessible
https://www.facebook.com/atr.channel	not restricted	accessible	accessible

Table 6: Comparison of over-blocking tendencies in Russia and Crimea

URLs	Category	Roskomnadzor's registry	Russian ISPs	Crimean ISPs
http://www.sobytiya.info/	Media Crimea	blocked pages	accessible	accessible 86%
http://www.blackseanews.net	Media Crimea	blocked pages	accessible 90%	accessible 43%
http://meridian.in.ua/	Media Crimea	not restricted	accessible	accessible 83%
http://qha.com.ua/	Media Tatar	blocked page	accessible 90%	accessible 71%
http://atr.ua/	Media Tatar	blocked page	accessible 96%	accessible 83%
https://atr.ua/	Media Tatar	not restricted	accessible 88%	accessible 71%
http://meydan.fm/ua	Media Tatar	not restricted	accessible 92%	accessible 71%
https://www.segodnya.ua/	Media UA	blocked pages	accessible 92%	accessible 83%
http://maidanua.org/	Media UA	blocked page	accessible 90%	accessible 71%
https://investigator.org.ua/	Media UA	blocked page	accessible	accessible 75%
http://uapolitics.com/	Media UA	blocked page	accessible	accessible 80%
https://www.eurointegration.com.u	Media UA	not restricted	accessible	accessible 86%
http://www.stb.ua/	Media UA	not restricted	accessible	accessible 86%
http://espreso.tv/	Media UA	blocked page	accessible 90%	accessible 57%
https://www.pravda.com.ua/	Media UA	blocked pages	accessible 89%	accessible 71%
https://www.obozrevatel.com/	Media UA	blocked page	accessible 89%	accessible 71%
https://112.ua/	Media UA	not restricted	accessible	accessible 86%
http://novy.tv/	Media UA TV	not restricted	accessible	accessible 86%
http://ictv.ua/	Media UA TV	not restricted	accessible	accessible 86%