DGAPkompakt

Nr. 3 / March 2019

Security First, Technology Second: **Putin Tightens his Grip on Russia's Internet – with China's Help**

Andrei Soldatov

Since his return to the Russian presidency in 2012, Vladimir Putin has sought to bring the Russian internet under his control. Digital businesses in Russia pay dearly for his expensive system of surveillance and censorship. This slows down the pace of innovation and puts the modernization of the economy at risk. Even then, technical control over the internet remains shaky. The Kremlin is seeking Chinese assistance to enforce restrictions and be able to cut Russia off from the global internet.

In 2011, the Arab Spring – largely organized through Twitter – demonstrated the power of the internet to help galvanize revolutions. Later that year, street-led protests also erupted in Moscow and other Russian cities. There, it was Facebook that played a crucial role in bringing tens of thousands of people together to protest against Vladimir Putin's return to the presidency. Frightened by the force of social media to organize the masses, Putin reacted quickly. In June 2012, just one month after he had taken office as president again, the Kremlin unleashed a program of internet censorship.

An Indiscriminate Blacklist

The State Duma, the lower house of parliament, introduced legislation for a nation-wide system of online filtering in 2012. Under the pretext of protecting children, a register of banned sites – essentially a black list – was created, which grew dramatically over the following seven years. It now consists of a large collection of lists drawn up by several government agencies, ranging from media sites openly critical of the government to online casinos, web pages with information about suicide, and cartoons.[1]

There are three government agencies involved in maintaining the register: Roskomnadzor (the Agency for the Supervision of Information Technology, Communications and Mass Media), the Interior Ministry, and the Federal Service for the Supervision of Consumer Rights and Public Welfare. All three submit data for the government's blacklist of sites. Roskomnadzor is in charge of compiling and updating the register and instructing host providers to remove the URLs. If the host provider does not react, the Internet Service Providers (ISPs) are required to block access to the site within twenty-four hours. The host providers must ensure that they are not in breach of current laws by checking their contents against the database of outlawed sites and URLs published in a special password-protected online version of the register open only to web hosts and ISPs.

Russia's regional courts very actively support the government's censorship. For the last seven years, they have rubberstamped decisions to block or take down websites with political commentaries critical of the Kremlin, Wikipedia articles, information on corruption and gossip, or even Japanese anime. By October 2018, more than 4 million websites had been permanently blocked according to the watchdog Roskomsvoboda, an NGO founded in 2012 to counter internet censorship. Most of them are victims of collateral damage because the Russian filtering system works through IP addresses, each of which can host thousands of sites. All these sites get blocked even if one single website is placed onto the register.[2]

The system is unable to discriminate between sites because internet filtering was not embedded into the Russian internet from the start. This is different from China where the censorship system was incorporated from the very beginning in the mid-1990s. To add censorship measures to an existing telecommunication infrastructure is technically very challenging.

Making Digital Businesses Pay

Russia has made the internet companies responsible by law for implementing the filtering rules. This includes carrying the costs: Companies are required to buy and install filtering equipment and constantly update it. They must also check and download the voluminous blacklist of banned IP addresses and domain names on a daily basis. These tasks are becoming ever more expensive as technology develops and new equipment is needed. In addition to banning pages and websites, companies are now required to patrol social messengers and block individual accounts on social media and videos on platforms such as YouTube.

The government is also keen to ensure that its intelligence services can continue to spy on users. Telecom companies are required to buy and update equipment for the national program of online surveillance known as SORM (System of Operative Research Measures).[3] This includes providing the data storage facilities required by what is known as the Yarovaya law: Since 2018, Russian internet and telecom providers have been obliged to store all data of all users for six months and metadata for three years.[4]

Making the companies pay for censorship and surveillance has a double advantage for the Kremlin: Not only is it cheap, but it also gives the authorities a powerful stick to assert their dominance over the IT industry. Companies can face hefty fines and even lose their telecom license if they fail to meet requirements that are often kept intentionally vague. In the face of this threat, large telecom companies tend to consult with the Kremlin on a frequent basis. This, in turn, gives officials leverage over the companies who are hardly in a position to refuse a favor if and when asked.

Security First, Technology Second

In 2019, the major Russian telecommunications companies are expected to start investing into 5G networks. They will, however, be slowed down by the need to spend an additional 200 billion rubles (3 billion US dollars) on updating the Russian surveillance program.[5] The Yarovaya law requires a massive expansion of data storage facilities paid for by IT and telecom companies. At the same time, the Russian secret services demand direct and remote (backdoor) access to the servers without alerting telecom personnel to the kind of information they extract. This same system is replicated on all levels, from Moscow to the regions and from national telecom companies to university-run local networks.

In Russia, security comes first, technology clearly comes second – and the national security concerns of the Russian leadership and security services outweigh the risk of slowing down the pace of technological innovation. This approach to controlling the cyber space is reflected by the updated Information Security Doctrine which was signed by President Vladimir Putin in December 2016.[6] The authors of the doctrine state that “the practice of introducing information technologies without first providing for information security” increases risks. As far as they are concerned, telecom and IT companies should always consult with the secret services ahead of introducing new services and technologies for their customers.

The doctrine refutes the very essence of the modern information society: the free flow of information across borders. “The possibilities of cross-border flow of information are used increasingly for geopolitical or military-political goals,” the document states in a thinly veiled hint at so-called twitter revolutions.[7] Accordingly, Russian legislation gives the government primacy over the cross-border fiber-optic cables and internet exchange points that constitute the architecture of the internet.

Crowding Out Small IT Companies

Big telecom companies like long-distance national operators and mobile phone operators can at least approach the Kremlin and the government and ask for clarification of the legislation. This option is out of reach for small and medium-sized ISPs, the companies which provide internet connections for users in cities and towns. They are kept in the dark about the future government plans and find themselves at the mercy of local government supervisors – the regional branches of the internet censorship agency Roskomnadzor – and the Russian secret services.

This is detrimental for business, and as a result, more and more ISPs are leaving the market – precisely those small and medium-sized providers which most strongly resisted the government's attempts to censor the internet. Many of these companies were founded by enthusiasts and entrepreneurs without any ties to Soviet-era regional telecom operators with traditionally close links to the secret services. As the independent regional providers disappear, major telecom companies – those who have learned the hard way to please the Kremlin – are filling the void.

Several of Russia's leading online businesses are now considering selling out to state-controlled companies. One example is Yandex, a paragon of the Russian internet economy and highly successful Google competitor (in September 2018, Yandex held 52.87 percent of the market share of search engines in Russia, compared to 43.32 percent for Google)[8]. It is well-connected, too: Herman Gref, the chief executive of Russian state-owned Sberbank, has been a member of the Yandex board since 2014. But while this might have been sufficient five years ago to ensure an effective level of protection from state intervention, it is no longer the case today. According to a report published in October 2018, Yandex is holding talks with Sberbank to cede to the latter a 30-percent stake in the company. Following that publication, Yandex's shares lost nearly 2 billion US dollars on the stock exchanges in Moscow and New York.

Targeting the Users

For the first several years, the Kremlin chose not to focus its censorship measures on the millions of internet users in Russia. Instead, it concentrated on forcing internet services companies into compliance. This seemed a wise choice: There are only a few thousand internet businesses, all of them required by law to comply with government requests. In addition, they can be made to carry the cost of censorship, surveillance, and patrolling the internet. Finally, incarcerating users for infringing censorship laws would have had an adverse effect on the government's image.

In 2016, however, as tensions with the West rose, the Kremlin's outlook changed. The wave of patriotism which emerged in response to Western sanctions allowed Russian law enforcement a free hand. It turned to repression against users, prosecuting alleged online extremism. Today, the majority of cases come via VKontakte, which reportedly readily surrenders data to the authorities. Convictions under laws against extremism have increased fourfold since 2011, with 604 people convicted in 2017.[9] Nine out of ten convictions for extremist speech in Russia in 2017 were based on comments made online, according to Maria Kravchenko, an expert with the human rights group "SOVA Center" which tracks hate crimes.[10]

A particularly troubling aspect is the randomness of these repressive measures which can be triggered by anything from a post about Ukraine to the Orthodox Church or regional officials to entirely innocent comments. The goal appears to be to keep everybody in the unknown about what is or is not allowed. The effect on the public debate is clearly noticeable: Russians have become much more cautious about expressing their opinions online.

Yet, not everybody complies. When an officer of Putin's National Guard recently released a YouTube video challenging opposition politician Alexei Navalny to a duel in an attempt to intimidate the latter, hundreds of users mocked his video, and in turn challenged the officer to a duel – in swimming, boxing, and so on. Another example is the Russian blogosphere's lively reaction to the Salisbury affair. State-owned television RT interviewed two men identified by the British government as suspects in the poisoning of a former Russian military intelligence officer in Salisbury. On television, the two men claimed to be innocent tourists and lovers of gothic cathedrals, but their statements came across as awkward and contrived. The interview became the most discussed topic online, with memes created and shared by thousands. Netizens even composed songs about the two suspects which were widely circulated.

In the Russian context, it is important to remember that the internet was designed as a technology for spreading information, not for repressing it. On social media in particular, most content is generated by users rather than by the companies running the platforms. Important events can lead to such an upsurge of user-generated content that government censorship is bound to fail. A system designed to control a few troublemakers will not be able to handle massive volumes of content generated by hundreds of thousands of users.

An Ambiguous Relationship with China

Russia is very ambiguous about providing Chinese officials and companies with access to its digital infrastructure. Yet, it has repeatedly sought the help of China – the world leader in cyber and surveillance technology – to overcome the technical difficulties of controlling the internet in Russia. Even today, Russia's methods of censoring are not very sophisticated. The internet filters can be outfoxed by simple tools in order to access banned information – in most cases, Google Translate is sufficient to achieve this. In any event, a considerable share of sensitive data is out in the open – be it about the Russian military presence in Ukraine and Syria, corruption scandals, or videos of Russian opposition leader Alexei Navalny. Technically, it has proven impossible to block all copies of any particular video.

In 2015, the Kremlin started to cooperate with the Chinese government to deal with the technical problems. A string of high-level meetings in Beijing and Moscow served to develop a new strategy to control the internet. In April 2016, top Chinese officials and their Russian counterparts gathered in Moscow for a cybersecurity forum. The secretary of the Security Council, Nikolai Patrushev, then held two meetings on information security with members of the Politburo of the Chinese Communist Party. In June 2016, Putin went to Beijing to sign a joint communiqué about cyber space.

The Russian side urgently desired technology from China, and the Kremlin saw no alternative to inviting Chinese heavyweights into the heart of its IT strategy. "China remains our only serious 'ally', including in the IT sector," said a source in the Russian information technology industry, adding that despite hopes that Russian manufacturers would fill the void created by sanctions, "we are in fact actively switching to Chinese [equipment]."

Bulat, the Russian telecom equipment manufacturer, started talks with Huawei, the Chinese telecom company, to buy data storage technology and to produce servers capable of implementing the Yarovaya law. The Chinese officials also ensured senior Huawei staff were present at key information security conferences in Russia.[11] Then, suddenly, cooperation ceased. The Russian security services became extremely cautious of allowing Chinese experts such deep access to Russian communications and feared to become heavily dependent on Chinese hard- and software. For a period of time, the stalemate seemed insurmountable.

Chinese-Russian Joint Ventures

It took until 2018 for the Kremlin to find a new solution. In September 2018, Mail.Ru, a large internet holding owned by Alisher Usmanov, a Russian tycoon with close ties to the Kremlin, announced a joint venture with China's largest e-commerce firm, Alibaba Group Holding Limited. The deal had received the Kremlin's blessing – as part of the agreement, the Russian Direct Investment Fund would invest an undisclosed amount of money in the newly-formed organization. Alibaba would hold 48 percent of the business; 24 percent would go to MegaFon, the second largest mobile phone operator in Russia, also under Usmanov's control; 15 percent to Mail.ru: and the remaining 13 percent would be allocated to Russian Direct Investment Fund. In addition, MegaFon has agreed to trade its 10-percent-stake in Mail.ru worth around 500 million US dollars to Alibaba. That would give the joint venture a valuation of around 2 billion dollars.[12]

The Mail.Ru holding controls most of the Russian social media – social networks like VKontakte, Odnoklassniki, and the country's most popular email service Mail.Ru. The deal between Mail.Ru and Alibaba grants China access to the data of the users of these services,[13] raising privacy concerns. At the same time, Usmanov is building up another holding called "Citadel" which already owns more than half of the Russian market for devices used in Systems of Operative Research Measures (SORM).[14] A surveillance equipment supplier which dominates the market and has the backing of a giant Chinese partner could make significant progress in solving the technical issues of control and surveillance.

Russia's two largest internet companies, Mail.Ru and Yandex, have been co-opted to support Russia's new Digital Sovereignty Law.[15] This Chinese-inspired legislation is supposed to introduce a technical system capable of cutting the country off from the global internet. There is another development which shows how similar both countries are becoming in their approach to controlling the internet. In the fall of 2018, the Kremlin activated its Russian "cyber brigades," which are groups of online vigilantes encouraged by the government. In December, Moscow decided that regional cyber brigades coordinate their activities with the Russian internet censorship agency Roskomnadzor. This move to combine government and pro-government civic activities is highly reminiscent of the Chinese approach.

But even in a worst-case scenario, it may not be possible for the Kremlin to fully implement the Chinese approach to the internet in Russia. Unlike China, the Russian internet was not built to include a system of surveillance and censorship from the beginning. Russia has far too many cross-borders channels, small and medium-sized internet service providers, and users who have not been trained to comply with the official line.

Mimicking the West

Internet regulation has become an essential part of the Kremlin's domestic agenda as well as its foreign policy. China now is its closest ally in the cyber domain. The two countries jointly promote the concept of digital sovereignty, according to which governments should have a free hand in controlling their national segments of the internet. That said, both Russian and Chinese leadership understand perfectly that this idea of censorship is difficult to sell to a global audience. Therefore, they are mimicking the language and terminology used by many European countries after the revelations of National Security Agency (NSA) whistleblower Edward Snowden in 2013.

It played into the Kremlin's hands when, upon discovering that the NSA had monitored her cell phone, German chancellor Angela Merkel suggested in February 2014 to build a European network that would keep data from passing through US servers. The language used in Germany and France to express reservations towards US intelligence agencies was quickly copied by Russia and other authoritarian countries. In Russia, doing so had a two-fold objective: firstly, to signal to their local user communities that Moscow was pursuing a similar line to European policies; and secondly, to try to win new allies in Europe. European policymakers should be well aware of this effect.

Conclusion

Over the past seven years, the Russian government has employed various methods from censorship and surveillance to the intimidation of internet companies to tighten its control over the internet. The Kremlin undoubtedly considers the costs of control insignificant compared to the costs of political instability – even if this means slowing down the pace of innovation in Russia's digital economy. Close cooperation with China increases its technical capabilities to restrict the freedom of internet. But just how much control the Kremlin is willing to relinquish to Chinese companies in order to better control Russian society will remain the key question for the years to come.

Andrei Soldatov is a Russian journalist, security services expert, founder and editor of the Agentura.Ru.

Notes

[1] "Internet Censorship Skyrockets in Russia in 2017, Study says," *The Moscow Times*, February 05, 2018 <https://themoscowtimes.com/news/internet-censorship-skyrockets-in-russian-in-2017-study-says-60389> (accessed February 14, 2019).

[2] Statistics of site blockings by Russian agencies, Roskomsvoboda Censorship watchdog <https://reestr.rublacklist.net/visual/> (accessed February 14, 2019.

[3] Irina Borogan and Andrei Soldatov, *The Red Web. The Kremlin's Wars on the Internet* (New York 2017).

[4] "Russia's 'Big Brother' Law Enters Into Force," *The Moscow Times*, July 1, 2018 <https://themoscowtimes.com/news/russias-big-brother-law-enters-into-force-62066> (accessed February 14, 2019).

[5] "Zakon Yarovoy soberet dividendi" [The Yarovaya law will collect dividends], *Kommersant*, p. 9, October 12, 2018.

[6] Kremlin, Information Security Doctrine of Russia approved, December 6, 2016 <http://kremlin.ru/acts/news/53418> (accessed February 14, 2019).

[7] Kremlin, Decree of the President of the Russian Federation of 05.12.2016, no. 646, On approval of the Information Security Doctrine of the Russian Federation, December 5, 2016 <http://static.kremlin.ru/media/acts/files/0001201612060002.pdf> (accessed February 14, 2019).

[8] Search Engine Market Share Russian Federation Feb 18 - Feb 19, StatCounter <http://gs.statcounter.com/search-engine-market-share/all/russian-federation> (accessed March 1, 2019).

[9] Andrew Roth, "The Guardian, Young Russians posting memes face jail for 'extremism'," *The Guardian*, September 1, 2018 <https://www.theguardian.com/world/2018/sep/01/young-russians-posting-memes-face-jail-for-extremism> (accessed February 14, 2019).

[10] Ibid.

[11] Irina Borogan and Andrei Soldatov, "Putin brings China's Great FireWall to Russia in cybersecurity pact," *The Guardian*, November 29, 2016 <https://www.theguardian.com/world/2016/nov/29/putin-china-internet-great-firewall-russia-cybersecurity-pact> (accessed February 14, 2019).

[12] Jon Russel, "Alibaba goes big on Russia with joint venture focused on gaming, shopping and more," *Techcrunch*, September 11, 2018 <https://techcrunch.com/2018/09/11/alibaba-russia-mail-ru/> (accessed February 14, 2019).

[13] See the interview of the chief of Russia's operations of Alibaba in RBC, October 22, 2018 <https://www.rbc.ru/technology_and_media/22/10/2018/5bc85bf39a79470c88b43b21> (accessed February 14, 2019).

[14] "Wiretapping Citadel: how FSB and Interior Ministry generals will help Usmanov's partner," *RusLETTER* <https://rusletter.com/articles/wiretapping_citadel_how_fsb_and_interior_ministry_generals_will_help_usmanovs_partner> (accessed February 14, 2019).

[15] "Mail.Ru Group i 'Yandex' podderzhali zakon o suverennom Runete" [Mail.Ru Group and Yandex supported the law on sovereign Runet], *Secret Firmi*, January 17, 2019 <https://secretmag.ru/news/mail-ru-i-yandeks-podderzhivayut-ideyu-suverennogo-runeta-17-01-2019.htm> (accessed February 14, 2019).

DGAP
Deutsche Gesellschaft
für Auswärtige Politik
German Council on
Foreign Relations

The opinions expressed in this publication are those of the author and do not necessarily reflect the views of the German Council on Foreign Relations (DGAP).

Rauchstraße 17 / 18 · 10787 Berlin
Tel. +49 (0)30 25 42 31 -0 / Fax -16
info@dgap.org · www.dgap.org

Publisher *DGAP e.V.*
ISSN 1611-7034

Editing Eva-Maria McCormack, Hanna Bianca Krebs
Layout Reiner Quirin
Design Concept Carolyn Steinbeck · Gestaltung