PONARS Eurasia
NEW APPROACHES TO RESEARCH AND SECURITY IN EURASIA

To Hack Abroad and Ban at Home

THE KREMLIN'S CYBER ACTIVISM

PONARS Eurasia Policy Memo No. 558
December 2018

Alexandra Yatsyk[1]
Polish Institute of Advanced Studies, Warsaw

Russia has been playing a multi-fold game in the digital arena. It engages in international cyber attacks, spreads select narratives strategically overseas using the open media rules of Western societies, and simultaneously restricts, piece-by-piece, independent media and individual Russian voices at home. Russian domestic and international cyber policies can be manifested through several recent cases. First, Russia's state-sponsored, disruptive, cyber activities abroad are analyzed, including those that targeted the U.S. political system in 2016. Second, a close look is given to the Russian government's increasingly restrictive policies concerning online freedoms at home, with a focus on the recent actions taken against the Telegram instant messaging application. It becomes clear from these situations that the Kremlin employs strategies of hacktivism and digital isolationism in pursuit of its policy goals. The tactics have worked, to some extent. Even though the government could not eradicate Telegram, many Russians are engaging in a degree of online self-censorship. Also, some Western societies have indeed been influenced by Russian social media campaigns; however, foreign influence gains are short-term at best because Western societies have begun to take protective measures against digital intrusions.

To Talk

For all the controversy that the first U.S.-Russian presidential summit in Helsinki in July 2018 generated, it was noteworthy with regard to President Vladimir Putin's brief mention of the idea of a U.S.-Russian cybersecurity task force. To be sure, this was floated a year earlier by U.S. President Donald Trump. In a July 9 Tweet, Trump noted that the two sides discussed the creation of "an impenetrable Cyber Security unit" to safeguard against election hacking. However, only a few days later, in what has become a fairly familiar pattern of reversals, Trump appeared to backtrack on this idea,

[1] Alexandra Yatsyk is Visiting Fellow at the Polish Institute of Advanced Studies in Warsaw, Poland.

indicating that the two leaders only had basic discussions. The Russian government has been pushing for talks on cyber security with the United Stated for some time now. On July 19, Putin's Envoy for International Cooperation in Information Security Andrei Krutskikh revealed that the U.S. government offered apologies for not sending a group of experts to cyber security talks that were supposed to take place in Geneva in February 2018.

Paradoxically, even as the U.S. intelligence community pointed fingers directly at the Russian government in January 2017 accusing it of interfering in the U.S. presidential election in 2016, this has done little to dissuade the Kremlin from entertaining an ambitious cyber security cooperation agenda with the United States (both bilaterally and multilaterally). An example on the global level is when the director of Russia's Federal Security Service (FSB), Alexander Bortnikov, on October 4, 2018, called for the establishment of an international legal regime that would ban the development of harmful computer software.

To Hack

On July 2, 2018, the *Wall Street Journal* revealed that Russian state-sponsored hackers had gained access to the online control centers of American power companies in 2017. The public admission in the article from officials indicated that the U.S. government had been alarmed and wanted the public to know the gravity of the situation, particularly as the U.S. midterm elections approached. The threat of Russian cyber mischief loomed large in the U.S. midterms. To allay public concerns, and growing criticism from the Democrats over the White House's inaction and lack of coherent policy responses, Trump briefly met with the National Security Council (NSC) on July 27, 2018, to discuss election security. Some preparations were made, including the allocation of $348 million from the federal Election Assistance Commission in early July to help states prepare for possible cyber intrusions during the midterms.

The day before Trump met with his NSC staff, Senator Claire McCaskill (D-Missouri), one of the fiercest critics of Putin, revealed that her office had been under unsuccessful cyber attacks that very year. McCaskill's statement is consistent with the assessment of Microsoft's Vice President for Customer Security and Trust Tom Burt, who acknowledged that at least three congressional campaigns were being targeted by Russian hackers in the run-up to the midterm elections. Moreover, speaking at a Hudson Institute event on July 13, Director of National Intelligence Dan Coats had acknowledged that the U.S. "digital infrastructure" was "literally under attack" and that the country was at a "critical point."

Indeed, it appears that the Russian government uses a wide range of cyber tools to undermine democratic political processes in the West, from troll farms to highly skilled hacker groups such as Energetic Bear (also known as DragonFly, Koala, and Iron

Liberty). One of the most well-documented recent cases of Russian cyber attacks was the NotPetya ransomware attack that mainly affected Ukraine in June 2017 and was blamed by both the United States and the UK on Russia. On October 11, 2018, Ukraine's Security Service (SBU) issued a press release about renewed attempts by the Russian special services to gain unauthorized access to Ukraine's critical infrastructure through the Industoyer virus.

Other recently revealed cases demonstrate that Russia's malicious cyber activities are not limited to targeting political processes and critical infrastructure, but are also employed against international organizations and laboratories. On October 4, 2018, the Dutch government revealed that four Russian military intelligence (GRU) operatives were expelled in April after they tried to remove equipment they had planted earlier that was geared to hack the Organization for the Prohibition of Chemical Weapons (OPCW) in The Hague. Subsequently, the Dutch authorities went further when on October 14 Defence Minister Ank Bijleveld admitted that the Netherlands was in a state of cyber war with Russia. Also, in July, the Swiss media reported that GRU-affiliated hackers from the group Sandworm unsuccessfully tried to hack into the government laboratory in Spiez, Switzerland, that had tested the samples of the Novichok nerve agent used in the Skripal poisonings in Salisbury, UK. In September, the thwarted hacking attempt against the Spiez laboratory was officially confirmed and linked to the GRU by the Swiss Federal Intelligence Service (NDB).

None of this appears to have fazed the Russian leadership. Against this backdrop of mounting evidence against Moscow, Russian officials and Putin himself emphatically and repeatedly deny state involvement in cyber attacks, as Putin did to Trump in Helsinki.

To Ban

The Russian government's aggressive approach to exploiting cyber vulnerabilities in other countries sharply contrasts with draconian restrictions of online freedoms at home. In May 2018, Maria Motuznaya, a 23-year-old native of Barnaul, faced up to six years in prison on accusation of extremism for posting memes on the Vkontakte social media platform.[2] The authorities claimed that these memes were insulting to the religious and racial feelings of two Russian citizens. Several satirical pictures with Orthodox priests and Jesus Christ, which she (re)posted in 2016 were deemed sufficiently offensive to charge her under Article 282 of the Criminal Code (which targets hate speech). Motuznaya was indicted for supporting extremist activity, although she suggested the real reason for her prosecution was her volunteer work for opposition leader Alexey Navalny. Motuznaya left Russia for Ukraine in October 2018 after the Barnaul district

[2] See: "Prosecuted 'for Words': Will Putin's Amendment Have a Liberalizing Effect?," Point & Counterpoint, PONARS Eurasia, October 2018.

court announced it would return her case to the local prosecutor's office. Another very similar case, also in Barnaul, is that of Daniil Markin who, in 2017, faced the same accusations as Motuznaya. Markin had posted memes involving John Snow, a popular television character in Game of Thrones, with a halo around his head, which apparently was offensive enough for the state to charge him with extremism.

There are many more cases. Most have involved Vkontakte, which was developed and run by Pavel Durov, who himself was forced to relinquish it in 2013 due to a major conflict with the Federal Security Service over content and control issues. Fearing a public backlash from such cases of wonton online censorship, on October 3, 2018, Putin decided to soften digital enforcement procedures by making any user's first violation only an "administrative offense," which entails fines, community service, or a short-term prison sentence. The punishments were more severe previously, such as larger fines (from 300,000 rubles to 500,000 rubles), forced labor for up to four years, or prison for two to five years. In blogger Motuznaya's circumstance, the Barnaul court returned her case to the prosecutor's office "for further investigation," which her lawyers took as a positive sign and possibly a result of Putin's decree on the partial decriminalization of the relevant Article 282.

This past April, Russian Internet regulator Roskomnadzor unsuccessfully attempted to ban Telegram, a popular instant messaging application and another of Durov's products. This demonstrated the emergence of two dominant trends in the Russian government's domestic cyber policy in the foreseeable future.

First, the Kremlin will intensify its surveillance of online activities with an increasing focus on young audiences. The participation of the so-called "Putin generation"—those who have only known life in Russia under Putin's leadership—in the anti-government protests of March 2017 showed that this segment is most active among Navalny's supporters and they tend to organize and communicate online, preferably on Telegram. This alarms the Russian authorities and led to the Expert Institute of Social Studies, a think tank with ties to the Presidential Administration, to embark on finding new ways to communicate with youths through digital media. In addition, in May 2017, Deputy Head of the Presidential Administration Sergei Kirienko appointed Maksut Shadayev, former head of information technologies for the Moscow region, his adviser for coordinating the public relations policy of regional authorities in social networks.

Second, the Russian government's failure to ban Telegram revealed its current technical and financial limitations in enforcing sweeping online restriction, while also showing that the government is willing to let Russian companies, even those in economic growth sectors like Internet companies, experience financial difficulty.

As early as 2014, Russia's Security Council instructed several state ministries, including the Ministry of Communications, to take measures to ensure the security of Russia's

internet infrastructure. In May 2016, Roskomnadzor revealed amendments to the state program "Information Society," which included the goal of having 99 percent of Russian internet traffic "transmitted domestically" by 2020 (it was at 70 percent in 2014). Also, the so-called "Yarovaya law" entered into force on July 1, 2018, that obliges all social platforms and instant messengers operating in Russia to provide the Federal Security Service access to the private conversations of users. Finally, there is the government's new 3 billion ruble ($48 million) program on "Cyber Economy" that was launched this past spring. It entails funding for upgrading information technology infrastructure, the creation of research competencies, and information security.

For its part, Telegram has been testing its Telegram Open Network blockchain platform with plans to have it operational before this year is over. Although this platform is geared for creating "a new decentralized economy," its parameters might seriously undermine the Kremlin's plans for total surveillance of the Russian digital discussion space. Russia's failures at reigning in Telegram indicate that the Kremlin's plans of creating a Russian version of China's "Great Internet Firewall" are not fully succeeding (probably due to the significant costs involved). Instead, the authorities have been utilizing the haphazard "Iranian model" of content policing by relying primarily on the courts. This approach tends to result in draconian punitive measures against citizens, often of specific people in a publicized way, in order to send, ironically, a message from the government to the masses.

Nonetheless, establishing some sort of comprehensive control remains an overarching objective for Moscow's Internet regulators. This was evident at the first meeting of the newly created Council on Digital Economy, held by the Federation Council (the upper house of the Federal Assembly) on August 1 of this year. Russia's telecoms minister, Konstantin Noskov, revealed that his ministry is drafting framework laws that would implement uniform requirements related to identifying citizens online. Obviously, the authorities will continue to try to establish comprehensive digital surveillance over those in Russia.

To Conclude

In foreign affairs, the Russian government has used, and continues to use, the West's free press and freedoms of expression to spread its policy preferences among both targeted and mass-market audiences. When there are attempts to characterize any of the content as Kremlin propaganda, the "free press" tactic is usually employed, as seen by Margarita Simonyan's retorts regarding criticisms of Russia Today.

Russia is playing a double card. If the West does not tighten its digital landscape, Russia will continue to spread disinformation and hack. If it does, then Russia's efforts to create separate Internets and restrict users will be seen as justified. Also, the diffuse nature of Russia's state-controlled cyber activities provides optimal context for plausible

deniability. The Russian leadership tends to deflect to "it was an individual's initiative" when any Russians are accused of nefarious digital activities, such as at the Helsinki summit when Putin described the twelve Russian citizens being investigated in the United States for interference as using their own "personal sympathies" to help Trump win the 2016 election. This line is remarkably similar to Putin's expressions that volunteers rather than Russian military personnel were fighting in eastern Ukraine during the war in the Donbas. It should be noted that Russia's foreign cyber activities not only seek to influence, but they can serve as blackmail tools designed to get the West to sit down and negotiate on cyber and other issues.

Russia's online activities in recent years have caught the United States and Europe largely unprepared. The nature of their democratic institutions means policy responses are slow. Democratic societies, with their checks and balances and deliberate decisionmaking processes, are particularly vulnerable to fast-moving, hostile cyber activities. One response may come from the re-activation of the U.S. Cyber Command, which has been largely idle since its creation in 2009. In May 2018, it was elevated to the status of a full, independent Unified Combatant Command, which very likely portends that the United States will start taking a more offensive cyber posture against adversaries, including Russia, as outlined in the Trump administration's cyber security strategy that was released on September 21, 2018.

Domestically, the Kremlin continues to silence dissenting and independent online voices. The Telegram case demonstrates the Russian government's efforts to enforce online restrictions but also its technical and financial inability to do so (at present). Instead, the Russian authorities have been selectively punishing ordinary citizen-bloggers by charging them with online extremism for content that seems to be, simply, disagreeable. Despite the government's progress and lapses in directly controlling free speech in Russia, it has been rather successful at cultivating a culture of online self-censorship. Russians sense that in time the Kremlin will have the tools to know the identities of all Russian Internet users.

PONARS EURASIA NEW APPROACHES TO RESEARCH AND SECURITY IN EURASIA

Elliott School of International Affairs
THE GEORGE WASHINGTON UNIVERSITY