Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

ISSUE BRIEF

# Reassessing RuNet

## Russian Internet Isolation and Implications for Russian Cyber Behavior

JULY 2021 JUSTIN SHERMAN

The **Scowcroft Center for Strategy and Security** works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.

The **Cyber Statecraft Initiative** works at the nexus of geopolitics and cybersecurity to craft strategies to help shape the conduct of statecraft and to better inform and secure users of technology. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.

## Executive Summary

The Russian government has long exerted control over the internet in Russia, but it has more aggressively pushed in recent years to technically isolate the internet within Russia from the rest of the world. It remains to be seen how successful the government will be in achieving this objective—due to a combination of political and especially technical factors—but the pursuit of a domestic internet may shift the layout of internet infrastructure in Russia and the state's control over it. This issue brief examines recent "RuNet" developments and explores how they could elevate national security risks for the United States and Europe by changing the internet landscape in Russia and potentially shifting Russian cyber behavior. In the process, it also analyzes the relationship between Russian President Vladimir Putin, the Kremlin, and Russian cyber strategy; the Russian government's notion of "information security"; and how the Russian model of internet control differs from the oft-cited Chinese model.

It concludes with five main points that the United States and Europe should take away: 1) the state's political willingness to push internet isolation costs on companies and citizens is an open question; 2) Kremlin perceptions of information onslaught from the West drive top-level attention to internet isolation; 3) RuNet isolation could increase Kremlin perceptions of insulation from foreign cyber threats—resulting in more assertive cyber operations abroad; 4) it could also prompt the Kremlin to selectively provide increased support to non-state cyber proxies; and 5) the Kremlin's pursuits may undermine the cybersecurity of Russian cyberspace itself.

## Introduction

The so-called RuNet, or the internet within Russia, has received growing attention from the US and European national security community over the last decade.[1] But recently, the Russian government has more aggressively pushed to technically isolate the internet within Russia from the rest of the world—the focus of a domestic internet law signed on May 1, 2019 and entered into effect on November 1, 2019. RuNet isolation would further harm free speech and human rights in Russia, which is itself reason for serious concern. Yet it could also prompt changes in the cyber operations of the Russian state and Russian government cyber proxies, raising security questions for the United States and Europe.

Internet isolation in authoritarian countries can present national security risks to other states. The successful consolidation of state control over the internet within state borders can allow authoritarian regimes to consolidate power. States may censor information and heighten state propaganda campaigns, for example. Restrictions on cross-border data flows and mandated government source code inspections also have security implications.

But the recent RuNet developments pose unique security risks compared to many other "cyber sovereignty" measures, and these domestic internet developments merit discussion in the context of global internet, information, and cyber security. This is because the Kremlin is pursuing internet isolation on a fundamentally deeper level than many other countries have pursued to date, including through the development a domestic Domain Name System (DNS) and the uprooting of Western hardware and software from Russia's internet infrastructure. Such a pursuit will not only impact perceptions of insulation from foreign cyber threats but could also shift the technical ways in which cyber operations must be conducted from within Russia—a country whose government already makes heavy use of cyber and information operations against foreign targets around the world. It may also undermine the cybersecurity of Russian cyberspace in the continued pursuit of a broader, regime-security-focused notion of "information security" online. This approach to internet restriction and isolation notably diverges from the more-studied model in China, meaning there is a greater need for policy makers in the United States and Europe to better understand recent RuNet developments and what security implications they may hold.

"RuNet" has been used in reference to several different technical definitions of the "Russian internet." Some analysts use the term to refer to the Russian-language portion of the global internet—e.g., former Soviet republics with Russian-speaking populations and Russian online content, plus those physically located in Russia. This paper focuses specifically on the internet digital and physical infrastructure within Russia's borders—a collection of networks rather than a completely centralized, top-down, government-built system as in China[2]—and the internet users located there.

This issue brief examines recent RuNet developments and explores how they could elevate national security risks for the United States and Europe by changing the internet landscape in Russia and potentially shifting Russian cyber behavior. It does this through five questions:

- First, what is the domestic internet law and how does it change the RuNet landscape?
- Second, what is the relationship between Putin, the Kremlin, and Russian cyber strategy?
- Third, how could RuNet isolation shift Russian state cyber operations?
- Fourth, how could RuNet isolation shift Russian proxy cyber operations?
- Finally, what are the five main takeaways for the United States and Europe?

In response, policy makers in the United States and Europe should monitor the political and technical challenges faced by Moscow, take a more cohesive conceptual and bureaucratic approach to the relationship between Russian internet control and Russian cyber operations, and invest in a more cohesive defense against Kremlin digital threats, among other actions.

[1] See, e.g.: M Ristolainen, "Should 'RuNet 2020' Be Taken Seriously? Contradictory Views about Cyber Security between Russia and the West," *Journal of Information Warfare* 16, no. 4 (2017): 113-131.

[2] Polina Kolozaridi and Dmitry Muravyov, "Contextualizing sovereignty: A critical review of competing explanations of the Internet governance in the (so-called) Russian case," *First Monday* 26, no. 5 (May 2021).

## The Domestic Internet Law

In December 2018, a bill was introduced into the State Duma, the lower house of Russia's parliament, that moved to consolidate the Russian government's control of internet architecture within Russia to ensure the internet could be isolated in the event of a security incident.[3] These isolation measures had been discussed by the Kremlin for years as part of the Russian government's drive to enact "cyber sovereignty" measures, or those that firmly project state borders over cyberspace.[4] In other words, desires to isolate the Russian internet have a history.

In the early 1990s, Russian authorities implemented SORM-1, a nationwide monitoring system for telephone lines.[5] In 1993, then-President Boris Yeltsin established by decree the Federal Agency of Government Communications and Information (FAPSI), whose responsibilities included signals interception abroad and at home.[6] The SORM surveillance system was then expanded to include SORM-2, which intercepted internet traffic through black boxes installed on internet gateways.[7] (Later, SORM-3 would begin collecting a range of internet and social media data.[8]) For the time being, though, FAPSI's main responsibilities entailed signals intelligence, "electronic interception and cryptoanalysis," electronic intelligence, and protecting networks from foreign intelligence service penetration.[9]

In September 2000, President Vladimir Putin approved the Information Security Doctrine of the Russian Federation, which laid out the Kremlin's view of the internet and goals for managing perceived threats.[10] This articulated a vision of "information security" that includes not only the confidentiality, integrity, and availability of systems and data—as "information security" typically refers to in the West—but also a notion of securing an online information space for the purposes of social and political stability (e.g., regime security). This focused on protecting the regime against ideas and opinions considered hostile. In the early 2000s, the internet picked up steam in Russia, though not nearly as quickly as in some other countries; Putin was meanwhile consolidating power, and increasingly driving Russian foreign policy in the process.[11] It was not until the web became increasingly entangled with political events at home and geopolitical events abroad—and the Federal Security Service (FSB), concerned about the internet since the 1990s, had more power—that the Kremlin focused more attention on the internet as a regime security matter.

"Color revolutions" in Georgia, Ukraine, and Kyrgyzstan from 2003–2005 alarmed the Kremlin and contributed to "a narrative of a continuous wave of pro-democracy, pro-reform movements sweeping through the former Soviet Union."[12] Events like the 2008 Russo-Georgian War raised red flags for the Kremlin about the way individuals, journalists, and regime critics could use the internet to spread information.[13] Fears of internet openness and conspiratorial views of Western online interference were accelerated in turn by the Arab Spring uprisings in the early 2010s,[14] protests against Putin's election rigging in 2011, online criticism of and protests against Putin's return to the presidency in

[3] Bill No. 608767-7, Russian Duma, last updated December 14, 2018, https://sozd.duma.gov.ru/bill/608767-7.

[4] As Julien Nocetti notes, "Russia has been adopting a threat-oriented lens towards the internet. By extension, the country's internet policy conveys a long-lasting national security fear." Julien Nocetti, "Russia's 'dictatorship-of-the-law' approach to internet policy," *Internet Policy Review* 4, no. 4 (November 2015), https://policyreview.info/node/380/pdf, 2.

[5] "Lawful interception: the Russian approach," Privacy International, March 4, 2013, https://privacyinternational.org/blog/1296/lawful-interception-russian-approach.

[6] "FAPSI Operations," Federation of the American Scientists, accessed November 21, 2020, https://fas.org/irp/world/russia/fapsi/ops.htm.

[7] Ibid.; Andrei Soldatov and Irina Borogan, *The Red Web: The Kremlin's Wars on the Internet* (New York: PublicAffairs, 2015), 66.

[8] See, e.g.: Catalin Cimpanu, "Some of Russia's surveillance tech leaked data for more than a year," *ZDNet*, August 30, 2019, https://www.zdnet.com/article/some-of-russias-surveillance-tech-leaked-data-for-more-than-a-year/; James Andrew Lewis, "Reference Note on Russian Communications Surveillance," Center for Strategic & International Studies, April 18, 2014, https://www.csis.org/analysis/reference-note-russian-communications-surveillance.

[9] Gordon Bennett, *The Federal Agency of Government Communications & Information* (Conflict Studies Research Centre: Camberley, August 2000), https://www.files.ethz.ch/isn/96806/00_Aug.pdf, 2; Andrei Soldatov and Irina Borogan, *The New Nobility: The Restoration of Russia's Security State and the Enduring Legacy of the KGB* (New York: PublicAffairs, 2010), 232. In 2003, FAPSI was dissolved, and its Third Directorate was mostly absorbed into the Federal Security Service (FSB), Russia's predominant intelligence agency.

[10] "Information Security Doctrine of the Russian Federation," Russian Federation, September 9, 2000, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf.

[11] On this second point, and how Putin has shaped Russian foreign policy, see: Michael McFaul, "Putin, Putinism, and the Domestic Determinants of Russian Foreign Policy," *International Security* 45, no. 2 (Fall 2020): 95-139.

[12] Katherine T. Hinkle, *Russia's reactions to the color revolutions* (Monterey: Naval Postgraduate School, 2017), i.

[13] Soldatov and Borogan, *The Red Web*, 110.

[14] See, e.g.: Yulia Nikitina, "The 'Color Revolutions' and 'Arab Spring' in Russian Official Discourse," *Connections* 14, no. 1 (Winter 2014): 87-104, https://www.jstor.org/stable/26326387, 88; and Soldatov and Borogan, *The Red Web*, 124, 125, 146.

2012,[15] the Snowden leaks in 2013,[16] the Ukrainian revolution in 2014,[17] and the Panama Paper leaks in 2016.[18]

Putin and his Kremlin advisors became more outspoken about the internet's risks as these events unfolded. In 2014, for example, Putin infamously labeled the internet a "CIA project" in a St. Petersburg address and called for Russia to "fight for its interests" online.[19] In 2016, Putin said the internet-disseminated Panama Papers were an "informational product" designed to "destabilize" Russia from within.[20] The Russian government is also concerned about the extent to which Russian citizens' use of the internet (especially among young people) makes those individuals less susceptible to state television propaganda.[21] For instance, in March 2021, following harsh repression of protests against Alexey Navalny's jailing and state corruption, Putin said the internet in Russia should be bound by rules to stop (in his words) the internet drawing children into opposition street protests.[22]

Thus, in the run-up to this domestic internet bill, the Russian government had already implemented policies spanning the blocking of foreign news websites[23] to the mandated local storage of internet data on Russian citizens within Russia's borders[24] to the creation of an internet website blacklist.[25] Accelerated particularly after Putin's return to the presidency in 2012, laws to restrict and monitor online behavior were supplemented with conventional tactics of authoritarian power consolidation, from physical coercion used to suppress dissent to state ownership of internet resources.[26] Internet control in Russia was not and is not merely about technological limitations. The Russian state's internet control strategies tended "to be more subtle and sophisticated and designed to *shape* and *affect* when and how information [was] received by users, rather than denying access outright."[27] (This also relates to the Russian government's propaganda abroad, manipulating instead of controlling narratives.) Intimidation, harassment by security services, court-ordered fines, and complex, restrictive, and inconsistently enforced speech laws are all employed to shape the internet in Russia and citizens' interactions with

"Intimidation, harassment by security services, court-ordered fines, and complex, restrictive, and inconsistently enforced speech laws are all employed to shape the internet in Russia and citizens' interactions with it."

[15] Samuel Rachlin, "Putin's Critics Hit Big With YouTube," *New York Times*, February 15, 2012, https://www.nytimes.com/2012/02/16/opinion/putins-critics-hit-big-with-youtube.html.

[16] Putin used the Snowden leaks to criticize the United States, but it also played into his existing worldview of US technologies and, in particular, US social media platforms as tools of Western subversion. See some of Putin's public comments: "Putin says Snowden was wrong to leak secrets, but is no traitor," Reuters, June 2, 2017, https://www.reuters.com/article/us-russia-putin-snowden/putin-says-snowden-was-wrong-to-leak-secrets-but-is-no-traitor-idUSKBN18T1T4.

[17] In December 2013, Putin was already blaming "outside actors" for protests in Ukraine. "Ukraine PM Mykola Azarov warns of coup in making," *BBC*, December 2, 2013, https://www.bbc.com/news/world-europe-25192792.

[18] Putin called the publication of the Panama Papers a "provocation" and blamed US officials and Goldman Sachs for an attempt to influence Russian elections. "Russia's Putin: Panama papers are a 'provocation'," Reuters, April 14, 2016, https://www.reuters.com/article/us-russia-putin-panamapapers-idUSKCN0XB16D.

[19] Noah Rayman, "Putin: The Internet Is a 'CIA Project,'" *TIME*, April 24, 2014, https://time.com/75484/putin-the-internet-is-a-cia-project/.

[20] "Putin on Panama Papers: 'Info product' aimed to destabilize Russia," *RT*, April 7, 2016, https://www.rt.com/news/338807-putin-panama-papers-reaction/.

[21] Denis Volkov, Stepan Goncharov, and Maria Snegovaya, "Russian Youth and Civic Engagement," Center for European Policy Analysis, September 29, 2020, https://cepa.org/russian-youth-and-civic-engagement/.

[22] "Putin calls for internet bound by moral rules, criticises opposition rallies," Reuters, March 4, 2021, https://www.reuters.com/article/us-russia-internet/putin-calls-for-internet-bound-by-moral-rules-criticises-opposition-rallies-idUSKCN2AW2D4.

[23] Nathalie Maréchal, "Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy," *Media and Communications* 5, no. 1 (2017): 29-41, https://www.cogitatiopress.com/mediaandcommunication/article/view/808/808, 32.

[24] Federal Law No. 242-FZ, "On Amending Certain Legislative Acts of the Russian Federation Regarding Clarifying the Personal Data Processing Procedure in Information and Telecommunication Networks," https://home.kpmg/be/en/home/insights/2018/09/the-localisation-of-russian-citizens-personal-data.html.

[25] "Russia internet blacklist law takes effect," *BBC*, November 1, 2012, https://www.bbc.com/news/technology-20096274.

[26] Carolina Vendil Pallin, "Internet control through ownership: the case of Russia," *Post-Soviet Affairs* 33, no. 1 (2017): 16-33.

[27] Ronald Deibert and Rafal Rohozinski, "Control and Subversion in Russian Cyberspace," in *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, ed. Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (Boston: MIT Press, 2010), 16.

it.[28] This is an important distinction from the oft-cited mechanisms of internet control deployed by the Chinese government, which involve physical coercion but, on the whole, lean far more technical. But Russian authorities do also use technical measures themselves, as when officials employ internet and communications shutdowns, such as turning off the internet in Ingushetia in 2018.[29]

The December 2018 bill, from the Kremlin's perspective, was another step in consolidating state control over the Russian internet. A memo attached to the bill cited "the aggressive nature of the US National Cyber Security Strategy adopted in September 2018" as a reason for the legislation. It specifically drew attention to the White House strategy's accusations of Russian cyber aggression and language about preserving peace through strength.[30] This apparent perception of US aggression may have been exacerbated by the US Defense Department's "defend forward" re-posturing that occurred shortly thereafter with the publication of the Defense Department's 2018 Cyber Strategy.[31] While the legislation is undoubtedly top cover for further extending offline repression into the digital domain,[32] Kremlin perceptions of a US-posed cyber threat are also genuine; these are not mutually exclusive drivers. The bill to pursue total RuNet isolation was signed by Putin on May 1, 2019[33] and went into effect on November 1, 2019.[34]

The law had several main components. First, it compelled companies to install technical equipment to counter what the government calls security threats (e.g., including information), which has in practice included the installation of deep packet inspection equipment on company networks. Second, it gave the state more authorities to centralize control over the internet infrastructure in Russia. Third, it aimed to create a national DNS for Russia, an idea which has been discussed for years but not yet called for in law.[35] And it also required the internet regulator, Roskomnadzor, to maintain registries of internet exchange points, communications lines crossing state borders, and autonomous system numbers (ASNs) responsible for the stable operation of the RuNet.[36]

Since the law's signing, the Russian government has been working to implement its provisions. For example, Roskomnadzor, Russia's internet and media regulator, began more widely testing deployments of deep packet inspection (DPI) in the late summer and fall of 2019 in an effort to block access to prohibited apps like encrypted messaging service Telegram[37] (though the Telegram ban was undone in June 2020).[38] More recently, Moscow has shifted further legal powers to Roskomnadzor to regulate the internet.[39] The government's semi-failed attempt to throttle Twitter in March 2021 evidently drew on more widely deployed DPI tools on internet company networks, though

[28] Robert Morgus, "The Spread of Russia's Digital Authoritarianism," in *Artificial Intelligence, China, Russia, and the Global Order*, ed. Nicholas D. Wright (Maxwell Air Force Base: Air University Press, 2019), 86; "Russia to fine social networks for luring minors into unauthorized protests," *TASS*, January 27, 2021, https://tass.com/society/1249709. On the inconsistent enforcement point, see: Nicola Habersetzer, "Interview with Andrei Soldatov on Digital Rights in Russia," Human Rights Watch, June 19, 2020, https://www.hrw.org/news/2020/06/19/interview-andrei-soldatov-digital-rights-russia.

[29] Maria Kolomychenko, "Russia stifled mobile network during protests: document," Reuters, November 16, 2018, https://www.reuters.com/article/us-russia-protests-internet/russia-stifled-mobile-network-during-protests-document-idUSKCN1NL1I6.

[30] Robert Morgus and Justin Sherman, "Analysis: Russia's Plans for a National Internet," New America, February 19, 2019, https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/russias-plans-for-a-national-internet/.

[31] *Summary: Department of Defense Cyber Strategy 2018*, US Department of Defense, 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

[32] See, e.g.: Alena Epifanova, *Deciphering Russia's "Sovereign Internet Law": Tightening Control and Accelerating the Splinternet* (Berlin: German Council on Foreign Relations, January 2020), https://dgap.org/sites/default/files/article_pdfs/dgap-analyse_2-2020_epifanova_0.pdf.

[33] "Putin Signs Internet Isolation Bill Into Law," *Moscow Times*, May 1, 2019, https://www.themoscowtimes.com/2019/05/01/putin-signs-internet-isolation-bill-into-law-a65461.

[34] "Russia internet: Law introducing new controls comes into force," *BBC*, November 1, 2019, https://www.bbc.com/news/world-europe-50259597.

[35] Epifanova, *Deciphering Russia's Sovereign Internet Law*, 2; and author conversations with American security analysts and internet activists in Russia.

[36] Ilona Stadnik, "Control by infrastructure: Political ambitions meet technical implementations in RuNet," *First Monday* 26, no. 5 (May 2021).

[37] "Russia starts rolling out DPI filtration tech that might finally block Telegram," *Meduza*, September 27, 2019, https://meduza.io/en/news/2019/09/27/russia-starts-rolling-out-dpi-filtration-tech-that-might-finally-block-telegram.

[38] "Russia 'Unblocks' Telegram Messenger in Surprise Reversal," *Moscow Times*, June 18, 2020, https://www.themoscowtimes.com/2020/06/18/russia-unblocks-telegram-messenger-in-surprise-reversal-a70620.

[39] Justin Sherman and Samuel Bendett, "Putin Takes Another Step in Bid to Control Russia's Internet," *Defense One*, April 8, 2020, https://www.defenseone.com/ideas/2020/04/putins-latest-step-his-bid-control-russias-internet/164467/.

the collateral damage the throttling caused highlights that DPI deployments are still imperfect and incomplete across the domestic internet sphere.[40] While there were important differences between the Twitter throttling and the Russian government's two-year failure to block Telegram, both episodes underscored the limits of the technical dimensions of the Russian state's internet control: technical filtering mechanisms were not sufficiently widely deployed to enable precise filtering of internet traffic.

The Russian government has also announced multiple planned tests for internet isolation. Tests were announced for April 2019[41] and then in October 2019,[42] for example, but ultimately were not carried out. Multiple Russian telecom operators issued reports to the government in November 2019 stating they had problems installing new equipment to isolate the Russian internet.[43] Officials claim a partial isolation test was successfully executed in December 2019, but also claim that users would not have noticed the difference.[44] There has been overwhelming silence on the matter since. All told, authorities continue running into technical difficulties with implementing components of the domestic internet law—and a successful, total isolation of the RuNet in the near future is far from certain. But on the path to this goal, the Russian government is escalating its consolidation of control over internet architecture and internet packet routing, changing what the Russian internet looks like to those inside and outside of the country in the process. Its goal is ultimately to be able to isolate the internet within Russia and from the rest of the world, which has implications for how the Kremlin thinks about and tangibly approaches cyberspace.

## The Kremlin and Russian Cyber Behavior

This internet isolation could shift how key Russian decision makers view their insulation from foreign cyber threats. It could also shift how they perceive their own deniability for cyber behavior originating in their borders, like offensive cyber operations and information operations. These shifts could change Russia's approach to cyber behavior focused on other countries.

Putin has continually consolidated authoritarian control over Russia since his first presidential term began in 2000, with tactics ranging from seizing control of media[45] to capturing major industries.[46] Decision making in the Kremlin is oriented around Putin, in addition to the *siloviki* (the military and intelligence elite), the Security Council, and some of Putin's close personal acquaintances.[47] Since Putin's return to the presidency in 2012, those outside the core *siloviki* circle, like economists, have increasingly been pushed out of the Kremlin's key decision-making processes.[48] This has only sharpened the Kremlin's Cold War view of the world: characterized as a "siege mentality,"[49] where Russia's enemies are constantly out to harm the country[50] and protests and free information are Western attempts to discredit Putin and stoke revolution.[51] In such a paranoid

[40] Dylan Myles-Primakoff and Justin Sherman, "Russia Can't Afford to Block Twitter—Yet," *Foreign Policy*, April 30, 2021, https://foreignpolicy.com/2021/04/30/russia-block-twitter-telegram-online-censorship/. For more on the Twitter throttling, see also: Diwen Xue et al., *Throttling of Twitter in Russia* (Ann Arbor: Censored Planet at the University of Michigan, April 6, 2021).

[41] Tamara Evdokimova, "Will Russia Disconnect From the Internet on April 1?," *Slate*, March 29, 2019, https://slate.com/technology/2019/03/russia-internet-shutdown-disconnect-test.html.

[42] "Internet isolation exercises to take place in Russia at least once every year," *Meduza*, October 21, 2019, https://meduza.io/en/news/2019/10/21/internet-isolation-exercises-to-take-place-in-russia-at-least-once-every-year.

[43] "Russian telecoms say tests of new Internet-isolation equipment caused slowdowns and service disruptions," *Meduza*, February 10, 2020, https://meduza.io/en/news/2020/02/10/russian-telecoms-say-tests-of-new-internet-isolation-equipment-caused-slowdowns-and-service-disruptions.

[44] "Russia's Internet Is Ready for Isolation, Officials Say After Partial Shutdown," *Moscow Times*, December 24, 2019, https://www.themoscowtimes.com/2019/12/24/russias-interent-ready-isolation-officials-say-after-partial-shutdown-a68728.

[45] Susan B. Glasser and Peter Baker, "Russian Network Seized in Raid," *Washington Post*, April 15, 2001, https://www.washingtonpost.com/archive/politics/2001/04/15/russian-network-seized-in-raid/e9679fb0-31cb-4b9c-b07f-204b488f40ad/.

[46] See, e.g.: Sergey Aleksashenko, *Putin's Counterrevolution* (Washington, D.C.: Brookings Institution Press, 2018).

[47] See, e.g.: Andrei Soldatov and Michael Rochlitz, "The *Siloviki* in Russian Politics," in *The New Autocracy: Information, Politics, and Policy in Putin's Russia*, ed. Daniel Treisman (Washington, D.C.: Brookings Institution Press, 2018), 91, 95-96.

[48] Steven Lee Myers, *The New Tsar: The Rise and Reign of Vladimir Putin* (New York: Knopf, 2015), 461.

[49] Masha Gessen, *The Man Without a Face: The Unlikely Rise of Vladimir Putin* (New York: Riverhead, 2012), 60-61.

[50] "In the view of many contemporary Russian leaders, the United States occupies a space on the world stage that rightly belongs to Russia." Maria Snegovaya, "What explains the sometimes obsessive anti-Americanism of Russian elites?," Brookings Institution, February 23, 2016, https://www.brookings.edu/blog/order-from-chaos/2016/02/23/what-explains-the-sometimes-obsessive-anti-americanism-of-russian-elites/.

[51] Myers, *The New Tsar*, 309; and Soldatov and Borogan, *The Red Web*, 155.

worldview, "the source of danger [is] a constantly moving target."[52]

This does not mean that Putin has a hand in every Kremlin decision, however. Gleb Pavlovsky, a "political technologist" (political manipulator)[53] and a Kremlin adviser until 2011, has spoken of "creating the illusion that Putin controls everything in Russia."[54] Putin has been described as a delegator, not a micromanager, who many times steps back from decisions and only becomes involved when there is a problem to be addressed.[55] He has ultimate control over decisions,[56] but that does not mean he literally makes them all. Where he steps back, it is often members of the military and intelligence elite that take the reins.[57] But even that, too, may not be centralized and is certainly not a homogenous enterprise; members of those inner *siloviki* circles may disagree on policy decision making.[58] They may also get involved in strategy implementation of their own volition, as the Kremlin's broader approach to security and conflict involves establishing overarching strategic objectives and allowing "adhocrats" across the elite to "become policy entrepreneurs, seeking and seizing opportunities to develop and even implement ideas they think will further the Kremlin's goal."[59]

What this power structure does mean, though, is that security fears of "color revolutions" in Russia underpin key Kremlin decisions. Putin routinely discusses "sovereignty" as critical to Russia's national objectives[60] and threats to Russian political sovereignty, conversely, as direct threats to Russian security.[61] Internet control fits into this worldview.[62] Moscow has long argued for state control of the internet under the "cyber sovereignty" banner,[63] and recent measures to accelerate RuNet isolation fit squarely into this perception of foreign actors threatening and hurting Russia through internet openness.[64] As with all of Putin's security-driven decisions,[65] when it comes to state control of the internet, he will not relent as long as he perceives a threat. The view is that something—even if not technically executable given current state capacity—must be done.

Into 2021, the "information security" concept remains key to Russian internet and cyber strategy.[66] The Russian govern-

[52] Masha Gessen, *The Future is History: How Totalitarianism Reclaimed Russia* (New York: Riverhead, 2017), 469.

[53] On this term, see: Peter Pomerantsev, "The Hidden Author of Putinism," *Atlantic*, November 7, 2014, https://www.theatlantic.com/international/archive/2014/11/hidden-author-putinism-russia-vladislav-surkov/382489/.

[54] Julia Ioffe, "What Putin Really Wants," *Atlantic Monthly* (January/February 2018), https://www.theatlantic.com/magazine/archive/2018/01/putins-game/546548/.

[55] Fiona Hill and Clifford G. Gaddy, "What makes Putin tick, and what the West should do," Brookings Institution, January 13, 2017, https://www.brookings.edu/research/what-makes-putin-tick-and-what-the-west-should-do/. This can also be an attempt to self-insulate from political blowback, as with Putin's handling of the Covid-19 pandemic.

[56] Political analyst Masha Lipman quoted in: Isaac Chotiner, "How Putin Controls Russia," *New Yorker*, January 23, 2020, https://www.newyorker.com/news/q-and-a/how-putin-controls-russia.

[57] This is not a hard-and-fast rule, however: oligarchs and other players are involved too in what Ben Judah describes as "Russia's neo-courtly politics." Judah also argues that dividing Putin associates into camps such as *siloviks* vs. liberals is often nothing more than a projection of an analyst's views. See: Ben Judah, *Fragile Empire: How Russia Fell In and Out of Love with Vladimir Putin* (New Haven: Yale University Press, 2014), 122-124.

[58] See, e.g.: David W. Rivera and Sharon Werning Rivera, "The Militarization of the Russian Elite under Putin," *Problems of Post-Communism* 65, no. 4 (2018): 221-232.

[59] Mark Galeotti, "Russia has no grand plans, but lots of 'adhocrats,'" IntelliNews, January 18, 2017, https://www.intellinews.com/stolypin-russia-has-no-grand-plans-but-lots-of-adhocrats-114014/. Thanks as well to Brian Whitmore for discussion of this point.

[60] See, e.g.: "Presidential Address to the Federal Assembly," Kremlin.ru, January 15, 2020, http://en.kremlin.ru/events/president/news/62582.

[61] Fiona Hill, "Mr. Putin and the Art of the Offensive Defense: Approaches to Foreign Policy (Part Two)," Brookings Institution, March 16, 2014, https://www.brookings.edu/articles/mr-putin-and-the-art-of-the-offensive-defense-approaches-to-foreign-policy-part-two/.

[62] See, e.g.: Alexandra Prokopenko, "What's Behind Russia's New Offensive Against the Internet Economy?" Carnegie Moscow Center, December 8, 2019, https://carnegie.ru/commentary/79660; and Soldatov and Borogan, *The Red Web*, 124, 125, 146, 155.

[63] The Information Security Doctrine of the Russian Federation approved by Vladimir Putin in 2000, for example, lists "the sovereignty and territorial integrity of the Russian Federation" as one of "the most important Russian information security targets in the domestic policy sphere." See: Russian Federation, *Information Security Doctrine of the Russian Federation*, Russian Federation, September 9, 2000, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf, 15.

[64] Juha Kukkola writes that "the idea of information and digital sovereignty developed along two different tracks": first, an externally facing "understanding that information weapons and operations posed a new kind of threat to the security of the state," and second, an internally facing idea "based on the writing of Russian information security and warfare scholars at the turn of the millennium" that drew from ideas "of territorial state sovereignty, judicial concepts and geopolitics which had wider support amongst the Russian intelligentsia" around the turn of the 21st century. See: Juha Kukkola, *Digital Soviet Union: The Russian national segment of the Internet as a closed national network shaped by strategic cultural ideas* (Helsinki: National Defence University, 2020), 213-214.

[65] Hill and Gaddy, "What makes Putin tick." "Putin's goal is security for Russia and his system…there is no definitive endgame. He will keep on playing as long as he perceives the threat to last."

[66] "Executive Order approving Basic Principles of State Policy on International Information Security," Kremlin.ru, April 12, 2021, http://en.kremlin.ru/acts/news/65350.

ment has continued introducing proposals of "codes of conduct for information security" at the United Nations that aim to encompass political speech in definitions of "cybercrime" and replace the Budapest Convention on Cybercrime, backed by the United States and many European countries, with one designed by Russia and China.[67] Putin and other officials, such as Andrei Lipov, head of Roskomnadzor, continue opportunistically using problems in the democratic internet sphere to justify internet control within Russia and the state's efforts to reshape the internet globally.[68] And the Russian government has apparently targeted undersea cables and other physical internet infrastructure around the world for strategic purposes.[69] Moscow has continued to demonstrate its commitment to the general pursuit of internet control within Russia in concert with undermining the open internet globally.

This all matters for evaluating the domestic internet law and implications for Russian cyber behavior. The Russian government uses its own military and intelligence services to conduct offensive cyber operations. It also leverages proxy actors, each working with varying levels of state backing or permission, to conduct offensive cyber operations and influence operations on the internet (e.g., targeting the 2016 US election).[70] In total, many related decisions, ranging from approval of military cyber operations to permitting of proxy cyber and information operations, center around the Kremlin's security decision makers. How they and Putin perceive the isolation of the Russian internet matters greatly for Kremlin decision making on Russian cyber behavior.

## RuNet and State Cyber Behavior

If the domestic internet law does produce further RuNet isolation, Kremlin leadership may see Russia as more insulated from foreign cyber threats when considering operational blowback. Russia may become more willing to assertively target digital internet systems abroad as a result, which may pair with its efforts to physically target internet infrastructure like undersea cables. Further isolation would also technically reduce the connectivity of the internet within Russia to the outside world. This, too, could prompt changes in how operations are executed.

On the state side, it is likely the Kremlin exerts tighter control over sophisticated offensive cyber operations compared to the control exerted over less sophisticated operations conducted by nonstate proxies. This is because "more advanced technical operations carry much greater strategic risk."[71] Poorly controlled or executed operations could lead to unintended escalations with foreign powers, particularly if the source of those intrusions is an entity like the GRU (military intelligence).[72] Thus, something like intelligence service penetration of a foreign nation's power grid would likely be subject to far more political oversight than a state-ignored crime ring's hack of a small e-commerce firm, which would likely have none at all. For example, the US government has stated that hacks of US political organizations in 2016, attributed to Russian intelligence-affiliated entities,[73] could only have been authorized by "Russia's senior-most officials."[74]

First, this means the Russian government may be more willing to assertively target internet systems abroad if internet isolation goes forth. The covert and classified nature of state cyber operations poses inherent challenges in this kind of analysis, and many questions remain. But where Kremlin officials play a greater role in sophisticated state operations, the views of Putin and his inner military and intelligence circles are important. And what is clear is that fears of internet openness and dependence on Western internet systems currently guide much of that inner circle's thinking on cyber policy. Perceived or actual reductions in that risk and dependence, through further RuNet isolation

[67] "Countering the use of information and communications technologies for criminal purposes," United Nations, November 25, 2019, https://www.undocs.org/A/74/401.

[68] "Meeting with Head of Roskomnadzor Andrei Lipov," Kremlin.ru, August 10, 2020, http://www.en.kremlin.ru/catalog/keywords/98/events/63874.

[69] Justin Sherman, *Cyber Defense Across the Ocean Floor: The Geopolitics of Submarine Cable Security*, Atlantic Council, forthcoming.

[70] For more on this topic, see, e.g.: Maria Snegovaya and Kohei Watanabe, *The Kremlin's Social Media Influence Inside the United States: A Moving Target* (Washington, D.C.: Free Russia Foundation, February 2021).

[71] Nina A. Kollars and Michael B. Petersen, "Feed the Bears, Starve the Trolls," *Cyber Defense Review* (2019): 145-158, 154.

[72] See, e.g.: "U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations," US Department of Justice Office of Public Affairs, October 4, 2018, https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and.

[73] See, e.g.: *Report of the Select Committee on Intelligence, United States Senate, on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election: Volume 4: Review of the Intelligence Community Assessment*, United States Congress, April 2020, https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume4.pdf.

[74] "Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security," US Department of Homeland Security, October 7, 2016, https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.

(i.e., reducing internet openness), could prompt more assertive state cyber operations.

Internet protocols are one case study. A key component of the RuNet push is reducing Russia's dependence on foreign-made hardware and software equipment, and that includes protocols for internet traffic routing, like the Domain Name System set up by coalitions of Western researchers and companies when the internet was first developed.[75] Putin views this dependence on Western-developed technology as a security threat. In the Kremlin's view, reducing this dependence through RuNet not only shores up Russia's defenses but could also open up the possibility for targeting those protocols abroad without worry of reciprocation. Alleged FSB documents indicate the Kremlin is exploring ways to attack the DNS.[76] Putin and the *siloviki* focus on asymmetrical advantage,[77] and more assertive operations against technologies and standards used abroad, but not in Russia's internet, could lend that kind of edge. Perceived insulation more broadly could prompt these kinds of more assertive cyber operations.

This does not mean developing a custom DNS for Russia, if the Kremlin could execute on the idea,[78] will bolster the cybersecurity of Russian cyberspace. To the contrary, it could present more opportunities for foreign actors to interfere with traffic routing on the internet within Russia. Developing a DNS purely used in the domestic internet environment means developing a point of vulnerability; that could be attractive to hackers and other states interested in facilitating narrowly targeted surveillance and cyber operations on the Russian internet. A custom DNS for Russia might also enable easier attribution of Russian malicious cyber activity through unique DNS signatures. Again, though, what is key is the Kremlin's perception, which by many accounts is that internet isolation will help strengthen the "information security" of Russian cyberspace.

Second, further RuNet isolation could shift how state cyber operations are technically executed. Military and intelligence cyber operations in Russia are presently predicated on a certain amount of cross-border access to internet systems abroad. In other words, some internet openness is what enables those state actors to attack foreign systems from within Russia. Official Russian statements and military literature on these kinds of state operations already "reveal a predilection for the development of offensive cyber capabilities and operations."[79] Limits on internet connectivity to the outside world could prompt shifts in the operational execution of those attacks, such as needing more specialized network equipment to access foreign systems, as well as shifts in overall strategy, such as increased targeting of key internet protocols abroad.

Third, and related, the Kremlin knows that foreign actors looking to penetrate Russian systems would have to contend with the operational impacts of RuNet isolation. For instance, it may be technically harder for foreign cyber actors to find connections into Russia should, for example, there be fewer in-country devices directly linked to the global internet. Systems could be moved around. Existing hardware could in several months be uprooted from Russian internet infrastructure entirely. Knowing foreign actors too would grapple with RuNet changes could also shift the state's willingness to engage in more assertive cyber activity abroad, even if that overlooks the domestic internet's likely harm to Russian internet cybersecurity. But questions about security risks to the United States and Europe do not just lie with state cyber actors.

## RuNet and Proxy Cyber Behavior

On the proxy side, Russia currently leverages numerous nonstate cyber proxies, from patriotic hacking collectives formed of their own volition[80] to state-backed operations like the

[75] Again, it remains unclear if the Russian government will be able to do this, including because of open questions about technical capacity to do so and political willingness to force internet companies to change their systems.

[76] Patrick Tucker, "Russia Has New Tool For Massive Internet Shutdown Attack, Leaked Documents Claim," *Defense One*, March 21, 2020, https://www.defenseone.com/technology/2020/03/russia-has-new-tool-massive-internet-shutdown-attack-leaked-documents-claim/163983/.

[77] Russian pursuit of asymmetry applies in the cyber domain as well. See, e.g.: Bilyana Lilly and Joe Cheravitch, *The Past, Present, and Future of Russia's Cyber Strategy and Forces* (Tallinn: 12th International Conference on Cyber Conflict, 2020), https://ccdcoe.org/uploads/2020/05/CyCon_2020_8_Lilly_Cheravitch.pdf, 137.

[78] Discussion over the last few years of a custom Domain Name System for Russia has been followed by no action.

[79] Bilyana Lilly and Joe Cheravitch, *The Past, Present, and Future of Russia's Cyber Strategy and Forces* (Tallinn: 12th International Conference on Cyber Conflict, 2020), https://ccdcoe.org/uploads/2020/05/CyCon_2020_8_Lilly_Cheravitch.pdf, 129.

[80] Françoise Daucé, Benjamin Loveluck, Bella Ostromooukhova, and Anna Zaytseva, "From Citizen Investigators to Cyber Patrols: Volunteer Internet Regulation in Russia," *Russian Review of Social Research* 11, no. 3 (2019): 46-70. However, some of these organizations may enjoy state backing and recruitment. See, e.g.: "'It's our time to serve the Motherland': How Russia's war in Georgia sparked Moscow's modern-day recruitment of criminal hackers," *Meduza*, August 7, 2018, https://meduza.io/en/feature/2018/08/07/it-s-our-time-to-serve-the-motherland.

Internet Research Agency's online campaigns in the 2016 US election.[81] Moscow's involvement varies case-by-case. For instance, this proxy activity may be state-integrated, state-ordered, state-coordinated, state-shaped, state-encouraged, or state-ignored.[82] This reflects broader Kremlin approaches to security and conflict which rely on a range of proxy groups to achieve or advance objectives, with often very thin lines between state-sponsored activity, state-enabled activity, and state-tolerated criminal activity.[83] Further isolation of the Russian internet could increase the Kremlin's willingness to rely on these kinds of proxy activity in cyberspace.

This is because deniability is an important part of Russia's political warfare strategy.[84] Proxies that conduct cyber and information operations (that Moscow supports or tolerates)[85] not only give the Kremlin this deniability but also lower costs for the state[86] and can obscure command-and-control specifics.[87] It is more about deniability than anonymity.[88] Even if attacks are ultimately attributed to Russia, there may be interims where the Kremlin can deny it.[89]

This cyber proxy activity within Russia is predicated on status quo connectivity to the internet beyond Russia. For example, offensive cyber and information operations launched against Estonia in 2007—by Russian attackers that Moscow claimed no involvement with, yet also refused to act against—originated primarily outside Estonian borders.[90] In cyberattacks on Georgia in 2008, Russian cyber proxies exploited the fact that most of Georgia's internet connectivity at the time ran through Turkish or Russian internet service providers.[91] The command and control server for multiple Distributed Denial of Service (DDoS) attacks launched against Georgia that year was even located in the United States.[92] The Internet Research Agency's information operations in the 2016 US election[93] are but another example of using worldwide internet connectivity.

If that connectivity to the outside world was curtailed, these proxy groups could have to shift their approach to hacking and information operations because of those technical alterations to the internet within Russia. In response, the

[81] Candace Rondeaux, "Yevgeny Prigozhin, 'Putin's Chef,' Continues to Sow Political Discord in the U.S.," *World Politics Review*, March 20, 2020, https://www.worldpoliticsreview.com/articles/28617/yevgeny-prigozhin-putin-s-chef-continues-to-sow-political-discord-in-the-u-s.

[82] Robert Morgus, Brian Fonseca, Kieran Green, and Alexander Crowther, *Are China and Russia on the Cyber Offensive in Latin America and the Caribbean?,* New America, July 2019, https://www.newamerica.org/cybersecurity-initiative/reports/russia-china-cyber-offensive-latam-caribbean/, 23. This draws from: Jason Healey, *Beyond Attribution: Seeking National Responsibility in Cyberspace* Atlantic Council, February 22, 2012, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/beyond-attribution-seeking-national-responsibility-in-cyberspace/.

[83] Thanks to Brian Whitmore for discussion of this point.

[84] Alina Polyakova and Spencer P. Boyer, *The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition,* Brookings Institution, March 2018, https://www.brookings.edu/wp-content/uploads/2018/03/the-future-of-political-warfare.pdf, 2. For an interesting discussion of plausible deniability and kinetic conflict, see: Kimberly Marten, "Russia's use of semi-state security forces: the case of the Wagner group," *Post-Soviet Affairs* 35, no. 3 (2019): 181-204, 187.

[85] There is of course debate on exactly how much the Kremlin controls or does not control various cybercrime, patriotic hacking, and other cyber-actor groups in its borders.

[86] Andrei Soldatov and Irina Borogan, "Russia's approach to cyber: the best defence is a good offence," in *Hacks, Leaks and Disruptions: Russian Cyber Strategies*, ed. Nicu Popescu and Stanislav Secrieru (France: European Union Institute for Security Studies, October 2018), https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf, 18; and Tim Maurer, "Cyber Proxies and Their Implications for Liberal Democracies," *Washington Quarterly* 41, no. 2 (Summer 2018): 181-188, 179.

[87] Erica D. Borghard, "The 'Known Unknowns' of Russian Cyber Signaling," Council on Foreign Relations, April 2, 2018, https://www.cfr.org/blog/known-unknowns-russian-cyber-signaling.

[88] Mark Galeotti quoted in: Andrew Roth, "How the Kremlin is sure to keep its fingerprints off any cyberattack," *Washington Post*, August 2, 2016, https://www.washingtonpost.com/world/europe/how-the-kremlin-is-sure-to-keep-its-fingerprints-off-any-cyberattack/2016/08/02/26144a76-5829-11e6-8b48-0cb344221131_story.html.

[89] For instance, the Russian government has "vehemently denied accusations" of influence over cyber proxies active in the conflict in Ukraine. But research by private-sector cybersecurity companies has since suggested there are links between Russian cyber proxy groups and the Russian government. See, e.g.: Tim Maurer, "Cyber Proxies and the Crisis in Ukraine," in *Cyber War in Perspective: Russian Aggression Against Ukraine*, ed. Kenneth Geers (Tallinn: NATO Cooperative Cyber Defence Center of Excellence, 2015), 85; Jack Detsch, "How Russia and others use cybercriminals as proxies," *Christian Science Monitor*, June 28, 2017, https://www.csmonitor.com/USA/2017/0628/How-Russia-and-others-use-cybercriminals-as-proxies.

[90] Rain Ottis, *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, October 2018), https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf; and Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *WIRED*, August 21, 2007, https://www.wired.com/2007/08/ff-estonia/.

[91] Sergei A. Medvedev, *Offense-defense theory analysis of Russian cyber capability* (Monterey: Naval Postgraduate School, March 2015), https://core.ac.uk/download/pdf/36737355.pdf, 24.

[92] John Markoff, "Before the Gunfire, Cyberattacks," *New York Times*, August 12, 2008, https://www.nytimes.com/2008/08/13/technology/13cyber.html.

[93] Alina Polyakova, "What the Mueller Report Tells Us About Russian Influence Operations," *Lawfare*, April 19, 2019, https://www.lawfareblog.com/what-mueller-report-tells-us-about-russian-influence-operations.

Kremlin may have to shift its relationship with some proxies. The Kremlin does not directly interact with all these groups all the time. In fact, "the narrative of a grand chess master, whether Putin, a Kremlin insider, or mercenary group, singlehandedly orchestrating Russia's proxy warfare strategy is a useful fiction for the Kremlin."[94] But some form of state tolerance, if not state sponsorship, is essential for many of these actors to survive.

It is therefore possible the Kremlin would increase state involvement in some cyber proxy activity in certain cases to ensure necessary access to foreign targets. This could include providing hardware or providing network connectivity to foreign internet-connected systems (bypassing RuNet isolation).[95] But this could further reduce the plausibility of the Kremlin's deniability for domestically based cyber proxy activity. The Russian government frequently looks the other way on domestic cybercrime activity so long as offenders focus on targets beyond Russia and do not contradict or undermine the Kremlin's interests.[96] If RuNet becomes much more isolated and the state further restricts cross-border data flows, regular bypasses of those restrictions—i.e., malware delivery, talking to foreign-based command and control servers—could make plausible deniability of certain operations harder for the Kremlin.

Further isolation from the global internet could also lead to greater state use of cyber proxies located abroad because those foreign bases would provide said groups with better global internet connectivity. There is some basis for this possibility of increased use of cyber proxies stationed outside Russia; for instance, Moscow recently allegedly leveraged a Russian IT front company running cyber operations out of the Czech Republic.[97] The Internet Research Agency has already set up offices in Ghana and Nigeria to run information operations on social media.[98] Doing so would continue to afford the Kremlin deniability of operations—a key part of its proxy activity—while not worrying about how RuNet isolation could hamper cyber proxy activity from within Russia. This would impact US and European security.

At the same time, further RuNet isolation could shift the Kremlin's willingness to materially support some cyber proxy groups—e.g., providing or allowing necessary connectivity to out-of-country systems—without shifting the Kremlin's worries about deniability. Certainly, Putin has already demonstrated his willingness to flatly deny cyber and information operations for which there remains copious attributional evidence. It is also possible that reductions in connectivity to the global internet would only hamper some proxy groups' skills and access to technologies necessary to conduct global operations. Shifts in Kremlin relationships with nonstate cyber proxies could take many forms depending on the changes made to the RuNet architecture.

## Conclusion

Further RuNet isolation would have security implications for the United States and Europe by shifting the architecture of the internet in Russia and potentially shifting Russia's approach to externally facing cyber behavior. This applies to state activity, as well as nonstate cyber proxy activity that is at least tolerated by the Kremlin. So, what should the United States and Europe know? There are five main points, each split into a takeaway and a policy implication.

First, Moscow is not abandoning its pursuit of RuNet isolation, but the state's political willingness to impose high costs on companies and individuals to achieve it is an open question.

- **Takeaway:** The Kremlin is hitting technical hurdles in implementing the domestic internet law, and the

[94] Candace Rondeaux, *Decoding the Wagner Group: Analyzing the Role of Private Military Security Contractors in Russian Proxy Warfare,* New America, November 7, 2019, https://www.newamerica.org/international-security/reports/decoding-wagner-group-analyzing-role-private-military-security-contractors-russian-proxy-warfare/, 8.

[95] Tim Maurer notes many ways a government can interact with a cyber proxy to sponsor or support its behavior, including "sharing knowledge of a zero-day vulnerability, blueprints for packaging modules of code into more sophisticated malware that makes the sum larger than its parts, or more sophisticated malware itself." See: Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge: Cambridge University Press, 2018), 156-157.

[96] See e.g.: John P. Carlin and Garrett M. Graff, *Dawn of the Code War* (New York: PublicAffairs, 2018), 280. But this also doesn't come without costs; see, e.g.: Mark Galeotti, *Russian political war: moving beyond the hybrid* (London: Routledge, 2019), 83 ("deniability and the opportunity to pick up 'off the shelf' assets often come at the expense of competence and discipline").

[97] "Czech intel reveals Russian hackers using IT company front: media," UNIAN, March 19, 2019, https://www.unian.info/world/10484166-czech-intel-reveals-russian-hackers-using-it-company-front-media.html.

[98] Taylor Hatmaker, "Russian trolls are outsourcing to Africa to stoke US racial tensions," *TechCrunch*, March 12, 2020, https://techcrunch.com/2020/03/12/twitter-facebook-disinformation-africa-ghana-nigeria-ira-russia/; and Clarissa Ward, Katie Polglase, Sebastian Shukla, Gianluca Mezzofiore, and Tim Lister, "Russian election meddling is back -- via Ghana and Nigeria -- and in your feeds," *CNN*, last updated April 11, 2020, https://www.cnn.com/2020/03/12/world/russia-ghana-troll-farms-2020-ward/index.html.

recent end to a ban on encrypted messaging app Telegram[99] may appear to some as the Kremlin relenting on internet censorship and control. But such a conclusion would be overly simplistic. Moscow continues to implement internet isolation measures and has censored the internet even more aggressively during the Covid-19 pandemic.[100] Internet openness is a security threat in Putin's eyes; Russian state efforts to limit it are not going away. Questions include to what extent the Kremlin and in particular Roskomnadzor, the internet regulator, have the political willpower to force companies to alter their internet networks and install filtering equipment, and to what extent they are willing to curtail citizens' and businesses' access to the global internet in pursuit of the "isolation" goal.

- **Implications:** Policy makers in the United States and Europe should focus on the technical difficulties that Moscow will face in this effort. It will be incredibly difficult, if not outright impossible, to politically deter or dissuade the Russian government from pursuing further internet control domestically. Instead, for American and European policy makers concerned about the human rights and national security implications of this control-exertion, the question is what forms that control will take—and if, for instance, more focus on the Kremlin's technical stumbling blocks and technical pressure points can reduce the likelihood of more severe internet isolation measures taking effect.

Second, Kremlin perceptions of information onslaught from the West drive top-level attention to internet isolation.

- **Takeaway:** Internet openness, in the view of Putin and his inner *siloviki* circles, is itself a security threat, one especially driven by social media platforms based in the United States. In their view, Russia is under information attack from Western powers every day by nature of the internet's design: a relatively decentralized system that enables the free flow of information and raises barriers to state control, including because of its multi-stakeholder governance model that mixes civil society actors and private firms with governments. Any consideration for how the United States and Europe may deter future cyber and information operations given growing RuNet isolation should factor in this existing Kremlin view.

- **Implications:** Policy makers in Europe and, especially, the United States should better integrate their own internal conversations about Russian information operations and information control with international conversations about Russian internet security and cyber operations. These concepts are not separate from the Kremlin's perspective, and a more assertive push for internet isolation is now visibly merging concepts of information control with cybersecurity implications for the United States and Europe. While it has long been recognized that the Russian government's conception of "information security" is far broader than the narrow focus in much of the West (e.g., on technically protecting the confidentiality, integrity, and availability of systems and data), there are still gaps in how these concepts are discussed in American and European policy discourse and handled in those countries' bureaucracies, which undermines the ability to fully address integrated threats in the cyber domain.

Third, RuNet isolation could increase Kremlin perceptions of insulation from foreign cyber threats—resulting in more assertive cyber operations abroad.

- **Takeaway:** There is already documentation suggesting the FSB is developing DNS-targeting capabilities as Russia works to reduce its own dependence on that system. Perceived or real, Russian insulation from foreign cyber threats, through RuNet isolation, could reduce decision makers' fears of operational reciprocity and blowback. So could knowledge that foreign actors would face a changed technical landscape when attacking Russia.

- **Implications:** Policy makers in the United States and Europe should consider the importance of perceived self-insulation when evaluating RuNet, ensuring that information-gathering about Russian internet control is in conversation with information about possible shifts in Russian strategy or policy on offensive cyber operations. These considerations must also be factored into international engagement with allies and partners in response to Russian proposals for inter-

[99] "Russia 'Unblocks' Telegram Messenger in Surprise Reversal," *Moscow Times*, June 18, 2020, https://www.themoscowtimes.com/2020/06/18/russia-unblocks-telegram-messenger-in-surprise-reversal-a70620.

[100] "Генеральная прокуратура Российской Федерации направила 120 требований в Роскомнадзор о блокировке недостоверной информации о коронавирусе," GenProc.Gov.Ru, June 8, 2020, https://genproc.gov.ru/smi/news/genproc/news-1858758/.

national cybercrime norms and treaties, such as with Moscow's continually introduced codes of conduct for information security at the United Nations.

Fourth, RuNet isolation could lead the Kremlin to increase its support of non-state cyber proxies conducting cyber and information operations against foreign targets, like with the Internet Research Agency in the 2016 US election.

- **Takeaway:** If RuNet becomes further isolated and these actors need connectivity to the global internet to keep attacking targets to the Kremlin's benefit, the state may need to become more involved in providing necessary connectivity and infrastructure in some cases. This may include shifting proxy activity outside of Russia's borders.

- **Implications:** The United States and the EU should continue tracking the movement of these operations beyond Russia's geographic borders, like with the recent establishment of Internet Research Agency facilities in Ghana and Nigeria, and they should better promote international cooperation with allies and partners to expose these activities. On proxy information operations, the United States should take lessons from Europe and realize that even if deterring the Russian state from sanctioning or ignoring nonstate information and cyber operations is infeasible, there is a massive opportunity to bolster defenses at home through embracing transparency and better funding public education and awareness around these threats.[101] The White House also needs to call out and condemn these practices. And on proxy cyber operations, the United States and Europe should continue criminal investigations into relevant activities alongside sanctions and other statecraft tools aimed at nonstate actors.

Finally, the Kremlin's domestic internet pursuit in the name of Putin and "information security" may very well undermine the cybersecurity of Russian cyberspace.

- **Takeaway:** In pursuing a domestic internet and its related initiatives (e.g., a custom DNS for Russia), the Kremlin is likely undermining the cybersecurity of Russian cyberspace in attempts to bolster "information security" (i.e., regime stability through internet control). Domestic digital internet architecture could make it easier for cyber actors to interfere with traffic routing on the Russian internet, spy on internet traffic in Russia, and even more easily attribute signatures of cyberattacks originating from within Russian borders. Data localization creates more opportunities for cybercrime groups, foreign intelligence services, and other actors to access sensitive information stored in known geographic areas (though if the RuNet were to be fully isolated, that would change). There is also the chance that routine errors and failures in centralized architecture could undermine the availability and resiliency of the internet within Russia.

- **Implications:** The United States and its allies and partners should pursue opportunities to emphasize the potential economic damage the Kremlin is inflicting on Russia in pursuing the domestic internet. While the Kremlin is focused on digital development and promoting domestic tech companies' goods and services, Russian technology companies have increasingly little maneuver to push back on state internet control.[102] It is for this reason that the United States and its allies and partners should also consider public-private engagement with US and other non-Russian firms operating in Russia that have to comply with data localization laws and other internet restrictions. Emphasizing economic costs to Russia should enable a different kind of conversation about the domestic internet's harms, alongside continued dialogues on digital human rights and internet cybersecurity.

Moscow's perception of the "information space" struggle as constant and without end "suggests that the Kremlin will have a relatively low bar for employing cyber in ways that U.S. decision makers are likely to view as offensive and

[101] Margaret L. Taylor, "Combating disinformation and foreign interference in democracies: Lessons from Europe," Brookings Institution, July 31, 2019, https://www.brookings.edu/blog/techtank/2019/07/31/combating-disinformation-and-foreign-interference-in-democracies-lessons-from-europe/; Alina Polyakova and Daniel Fried, "Europe is starting to tackle disinformation. The U.S. is lagging," *Washington Post*, June 17, 2019, https://www.washingtonpost.com/opinions/2019/06/17/europe-is-starting-tackle-disinformation-us-is-lagging/; Erik Brattberg and Tim Maurer, *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks,* Carnegie Endowment for International Peace, May 2018, https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435.

[102] Dylan Myles-Primakoff and Justin Sherman, "Russia's Internet Freedom Shrinks as Kremlin Seizes Control of Homegrown Tech," *Foreign Policy*, October 26, 2020, https://foreignpolicy.com/2020/10/26/russia-internet-freedom-kremlin-tech/.

escalatory in nature."[103] This was already the case before further internet isolation was called for under the May 2019 law. Should internet isolation be further pursued, or even be successful to the extent the Kremlin desires (subject to overcoming notable technical hurdles), it could change the Russian internet landscape and shift Russian cyber behavior in ways that harm human rights, shift and increase security risks to the United States and Europe, and possibly undermine the cybersecurity of the Russian internet in the process. Policy makers ought to pay attention.

**Justin Sherman** is a nonresident fellow at the Atlantic Council's Cyber Statecraft Initiative, where his work focuses on the geopolitics, governance, and security of the global internet. He is also a research fellow at the Tech, Law & Security Program at American University Washington College of Law, a cyber policy fellow at the Duke Tech Policy Lab, and a contributor at *WIRED* Magazine.

**The author would like to thank Trey Herr, Rafal Rohozinski, Kenneth Geers, Jaclyn Kerr, Dylan Myles-Primakoff, Brian Whitmore, Maria Snegovaya, Matthew Kroenig, and one reviewer who wished to remain anonymous for their comments on earlier versions of this document. The author would also like to thank all of the participants, who shall remain anonymous, in a workshop on the topic for their insights, as well as Trey Herr and Simon Handler for their support.**

[103] Michael Connell and Sarah Vogler, *Russia's Approach to Cyber Warfare,* Center for Naval Analyses, March 2017, https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf, 1.

Atlantic Council

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org