CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

КООРДИНАЦИОННЫЙ ЦЕНТР ПРАВИТЕЛЬСТВА РОССИЙСК
ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ
КООРДИНАЦИОННЫЙ ЦЕНТР ПРАВИТЕЛЬСТВА РОСС

APRIL 2021 | THE RETURN OF GLOBAL RUSSIA

New Tools, Old Tricks: Emerging Technologies and Russia's Global Tool Kit

Andrew S. Weiss

New Tools, Old Tricks: Emerging Technologies and Russia’s Global Tool Kit

Andrew S. Weiss

Carnegie does not take institutional positions on public policy issues; the views represented herein are those of the author(s) and do not necessarily reflect the views of Carnegie, its staff, or its trustees.

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

Cover photo: Mikhail Metzel\TASS via Getty Images

CONTENTS

Summary

How will the Kremlin's tool kit evolve as emerging technologies like artificial intelligence, machine learning, and deepfake forgeries become more widespread?

Russia has long struggled to overcome the constraints imposed by the country's chronic inability to retain talent in support of homegrown innovation and R&D. That reality may consign it to a follower role in the technological realm. Russia's global activism continues to lean heavily on tried-and-true tactics and capabilities that are popping up more frequently in a variety of far-flung venues. The blatant and often sloppy nature of such efforts suggests the Russian leadership believes that even adverse publicity helps strengthen Moscow's claim to the status of a global power.

Part of what makes the Kremlin's current calling cards easier to spot—and more difficult to counter or deter—is a remarkable indifference to their knock-on effects. Present-day Russian cyber and influence campaigns are capable of doing a lot of damage—even if they can also sometimes be quite clumsy or fail to advance Russian strategic objectives. At the same time, Russia's operators are likely to remain highly technically capable and to make their mark by being operationally aggressive rather than by pioneering major technological advances.

> "Myths work as conceptual aids, reducing complexity, condensing narratives, and making novel yet unknown technologies approachable, either in a utopian or dystopian way."
>
> Thomas Rid, *Rise of the Machines* (2016)

Introduction

Russia's decline and technological backwardness have been touchstones for Western analyses and threat perceptions for centuries. The notion that it could not possibly compete head-to-head with more advanced countries has frequently provided false comfort to Western leaders. Even today overstated assessments of the fragility of the Russian economy encourage wishful thinking that the Kremlin will eventually come around and see the benefits of a more stable and cooperative relationship with the outside world.

In the wake of Russia's undeclared war against Ukraine in 2014 and interference in the 2016 U.S. presidential election, a common reverse of such thinking has taken hold in some Western policy and analytical circles, focusing on the Kremlin as a larger-than-life, all-powerful adversary that cunningly generates many of the ills that have befallen the West. As the cyber and disinformation expert Thomas Rid has warned, "The Kremlin's rulers are particularly adept at gaming elements of this new age, or at the very least are good at getting everyone to talk about how good they are, which could be the most important trick of all."[1]

A closer look at Russia's capabilities, intentions, and recent behavior, along with an examination of its likely path of development, tell the story of something in-between. To be sure, the dark arts practiced by the Russian security establishment have rattled much stronger adversaries like the United States. With Russia's ambitions becoming increasingly global, many of these tactics are now being utilized in various parts of Europe, the Balkans, the Middle East, sub-Saharan Africa, and Latin America.

At the same time, though, Russia's global tool kit has not evolved all that much. Time and again, it tries out the same approaches in different regions, with varying results.[2] For the most part, Moscow leverages the cultivation of high-level political and diplomatic relationships, arms sales, intelligence cooperation, security assistance and military training, propaganda and disinformation, energy and commercial opportunities involving Russian private and state-sector players, debt forgiveness, and using proxies. Many of the Kremlin's current approaches to global competition have clear analogues in the Cold War struggle with the United States in the developing world.[3]

Yet part of what makes the Kremlin's current calling cards easier to spot—and more difficult to counter or deter—is a remarkable indifference to the knock-on effects of its behavior. Present-day Russian cyber and influence campaigns are capable of doing a lot of damage—even if they can also sometimes be clumsy or fail to advance Russian strategic objectives (and even if some of that damage stems from U.S. misperceptions or mis-reactions to Russian activity). Russia's operators are highly technically capable, but more than that they are operationally aggressive and innovative. This kind of operational art and bravado can mean more sometimes than pure technical chops.

Russia has had a lot of "firsts" in this domain. Since the mid-2000s, it has piloted and refined strategies that combine traditional cyber operations with asymmetric attacks to undermine adversaries' information ecosystem and political processes. The war in Ukraine pushed these efforts to the next level. In 2015 the BlackEnergy cyber operation against a Ukrainian power utility turned off the lights and heat in the dead of winter in the Ivano-Frankivsk region, leaving thousands in the dark and cold on Christmas Eve. Industroyer, a substantially more sophisticated attack in December 2016, caused dangerous and widespread electricity outages in Ukraine's capital, Kyiv. In June 2017, the NotPetya attack, disguised as a run-of-the-mill ransomware virus, partially crippled the Ukrainian economy by destroying vast amounts of data and computers belonging to the government, private sector, and critical infrastructure. The NotPetya worm, which Donald Trump's administration described as "the most destructive and costly cyber-attack in history," quickly spread beyond Ukraine's borders and caused billions of dollars in losses.[4]

More recently, the SolarWinds hack conducted by Russia's Foreign Intelligence Service (SVR) exposed the vulnerabilities of the cyber supply chain and had a broad impact on thousands of private sector companies in the United States and other countries. (Attacks on the cyber supply chain are not a new phenomenon and have been documented by security experts since at least 2015.) Some cyber experts, including Dmitri Alperovitch, have suggested this type of cyber-espionage operation should not be portrayed as being outside the bounds of permissible activities.[5] There is a countervailing argument that certain types of mega-hacks, even if not explicitly or initially destructive, should be considered destabilizing and subject to norms of restraint or at least met with forceful responses by the U.S. government.

This long-running Russian campaign of technology-enabled troublemaking has greatly magnified fears about future threats. Given the track record of the Kremlin and its proxies in seizing upon the harmful capabilities offered by social media and other online platforms, there is growing worry that Russia will make similar use of rapidly maturing advanced technologies such as artificial intelligence (AI), machine learning, and the sophisticated audiovisual fabrications and manipulations known as "deepfakes." According to the final report of the U.S. National Security Commission on AI, published last month, "AI is deepening the threat posed by cyber attacks and disinformation campaigns that Russia, China, and other state and non-state actors are using to infiltrate our society, steal our data, and interfere in our democracy. The limited uses of AI-enabled attacks to date are the tip of the iceberg."[6]

In light of such sweeping predictions, a look at the state of Russia's tool kit, the country's capacity for technological innovation, particularly in the areas of AI and machine learning, and the long-term challenges facing the Russian tech sector is timely. Assembling a completely accurate picture of Russia's future global tool kit is an impossible task. Russian government entities have every incentive to shroud advanced technologies or exquisite capabilities that are currently under development. This paper, which is based on open source reporting, assesses the extent to which Russian actors have successfully embraced certain technological innovations to enhance the Kremlin's global activism. It also examines whether existing, off-the-shelf capabilities are largely adequate for the Kremlin's purposes. Finally, the paper also draws inferences regarding the possible future evolution of Russia's tool kit.

At the end of the day, Russia's claim to major-power status and ability to act as one will be rooted primarily in its nuclear and hard-power capabilities, not on generating false personas on social media or spreading disinformation using machine learning. Ongoing military modernization efforts such as the development of strategic conventional systems, anti-satellite weapons, and the like lie outside the scope of this paper.

It is also worth asking what lessons to take away from the avalanche of embarrassing revelations about rogue activities by Russian state actors and proxies. Some have been so noisy and conspicuous that one is left with the impression nobody on the Russian side actually expected them to remain secret. For example, the Main Intelligence Directorate (GRU) team that carried out the botched Novichok attack on Sergei and Yuliya Skripal in the United Kingdom in 2018 and the recently disclosed attack on an arms depot in the Czech Republic in late 2014 displayed remarkably sloppy tradecraft and a lack of attention to the conspicuous dangers that their actions posed to innocent citizens.[7] The same can be said for the Internet Research Agency (IRA) and its easily discoverable activities in the United States and other parts of the world in the wake of the 2016 election.[8] In recent years, the IRA has appeared less interested in global domination than trolling U.S.-based adversaries or generating favorable public relations for its paymaster Yevgeny Prigozhin in his quest for the Putin regime's patronage and largesse.[9]

Falling Further Behind

It is increasingly difficult to reconcile the image of Russia as a rising global power with the country's stagnant economy and long-standing difficulties in developing advanced technologies. With the Putin system now in its third decade, a familiar list of ills continue to hold Russia back: the failure to shift the economy away from its overwhelming reliance on the export of hydrocarbons, the increasingly dominant and predatory role of the state sector, and the lack of strong protections for private property and the rule of law. As with any country, Russia's ability to promote innovation will be driven by disparate factors—for example, the level of research and development (R&D) spending by the private sector and government, the education level and talents of the country's workforce, demographics, the emergence of globally competitive Russian firms, the pace of adoption of advanced technologies, and the clustering of innovation activities in certain regions.

As of now, the picture is, putting it charitably, mixed. The state has long been the dominant force behind the level of R&D spending, but this has barely budged since the 1990s (see figure 1). A deep-seated aversion to structural reforms makes it unlikely that the Russian leadership will transform the status quo and poor investment climate over the next five years. Nor does Russia seem likely to witness the emergence of a vibrant cohort of small and medium-sized enterprises capable of generating innovation for the rest of the economy.

Despite abundant human capital and a rich history of scientific and technological accomplishment inherited from the Soviet period, Russia today barely cracks the Top 50 of the Global Innovation Index prepared by the UN World Intellectual Property Organization.[10] It lags behind countries like Thailand, Ukraine, and Romania. Since the late 1990s a large number of Russians with advanced technical skills have left the country in search of professional opportunities and higher living standards. The leading lights of Russia's scientific and engineering communities are increasingly found in the United States, Israel, and a great many other countries. Meanwhile, the total number of scientific and technology researchers working in Russia today has declined by nearly 65 percent compared to 1990 levels, and the number of graduate students was cut almost in half over the past decade.[11] The number of researchers departing Russia annually has increased sharply since 2012, according to Russian Academy of Sciences head scientific secretary Nikolai Dolgushkin.[12] Senior Federal Security Service (FSB) officials portray the continued emigration of IT specialists as a serious threat to national security (see figures 2 and 4).[13]

Despite frequent lip service from political figures about the importance of creating a competitive digital economy based on homegrown champions like Yandex and Sber, both of which spend heavily on R&D, the government's actions tell a different story. The tech sector has been hurt by increasingly heavy-handed moves carried out in the name of national security. Opportunities for collaboration with and investment opportunities involving Western firms have slowly dried up in the wake of U.S. and EU sanctions and the spate of well-publicized Russian cyber operations against Western targets. Meanwhile, bans on the use of

Russian President Vladimir Putin visits Yandex headquarters in Moscow.
(Photo by Alexei Druzhinin\TASS via Getty Images)

foreign-origin software and tech equipment by firms designated as critical infrastructure will enter into force in January 2024 and January 2025, respectively. These politically inspired moves to promote import substitution have been challenged by regime stalwarts such as Gazprom CEO Alexei Miller, but they are unlikely to disappear.[14]

Targeted top-down government initiatives to foster innovation have been mainstays of Russian science and technology policy since the mid-1990s. But they have done little to change the trajectory of technological development. According to a recent report by the Higher School of Economics in Moscow, the country's failure to develop advanced technologies risks consigning it to a position of being "permanently left behind."[15] Despite outlays of nearly a trillion rubles (roughly $13 billion at today's exchange rate) between 2006 and 2020 on state programs to foster innovation, spending on R&D in 2020 was an anemic 1.16 percent of total GDP and well below the government's 3 percent target (see figure 3).[16] The Russian government continues to out-spend the private sector on a roughly two-to-one basis, which is the inverse of the situation in countries that Russia seeks to emulate, according to Academy of Sciences chief Aleksandr Sergeyev.[17]

The launch of the Skolkovo tech park in Moscow and smaller tech incubators in other parts of the country served as signature initiatives during Dmitri Medvedev's presidency. They briefly attracted interest from prominent Russian firms and foreign tech players but generally have failed to disrupt these broader trends. The national project Nauka (Russian for "science") initiated by Putin in 2018 to bolster scientific expertise has fallen far short of its targets; there are few signs that such initiatives have had a transformative impact on the overall dynamics and incentives at work in the economy or government policymaking.[18]

Russian President Vladimir Putin listens to Sber CEO German Gref.
(Photo by Alexey Nikolsky/Sputnik/AFP via Getty Images)

The initiatives that have worked somewhat better often appear to be aimed primarily at gaming Russia's standings in various technology-related indices and league tables. For example, offering cash incentives for Russian researchers to increase the number of articles they submitted for publication created a flood of contributions on various topics in indexed journals between 2012 and 2018. However, their scientific merit has been questioned, given the significant number of articles by single authors and their relatively low levels of citations by other researchers.[19] The reputational effects of a major plagiarism scandal at the Russian Academy of Sciences in early 2020 also continue to linger (see table 1).[20]

Clearly, the challenges facing technology development in Russia will not be overcome through such bureaucratic sleight of hand. Unlike their peers in China, with its vast population and burgeoning economy, Russian engineers have few innate national advantages when it comes to developing the large data sets or commercial applications that underlie innovation in fields like AI. Meanwhile, the authorities and security services have steadily sought to choke off exchanges and foreign scientific cooperation. Most recently, in March, the Duma passed a new law requiring educational institutions and universities to seek approval from federal ministries for foreign-related activities.[21] Its expansive wording conceivably covers foreign participation in joint educational and scientific activities, foreign travel, and participation in foreign conferences and organizations, among other things. A series of high-profile espionage prosecutions against academic researchers has also had a chilling effect inside major research institutions.[22]

The government is counting primarily on the defense sector to generate major technological advances in the field of AI. By necessity, the scope of defense-related AI research is fairly narrow with a particular focus placed on applications and systems in a handful of areas: robotics and autonomous systems, unmanned aerial vehicles, electronic warfare (EW), and information operations. As researchers Samuel Bendett and Margarita Konaev point out, some of these efforts are paying off.[23] For example, the military tested various AI-enabled systems during the ongoing campaign in Syria with decent results in areas such as EW jamming equipment and unmanned ground vehicles for demining operations. But Russia is so far behind other countries in its effort to develop AI that its start-ups and researchers barely register in a landscape dominated by Chinese and U.S. competitors.[24]

Количественное голосование
Государственная Дума
12:00:06
За .... 432 ч. 96.0%
Против .... 0 ч. 0.0%
Воздержалось .... 0 ч. 0.0%
Голосовало .... 432 ч. 96.0%
РЕШЕНИЕ ПРИНЯТО

Plenary session of the Russian State Duma.
(Photo by Sergei Savostyanov\TASS via Getty Images)

A Tool Kit Consisting of Oldies But Goodies

There are major differences between how Russia behaves in conflict zones when it is engaged in full-scale military operations and the types of actions that are part and parcel of its broader quest for global influence. In the latter context—specifically, situations where it faces formidable long-term competitors like the United States—Russian actors demonstrate appreciation of their limitations as well as awareness of their adversaries' strengths and weaknesses. In countries like France and Germany, where Russian figures continue to enjoy considerable entrée in political and commercial circles, there is far less need to rely on exotic capabilities to exert influence.

There is a strong argument to be made when it comes to Russia's global activism that what really matters is intent, and not necessarily the country's capacity to foster technological innovation. Much of the Kremlin's disruptive efforts in support of Trump's campaign in the 2016 election were produced on the back of existing internet platforms. It was Russian actors' level of skill and drive in exploiting these tools that distinguished them from the other international players that employ them. It seems safe to assume that there will be sufficient technical expertise in various parts of the Russian national security apparatus to devise similar gambits in the future.

Still, it is difficult to pinpoint signs of major technological advances in the conduct of recent Russian influence operations or malign activities. For example, fears of Russian interference ran extremely high ahead of the 2020 U.S. presidential election, but the techniques that the Kremlin eventually used had more in common with the 1920s heyday of the Comintern than sensationalized emerging technologies like AI and deepfakes. This is a common thread that runs through the 2020 U.S. presidential election and other high-profile instances of Russian election interference (for example, the 2018 U.S. midterm Congressional elections, the 2017 French presidential election, the 2016 Dutch referendum on the EU association agreement with Ukraine, and the 2016 U.S. presidential election). More recently, many Russian efforts have been so blatant or clumsy that they seem to betray a desire to be uncovered.[25]

According to a March 2021 unclassified assessment by the Office of the Director of National Intelligence (ODNI), the Kremlin's main focus was on "conduct[ing] influence operations aimed at denigrating President Biden's candidacy and the Democratic Party, supporting former President Trump, undermining public confidence in the electoral process, and exacerbating sociopolitical divisions in the U.S."[26] The main difference between 2016 and 2020 was that there was no hack-and-release operation. Nor were there any attempts to alter "any technical aspect of the voting process, including voter registrations, ballot casting, vote tabulation, or reporting results," according to the ODNI report. As the former director of the Cybersecurity and Infrastructure Security Agency, Christopher Krebs, has explained, "Election Day was just another Tuesday on the internet."[27]

Indeed, Russian efforts relied heavily on two Ukraine-related figures with checkered pasts: Konstantin Kilimnik, a "Russian influence agent" (in the terminology of the U.S. intelligence community) and longtime colleague of Donald Trump's former campaign manager, Paul Manafort, and Andrii Derkach, a politician/agent provocateur tied to Russian intelligence. In May 2020 Derkach leaked tapes of sensitive conversations between Joe Biden when he was vice president and then president Petro Poroshenko of Ukraine, which Derkach claimed implicated Biden and his son Hunter in corrupt dealings in the country. The Russian government made no serious attempt to disguise its hand in any of these efforts. (The U.S. government sanctioned Derkach last September and called out ongoing Russia efforts "to sow discord between political parties and drive internal divisions to influence voters."[28])

Disturbingly, Trump, his closest associates, pro-Trump media outlets, and grassroots supporters eagerly embraced and promoted these materials, just as they had done with the embarrassing emails stolen by Russian intelligence operatives from Hillary Clinton's campaign and the Democratic National Committee in 2016.[29] In the end, the information supplied by Russia-tied actors like Derkach failed to generate levels of media attention comparable to what happened with the information released by Wikileaks in 2016. Still, it remains remarkable that a Russian active-measures operation was so closely connected to a sitting U.S. president and key members of his team. It is hard to imagine a more successful disinformation campaign that could have been produced using AI or machine learning.

Russian influence operations during the COVID-19 pandemic also deserve close examination. Up to now, the lion's share of attention has been focused on Russian efforts to promote the Sputnik-V vaccine and to tarnish Western governments' track records in dealing with the coronavirus. Surprisingly little attention has been paid to the fact that in December 2020 the European Medicines Agency (EMA)—the EU's drug regulator—was hacked, reportedly by both Russia- and China-tied hackers.[30] The Russia-tied threat actors reportedly obtained internal EMA documents, doctored some of them, and then made them available on an online hacker bulletin board.[31] Portions of the documents were subsequently published in the French newspaper *Le Monde*, which helped to amplify suggestions that the EMA had been subject to undue political pressure by the European Commission and ignored safety concerns as it fast-tracked approval of the Pfizer vaccine.[32] Anti-vaccination groups and conspiracy theorists have seized on the doctored documents, which continue to circulate on social media and in vaccine-hesitant communities in parts of Europe and the United States.

Such Russian efforts involve a level of human involvement (that is, a person sitting behind a keyboard) that has hardly changed in recent years. Human involvement remains a prerequisite for the types of activities that are at the heart of Russian disinformation campaigns, of spear-phishing campaigns against politicians, political campaigns, and government entities, and of the hijacking of social media platforms for nefarious purposes. The time-intensive and often tedious nature of such active measures is laid out in considerable detail in Department of Justice indictments of several Russian actors, the final report of Special Counsel Robert Mueller's investigation, and a Senate Select Committee on Intelligence report.[33]

Will the advent of new technologies create a major shift in the Russian tool kit? Perhaps. A recent report from the U.S. National Intelligence Council warns about the impending arrival of a world in which "propagandists could leverage AI, the Internet of Things, and other tools to tailor communications to large audiences, anticipate their reactions, and adapt messaging in near real time."[34] However, there is, as of this writing, no sign that such approaches are being adapted at scale for the Russian tool kit or employed as part of the Kremlin's ongoing global malign activities.

The reason for this lag may have as much to do with the nature of contemporary influence operations as they do with Russian technological backwardness. Target audiences can be reached quite effectively with less sophisticated means, as shown above. As the technology researcher Tim Hwang has argued, "Online propagandists are pragmatists. They seek to wield the greatest degree of social and political influence at the lowest possible cost. . . . There is no need to spend additional resources creating an elaborate fake video when simply copying an image from elsewhere and misleadingly captioning it will achieve the same impact."[35] At the same time, it is conceivable that advanced players like Russia could be more successful with a bit of money and persistence.

A similar reality check may be in order when assessing the state of Russia's offensive cyber capabilities and how ongoing technological advances may—or may not—enhance their future role in its global tool kit. Undoubtedly, Russia will remain a top-tier cyber state actor for the foreseeable future. But we should be careful not to mythologize its capabilities. According to Marcus Willet, former senior cyber expert at the Government Communications Headquarters (GCHQ), a UK intelligence agency,

> "We should not conclude that Russia is in any way the master of the internet, or that it outclasses the U.S. at cyber operations. Far from it—Russia is so worried about what it has learned about U.S. and allied cyber capabilities from U.S. intelligence leaks (especially Edward Snowden's) and by U.S. commercial dominance of internet technology (exemplified by U.S. pressure on the Chinese IT company Huawei) that the Russian government is seeking ways to isolate Russia physically from the global internet, despite the economic and social disadvantages of doing so."[36]

Assessments of the SolarWinds hack suggest that the operation's success was largely driven by fundamental weaknesses present in the cyber supply chain and the remarkable degree of stealth and discipline displayed by the SVR operators who conducted it. As former GCHQ Director Robert Hannigan has explained, "The truth is that enterprise IT and software companies—and many of the thousands of smaller companies in the average supply chain—often have significant weaknesses. Far from being unforeseen and unpreventable, these attacks are becoming wearily predictable."[37]

As Western policymakers ponder the future evolution of Russian capabilities, they should also take note of a vigorous debate in expert circles on whether AI and machine learning will have a truly transformative effect on the potency of offensive cyber operations. The question is not whether automation will become an important feature of Russian cyber operations—it already is. Indeed, much of the reason why the NotPetya malware spread so quickly and uncontrollably to such a wide array of victims was due to automation. In a recent paper on automating cyber attacks, Ben Buchanan, John Bansemer, Dakota Cary, Jack Lucas, and Micah Musser acknowledge that "certain offensive techniques [may] benefit from machine learning, including spearphishing, vulnerability discovery, delivering malicious code into networks, and evading cyber defenses."[38] At the same time, they caution that predictions that machine learning will transform cyber attacks are possibly overblown. "Attackers, especially states, are generally rational and will only turn to machine learning techniques," they write, "if these techniques are simpler, cheaper, or more effective than the automated tools that are already available and easy to use."

Conclusions

As Carnegie's ongoing research project on the Return of Global Russia has shown, Russia's activity around the world needs to be taken seriously and scrutinized carefully.[39] At the same time, its capabilities should be evaluated without yielding to alarmism or exaggeration. This is essential for forming an accurate yet clear-eyed assessment of the Kremlin's actual influence beyond its immediate periphery. It also means recognizing the gap between actual Russian capabilities and the Russian government's aspirations and self-serving narratives.[40]

Western policymakers should pay greater attention to pertinent instances of Russia's overreach and failure on the global stage. Such examples typically point not only to the meagerness of the existing Russian tool kit but also to long-term sources of Western strength and resilience. None of this is to downplay the risks that lie ahead or the harmful nature of recent Russian behavior. As CIA Director (and former Carnegie Endowment for International Peace president) Bill Burns has repeatedly warned, "Declining powers can be at least as disruptive as rising powers."[41] At the same time, Western policymakers must be able to set clear priorities and avoid playing into the Kremlin's hands. After all, one key motivating factor behind Russian global activism is simply to distract Western policymakers from issues closer to home that the Kremlin actually thinks are of paramount importance and to throw them off-balance.

That means being able to identify the types of Russian actions that are most concerning and resisting the temptation to enter into a game of whack-a-mole in theaters of lesser importance. To be sure, serious harm can be done to the national security and prosperity of the United States and the EU through, say, careless Russian cyber attacks like NotPetya or destabilizing military moves in Ukraine. The flow of disinformation from niche online platforms operated by the Russian security services or the presence of Russian mercenaries in the Central African Republic are the kinds of problems that Western policymakers can afford to live with, albeit unhappily.

At the same time, they must stay closely attuned to the potential evolution of the Russian tool kit and be prepared for the Kremlin's use of AI and machine learning to match the pattern that has been observed in the information domain. If these technologies disseminate somewhat widely, Russia can be a "fast follower" and operational innovator in applying such tools to its global activism, even if Russian engineers are not the ones actually inventing, for example, new forms of deep learning.

Hence, Russia's small AI/machine learning research field and its structurally challenged tech sector may matter less than its durable criminal and intelligence/military sectors, which have proven capable of funding a large and dangerous cyber/influence enterprise that continually develops or incorporates new techniques and patterns of activity. These actors will help determine the balance between the assimilation of increasingly sophisticated and destabilizing technologies and the continued reliance on tried-and-true tactics. For the foreseeable future, tools in the latter category appear likely to dominate.

About the Author

Andrew S. Weiss is the James Family Chair and a vice president for studies at the Carnegie Endowment for International Peace, where he oversees research in Washington and Moscow on Russia and Eurasia.

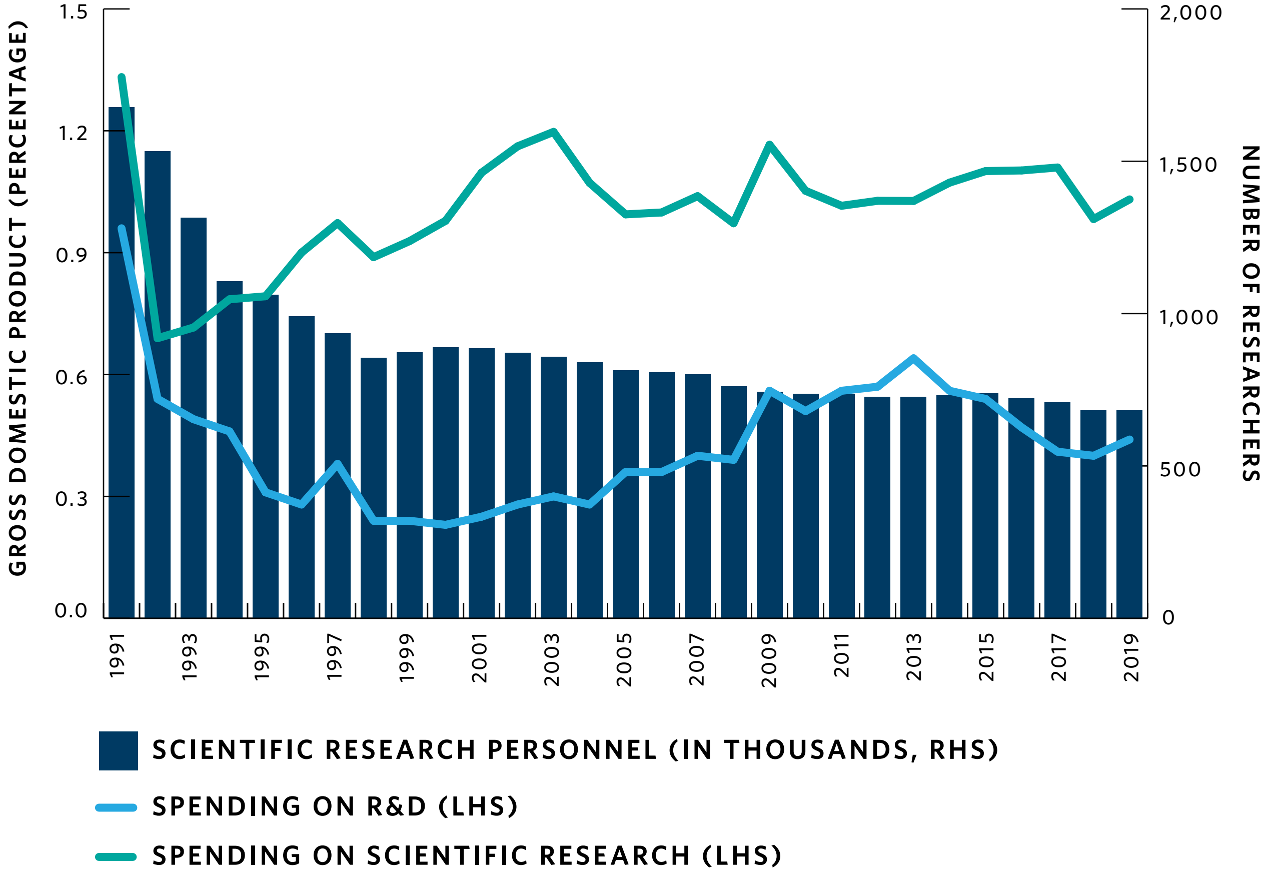
Acknowledgements

The author is grateful to Jon Bateman, Christopher Chivvis, Steven Feldstein, Leonid Kovachich, Robert Otto, and Nathaniel Reynolds for their exceptionally helpful and constructive comments on an earlier draft of this paper. Grace Kier provided outstanding research assistance, which also benefited from Tatyana Pyak's energetic contributions. The author bears full responsibility for any remaining errors of fact or judgment. This study was undertaken with generous financial support from the Royal Norwegian Ministry of Foreign Affairs.

Appendix: Figures on Russia’s Struggle With Innovation

FIGURE 1

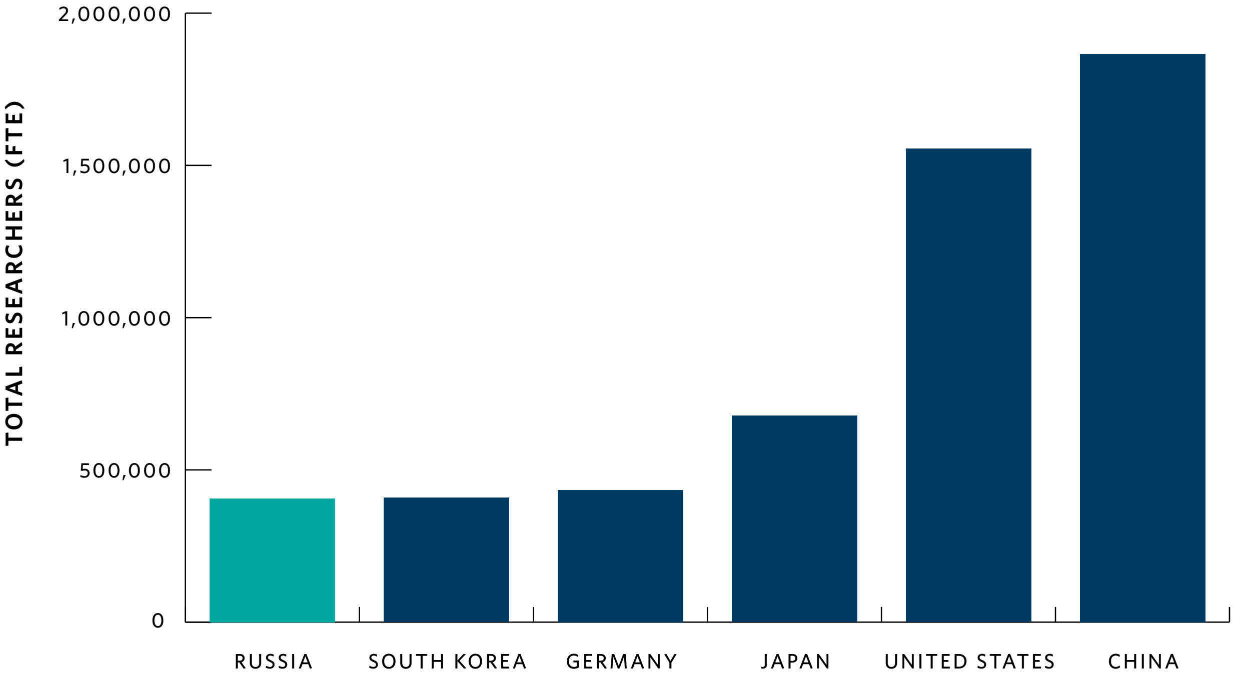
Russia's R&D Challenge



SOURCE: Federal State Statistics Service, "Nauka i innovatsii" [Science and Innovation], Rosstat, https://rosstat.gov.ru/folder/14477.

FIGURE 2

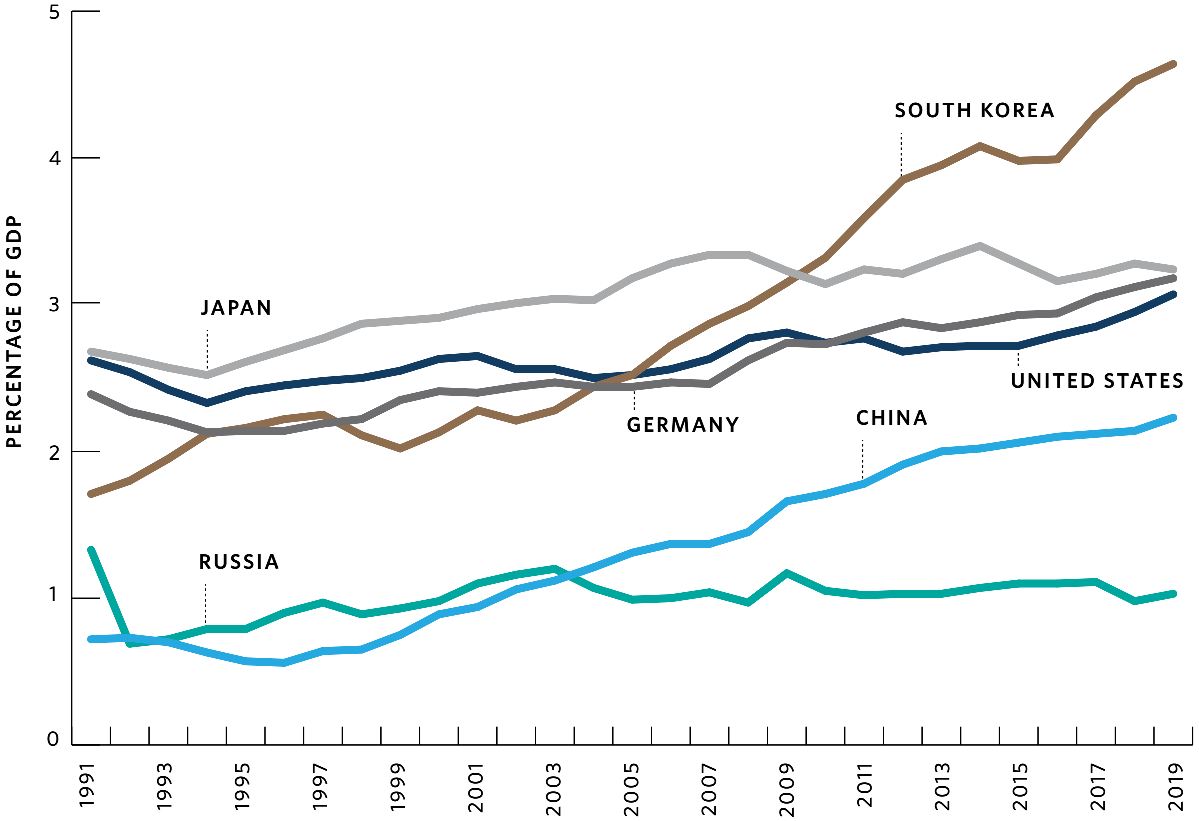
Number of Scientific Researchers in Select Countries (2018)



SOURCE: OECD.stat, "Main Science and Technology Indicators," Organisation for Economic Co-operation and Development, https://stats.oecd.org/Index.aspx?DataSetCode=MSTI_PUB.

FIGURE 3

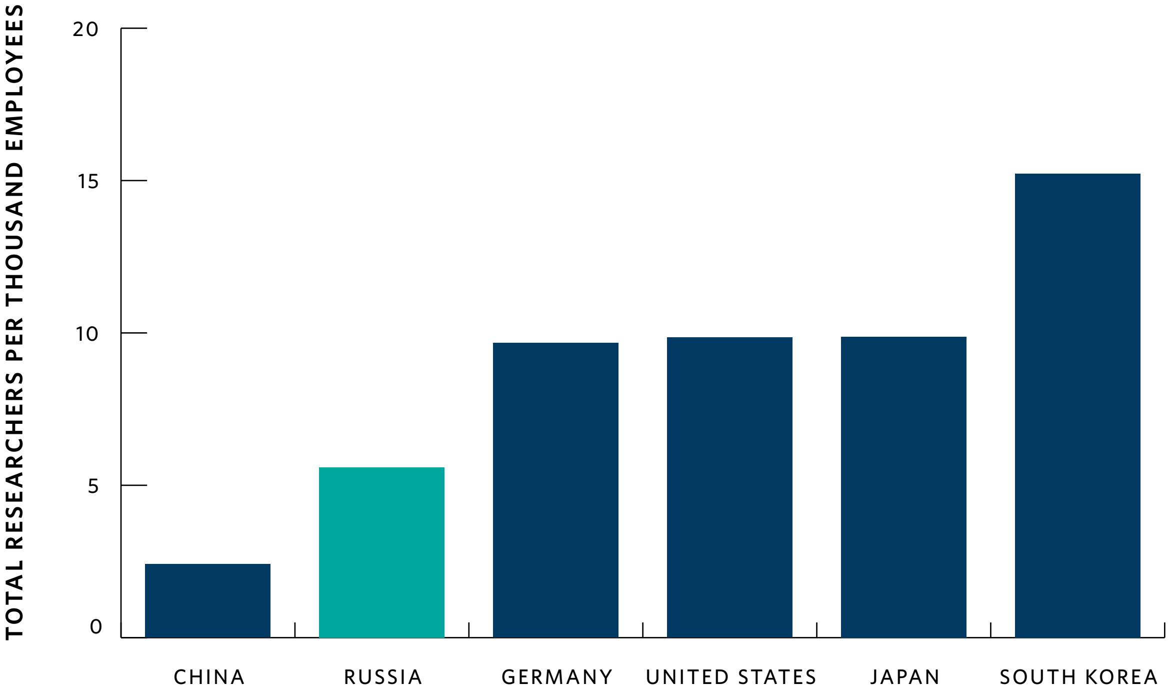
R&D Spending as a Percentage of GDP in Select Countries



SOURCE: OECD Data, "Gross domestic spending on R&D (indicator)," Organisation for Economic Co-operation and Development, 2021, https://data.oecd.org/rd/gross-domestic-spending-on-r-d.htm.

FIGURE 4

Scientific Workforce Per 1,000 Employees in Select Countries (2018)



SOURCE: OECD.stat, "Main Science and Technology Indicators," Organisation for Economic Co-operation and Development, https://stats.oecd.org/Index.aspx?DataSetCode=MSTI_PUB.

TABLE 1
Russia-Based Scientists Struggle for Recognition

Rank	Country	Number of Highly Cited Researchers	Percent of Highly Cited Researchers
1	United States	2,650	41.5%
2	China	770	12.1%
3	UK	514	8.0%
4	Germany	345	5.4%
5	Australia	305	4.8%
6	Canada	195	3.1%
7	Netherlands	181	2.8%
8	France	160	2.5%
9	Switzerland	154	2.4%
10	Saudi Arabia	104	1.6%
33	Russia	6	0.09%

SOURCE: Clarivate Web of Science, "Highly Cited Researchers," Clarivate, 2020, https://recognition.webofscience.com/awards/highly-cited/2020/?campaignname=Highly_Cited_Researchers_Parent_SAR_Global_2020&campaignid=7014N000001r&utm_campaign=Highly_Cited_Researchers_Parent_SAR_Global_2020&utm_source=earned_coverage&utm_medium=press.

Notes

[1] Joshua Yaffa, "Is Russian Meddling as Dangerous As We Think?," *New Yorker*, September 7, 2020, https://www.newyorker.com/magazine/2020/09/14/is-russian-meddling-as-dangerous-as-we-think.

[2] See Paul Stronski and Richard Sokolsky, "The Return of Global Russia: An Analytical Framework," Carnegie Endowment for International Peace, December 14, 2017, https://carnegieendowment.org/2017/12/14/return-of-global-russia-analytical-framework-pub-75003; Julia Gurganus and Eugene Rumer, "Russia's Global Ambitions in Perspective," Carnegie Endowment for International Peace, February 20, 2019, https://carnegieendowment.org/2019/02/20/russia-s-global-ambitions-in-perspective-pub-78067.

[3] See, for example, "The Soviet State Propaganda Apparatus," declassified CIA Research Paper, April 1986, https://www.cia.gov/readingroom/document/cia-rdp87t00787r000200170003-4, and "The Soviet Military Advisory and Training Program for the Third World," declassified CIA Research Paper, April 1984, https://www.cia.gov/readingroom/docs/DOC_0000497180.pdf.

[4] Sarah Sanders, "Statement from the Press Secretary," White House, February 15, 2018, https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/.

[5] Dmitri Alperovitch and Ian Ward, "How Should the U.S. Respond to the SolarWinds and Microsoft Exchange Hacks?," Lawfare, March 12, 2021, https://www.lawfareblog.com/how-should-us-respond-solarwinds-and-microsoft-exchange-hacks.

[6] National Security Commission on Artificial Intelligence, "Final Report," NSCAI, March 19, 2021, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

[7] Bellingcat Investigation Team, "Senior GRU Leader Directly Involved With Czech Arms Depot Explosion," Bellingcat, April 20, 2021, https://www.bellingcat.com/news/2021/04/20/senior-gru-leader-directly-involved-with-czech-arms-depot-explosion/.

[8] See https://home.treasury.gov/news/press-releases/jy0126, https://home.treasury.gov/news/press-releases/sm0312, https://home.treasury.gov/news/press-releases/sm577. For more on the flamboyance and incompetence of top Prigozhin lieutenants Maksim Shugalei and Alexander Malkevich, see https://www.proekt.media/en/article/evgeny-prigozhin-africa/ and https://www.nytimes.com/2020/06/18/world/middleeast/russia-libya-maksim-Shugalei.html.

[9] See Nathaniel Reynolds, "Putin's Not-So-Secret Mercenaries: Patronage, Geopolitics, and the Wagner Group," Carnegie Endowment for International Peace, July 8, 2019, https://carnegieendowment.org/2019/07/08/putin-s-not-so-secret-mercenaries-patronage-geopolitics-and-wagner-group-pub-79442.

[10] Soumitra Dutta, Bruno Lanvin, and Sacha Wunsch-Vincent (eds.), *Global Innovation Index 2020* (Geneva, Switzerland: World Intellectual Property Organization, 2020).

[11] "RAN: kolichestvo uchenykh, uyezzhayushchikh iz Rossii, vyroslo v pyat' raz s 2012 goda" [RAS: the number of scientists leaving Russia has grown fivefold since 2012], NEWSRu.com, April 20, 2021, https://www.newsru.com/russia/20apr2021/ran.html.; TASS, "Glava RAN rasskazal, chto kolichestvo aspirantov v Rossii sokratilos' pochti vdvoye" [The head of the Russian Academy of Sciences said that the number of graduate students in Russia has almost halved], TASS, April 20, 2021, https://nauka.tass.ru/nauka/11194719.

[12] "RAN: kolichestvo uchenykh, uyezzhayushchikh iz Rossii, vyroslo v pyat' raz s 2012 goda" [RAS: the number of scientists leaving Russia has grown fivefold since 2012], NEWSRu.com.

[13] Interfax, "V FSB nazvali ser'yeznym vyzovom ottok kvalifitsirovannykh IT-spetsialistov za rubezh" [The FSB called the outflow of qualified IT specialists abroad a serious challenge], Interfax, April 21, 2021, https://www.interfax.ru/russia/762434.

14 Lyudmila Podobedova, Inna Sidorkova, and Daria Chebakova, "Glava «Gazproma» otsenil v ₽180 mlrd perekhod kompanii na rossiyskoye PO" [The head of Gazprom estimated the company's transition to Russian software at ₽180 billion], RBK, March 23, 2021, https://www.rbc.ru/business/23/03/2021/605887c89a79476b5398b6ab.

15 Daria Chebakova, Ivan Tkachev, and Vladislav Skobelev, "Eksperty predupredili o riske dlya Rossii «navsegda otstat'» v tekhnologiyakh" [Experts warn about the risk for Russia to "lag behind forever" in technology], RBK, April 13, 2021, https://www.rbc.ru/technology_and_media/13/04/2021/607478fc9a794731d03611ab; Yu. V Simachev, A.A. Fedyunina, M.A. Yurevich, M.G. Kuzyk, N.N. Zudin, and N.A. Gorodny, *Rossiya na rynkakh peredovogo proizvodstva [Russia in advanced production markets]* (Moscow, Russia: Higher School of Economics, 2021), 6.

16 Alexander Sokolov, "Instituty razvitiya provalili innovatsii" [Development Institutions Failed Innovation], Vedomosti, March 2, 2021, https://www.vedomosti.ru/economics/articles/2021/03/01/859742-instituti-razvitiya.

17 Igor Chernyak, "Budet nam nauka. Prezident RAN—o nasushchnykh problemakh i nadezhdakh uchonykh" [There will be science for us. President of the Russian Academy of Sciences—on the pressing problems and hopes of scientists], Argumenty i Fakti, December 16, 2020, https://aif.ru/society/science/budet_nam_nauka_prezident_ran_o_nasushchnyh_problemah_i_nadezhdah_uchyonyh.

18 YUSI Administrator, "Natsional'nyy proyekt «Nauka»," [National project "Science"], Strategiya 24, January 10, 2019, https://strategy24.ru/rf/innovation/projects/natsional-nyy-proyekt-nauka.

19 Quinn Schiermeier, Russia aims to revive science after era of stagnation," Nature, March 18, 2020, https://www.nature.com/articles/d41586-020-00753-7.

20 Dalmeet Singh Chawla, "Russian journals retract more than 800 papers after 'bombshell' investigation," Science, January 8, 2020, https://www.sciencemag.org/news/2020/01/russian-journals-retract-more-800-papers-after-bombshell-investigation.

21 Legislative Support System, "O vnesenii izmeneniy v Federal'nyy zakon "Ob obrazovanii v Rossiyskoy Federatsii'" [On amendments to the Federal Law "On Education in the Russian Federation"], Duma, November 18, 2020, https://sozd.duma.gov.ru/bill/1057895-7.

22 Vera Chelishcheva, "FSB vedet okhotu na uchenykh" [FSB is hunting scientists], Novaya Gazeta, November 27, 2020, https://novayagazeta.ru/articles/2020/11/27/88134-berut-lyudey-s-opytom-lomayut-zhizni-otnimayut-rabotu-i-zdorovie.

23 Margarita Konaev and Samuel Bendett, "Russian AI-Enabled Combat: Coming to a City Near You?", War on the Rocks, July 31, 2019, https://warontherocks.com/2019/07/russian-ai-enabled-combat-coming-to-a-city-near-you/.

24 "Between 2010 and 2018, Russian researchers published 7,095 papers related to AI, while U.S. researchers published 271,464 papers and Chinese researchers published 262,112 papers." See Margarita Konaev and James Dunham, "Russian AI Research 2010 to 2018: Topics, Trends, and Institutions," Center for Security and Emerging Technology, October 2020, https://cset.georgetown.edu/wp-content/uploads/CSET-Russian-AI-Research-2010-to-2018-2.pdf, 10.

25 IRA-backed disinformation platforms active during 2020 were more notable for their clever vulgar Russian word play than the size of their American audience. PeaceData, a left-wing site that commissioned contributions from American freelancers, "sounds like *pizdato*, the obscenity for "f***-ing amazing" in the [Russian] *mat* swearing language. "Only Prigozhin would think that this influence campaign is f***** great; any reasonable observer would conclude that this is f***** insane," tweeted Sergei Radchenko, a professor of international relations at Cardiff University." See https://www.ft.com/content/447724b0-bc98-4690-a150-674f451d1b3e. An IRA-created website aimed at right-wing audiences was named NAEBC, "a pun on a Russian expletive meaning to deceive or 'screw over.'"

See https://www.reuters.com/article/usa-election-russia-disinformation/exclusive-russian-operation-masqueraded-as-right-wing-news-site-to-target-u-s-voters-sources-idUSKBN26M5OP. IRA affiliates were also active in the Central African Republic and Madagascar but their information operations model had limited effect on either country. See https://www.theguardian.com/technology/2020/dec/15/central-african-republic-facebook-disinformation-france-russia; and https://www.nytimes.com/2019/11/11/world/africa/russia-madagascar-election.html.

[26] National Intelligence Council, "Foreign Threats to the 2020 US Federal Elections," National Intelligence Council, March 10, 2020, https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf.

[27] Christopher Krebs, "We prepared for more Russian interference. But this year the assault on democracy was from within the US," CNN, December 15, 2020, https://www.cnn.com/2020/12/15/opinions/assault-on-democracy-within-the-us-krebs/index.html.

[28] U.S. Department of the Treasury, "Treasury Sanctions Russia-Linked Election Interference Actors," U.S. Department of the Treasury, September 10, 2020, https://home.treasury.gov/news/press-releases/sm1118.

[29] See, for example, Donald J. Trump, "Remarks by President Trump in Press Conference," The White House, September 7, 2020, https://trumpwhitehouse.archives.gov/briefings-statements/remarks-president-trump-press-conference-september-7-2020/; The Commission on Presidential Debates, "September 29, 2020 Debate Transcript," Commission on Presidential Debates, September 29, 2020, https://www.debates.org/voter-education/debate-transcripts/september-29-2020-debate-transcript/; Andrew S. Weiss, @andrewsweiss, Twitter post, August 17, 2020, 11:06 a.m., https://twitter.com/andrewsweiss/status/1295376467166199808?s=20.; Andrew S. Weiss, @andrewsweiss, Twitter post, September 10, 2020, 12:09 p.m., https://twitter.com/andrewsweiss/status/1304089638794145794?s=20; Laura Ingraham, @IngrahamAngle, Twitter post, October 25, 2020, 4:46 p.m., https://twitter.com/IngrahamAngle/status/1320285569621032961?s=20.

[30] European Medicines Agency press office, "Cyberattack on the European Medicines Agency," EMA, December 9, 2012, https://www.ema.europa.eu/en/news/cyberattack-european-medicines-agency.

[31] European Medicines Agency press office, "Cyberattack on EMA - update 5," EMA, January 15, 2021, https://www.ema.europa.eu/en/news/cyberattack-ema-update-5.; Huib Modderkolk, "Russian and Chinese hackers gained access to EMA," de Volkskrant, March 6, 2021, https://www.volkskrant.nl/nieuws-achtergrond/russian-and-chinese-hackers-gained-access-to-ema~bdc61ba59/.

[32] Lise Barnéoud, "Ce que disent les documents sur les vaccins anti-Covid-19 volés à l'Agence européenne des medicaments" [What documents say about anti-Covid-19 vaccines stolen from the European Medicines Agency], *Le Monde*, January 16, 2021, https://www.lemonde.fr/planete/article/2021/01/16/vaccins-ce-que-disent-les-documents-voles-a-l-agence-europeenne-des-medicaments_6066502_3244.html.

[33] See, for example, Rid, *Active Measures*, (New York: Farrar, Straus, and Giroux), 362-372; United States of America v. Viktor Borisovich Netyshko, et al., No. 1:18-cr-215 (U.S. District Court for the District of Columbia), 6-19, https://www.justice.gov/file/1080281/download;
Robert S. Mueller, Report On The Investigation Into Russian Interference In The 2016 Presidential Election (U.S. Washington, D.C.: Department of Justice, March 2019), 14-41, https://www.justice.gov/archives/sco/file/1373816/download; Senate Select Committee on Intelligence, Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 2: Russia's Use of Social Media with Additional Views (116 S. Rpt. 290), 22-29, https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf; United States of America v. Elena Alekseevna Khusyaynov. No. 1:18-MJ-464 (U.S. District Court for the Eastern District of Virginia), 6-38, https://www.justice.gov/opa/press-release/file/1102316/download; United States of America v. Artem Mikhaylovich Lifshits. No. 1:20-mj-256 (U.S. District Court for the Eastern District of Virginia), 9-33, https://www.justice.gov/opa/press-release/file/1315491/download.

[34] National Intelligence Council, "Global Trends 2040: A More Contested World," National Intelligence Council, March 2021, https://www.dni.gov/files/ODNI/documents/assessments/GlobalTrends_2040.pdf.

[35] Tim Hwang, "Deepfakes: A Grounded Threat Assessment," Center for Security and Emerging Technology, July 2020, https://cset.georgetown.edu/research/deepfakes-a-grounded-threat-assessment/.

[36] Marcus Willet, "Lessons of the SolarWinds Hack," *Survival* 63, no. 2 (April-May 2021): 7-26. https://www.iiss.org/publications/survival/2021/survival-global-politics-and-strategy-april-may-2021.

[37] Robert Hannigan, "SolarWinds hack exploited weaknesses we continue to tolerate," *Financial Times*, December 20, 2020, https://www.ft.com/content/2bed3013-b21f-4b2c-8572-b2da016d1b4e.

[38] Ben Buchanan, John Bansemer, Dakota Cary, Jack Lucas, Micah Musser, "Automating Cyber Attacks: Hype and Reality," Center for Security and Emerging Technology, November 2020, https://cset.georgetown.edu/research/automating-cyber-attacks/.

[39] Eugene Rumer, Richard Sokolsky, Paul Stronski, and Andrew S. Weiss, "The Return of Global Russia: A Reassessment of the Kremlin's International Agenda," Carnegie Endowment for International Peace, https://carnegieendowment.org/specialprojects/thereturnofglobalrussia/.

[40] These themes are explored in greater depth in a forthcoming article by Eugene Rumer and Richard Sokolsky, "Getting Russia Wrong: A Retrospective and Lessons for the Future," Carnegie Endowment for International Peace, Summer 2021.

[41] William J. Burns, "How We Fool Ourselves on Russia," *New York Times*, January 7, 2017, https://www.nytimes.com/2017/01/07/opinion/sunday/how-we-fool-ourselves-on-russia.html.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

1779 Massachusetts Avenue NW | Washington, DC 20036 | P: + 1 202 483 7600

CarnegieEndowment.org