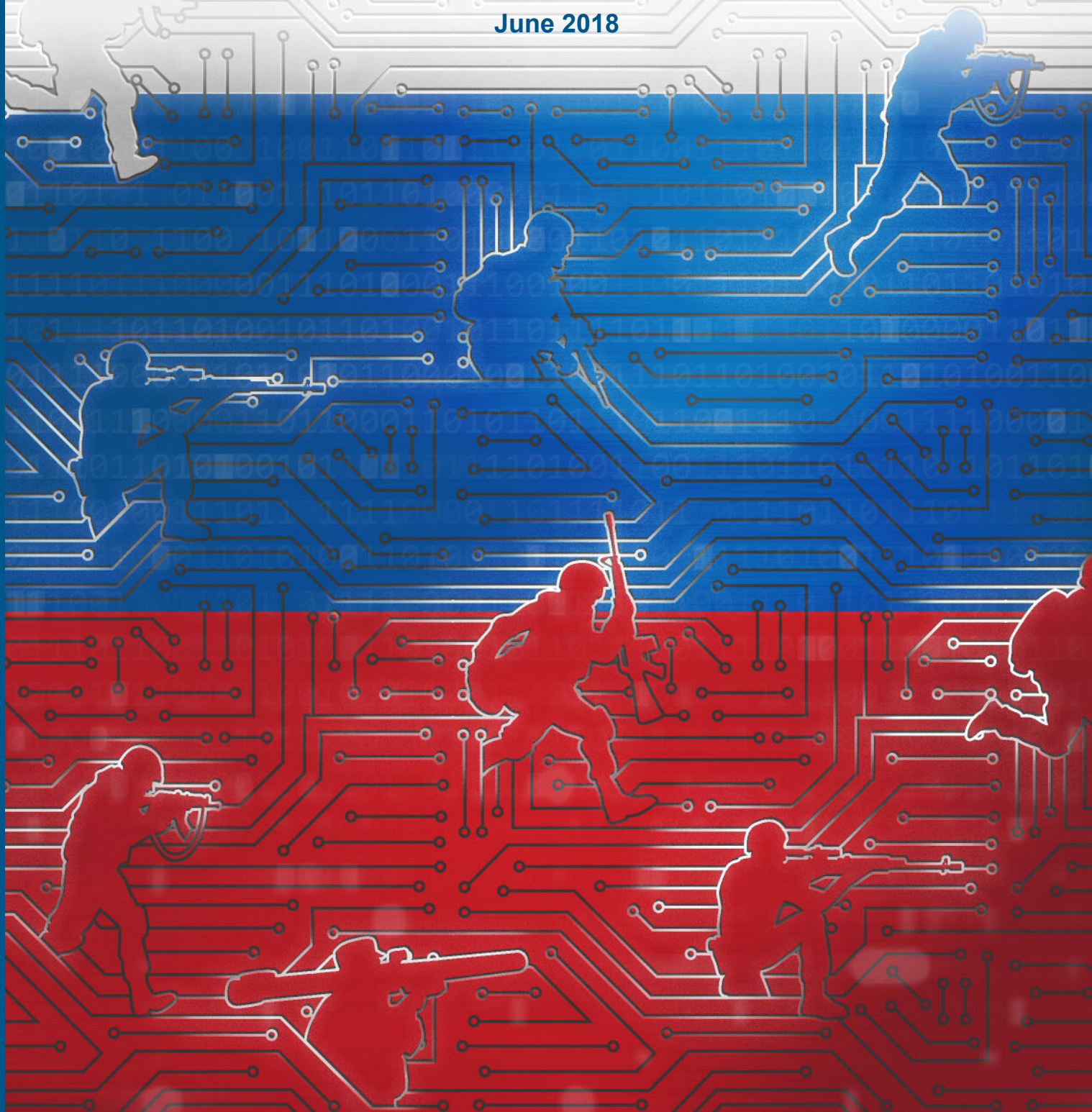
FOUNDATION FOR DEFENSE OF DEMOCRACIES

Kaspersky and Beyond

Understanding Russia's Approach to Cyber-Enabled Economic Warfare

Boris Zilberman

June 2018



Kaspersky and Beyond
Understanding Russia's Approach to Cyber-Enabled Economic Warfare

Boris Zilberman

June 2018

FDD PRESS

A division of the
FOUNDATION FOR DEFENSE OF DEMOCRACIES
Washington, DC

Table of Contents

INTRODUCTION 6

THE RISE OF KASPERSKY 7

THE KREMLIN'S LEGAL FRAMEWORK AND DOCTRINE 11

MOSCOW'S PROXIES: CYBER CRIMINALS AND TECH COMPANIES 13

BEYOND KASPERSKY 15

CONCLUSION AND POLICY RECOMMENDATIONS 17

Introduction

One of the most iconic images of the 20th century is that of U.S. Army troops wading ashore onto Omaha Beach from their landing craft on June 6, 1944 under Nazi machine gun fire to create a beachhead for the Allies.[1] The beachheads of the future, however, are being established today in cyber space. In military strategy, creating a beachhead means concentrating efforts on one area which can become a jumping-off point for a bigger operation. For America's adversaries, penetrating our technology sector is a smart and cost-effective beachhead strategy – whether the end goal is economic warfare, influence operations, or support for kinetic military operations. It is through the technology sector that America's adversaries can infiltrate the supply chains of the national security industrial base and establish backdoors into government and private networks.[2]

Hostile cyber actions against a nation's private industry are an increasingly dangerous and effective component of modern-day economic warfare, or "cyber-enabled economic warfare (CEEW)," as my colleague Dr. Samantha Ravich described it. "Both states and non-state actors are increasingly able to contemplate and deploy pernicious cyber attacks against the critical economic assets and systems of their adversaries, targeting their national security and military capabilities," Ravich and another colleague, Annie Fixler, explain.[3]

In 2016 alone, malicious cyber activity cost the U.S. economy as much as $100 billion,[4] and analyses of the direct cost of cyber crime estimate that the total will reach $6 trillion by 2021.[5] China and Russia constitute two of the biggest nation-state threats in the cyber domain. These countries use their technology sectors to conduct CEEW and to create the beachheads of the 21st century. As a 2017 report from the U.S. director of national intelligence made clear, "Russia is a full-scope cyber actor that will remain a major threat to US Government, military, diplomatic, commercial, and critical infrastructure. Moscow has a highly advanced offensive cyber program, and in recent years, the Kremlin has assumed a more aggressive cyber posture."[6]

Much of the analysis of Russia's use of asymmetric tools has focused on its efforts to undermine democratic institutions through information warfare. In the case of Russia's election interference – in the United States and across Europe – the intentions are clear: "[S]ow chaos and cynicism through exploiting divisions in society as a means of undermining democracy."[7]

---

1. Robert F. Sargent, "Landing on the coast of France under heavy Nazi machine gun fire," *National Archives and Records Administration*, June 6, 1944. (https://www.archives.gov/exhibits/picturing_the_century/worldflames/worldflames_img59.html)

2. For more information on supply chain threats, see: U.S. Defense Science Board, "DSB Task Force Report on Cyber Supply Chain," *Office of the Undersecretary for Defense*, February 2017. (https://www.hsdl.org/?abstract&did=799509); U.S. Federal Bureau of Investigation, Intelligence Bulletin, "Supply Chain Poisoning: A Threat to the Integrity of Trusted Software and Hardware," June 27, 2011; Office of National Counterintelligence Executive, "Foreign Spies Stealing US Economic Secrets in Cyberspace," *Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011*, October 2011. (https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf)

3. Samantha F. Ravich and Annie Fixler, "Framework and Terminology for Understanding Cyber-Enabled Economic Warfare," *Foundation for Defense of Democracies*, February 22, 2017. (http://www.defenddemocracy.org/content/uploads/documents/22217_Cyber_Definitions.pdf)

4. White House Council of Economic Advisors, "The Cost of Malicious Cyber Activity to the U.S. Economy," February 2018. (https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf)

5. Nick Eubanks, "The True Cost Of Cybercrime For Businesses," *Forbes*, July 13, 2017. (https://www.forbes.com/sites/theyec/2017/07/13/the-true-cost-of-cybercrime-for-businesses/#286ccc5a4947)

6. DNI Director Daniel R. Coats, "Worldwide Threat Assessment of the US Intelligence Community," *Statement for the Record for the Senate Select Committee on Intelligence*, May 11, 2017. (https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf)

7. Laura Rosenberger and Jamie Fly, "Shredding the Putin Playbook," *Democracy Journal*, Winter 2018. (https://democracyjournal.org/magazine/47/shredding-the-putin-playbook/)

This is very much the case, yet an emphasis on the propaganda value of cyber attacks should not obscure their significance as a form of CEEW. For example, Russia's 2007 attacks on Estonia may be one of the earliest cases of cyber-enabled economic warfare. When Russian hackers crippled the Ukrainian electric grid nearly a decade later, some experts continued to focus only on the propaganda value and the impact on public confidence in Kiev's government – a government which cannot reliably deliver electricity to the people loses public trust and "create[s] the perception of a failed state" – rather than also assessing the adverse economic effects and the ways they undermine Ukraine's national security.[8]

"Kaspersky Lab, the Russian antivirus company built by Eugene and Natalya Kaspersky, provides one of the best examples of how technical knowhow, market foresight, and government cooperation can produce not only a global tech giant but also a serious national security threat."

While more analysis and intelligence gathering is necessary to fully understand how Russia's military cyber doctrine seeks to weaken a nation's economy and thereby its ability to deploy military power, the United States and its allies are already feeling the effects.

Kaspersky Lab, the Russian antivirus company built by Eugene and Natalya Kaspersky, provides one of the best examples of how technical knowhow, market foresight, and government cooperation can produce not only a global tech giant but also a serious national security threat. But while Kaspersky Lab has gotten public scrutiny, other Russian tech companies, including those that are direct outgrowths of Kaspersky, have received less attention. These technology companies provide Russian authorities beachheads for other strategic initiatives.

The Rise of Kaspersky

In the 20 years since its founding in 1997, Kaspersky has seen massive growth. Today, it has over 400 million users worldwide and remains the largest software vendor in Europe.[9] In some ways, Kaspersky was the natural Russian answer to the rise of American software giants such as Microsoft and Oracle. Russian innovation tends to be spurred on not by aspirational visions of positive global or domestic change, but by perceived threats to Russian greatness or global standing. Reeling from the collapse of the Soviet Union and finding itself quickly being left behind by the technology and internet boom of the 1990s, Moscow leaned on its security services as the natural place for Russia to enhance its position in the new digital global economy.[10]

As Mikhail Gorbachev's *perestroika* initiative began to impose reform on the Soviet Union, a young Eugene Kaspersky graduated from the Technical Faculty of the KGB Higher School in 1987 (later known as the Institute of Cryptography, Telecommunications, and Computer Science).[11] After graduation, he went on to be a software engineer for the Soviet Ministry of Defense.[12] While on vacation at a KGB holiday resort in 1987, Eugene met his future wife Natalya, who was

8. For example: "Podcast: Russia's Disinformation Offensive," *FDD's Foreign Podicy*, February 6, 2018. (https://soundcloud.com/defenddemocracy/for-review-episode-7-jamie-fly-laura-rosenberger?in=defenddemocracy/sets/foreign-podicy); "Experts Suspect Russia Is Using Ukraine As A Cyberwar Testing Ground," *NPR's Fresh Air*, June 22, 2017. (https://www.npr.org/2017/06/22/533951389/experts-suspect-russia-is-using-ukraine-as-a-cyberwar-testing-ground)

9. David Goldstein and Greg Gordon, "Documents could link Russian cybersecurity firm Kaspersky to FSB spy agency," *McClatchy*, July 3, 2017. (http://www.chicagotribune.com/news/nationworld/ct-kaspersky-cyber-russia-spy-agency-20170703-story.html)

10. "The making of a neo-KGB state," *The Economist*, August 23, 2007. (https://www.economist.com/node/9682621)

11. Senator Jeanne Shaheen (D-NH), "The Russian Company That Is a Danger to Our Security," *The New York Times*, September 4, 2017. (https://www.nytimes.com/2017/09/04/opinion/kapersky-russia-cybersecurity.html)

12. Cory Flintoff, "Kaspersky Lab: Based in Russia, Doing Cybersecurity In The West," *NPR*, August 10, 2015. (https://www.npr.org/sections/alltechconsidered/2015/08/10/431247980/kaspersky-lab-a-cybersecurity-leader-with-ties-to-russian-govt)

finishing a degree in applied mathematics from the Moscow Institute of Electronic Engineering.[13]

With the fall of the Soviet Union in 1991, Eugene Kaspersky transitioned into the private sector, joining the KAMI Information Technologies Center where he developed antivirus solutions.[14] Natalya joined the company in 1994 to work on the Antivirus Project (AVP). In 1997, Eugene and Natalya created Kaspersky Lab as an outgrowth of their AVP work at KAMI. While Natalya and Eugene divorced in 1998, they continued to run Kaspersky Lab together until 2007 when she became CEO of Infowatch, a former subsidiary of Kaspersky Lab.[15]

Natalya ultimately assumed the role of CEO of Kaspersky in 1997, as Eugene became more focused on antivirus research. A biographical video on Natalya's Infowatch website claims that Eugene lacked interest in running Kaspersky Lab.[16]

In 1998, Kaspersky Antivirus was the only antivirus product on the market that was available to identify, remove, and quarantine[17] the notorious CIH computer virus (also referred to as Chernobyl) unleashed in June of that year.[18] The virus corrupted data stored on both hard drives and motherboards. Antivirus companies around the world approached Kaspersky Lab hoping to include Kaspersky solutions in established product lines.[19] The demand for, and reach of, Kaspersky exploded.

"Antivirus companies around the world approached Kaspersky Lab hoping to include Kaspersky solutions in established product lines. The demand for, and reach of, Kaspersky exploded."

In August 1998, Russia experienced a major financial crisis known as the "Ruble crisis," or the "Russian Flu." The crisis resulted in a devaluation of the ruble and eventual default on public and private debt.[20] High-technology industries played a role in the eventual recovery. A 1999 McKinsey Global Institute report showed "the software sector had the highest labor productivity in the Russian economy."[21] While other Russian software companies also gained prominence during that time, it was Kaspersky Lab with its CIH defenses that made the most impact.

Revenue for Kaspersky Lab in 1999 was reported at $1.8 million and remained relatively flat until the mid-2000s. Between 2008 and 2011, revenue doubled to $612 million.[22] In that same timespan, Kaspersky's market share in the global consumer IT security market saw a

13. "Eugene Kaspersky, Cryptologist and business executive; Natalya Kaspersky: Business executive," *Salem Press*, accessed June 12, 2018. (https://salempress.com/store/pdfs/bios_com_pgs.pdf)
14. Kaspersky Lab, Press Release, "Eugene Kaspersky receives National Friendship Award of China," October 2, 2009. (https://www.kaspersky.com/about/press-releases/2009_eugene-kaspersky-receives-national-friendship-award-of-china)
15. "Eugene Kaspersky, Cryptologist and business executive; Kaspersky, Natalya: Business executive," *Salem Press*, accessed June 12, 2018. (https://salempress.com/store/pdfs/bios_com_pgs.pdf)
16. InfoWatch, "About Natalya Kaspersky," *YouTube*, April 7, 2017. (https://www.youtube.com/watch?v=a9orFW71lFs)
17. "Eugene Kaspersky, Cryptologist and business executive; Kaspersky, Natalya: Business executive," *Salem Press*, accessed June 12, 2018. (https://salempress.com/store/pdfs/bios_com_pgs.pdf)
18. "CIH," *Virus Information*, accessed June 12, 2018. (http://virus.wikia.com/wiki/CIH)
19. "Kaspersky, Eugene: Cryptologist and business executive; Kaspersky, Natalya: Business executive," *Salem Press*, accessed June 12, 2018. (https://salempress.com/store/pdfs/bios_com_pgs.pdf)
20. Abigail Chiodo and Michael Owyang, "A Case Study of a Currency Crisis: The Russian Default of 1998," *Federal Reserve Bank of St. Louis*, November/December 2002. (https://files.stlouisfed.org/files/htdocs/publications/review/02/11/ChiodoOwyang.pdf)
21. Keith Crane and Artur Usanov, "Role of High-Technology Industries," *Russia After the Global Economic Crisis*, Eds. Anders Aslund, Sergei Guriev, and Andrew Kuchins, (Washington, DC: Peterson Institute for International Economics, 2010). (https://piie.com/publications/chapters_preview/4976/05iie4976.pdf)-
22. Hannes Glorieux, "Kaspersky Lab Channel," *Kaspersky Lab*, 2013. (https://www.slideshare.net/Kappadata/kaspersky-26695868)

7 percent increase, reaching 9 percent.[23] More recently, Kaspersky has rolled out free, albeit stripped-down versions, of its software to grow its user base.[24] Kaspersky is thus positioned to be a major strategic asset for the Russian Federation for nearly a decade.

We do not know if Vladimir Putin and Eugene Kaspersky crossed paths in their days within the Russian intelligence community, or what relationship they had in the early days of Putin's reign when Eugene Kaspersky was at the cutting edge of Russia's high-tech industry. However, in its earlier years, Kaspersky Lab was not shy about touting its connections to Russian intelligence, as an ad campaign from Japan in 2007 made clear. Its slogan read, "A Specialist in Cryptography from KGB."[25]

Natalya Kaspersky, meanwhile, has never been shy about asserting a substantial role for the Russian government in the IT security field, saying on multiple occasions that the data of Russian individuals should and does belong to the government. She has justified these statements by saying that this is the only way the Russian government can protect its citizens' data from exploitation by other countries.[26]

Yet, only in the past year have U.S. government officials begun to publicly raise concerns about Kaspersky Lab's relationship with the Putin government.[27] In May 2017, Senator Marco Rubio (R-FL) asked leaders of the CIA, NSA, DIA, DNI, NGA, and FBI if any of them would be comfortable with Kaspersky Lab software on their computers.[28] The answer was a unanimous no. Senate Select Committee on Intelligence members have meanwhile hinted that classified intelligence buttresses publicly reported concerns about Kaspersky's activities.[29] For its part, Kaspersky Lab currently denies any connection to Russian intelligence and stated that it "has never helped … any government in the world with its cyberespionage efforts."[30]

We do, however, have an inkling of some of the ways in which Russian intelligence services have used Kaspersky software, whether with willing participation by the company or by infiltrating it without the knowledge or consent of its executives. *The New York Times* published a bombshell report in October 2017 claiming that Israeli intelligence officers monitored as Russian government cyber operatives used Kaspersky software as a digital Trojan horse to steal highly classified documents from the NSA. Russian intelligence used Kaspersky software as "a sort of Google search for sensitive information."[31] As the *Times* report explains:

> Like most security software, Kaspersky Lab's products require access to everything stored on a computer in order to scour it for viruses or other dangers. Its popular antivirus software scans for signatures of malicious software, or malware,

23. Kaspersky Lab, Press Release, "Kaspersky Lab is Ranked Among the Top Three Vendors of Consumer IT Security Software," April 12, 2011. (https://usa.kaspersky.com/about/press-releases/2011_kaspersky-lab-ranked-among-the-top-three-vendors-of-consumer-it-security-software)
24. Greg Synek, "Kaspersky Lab rolls out free antivirus software," *Techspot*, July 26, 2017. (https://www.techspot.com/news/70300-kaspersky-labs-rolls-out-free-antivirus-software.html)
25. Carol Matlack, Michael Riley, and Jordan Robertson, "The Company Securing Your Internet Has Close Ties to Russian Spies," *Bloomberg*, March 19, 2015. (https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies)
26. Catherine Kazachenko, "Касперская: 'большие данные россиян' должны принадлежать государству (Kaspersky: 'Large Data' of Russians Should Belong to the State)," *Tass Information Agency* (Russia), November 29, 2016. (http://tass.ru/ekonomika/3824223),
27. Dustin Volz, "Trump signs into law U.S. government ban on Kaspersky Lab software," *Reuters*, December 12, 2017. (https://www.reuters.com/article/us-usa-cyber-kaspersky/trump-signs-into-law-u-s-government-ban-on-kaspersky-lab-software-idUSKBN1E62V4)
28. Senator Marco Rubio (R-FL), *Hearing before Senate Select Committee on Intelligence*, May 11, 2017. (https://www.youtube.com/watch?v=TJdEq8YqzIg)
29. Senator Jeanne Shaheen (D-NH), "The Russian Company That Is a Danger to Our Security," *The New York Times*, September 4, 2017. (https://www.nytimes.com/2017/09/04/opinion/kapersky-russia-cybersecurity.html)
30. Nicole Perlroth and Scott Shane, "How Israel Caught Russian Hackers Scouring the World for U.S. Secrets," *The New York Times*, October 10, 2017. (https://www.nytimes.com/2017/10/10/technology/kaspersky-lab-israel-russia-hacking.html)
31. Ibid.

> then removes or neuters it before sending a report back to Kaspersky. That procedure, routine for such software, provided a perfect tool for Russian intelligence to exploit to survey the contents of computers and retrieve whatever they found of interest.[32]

U.S. government officials have also raised concerns about Kaspersky Security Network system, a cloud-based antivirus system. Although the company denies any nefarious activities, a September 2017 U.S. Department of Homeland Security memo accused the company of being able to transfer user data to its own servers where the Russian Federal Security Services (FSB) could access the data and banned Kaspersky products from federal government computers.[33] Even as Best Buy took Kaspersky Lab products off its shelves following the U.S. government announcement banning the software – with the caveat that Kaspersky code embedded in the products of other companies would be allowed – American consumers can still find it at other "retailers near you."[34] And despite the U.S. government ban, some 15 percent of U.S. federal agencies continued to run its software on their networks in late 2017.[35] Kaspersky closed its office in Washington, DC, but it has continued its commercial sales in America.[36]

In July 2017, *McClatchy* obtained documents revealing that Kaspersky Lab certifications included a "military intelligence unit number matching that of an FSB program." Kenneth Geers, a cyber expert formerly with NATO, told *McClatchy* he believed a backdoor for Russian intelligence within Kaspersky software could very well exist: "A worldwide deployment of sensors may be too great a temptation for any country's intelligence services to ignore." Former Moscow CIA station chief Steve Hall went on to tell *McClatchy* that Kaspersky may have had little choice but to cooperate with Russian intelligence requests, if it was not already a willing participant. "Any time [Putin] wants Kaspersky to do something – anything – he'll remind them that's where their families are and where their bank accounts are. There's no doubt in my mind it could be, if it's not already, under the control of Putin," Hall said.[37]

Kaspersky Lab in March 2018 publicly exposed an "active, U.S.-led counterterrorism cyber-espionage operation" targeting Islamic State and al-Qaeda members. Kaspersky Lab did not respond to answers

---

32. Ibid.

33. Ilya Zhegulev, "Inside The Fight For The Soul Of Kaspersky Lab," *BuzzFeed*, January 22, 2018. (https://www.buzzfeed.com/ilyazhegulev/russia-kaspersky-antivirus?utm_term=.yxlmlgb7Y#.ue9kZ47dx)

34. Chris Hamby, "FBI Software For Analyzing Fingerprints Contains Russian-Made Code, Whistleblowers Say," *BuzzFeed*, December 26, 2017. (https://www.buzzfeed.com/chrishamby/fbi-software-contains-russian-made-code-that-could-open-a?utm_term=.vxE2jzYVW#.iqMX1nqBk); Subsequently, Office Max, Office Depot, and Staples have also stopped selling Kaspersky Lab products. See: Allen St. John, "What the Kaspersky Antivirus Hack Means for Consumers," *Consumer Reports*, October 12, 2017. (https://www.consumerreports.org/privacy/what-to-do-about-the-kaspersky-data-hack-/); Andrew Blake "Staples Drops Kaspersky Lab Products Amid Russian Spying Claims," *The Washington Times*, October 13, 2017. (https://www.washingtontimes.com/news/2017/oct/13/staples-drops-kaspersky-lab-products-amid-russian-/)

35. Dustin Volz, "About 15 percent of U.S. agencies found Kaspersky Lab software: official," *Reuters*, November 14, 2017. (https://www.reuters.com/article/us-usa-cyber-kaspersky-congress/about-15-percent-of-u-s-agencies-found-kaspersky-lab-software-official-idUSKBN1DE28P)

36. Ilya Khrennikov, "Kaspersky to Close Washington Office But Expand Non-State Sales," *Bloomberg*, December 7, 2017. (https://www.bloomberg.com/news/articles/2017-12-07/kaspersky-to-close-washington-office-but-expand-non-state-sales); President Trump signed a ban on Kaspersky Lab products in December 2017. A few days later, Kaspersky filed a lawsuit contesting the ban. See: Dustin Volz, "Trump signs into law U.S. government ban on Kaspersky Lab software," *Reuters*, December 12, 2018. (https://www.reuters.com/article/us-usa-cyber-kaspersky/trump-signs-into-law-u-s-government-ban-on-kaspersky-lab-software-idUSKBN1E62V4); Dustin Volz and Jim Finkle, "Kaspersky Lab asks court to overturn U.S. government software ban," *Reuters*, December 18, 2017. (https://www.reuters.com/article/us-usa-cyber-kasperskylab/kaspersky-lab-asks-court-to-overturn-u-s-government-software-ban-idUSKBN1EC2CK)

37. David Goldstein and Greg Gordon, "Documents could link Russian cybersecurity firm Kaspersky to FSB spy agency," *McClatchy*, July 3, 2017. (http://www.chicagotribune.com/news/nationworld/ct-kaspersky-cyber-russia-spy-agency-20170703-story.html)

for comment on whether or not this disclosure would in effect kill a U.S. intelligence operation.[38] We do not know whether Kaspersky knew of the U.S. operation and purposely tried to undermine it (with or without the direction of the Russian government) or whether, as the company claims, it was merely reporting a piece of malware that could harm its customers.[39]

The Kaspersky challenge extends even further. Kaspersky antivirus solutions are "integrated in a range of routers, chip and software products from such household names as Cisco, Juniper, D-Link, Broadcom, Amazon and Microsoft."[40] In other words, decoupling the U.S. government from Kaspersky or other suspicious foreign companies is not quite as easy as banning the installation of software, even though that is an important first step. More broadly, the U.S. government needs to understand and secure the technical supply chain, both to address security needs and to ensure key sectors of our economy are not vulnerable to subversion by our adversaries.

"Russian tech companies, and those of other similar security-hostile states such as China, can be weaponized by those states' security services."

Whether or not companies such as Kaspersky are willing participants in Russian cyber operations or are being compelled to conduct nefarious activities makes little difference for U.S. national security interests as the net effect is the same. Russian tech companies, and those of other similar security-hostile states such as China, can be weaponized by those states' security services. The Kaspersky Lab case should serve as a prime example of the potential dangers multinational technology companies based in adversarial states pose. The U.S. and our allies should treat such companies with extreme suspicion when it comes to incorporating their services on any platforms.

The Kremlin's Legal Framework and Doctrine

Since taking over the Russian Federation in 2000, Vladimir Putin has worked to grow and sharpen his power by using the legal system to bolster his strategic initiatives.[41] As one expert explained, "In Putin's Russia, the sovereign uses the law and legal institutions to fulfill political goals, to communicate them to society, and to manage the authoritarian coalition that helps the president govern. As a result, the law is highly consequential, but its use tends to be arbitrary, expedient, and instrumental, rather than predictable and principled."[42] Russian laws and regulations governing information systems, telecommunications, and encryption give the Kremlin and its security services a strategic advantage both internally and externally.

For instance, one law (Federal Law N 128-FZ) requires encryption activities to be licensed and another (Resolution N 587) sets the FSB as the licensing authority.[43] Another law (Federal Law N 40-FZ) grants the FSB wide-ranging authorities in the information

38. Chris Bing and Patrick Howell, "Kaspersky's 'Slingshot' report burned an ISIS-focused intelligence operation," *Cyberscoop*, March 20, 2018. (https://www.cyberscoop.com/kaspersky-slingshot-isis-operation-socom-five-eyes/)
39. David Swan, "Eugene Kaspersky defends 'Slingshot' report," *The Australian*, March 27, 2018. (https://www.theaustralian.com.au/business/technology/eugene-kaspersky-defends-slingshot-report/news-story/a8344f750b82dad38b6812aad0299b96)
40. Adam Mazmanian, "Kaspersky axed from governmentwide contracts," *Federal Computer Week*, July 12, 2017. (https://fcw.com/articles/2017/07/12/kaspersky-gsa-nasa-intel.aspx)
41. William Partlett, "Mr. Putin's 'Rule-By-Law State,'" *Brookings*, June 19, 2012. (https://www.brookings.edu/opinions/mr-putins-rule-by-law-state/)
42. Maria Popova, "Putin-Style 'Rule of Law' & The Prospects for Change," *Daedalus*, March 27, 2017. (https://www.mitpressjournals.org/doi/full/10.1162/DAED_a_00435)
43. "Russian Laws and Regulations: Implications for Kaspersky Labs," *TAIA Global*, 2012. (https://www.wired.com/images_blogs/dangerroom/2012/07/Russian-Laws-and-Regulations-and-Implications-for-Kaspersky-Labs.pdf)

security field to combat "threats to Russia's safety."[44] This includes everything from fighting crime and corruption to counterintelligence operations. It also includes authority for the FSB to help companies protect trade secrets. It does not spell out whether this should only be done in a defensive manner or if offensive means are authorized as well. This law also gives broad authority for the FSB to require entities of all stripes (public, private, etc.) to provide assistance to the FSB in conducting its business in this sphere. As such, any entity in Russia that is engaged in telecommunication of any kind can be called upon by the FSB to assist in its operations.[45] As one analysis of the laws put it, "if the FSB asks for your help, you help."[46]

Understanding Russia's legal framework is important to assess the threat that Russia's information and technology sector poses to the United States. What we know is that Russian security services legally and practically are able to mobilize Russian companies for their own means. When a Russian company, such as Kaspersky Lab, claims independence or says that it does not work with Russian security services, it is relying on its customers not understanding the legal system under which the company operates. The fact of the matter is that any Russian company in this sector can be utilized by Russia's security services to serve as a strategic tool for the Kremlin.

Moscow has flexed its cyber capabilities increasingly over the last decade. In 2010, the Russian Ministry of Defense published its military doctrine, which defines information war and its role in cyber space.[47] For the Russian military, information operations go beyond just disinformation or propaganda. The Defense Ministry defines it as actions "that may damage information systems and resources; undermine political, economic, and social systems; brainwash the population; or coerce the victim government."[48] Prior to and since the publication of this document, Russia has conducted extensive cyber espionage, warfare, and influence operations, including, but not limited to, the 2007 cyber attacks on Estonia,[49] attacks during Russia's wars with Georgia and Ukraine,[50] hacking of the German parliament in 2015,[51] interference in the 2016 U.S. elections,[52] targeting of the U.S. energy grid and other key sectors in 2016, and the hacking of the French election infrastructure in 2017.[53]

---

44. European Commission for Democracy Through Law (Venice Commission), "Federal Law of the Federal Security Service of the Russian Federation," February 24, 2012. (http://www.icla.up.ac.za/images/un/use-of-force/eastern-europe/Russia/Federal%20Law%20on%20Federal%20Security%20Service%20Russia%201995.pdf)
45. Ibid.
46. "Russian Laws and Regulations: Implications for Kaspersky Labs," *TAIA Global*, 2012. (https://www.wired.com/images_blogs/dangerroom/2012/07/Russian-Laws-and-Regulations-and-Implications-for-Kaspersky-Labs.pdf)
47. For a discussion of these concepts and cases, see: Michael Connell and Sarah Vogler, "Russia's Approach to Cyber Warfare," *CNA*, March 24, 2017. (https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf); See also: Sergei A. Medvedev, "Offense-defense theory analysis of Russia cyber capability," *Naval Postgraduate School*, March 2015. (https://calhoun.nps.edu/bitstream/handle/10945/45225/15Mar_Medvedev_Sergei.pdf;sequence=3)
48. Ibid.
49. Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia," *The Guardian* (UK), May 16, 2007. (https://www.theguardian.com/world/2007/may/17/topstories3.russia)
50. Sergei A. Medvedev, "Offense-defense theory analysis of Russia cyber capability," *Naval Postgraduate School*, March 2015. (https://calhoun.nps.edu/bitstream/handle/10945/45225/15Mar_Medvedev_Sergei.pdf;sequence=3)
51. Patrick Beuth, Kai Biermann, Martin Klingst, and Holger Stark, "Merkel and the Fancy Bear," *Zeit* (Germany), May 12, 2017. (http://www.zeit.de/digital/2017-05/cyberattack-bundestag-angela-merkel-fancy-bear-hacker-russia)
52. Office of the Director of National Intelligence, "Background to 'Assessing Russian Activities and Intentions in Recent US election': The Analytic Process and Cyber Incident Attribution," January 6, 2017. (https://www.dni.gov/files/documents/ICA_2017_01.pdf)
53. Tim Starks, "U.S. says Russian hackers targeted American energy grid," *Politico*, March 15, 2018. (https://www.politico.com/story/2018/03/15/dhs-fbi-russia-hackers-targeted-energy-grid-813745); Andy Greenberg, "The NSA Confirms It: Russia Hacked French Election 'Infrastructure,'" *Wired*, May 9, 2017. (https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/)

In theory and in practice, these types of operations fit neatly into Russia's concept of hybrid warfare, an approach that seeks to achieve political goals by using instruments that leverage all elements of its power, of which cyber and information operations are a key element.[54] In 2013, General Valery Gerasimov elaborated on Moscow's use of information warfare by explaining that it "opens wide asymmetrical possibilities for reducing the fighting potential of the enemy."[55] His views show that the Kremlin believes the purpose of information warfare is not just to shape the information space in its favor, but to actively degrade the response capabilities of its adversaries.

"...any Russian company in this sector can be utilized by Russia's security services to serve as a strategic tool for the Kremlin."

Vladimir Putin's own history as a KGB officer in East Germany is important to consider when analyzing Russia's cyber strategy. As part of his KGB career, Putin ran "illegal intelligence" networks, which relied on his ability to train and control agents deep undercover in foreign countries.[56] This is a potential window into how Putin may think about the use of cyber. As a "sophisticated practitioner and advocate for HUMINT," Putin is adept at camouflaging his true intentions and exploiting relationships to make national security gains. This strategic mindset is particularly valuable as Russia's intelligence agencies have utilized cyber intrusions in intelligence operations.[57] Camouflaging Russian state-backed cyber ventures as private sector firms is a strategy consistent with Russian intelligence operations.[58]

Moscow's Proxies: Cyber Criminals and Tech Companies

Following the 1998 financial crash, Russia's cyber criminal community exploded. "The combination of overeducated and underemployed specialists has made Russia an ideal breeding ground for hackers," according to business journalist John Blau.[59] The scarcity of work and low salaries for legitimate technology jobs in private industry and government service led to a booming criminal hacker market, valued according to some estimates at $2.3 billion.[60]

Then and today, as long as hackers largely constrain themselves to targeting victims abroad, Russian law enforcement turns a blind eye.[61] The Kremlin, in fact, leverages cyber criminals because doing so is cost effective and provides a layer of plausible deniability.[62] A former head of the KGB office in London explained the choice given to cyber criminals in Russia as "either

54. Sergei A. Medvedev, "Offense-defense theory analysis of Russia cyber capability," *Naval Postgraduate School*, March 2015. (https://calhoun.nps.edu/bitstream/handle/10945/45225/15Mar_Medvedev_Sergei.pdf;sequence=3)
55. Valery Gerasimov, "The Value of Science Is in the Foresight New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," *Military Review*, January-February 2016, page 27. (http://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/January-February-2016/)
56. Emily Saul, "Putin admits he once ran an international spy network," *The New York Post*, June 25, 2017. (https://nypost.com/2017/06/25/putin-i-used-to-run-an-illegal-international-spy-network/)
57. Daniel Hoffman, "Vladimir Putin and the Art of Intelligence," *The Cipher Brief*, July 7, 2017. (https://www.thecipherbrief.com/vladimir-putin-and-the-art-of-intelligence)
58. Levi Maxey, "Inside the Competitive, Corrupt World of Russian Intelligence," *The Cipher Brief*, April 20, 2018. (https://www.thecipherbrief.com/inside-competitive-corrupt-world-russian-intelligence)
59. John Blau, "Russia - a happy haven for hackers," *ComputerWeekly.com*, May 2004. (http://www.computerweekly.com/feature/Russia-a-happy-haven-for-hackers)
60. Tim Mauer, *Cyber Mercenaries: The State, Hackers, and Power*, (New York: Cambridge University Press, 2018), page 94.
61. Ibid, pages 94 and 105.
62. David J. Smith, "How Russia Harnesses Cyberwarfare," *American Foreign Policy Council's Defense Dossier*, August 2012, page 9. (http://www.afpc.org/files/august2012.pdf)

prison or cooperation with the FSB."[63] The FSB is thus able to turn hackers into "proxies for internal and external offensive cyber operations," as Sergei Pokrovsky, the head of the Moscow Civil Hacking School, explained.[64] Russian authorities reportedly latch intelligence operations onto existing criminal schemes. After criminals gain valuable access to foreign networks, Russian espionage and information warfare apparati exploit these efforts, "sparing themselves the hard work of hacking into the computers themselves."[65] Utilizing a privateer model and private criminal hacker groups also enables Moscow to deny involvement and complicates attribution.[66] This model can also be seen in the Kremlin's use of mercenaries, or "little green men," in its military engagements.[67]

And the Kremlin protects its proxies. Moscow exerts great efforts to ensure that its hackers caught abroad are extradited back to Russia. The Kremlin has a track record of filing competing extradition requests when a Russia-linked cyber criminal has been captured, and in some cases, this has proven to be an effective strategy.[68] Take for instance the case of Yevgeniy Nikulin, who was arrested in Prague in 2016 for compromising the personal details of more than 100 million social media users.[69] Thanks in part to a competing Russian request, Nikulin's extradition to the United States was delayed for two years. Upon Nikulin's successful extradition in 2018, U.S. Attorney General Jeff Sessions observed, "deeply troubling behavior once again emanating from Russia."[70]

Just as Russian authorities reportedly grafted their operations onto the hacking efforts of one of the FBI's most-wanted cyber criminals,[71] U.S. policymakers are concerned that the FSB can similarly use Russian technology companies as proxies to access U.S. government documents and private sector networks.[72] From both an espionage and information warfare perspective, if a state wants to be effective in its operations, it needs access to foreign networks. Either it can gain access itself, or it can use proxies. In addition to providing access to systems, supporting the development of technology companies may also assist the development of human capital and expertise for conducting reconnaissance and offensive cyber operations.

From an economic perspective, supporting the growth of technology companies provides both relative and absolute advantages. To the extent that Russian firms can displace U.S. competitors from the IT and cyber security sectors, the expansion of Russian firms into their own domestic market, foreign markets, and

63. Tim Maurer, "Why the Russian Government Turns a Blind Eye to Cybercriminals," *Slate*, February 2, 2018. (https://slate.com/technology/2018/02/why-the-russian-government-turns-a-blind-eye-to-cybercriminals.html)
64. Ibid.
65. Michael Schwirtz and Joseph Goldstein, "Russian Espionage Piggybacks on a Cybercriminal's Hacking," *The New York Times*, March 12, 2017. (https://www.nytimes.com/2017/03/12/world/europe/russia-hacker-evgeniy-bogachev.html?_r=0)
66. Michael Connell and Sarah Vogler, "Russia's Approach to Cyber Warfare," *CNA*, March 2017, page 23. (https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf)
67. Joseph Trevithick, "Russian Mercenaries Take The Lead In Attacks On US And Allied Forces In Syria," *The Drive*, February 15, 2018. (http://www.thedrive.com/the-war-zone/18533/russian-mercenaries-take-a-lead-in-attacks-on-us-and-allied-forces-in-syria)
68. Andrew Kramer, "A New Russian Ploy: Competing Extradition Requests," *The New York Times*, December 20, 2017. (https://www.nytimes.com/2017/12/20/world/europe/russia-extradition-levashov.html)
69. Jan Lopatka and Jonathan Stempel, "Russian accused of massive U.S. hacking is extradited, pleads not guilty," *Reuters*, March 30, 2018. (https://www.reuters.com/article/us-czech-usa-russia-cybercrime/czechs-extradite-suspected-russian-hacker-nikulin-to-united-states-idUSKBN1H60VU)
70. U.S. Department of Justice, Press Release, "Yevgeniy Nikulin Appears in U.S. Court Following Extradition," March 30, 2018. (https://www.justice.gov/usao-ndca/pr/yevgeniy-nikulin-appears-us-court-following-extradition)
71. Michael Schwirtz and Joseph Goldstein, "Russian Espionage Piggybacks on a Cybercriminal's Hacking," *The New York Times*, March 12, 2017. (https://www.nytimes.com/2017/03/12/world/europe/russia-hacker-evgeniy-bogachev.html?_r=0)
72. 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)

even into the United States grows Russian GDP and decreases American economic benefits and perhaps even global market clout. While Chinese firms are the greatest current competition to the U.S., over the longer term, if Russian companies are able to undercut U.S. industry and undermine American competitive advantages, even in niche sectors, Moscow can weaken American economic power. Furthermore, if Russian companies can embed themselves in the supply chain of the national security industrial base, Washington may find its qualitative advantage reduced and its vulnerability increased.

On the defensive side, technology companies may also enable Russian authorities to preposition assets in foreign networks to serve as a deterrent and reduce the ability of the United States and its allies to take actions against Russia or its interests. Moscow could ensure that the systems we rely on for cyber operations could be blunted.

Until recently, U.S. analysts were not attuned to Moscow's employment of prominent private sector firms, or "national champions," as part of its economic warfare campaign. Of course, the U.S. government and policy community has for many years raised concerns about China's state-owned enterprises and Beijing's ability to use technology companies – Huawei and ZTE, in particular – to engage in cyber espionage and theft to undermine U.S. national security.[73] Yet, it has taken more time for the U.S. government to recognize the threat from the Russian corporate sector. Only in September 2017 did the U.S. Department of Homeland Security issue a directive to federal agencies to begin taking steps to remove Kaspersky software from their networks.[74]

In the case of Kaspersky Labs, Russian government officials and company representatives have denied wrongdoing, and Eugene Kaspersky himself has called such allegations "like the script of a C movie."[75]

Beyond Kaspersky

U.S. policymakers are coming around to the understanding that Kaspersky is but one problem. While Kaspersky Lab is now globally notorious, Russia has a number of other companies in the tech sector that raise questions. Not only should these companies be further scrutinized, but so should the supply chain of the source code that software providers sell to the U.S. government and to private and public entities overseeing critical infrastructure and other homeland security-related industries. As we have seen in the case of Kaspersky, once a company's products are in the system, getting rid of them is a long and hard process.[76]

The following are three Russian firms which may warrant scrutiny by U.S. intelligence officials and policymakers:

Dr. Web: In 1992, Dr. Web became the first antivirus service available in Russia. The FSB has only licensed two antivirus companies to work with state secret information – Kaspersky Labs and Dr. Web.[77] These licenses allow all Russian government institutions to use

73. For example, see: Reps. Mike Rogers (R-MI) and C.A. Dutch Ruppersberger (D-MD), "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE," *House Permanent Select Committee on Intelligence*, October 8, 2012. (https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf)

74. U.S. Department of Homeland Security, Press Release, "DHS Statement on the Issuance of Binding Operational Directive 17-01," September 13, 2017. (https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01)

75. James Titcomb, "Russian security firm Kaspersky denies deliberately lifting US spy tools," *The Telegraph* (UK), November 16, 2017. (http://www.telegraph.co.uk/technology/2017/11/16/russian-security-firm-kaspersky-denies-deliberately-lifting/)

76. Andrew Desiderio and Kevin Poulsen, "Exclusive: U.S. Government Can't Get Controversial Kaspersky Lab Software Off Its Networks," *The Daily Beast*, May 23, 2018. (https://www.thedailybeast.com exclusive-us-government-cant-get-controversial-kaspersky-lab-software-off-its-networks)

77. "Russian Laws and Regulations: Implications for Kaspersky Labs," *TAIA Global*, 2012. (https://www.wired.com/images_blogs/dangerroom/2012/07/Russian-Laws-and-Regulations-and-Implications-for-Kaspersky-Labs.pdf); "Dr. Web 5.0 certified by FSB," *Dr.WEB Anti-virus*, January 19, 2010. (https://news.drweb.com/show/?i=861&lng=en)

their software as part of government networks.[78] While Dr. Web does not focus on the U.S. market and has no U.S. distributors, it has an international presence with offices across Europe and Asia and distributes to more than 30 countries worldwide. Its products are also available for anyone to download online. What is not known about Dr. Web or other Russian software companies is whether their code is being used by other vendors who then sell to U.S.-based customers, and if so, whether that presents any risk. While there is no evidence that Dr. Web has engaged in any nefarious activities, given the accusations against Kaspersky, in addition to the fact that Dr. Web is the only other antivirus company licensed by the FSB, the U.S. intelligence community should investigate.

Prognoz: The Russian business analytics software company Prognoz does business with the U.S. government and has offices in Washington, DC and around the world. On its Russian website, the company's list of customers includes a number that the U.S. Treasury Department has sanctioned.[79] This information is omitted from the English version.[80] This is not proof of nefarious activity by this company or other Russian companies, but it should raise questions about whether the company is purposefully hiding its dealings with the Russian government or sanctioned persons, and if so, why. The issue is not simply that sanctioned entities are using Prognoz products, but rather that the company considers these contracts as a selling point. U.S. policymakers must now determine whether Prognoz provides those entities with technology, knowledge, intelligence, or personnel.

Speech Technology Center (STC): Founded in 1990 as an outgrowth of the KGB's applied acoustics unit,[81] STC is a leading voice and multimodal biometric system company working in 75 nations around the world.[82] The company has worked with law enforcement agencies in the United States.[83] In 2011, state-owned Gazprombank (sanctioned by the U.S. Treasury Department in 2014[84]) became a major shareholder of STC.[85] Policymakers should be made aware if U.S. law enforcement agencies continue to use STC's services in light of its connections to the Russian intelligence services and a sanctioned company.[86]

Other areas of the technology sector are worth watching as well. Artificial intelligence (AI) is an area that Putin is focusing on, saying last year that "the one who becomes the leader in this sphere will be the ruler of the world."[87] Further, a recent Congressional Research Service report warned that "Russian venture capitalists are actively seeking opportunities in the AI market abroad, indicating that there might be a united effort

78. "Dr. Web 5.0 certified by FSB," *Dr.WEB Anti-virus*, January 19, 2010. (https://news.drweb.com/show/?i=861&lng=en)
79. Prognoz website, accessed April 27, 2018. (http://www.prognoz.ru/?_ga=2.132338634.597749552.1520454103-15020166.1518458893)
80. Prognoz website, accessed April 27, 2018. (http://www.prognoz.com/)
81. Andrew Soldatov and Irina Borogan, "5 Russian-made Surveillance Technologies Used in The West," *Wired*, May 10, 2013. (https://www.wired.com/2013/05/russian-surveillance-technologies/)
82. "About Company," *Speech Technology Center*, accessed April 12, 2018. (http://speechpro.com/company)
83. Ryan Gallagher, "Watch Your Tongue: Law Enforcement Speech Recognition System Stores Millions of Voices," *Slate*, September 20, 2012. (http://www.slate.com/blogs/future_tense/2012/09/20/speechpro_voicegrid_nation_voice_recognition_software_for_use_by_law_enforcement_.html)
84. U.S. Department of the Treasury, Press Release, "Announcement of Treasury Sanctions on Entities Within the Financial Services and Energy Sectors of Russia, Against Arms or Related Materiel Entities, and those Undermining Ukraine's Sovereignty," July 16, 2014. (https://www.treasury.gov/press-center/press-releases/Pages/jl2572.aspx)
85. "Gazprombank Joins Speech Technology Center," *Speech Technology Center*, September 12, 2011. (http://speechpro.com/media/news/2011-09-12)
86. Andrei Soldatov and Irina Borogan, "Building the Kremlin's Big Brother," *Foreign Policy*, September 16, 2015. (http://foreignpolicy.com/2015/09/16/we-just-come-up-with-the-hardware-russia-red-web-surveillance-technology/)
87. "Putin: Leader in artificial intelligence will rule world," *Associated Press*, September 4, 2017. (https://www.cnbc.com/2017/09/04/putin-leader-in-artificial-intelligence-will-rule-world.html)

in Russia to pursue AI technology."[88] Russia has the knowledge and experience, as it has shown in the last two decades, to be a competitive force when it comes to evolving technologies. Understanding the national security dimensions of Russia's interest in this and other emerging technologies is critical to evaluating the threat and to developing policy options to mitigate their potential impact.

Conclusion and Policy Recommendations

The United States and its allies must look at our software and hardware supply chain with eyes wide open. It has been far too easy for our adversaries to infiltrate our government, personal, and commercial data using what are literally off-the-shelf solutions.

"De-conflicting our software and hardware from potentially malicious sources may very well be costly and cause diplomatic anxiety, but doing so is clearly in our national security interest."

To borrow a slogan from Moscow's propaganda outlet *Russia Today*, we must "question more." Decision makers need to evaluate fully what we invite onto our systems and networks, whether it be a cheap Chinese-made thumb drive, Russian antivirus software, or more complex technical hardware that make up the veins of our national and government infrastructure. De-conflicting our software and hardware from potentially malicious sources may very well be costly and cause diplomatic anxiety, but doing so is clearly in our national security interest.

The U.S. government should use Treasury's financial sanctions tools, the Commerce Department's tools to block trade through the Bureau of Industry and Security's Entity List, and all other tools of U.S. power to deter and punish nefarious cyber actors. For example, in early June, Treasury designated five Russian companies and three individuals for being controlled by, or providing material and technological support to, the FSB.[89] Such designations are important for communicating risk to the private sector, but sanctions enforcement demands greater resources to uncover front companies and new cutouts that designated entities use to evade sanctions. Financial, human, and intelligence resources should be invested to ensure U.S. sanctions are effective.

Additionally, the recommendations below outline defensive and offensive steps to mitigate the specific threats posed by Russia's multinational corporations:

- The U.S. Computer Emergency Readiness Team within the Department of Homeland Security should create a watch list of software companies believed to be acting on behalf of, or are being used by, adversarial states in ways that pose a security risk to U.S. entities. The team already provides timely information on key security vulnerabilities and as such could host a similar watch list.
- The U.S. Department of Homeland Security should amend its Kaspersky Lab software ban decision to include Kaspersky code embedded in the products of other companies. Currently, there is an explicit cutout for such scenarios. Implementing such a decision gradually would give government agencies enough time to find suitable and secure replacements.
- The United States should cooperate more closely with our allies in identifying potentially nefarious software or hardware providers. A mutually beneficial consortium could be created for this purpose, and an internal red notice on foreign software and hardware of concern can be created to trigger immediate reviews.

88. Daniel Hoadley and Nathan Lucas, "Artificial Intelligence and National Security," *Congressional Research Service*, April 26, 2018. (https://fas.org/sgp/crs/natsec/R45178.pdf)

89. U.S. Department of the Treasury, Press Release, "Treasury Sanctions Russian Federal Security Service Enablers," June 11, 2018. (https://home.treasury.gov/news/press-releases/sm0410)

- While the U.S. Department of Homeland Security sends out alerts that help inform the private sector of potential cyber threats, and the private sector reports cyber incidents to the Federal Bureau of Investigation, a mechanism for more substantial cooperation is lacking. The intelligence community and the private sector need to form secure and trusted partnerships so that the intelligence community can collect and disseminate (with proper source protection) information about Russian or other threats to private sector companies.

Low tech is high tech. The government should continue its drive to decrease private mobile phones' access to key government facilities and reduce the amount of computers with access to external communications.

In addition to devoting more resources to understanding the threat that the Russian technology sector poses to U.S. economic and national security, the intelligence community should be tasked with evaluating Russian intentions: To what extent is the Kremlin supporting the establishment and expansion of Russian companies for the express purpose of gaining access to the IT networks of its adversaries? What do they intend to do with that access? Is Moscow forcibly grafting information and espionage operations onto otherwise private companies? Does Moscow have a formal campaign of coercive mercantilism? Are Russian venture capital firms' investment strategies in Silicon Valley leading to potential influence and access to sensitive information and technology?

Our adversaries are today using what can generously be described as coercive mercantilism as an instrument of national power. For a nation that is the leading bastion of free market economics, this threat is particularly potent. Nations like Russia and China are using and augmenting their own technological sectors at the expense of U.S. national security and economic power. By identifying the threats and taking actions to mitigate their impact – largely by plugging the holes that exist in our own system – we can better ensure that our adversaries' efforts to undermine the United States fail.

Acknowledgments

The author would like to thank Samantha Ravich, Annie Fixler, Daniel Hoffman, Jamie Fly, Jonathan Schanzer, Nathan Siegel, Richard Brahm, Toby Dershowitz, David Adesnik, Nicole Salter, Clifford May, Mark Dubowitz, Erin Blumenthal, and Daniel Ackerman. Any errors are the author's sole responsibility.

This report is part of a series of studies on adversarial strategies from FDD's project on cyber-enabled economic warfare. The project aims to promote a greater understanding within the U.S. government, private sector, and allied countries of the threats and opportunities that the new environment poses and assist as policymakers develop and implement a winning strategy for the United States within this domain.

Cover Illustration by Daniel Ackerman

About The Author

Boris Zilberman is Deputy Director of Congressional Relations at the Foundation for Defense of Democracies (FDD). He lends his background and expertise on a range of legislative issues encompassing defense and foreign affairs to FDD's relationship with Washington's leading policy makers. With a focus on the Middle East and Russia, Boris is an authoritative voice helping to frame complex issues affecting America and her allies.

Boris leads FDD's Russia work as part of the Center on Sanctions and Illicit Finance which focuses on the evolving financial and strategic developments in the U.S.-Russia relationship.

Prior to joining FDD, Boris spent five years working as Manager of Defense Programs in the policy and government affairs department at the American Israel Public Affairs Committee (AIPAC). He also carries coalition-building experience from his time at a Washington-based public affairs firm.

Boris holds an MA in Global Security Studies from Johns Hopkins University and a BA degree in Political Science and Russian from The University of Alabama. He was born in Moscow and is fluent in Russian.

About the Foundation for Defense of Democracies' Center on Sanctions and Illicit Finance

The Foundation for Defense of Democracies (FDD) is a Washington, DC-based non-partisan policy institute focusing on foreign policy and national security. FDD's Center on Sanctions and Illicit Finance (CSIF) expands upon FDD's success on the use of financial and economic measures in national security. The Center's purpose is to provide policy and subject matter expertise in areas of illicit finance, financial power, and economic pressure to the global policy community.

CSIF seeks to illuminate the critical intersection between the full range of illicit finance and national security, including money laundering, terrorist financing, sanctions evasion, proliferation financing, cyber crime and economic espionage, and corruption and kleptocracy. This includes understanding how America can best use and preserve its financial and economic power to promote its interests and the integrity of the financial system. The Center also examines how America's adversaries may be leveraging economic tools and power.

CSIF focuses on global illicit finance, including the financing of terrorism, weapons and nuclear proliferation, corruption, and environmental crime. It has a particular emphasis on Iran, Saudi Arabia, Kuwait, Qatar, Turkey, Russia, and other autocratic states as well as drug cartels and terrorist groups including Hamas, Hezbollah, al-Qaeda, and the Islamic State.

For more information, please visit www.defenddemocracy.org.

FDD
FOUNDATION FOR
DEFENSE OF DEMOCRACIES

P.O. Box 33249
Washington, DC 20033-3249
(202) 207-0190
www.defenddemocracy.org