How the Collapse of the Soviet Union Made Russia a Great Cyber Power

Alec Jackson

INTRODUCTION

As a result of the unique circumstances created by the collapse of the Soviet Union, Russia has developed disproportionate cyber power relative to its economic stature. The Belfer Center for Science and International Affairs defines cyber power as "the effective deployment of cyber capabilities by a state to achieve its national objectives."[1] In general, the operational capacity of a state's national security infrastructure, and especially its cyber power, scales directly with that of its innovation economy.[2] Russia is only the world's eleventh-largest economy by gross domestic product (GDP),[3] and its information technology (IT) sector constituted just under 6% of the country's GDP before Russia's 2022 invasion of Ukraine.[4] Despite these limitations, Russia is commonly recognized as an elite cyber power.[5] Importantly, Russia relies heavily on cyber professionals from outside its security agencies, including talent from the private sector and associated with organized criminal groups (OCGs), to conduct offensive cyber operations on the state's behalf.[6]

In analyzing the ways that Russia leverages non-state cyber talent, this article details how the Soviet Union's history impacted the development of Russia's internet, and the

Alec Jackson works as an analyst in the Office of the Secretary of Defense. He completed the International Security Master of Arts program at George Mason University's Schar School of Policy and Government earlier this year and authored "Managing Russia in the Middle East: The Case for Selective Engagement" (2022).

competitive advantages enjoyed by the Russian IT industry. This article also examines the legal and economic environment that rewards non-state actors that engage in cybercrime, and how the Russian state employs corruption networks to mobilize cyber talent outside the direct control of its security agencies. Corruption is the glue that binds Russian IT professionals, Russian OCGs, and the Russian security apparatus together, and allows the state to leverage cyber talent outside the state to pursue Russian President Vladimir Putin's strategy of "offensive defense" against the West. This article concludes with an analysis of the impacts of the Ukraine invasion and subsequent Western sanctions on Russian cyber power, and recommendations for containment by Western policymakers on Russian cyber power in the future.

The History of the Russian Internet

The development of the Russian internet was largely shaped by the unique circumstances surrounding the collapse of the Soviet Union. These conditions were made possible by Russian government agencies, Russian state-owned entities, domestic commercial actors, foreign corporations, and international non-governmental organizations. In the early 1990s, Russia lacked developed civilian telecommunication networks.[7] Infrastructure that did exist largely consisted of Soviet-era analog telephone lines almost entirely owned by the state operator, Rostelekom.[8] Early internet networks in Russia were mostly concentrated around Moscow and used this analog infrastructure to provide basic services. Many independent Russian internet service providers (ISPs) were founded during the 1990s, but Rostelekom was key to the growth of the Russian internet. In 1996, Rostelekom created the Moscow–Khabarovsk Radio Relay Communication Channel,[9] a network of radio-relay cables from Vladivostok to Novorossiysk that connected Russia's regional ISPs to their counterparts in Moscow.[10] Between 1995 and 1999, Rostelecom also constructed a nationwide

fiber-optic backbone system, which helped link the Russian internet with international networks.[11] By the end of 2000, 6.6 million Russians had access to the internet.[12]

Western businesses like Sprint and non-profit organizations like George Soros's Open Society Institute leveraged Russia's political and economic opening to build Russia's internet infrastructure. The Open Society Institute established major internet centers at 33 Russian universities between 1996 and 1999.[13] The internet infrastructure created for Russia's universities and research centers helped drive internet adoption in Russia outside of Moscow and Saint Petersburg. In addition to enabling internet connectivity, these networks (which included the Moscow State University-affiliated Radio-MSU and MSUnet, as well as the Russian Research Institute for the Development of Public Networks's RELARN-IP) helped to create a market for internet services in the Russian regions.[14] In fact, the university centers themselves became internet service providers in numerous Russian oblasts.[15]

When the Soviet Union collapsed in 1991, so did the primary source of research funding in the territory it controlled. Between 1991 and 1999, Russia's budget for science dropped 90%.[16] In constant 1995 U.S. dollars, Russian funding for research and development dropped from $28.4 billion in 1990 to $7.2 billion in 1998.[18] Similarly, domestic funding for Russian defense procurement fell by at least 80% during the 1990s. Many Russian scientists emigrated abroad as a result. Those who stayed were forced to seek new sources of income. These included large numbers of programmers[19] who found work in the nascent internet economy.[20] Indeed, some say the Russian internet was "born in the kitchens of the intelligentsia."[21] Minimal state regulation of the internet in the 1990s and 2000s allowed early Russian internet entrepreneurs to flourish.

Unlike many pre-fall-of-the-Soviet-Union manufacturing and energy companies that were then captured by Russian oligarchs, no regional or inter-regional civilian telecommunications infrastructure or even physical assets existed to capture.[22] For example, Russian Prime Minister Viktor Chernomyrdin looted energy company Gazprom's assets and sold them to his relatives and associates[23] before Putin began his drive to suborn Russia's oligarchs in 2000. In contrast, Russian IT companies that made use of the newly built internet infrastructure possessed no Soviet Union "legacy assets."[24] Most Russian ISPs, at least at the regional level, were built "from scratch"[25] by their founders in the mid-to-late 1990s. Even as the Russian internet began to take shape, companies building it were too small to attract oligarch attention.

Competitive Advantages of the Russia Information Technology Sector

While the vast expanse of Russia's landmass has posed logistical challenges to expanding remote internet access, internet connectivity is highly affordable to average Russians in areas where it is available. A 2015 World Bank study reports that more than 80% of Russians are able to afford broadband internet access.[26] This is because minimal government regulation of ISPs, at least from a commercial standpoint, even if not from a content standpoint, has promoted healthy competition among Russian ISPs. Rostelekom, still partially state-owned,

enjoys a dominant market position in backbone connectivity, but it is not a monopoly.[27] Literally thousands of ISPs operate in Russia,[28] although many independent ISPs use Rostelekom's infrastructure.[29] The affordability of internet access in Russia is a key contributor to internet-enabled enterprises, commercial or otherwise. It not only helps connect Russian IT professionals with each other and with international clients, it also facilitates the transfer of technical knowledge, whether academic, commercial, or criminal. Finally, internet access is recognized as an important structural factor that influences career choice.[30] The affordability of household internet access in Russia helps encourage young Russians to pursue IT careers.

The U.S., another geographically large country with a comparatively highly regulated telecommunications sector from a commercial standpoint, enjoys very little competition among ISPs. The U.S. market for home internet is an oligopoly dominated by four large ISPs that often enjoy local monopolies[31] and rarely are forced to compete on price in local markets. This limits consumer choice, stifles competition, and raises internet prices for U.S. households. Because cost is the primary barrier to Internet access in the U.S., the result of limited competition between ISPs is that 14% of Americans with annual incomes under $30,000 do not use the Internet,[32] and 43% of American adults with annual household incomes under $30,000 have no broadband internet subscription.[33] Despite massive federal investment in improving broadband access, especially for rural communities, serious affordability challenges remain.[34]

Legacy of the Soviet Union's Science, Technology, Engineering, and Mathematics (STEM) Education

Russian cyber power has benefited from inheriting the Soviet Union's education system, which strongly emphasized STEM education. To this day, "scientific and technical education is particularly valued within Russia"[35] where 37 percent of Russian undergraduate students major in a STEM field,[36] compared to 21 percent of U.S. undergraduate students.[37] Russia also inherited from the Soviet Union a massive system of national research laboratories and research institutes, though it has struggled to maintain this network.[38] The Russian education system also fosters a creative, problem-solving mindset in the IT workers it trains.[39] Indeed, many multinational corporations believe employing Russian IT workers, instead of Chinese or Indian tech workers, give companies a competitive advantage.[40]

Cultural compatibility between Russian IT professionals and their clients, particularly clients in the native English-speaking world, is another important competitive advantage of Russian IT firms. Russian IT firms, especially software offshoring companies, are characterized by small teams of "creative and strong-willed"[41] experts willing to debate client methodologies and timelines. According to one European client of a Russian IT outsourcing firm, these qualities render Russian IT firms highly compatible with American clients.[42] Historically, most customers of Russian IT companies were from the U.S. and Canada,[43] and many U.S. start-ups founded by Russian-born entrepreneurs rely on Russia-based IT professionals.[44]

Incentives for Cybercrime

However, Russia's strong STEM education is no guarantee that Russian IT professionals can find gainful employment. On the one hand, high levels of educational attainment are clearly valued in Russian society. In 2019, 63 percent of Russian 25-34 year-olds had achieved some level of tertiary education, compared with the Organization for Economic Co-operation and Development (OECD) average of 44 percent.[45] Many Russian postsecondary students pursue degrees in IT specifically.[46] Yet the Russian labor market, like those of many other post-Soviet economies, is inefficient and struggles to place well-educated workers in their fields of study.[47] In addition, while many prospective Russian IT students cite job prospects and high wages as their motivation for choosing their field of study, they may have unrealistic expectations regarding entry-level wages.[48] Finally, there may well be more highly-educated IT professionals in Russia than there are legitimate IT jobs.[49] Even the IT professionals who can find jobs work for "economical wages,"[50] at least by international standards. While this represents a great deal for multinational corporations seeking to develop software on the cheap, this presents Russian IT workers with powerful economic incentives to supplement their incomes.

The retributive legal barriers to cyber criminality that might dissuade an underemployed IT professional in other countries are much less compelling in Russia. Cybercrime is profitable globally,[51] but Russia is particularly permissive as it relates to cybercrime. Legal penalties for cybercrime under the Russian Criminal Code are considered quite weak by international standards,[52] and enforcement of those laws is selective, haphazard, and sometimes non-existent. According to Kyle Wilhoit, an internationally-recognized cybersecurity expert, "hackers only really get prosecuted when they attack targets inside Russia."[53] And Russian domestic authorities generally do not cooperate with the international law enforcement agencies that investigate cybercrimes.[54]

In addition, the early geographic concentration of Russia's internet infrastructure has exacerbated cost-of-living concerns for its cyber professionals. The build-out of Russia's early internet infrastructure around the country's academic and scientific institutions, made possible by the financial and technical assistance of foreign benefactors, created an "academic bias"[55] in Russian internet access. For the first two decades of internet connectivity, Russia's internet users, at least outside of the major metropolitan areas of Moscow and St. Petersburg, were concentrated around research centers in places like Novosibirsk. For many years, the Russian software industry was concentrated in those three cities.[56] This spatial polarization had important implications for the geographic distribution of the broader Russian economy. The economic benefits unlocked by digitization and electronic commerce were only available to populations living around places with existing internet infrastructure, places that were already home to most of Russia's most educated workers. Until the advent of mobile broadband, the Internet was a force for further economic concentration around a very few large cities rather than an economic leveler for the Russian regions. As a result, Russia's two

major metropolitan areas, Moscow and Saint Petersburg, are noteworthy for their high cost of living relative to local wages.

As a result, a significant number of Russian IT professionals may supplement legitimate incomes with criminal activity, leveraging professional talents to commit cybercrime that either targets or uses a computer, a computer network, or a networked device.[57] These Russian cybercriminals are representative of the broader Russian criminal population where members of Russian OCGs often straddle criminal and non-criminal careers.[58]

Early Russian cyber criminals operated independently in a disaggregated fashion, seeking to avoid drawing the attention of the state. Beginning in the late 2000s, this changed, with Russian cybercriminal activities increasingly coming under the control of traditional OCGs, which sought to extend their control over criminal activities from physical space to cyberspace.[59] Eight to twelve major nationwide OCGs operate in Russia today, with smaller nodes within these networks focused on particular aspects of criminal activity.[60] Russian OCGs are active across the full spectrum of criminality, engaging in illicit finance, the trafficking of weapons, drugs and people, and assassination for hire.[61] These OCGs now are also heavily involved in cybercrime, including credit card fraud, identity theft, the use of malware and ransomware for financial gain, and malware development for sale to external criminal actors.

One result of the co-opting of disaggregated, independent Russian cyber criminals by Russian OCGs is that cybercrime has become increasingly professionalized, and ironically mirrors somewhat the legitimate Russian IT industry. Today, organized cybercrime teams enable "individuals to branch out into a specific area of expertise,"[62] such as team leaders, coders, network administrators, intrusion specialists, data miners, and even financial specialists. The combination of increased professionalization and financial backing provided by established Russian OCGs has enabled Russian cybercriminal teams to increase the scope and scale of their hacking operations.[63] Recent examples of hacks by Russian OCG-backed cybercriminal groups include the high-profile ransomware attacks against Colonial Pipeline, JBS, and Kaseya,[64] as well as ongoing malicious cyber activities targeting Ukraine.[65]

Leveraging Corruption to Advance Foreign Policy Goals

Russia's pervasive culture of corruption helps explain how Russia's IT professionals are mobilized on the state's behalf to engage in offensive cybercrime in pursuit of Russia's geopolitical goals. While some hackers may be motivated in part by patriotism, corruption is the glue that binds together Russian IT professionals, cyber-criminals, and state security actors. While money is one factor that encourages participation in corrupt practices, self-preservation is another important motivation. In Russia, police and other government agents are known to violently enforce payment of protection money.[66] Paying bribes to government officials, police and tax inspectors by IT firms large and small is often necessary to avoid violence, imprisonment, and the shutdown of one's business. In the 1990s, most Russian IT out-

sourcing companies sought to "keep off the radar of the state and the tax police" until they became large enough to join the formal economy.[67] Importantly, corruption in Russia today extends far beyond the passing of bribes. For some Russian IT companies and professionals, hacking on behalf of the Russian state may be a way to avoid violent disruptions to their workplaces by the security services. While corruption seriously impedes the development of the Russian IT industry as a legitimate business sector, powerful incentives push Russian IT professionals to engage in malicious cyber activity on behalf of the Russian government.

The reciprocal nature of the relationship between organized crime and the state is also key to understanding how Russian cybercriminals mobilize on behalf of Russian foreign policy objectives. Cybercriminals are allowed to enrich themselves financially, provided the Russian state protecting cybercriminals can use their skills in support of Russia's goals.[68] Russian OCGs are also expected to avoid hacking targets within Russia. Committing cybercrimes on behalf of the state obviously allows willing participant OCGs to curry favor with political authorities and maintain their continued access to illicit opportunities.[69]

Relationships between the Russian state and Russian OCGs have their roots in the Soviet era but have shifted dramatically since then. The weakened central state of the 1990s presented OCGs with opportunities for massive financial gain as state assets were privatized.[70] Whereas OCGs concealed wealth from the state and the public during Soviet times, economic liberalization presented these entities the opportunity to convert criminal proceeds to legitimate wealth and ascend the ranks of Russian society.[71] The Russian state ultimately regained the upper hand, but did so without confronting or crushing empowered criminal enterprises.

One account describes the Russian state and Russian OCGs as having engaged in a process of reciprocal assimilation "in which intertwined networks of legality and illegality work in concert"[72] to maintain a grip on power in which the state and OCGs are mutually-dependent, semi-autonomous groups that share ideologies and resources. OCGs have "become an integral part of civil society"[73] and enjoy ties with the state at every level of socio-political power. While the state is the stronger of the two partners, it cooperates with OCGs to gain access to a deniable source of "private violence and illegal expertise."[74] This private expertise is enlisted by the state for its own purposes. Cybercriminal expertise is just one of these specialties, but is perhaps the most relevant criminal skillset to Russia's cyber power and global policy ambitions. The same technical knowledge that allows Russian OCGs to steal as much as trillions of dollars annually[75] can be leveraged for computer network exploitation and computer network attacks against foreign governments.

Cyber and Information Warfare

Cyber warfare, enabled by non-state cyber talent, has become a key tool in Russia's offensive defense strategy.[76] Putin professes that Russia and the West are already engaged in full-spectrum conflict,[77] and that the information sphere is but one key battleground in

this conflict. Putin purports to also believe that various democratic movements across the post-Soviet space, from the Orange Revolution to the Maidan Revolution, were organized by Western intelligence agencies with the ultimate goal of bringing about regime change in Russia.[78] In response, Russia has used its cyber power as part of a holistic information warfare strategy to sow discord across the West[79] and undermine unity between and within Western nations.[80] The cyber blockade of Estonia in 2007 by Russian non-state patriotic hackers and criminals[81] is the first known example of this trend, which arguably reached its apex in the Russian election interference campaigns in the United Kingdom, U.S. and France between 2015 and 2017.[82]

Russian leaders see the internet inside Russia primarily in terms of its potential to undermine regime stability.[83] Domestic legal and regulatory governance of the Russian internet lagged behind the build-out of the actual internet infrastructure,[84] yet state regulation of the Russian internet, or RuNet, increased following Putin's return as Russia's president in 2012. These regulations focus primarily on enabling surveillance of digital communications and restricting information flow that the Putin regime deems subversive to its aims. The origins of this approach can be found in the 2000 Information Security Doctrine of the Russian Federation, which declared that "the national security of the Russian Federation substantially depends on the level of information security." This doctrine defines information security as "national interests in the information sphere," referring to the regime's control over information flow to the public and not the safeguarding of networks and data.[85] In modern Russia, internet governance, cybersecurity, and media policy are all overseen by the same state agency, Roskomnadzor,[86] underscoring Russia's priority for internet governance being information control. Yet in line with Putin's alleged promise of "a decade of free development"[87] to the Russian IT industry at a December 28, 1999 meeting, internet entrepreneurship and commercial activity in Russia remain highly deregulated, a surprising approach for the Russian government, which is inclined towards "active regulation of most spheres of economic activity."[88]

Russia has begun to lay the technical groundwork to isolate the RuNet from the broader World Wide Web. In 2019, the Duma amended Russian federal law to provide a legal framework for the "centralized management of a public communications network." This framework empowers Roskomnadzor to "prohibit the routing of telecommunication messages through communication networks located outside of the territory of the Russian Federation" in the face of certain threats.[89] These amendments also call for the creation of a national Domain Name System (DNS), with its own proprietary infrastructure, which would be the first of its kind if implemented, and would render the RuNet inaccessible to the outside world. It also likely would disable internet users inside Russia from accessing parts of the Internet that use the existing global DNS.[90] This outcome would give Roskomnadzor unparalleled ability to control the flow of information into Russia.

Early Impacts of the Russo-Ukrainian War

Russia's invasion of Ukraine has shaken Russia's IT industry, with potential future consequences for Russian cyber power. In the first weeks after the invasion, tech workers fled Russia in droves. The Russian Association of Electronic Commerce, a Russian tech industry trade group, estimated some 50,000-70,000 tech workers left Russia during the first few weeks of the war.[91] At first, the Russian government sought to reassure the country's tech industry. In his annual address to the Russian Duma in early April 2022, Russian Prime Minister Mikhail Mishustin addressed the Russian IT industry directly, and Russia's government extended several guarantees to Russian IT professionals, including a promise that Russia's IT professionals would not be conscripted into the army. Other incentives included "exemptions from paying income tax, preferential mortgage rates, and additional funding for grants."[92] Yet Putin's so-called "partial mobilization" order in September 2022, seeking to press 300,000 men into military service, prompted a second mass exodus of IT professionals. Nikolay Komlev, director of Russia's Information & Computer Technologies Industry Association, claimed this wave of departures, notwithstanding Kremlin promises to exempt IT professionals from the draft, was "roughly two to three times" the size of the spring wave.[93] Many tech workers fled to other post-Soviet states like Armenia and Kazakhstan, even if they still worked for Russian companies.

The Russian government's crackdown on foreign platforms to more tightly control information flow to its citizens has also intensified. Post-invasion Russia has blocked Facebook, Twitter, and the Russian-language websites of several international news outlets.[94] In announcing the bans, Roskomnadzor accused Facebook, which had blocked the pages of state-controlled Russian media outlets like Russia Today and Sputnik, of violating "the key principles of free dissemination of information."[95]

In the near term, the Ukraine invasion is unlikely to degrade Russia's cyber power. It is likely the Russian IT industry will feel pressure to avoid or accommodate state attention, and this may improve the Kremlin's ability to leverage native IT talent in pursuit of its geopolitical ambitions. Western sanctions and export controls also may have the unintended effect of catalyzing Russian import substitution. Sanctions not only have limited Russia's access to key technologies but also have prompted U.S.-based technology firms like Microsoft to leave the Russian market.[96] This could present a market opportunity for Russian IT firms to develop domestically-produced alternatives to Western products, at least as to software, where the barriers to development are lower. Similarly, many Western research organizations halted collaborative efforts with Russian scientists after the Ukraine invasion.[97] Russians reportedly are increasingly collaborating with Chinese and Indian researchers, which may represent a model for collaboration in the Russian IT sector, although both India and China have deep state involvement in their respective technology sectors, thus making such partnerships less appealing to Russian firms.

In the medium-to-long term, the floodgate of departed Russian IT talent likely will limit Russia's ability to develop high-end cyber capabilities. Importantly, many departures during the first year of the war included those IT workers with international ties and some amount of financial resources. These IT professionals are likely some of Russia's best and brightest.[98] Another big risk Russia faces is that departed IT talent will hamper the education and training of future generations of Russian cyber talent, an effect that could compound as time passes.

CONCLUSION

Russia's disproportionate cyber power stems largely from its unique political, economic, and regulatory circumstances post-dating the collapse of the Soviet Union. Pervasive networks of corruption connect Russian IT professionals, Russian OCGs, and the Russian state, allowing the state to mobilize the tech industry's cyber talent for geopolitical goals. To formulate policies towards Russia that counter Russia's pervasive cybercrimes, Western governments should recognize that failing to address these three entities holistically is a fool's errand. Incentives that bind Russia's networks of corruption are far too strong to be effectively countered with piecemeal high-level diplomatic summits. But Russia's invasion of Ukraine presents the West with a unique opportunity to exploit the mass exodus of human capital Russia desperately needs in order to remain a top-tier cyber power. Western governments should further facilitate this exodus of Russian IT professionals with proactive integration into friendly nation workforces. For example, tens of thousands of Russian IT professionals now reside and work in the nation of Georgia.[99] In response, the Georgian government stood up a task force to help Russian companies and entrepreneurs navigate financial and bureaucratic hurdles. Western governments can and should pursue similar initiatives and find ways to incentivize companies that facilitate this migration.

NOTES

1. Voo, Julia, Irfan Hemani, and Daniel Cassidy. "National Cyber Power Index 2022." (Cambridge: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2022), 7. https://www.belfercenter.org/publication/national-cyber-power-index-2022
2. Whyte, Christopher, and Brian Mazanec. In *Understanding Cyber Warfare: Politics, Policy and Strategy*, (New York: Routledge, 2019), 119-20.
3. "World Economic Outlook Update, January 2024: Moderating Inflation and Steady Growth Open Path to Soft Landing." (World Economic Outlook. International Monetary Fund, January 2024), 6. https://www.imf.org/en/Publications/WEO/Issues/2024/01/30/world-economic-outlook-update-january-2024.
4. Chernova, Yuliya. "Departure of Tech Workers Weighs on Russian Economy." WSJ, November 13, 2022. https://www.wsj.com/articles/departure-of-tech-workers-weighs-on-russian-economy-11668172429.
5. Voo, et al.,. "National Cyber Power Index 2022," 9.
6. Insikt Group. "Dark Covenant 2.0: Cybercrime, the Russian State, and War in Ukraine." Recorded Future, January 31, 2023, 2. https://go.recordedfuture.com/hubfs/reports/cta-2023-0131.pdf.
7. Perfiliev, Yuri. "Development of the Internet in Russia: Preliminary Observations on Its Spatial and Institutional Characteristics." (Eurasian Geography and Economics 43, no. 5, July 2002): 412. https://doi.org/10.2747/1538-7216.43.5.411.
8. Bulashova, Natlia, Dmitri Burkov, Alexey Platonov, and Alexey Soldatov. "An Internet History of Russia in 1990s." In An Asia Internet History: First Decade (1980-1990), edited by Kilnam Chon, 227–64. (Seoul: Seoul National University Press, 2013). Accessed date, Asia Internet History Projects at https://sites.google.com/site/internethistoryasia/book1/ru.
9. Perfiliev. "Development of the Internet in Russia: Preliminary Observations on Its Spatial and Institutional Characteristics," 414.
10. Kolarova, Desislava, Asel Samaganova, Ivan Samson, and Patrick Ternaux. "Spatial Aspects of ICT Development in Russia." The Service Industries Journal 26, no. 8 (2006): 877. https://doi.org/10.1080/02642060601011673.
11. Perfiliev, "Development of the Internet in Russia: Preliminary Observations on Its Spatial and Institutional Characteristics," 414.
12. Bulashova, et al., "An Internet History of Russia in 1990s".
13. Kolarova, et al., "Spatial Aspects of ICT Development in Russia," 876.
14. Bulashova, et al., "An Internet History of Russia in 1990s".
15. Kolarova, et al., "Spatial Aspects of ICT Development in Russia," 876.
16. Loren, Graham. "Science in the New Russia." Issues in Science and Technology (blog), July 1, 2003. https://issues.org/graham-2/.
17. "Science and Engineering Indicators, 2004. Volume 2: Appendix Tables. NSB 04-01." (Arlington: National Science Foundation, 2004).
18. Aslund, Anders, Sergei Guriev, and Andrew Kuchins. *Russia after the Global Economic Crisis*. (Washington: Peterson Institute for International Economics, 2010), 96.
19. Perfiliev. Development of the Internet in Russia: Preliminary Observations on Its Spatial and Institutional Characteristics." 412.
20. Satinsky, Daniel. "The Growth of Russia's IT Outsourcing Industry: The Beginning of Russian Economic Diversification?" Wilson Center, April 17, 2006. https://www.wilsoncenter.org/publication/the-growth-russias-it-outsourcing-industry-the-beginning-russian-economic.
21. Gritsenko, Daria, Mikhail Kopotev, and Mariëlle Wijermars. "Digital Russia Studies: An Introduction." In The Palgrave Handbook of Digital Russia Studies, edited by Daria Gritsenko, Mariëlle Wijermars, and Mikhail Kopotev. (Cham: Springer International Publishing, 2021), 6. https://doi.org/10.1007/978-3-030-42855-6_1.
22. Perfiliev, "Development of the Internet in Russia: Preliminary Observations on Its Spatial and Institutional Characteristics." 412.
23. Goldman, Marshall I. *In Petrostate Putin, Power, and the New Russia.* (Oxford ; Oxford University Press, 2008), 61.
24. Aslund, et al., *Russia after the Global Economic Crisis*, 100.

NOTES

25. Satinsky, "The Growth of Russia's IT Outsourcing Industry: The Beginning of Russian Economic Diversification?'
26. Rossotto, Carlo Maria, Natalija Gelvanovska, Dr Yuri Hohlov, Dr Vaiva Mačiulė, and Sergei Shaposhnik. "A Sector Assessment: Broadband in Russia," (Washington: The World Bank, 2015), accessed via Research Gate at https://www.researchgate.net/publication/293485750_A_Sector_Assessment_Broadband_in_Russia, 30.
27. Rossotto, et al.,. "A Sector Assessment: Broadband in Russia," 7.
28. Galushkin, Alexander. "Internet in Modern Russia: History of Development, Place and Role." Asian Social Science 11 (June 5, 2015): 306. https://doi.org/10.5539/ass.v11n18p305.
29. Rossotto, et al. "A Sector Assessment: Broadband in Russia," 7.
30. Adya, Monica, and Kate M. Kaiser. "Early Determinants of Women in the IT Workforce: A Model of Girls' Career Choices." Information Technology & People 18, no. 3 (2005): 237–238. https://doi.org/10.1108/09593840510615860.
31. Yarrow, Andrew L. "The Scandalous Cost of Internet in America." (Santa Monica: Milken Institute, June 17, 2021). https://www.milkenreview.org/articles/the-scandalous-cost-of-internet-in-america.
32. Pew Research Center. "Internet/Broadband Fact Sheet," April 7, 2021. https://www.pewresearch.org/internet/fact-sheet/internet-broadband/.
33. Powell, Alison, Amelia Bryne, and Dharma Dailey. "The Essential Internet: Digital Exclusion in Low-Income American Communities." *Policy & Internet* 2, no. 2 (January 18, 2010): 159–90. https://doi.org/10.2202/1944-2866.1058.
34. Lee, Nicol Turner, James Seddon, Samantha Lai, and Brooke Tanner. "Why the Federal Government Needs to Step up Efforts to Close the Rural Broadband Divide." *Brookings* (blog), October 4, 2022. https://www.brookings.edu/research/why-the-federal-government-needs-to-step-up-their-efforts-to-close-the-rural-broadband-divide/.
35. Kleist, Virginia Franke, Amy B. Woszcynski, Humayun Zafar, and Pamila Dembla. "The Russian and Ukrainian Information Technology Outsourcing Market: Potential, Barriers and Management Considerations." Journal of Global Information Technology Management 18, no. 1 (January 2, 2015): 7. https://doi.org/10.1080/1097198X.2015.1015824.
36. Oliss, Brendan, Cole McFaul, and Jaret C. Riddick. "The Global Distribution of STEM Graduates: Which Countries Lead the Way?" Center for Security and Emerging Technology (blog), November 27, 2023. https://cset.georgetown.edu/article/the-global-distribution-of-stem-graduates-which-countries-lead-the-way/.
37. National Center for Education Statistics. "COE - Undergraduate Degree Fields," May 2023. https://nces.ed.gov/programs/coe/indicator/cta.
38. Aslund, et al., *Russia after the Global Economic Crisis,* 97.
39. Kleist, Virginia Franke, Amy B. Woszcynski, Humayun Zafar, and Pamila Dembla. "The Russian and Ukrainian Information Technology Outsourcing Market: Potential, Barriers and Management Considerations." Journal of Global Information Technology Management 18, no. 1 (January 2, 2015): 9. https://doi.org/10.1080/1097198X.2015.1015824.
40. Satinsky, "The Growth of Russia's IT Outsourcing Industry: The Beginning of Russian Economic Diversification?"
41. Gibson, Stan. "Outsourcing: The Russian Revelation." eWEEK, June 12, 2006. https://www.eweek.com/it-management/outsourcing-the-russian-revelation/.
42. Gibson, "Outsourcing: The Russian Revelation"
43. Satinsky, "The Growth of Russia's IT Outsourcing Industry: The Beginning of Russian Economic Diversification?"
44. Metz, Cade, and Adam Satariano. "Russian Tech Industry Faces 'Brain Drain' as Workers Flee." The New York Times, April 13, 2022, sec. Technology. https://www.nytimes.com/2022/04/13/technology/russia-tech-workers.html.
45. Organisation for Economic Co-Operation and Development (OECD). Education at a Glance 2019: OECD Indicators. Education at a Glance. 2. https://www.oecd.org/education/education-at-a-glance/
46. Regnum News Agency. "What professions do Russian school graduates choose in 2021?," March 19, 2021. https://regnum.ru/news/3219644, translated by Google.
47. Round, John, Colin C. Williams, and Peter Rodgers. "Corruption in the Post-Soviet Workplace: The Experiences of Recent Graduates in Contemporary Ukraine." Work, Employment and Society 22, no. 1 (March 1, 2008), at 152. https://doi.org/10.1177/0950017007087421.
48. Alekseev, Dmitry. "Increased Demand: Russian Schoolchildren Choose IT Professions." (February 25, 2022). https://iz.ru/1295504/dmitrii-alekseev/povyshennyi-spros-rossiiskie-shkolniki-vybiraiut-it-professii.
49. Kadlecová, "Russian-Speaking Cyber Crime: Reasons behind Its Success." The European Review of Organised Crime, 2015, 8. https://www.academia.edu/16548880/Russian_speaking_Cyber_Crime_Reasons_behind_Its_Success.

NOTES

50. Kleist, Virginia Franke, Amy B. Woszcynski, Humayun Zafar, and Pamila Dembla. "The Russian and Ukrainian Information Technology Outsourcing Market: Potential, Barriers and Management Considerations." Journal of Global Information Technology Management 18, no. 1 (January 2, 2015): 7.
51. Trellix. "Growling Bears Make Thunderous Noise," June 6, 2022. https://www.trellix.com/blogs/research/growling-bears-make-thunderous-noise/.
52. Kadlecová, "Rusasian-Speaking Cyber Crime: Reasons behind Its Success," 10.
53. KNBC News. "Skilled, Cheap Russian Hackers Power American Cybercrime," February 5, 2014. https://www.nbcnews.com/news/world/skilled-cheap-russian-hackers-power-american-cybercrime-n22371.
54. Kadlecová, "Russian-Speaking Cyber Crime: Reasons behind Its Success," 10.
55. Kolarova, et al. "Spatial Aspects of ICT Development in Russia," 877.
56. Kolarova, et al, "Spatial Aspects of ICT Development in Russia," 884.
57. Kaspersky Labs. "What Is Cybercrime? How to Protect Yourself from Cybercrime," June 9, 2023. https://usa.kaspersky.com/resource-center/threats/what-is-cybercrime.
58. Stephenson, Svetlana. "It Takes Two to Tango: The State and Organized Crime in Russia." Current Sociology 65, no. 3 (May 1, 2017): 413. https://doi.org/10.1177/0011392116681384.
59. Kadlecová, "Russian-Speaking Cyber Crime: Reasons behind Its Success," 6.
60. Global Organized Crime Index. "Criminality in Russia - The Organized Crime Index," 2021. https://ocindex.net/.
61. Galeotti, Mark. "Crimintern: How the Kremlin Uses Russia's Criminal Networks in Europe." ECFR, April 18, 2017. https://ecfr.eu/publication/crimintern_how_the_kremlin_uses_russias_criminal_networks_in_europe/.
62. Google Threat Analysis Group. "Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape." Google Threat Analysis Group, February 16, 2023. https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/.
63. Kadlecová, "Russian-Speaking Cyber Crime: Reasons behind Its Success." 6.
64. Dark Covenant: Connections Between the Russian State and Criminal Actors." Recorded Future, September 9, 2021. https://go.recordedfuture.com/hubfs/reports/cta-2021-0909.pdf.
65. Insikt Group. "Dark Covenant 2.0: Cybercrime, the Russian State, and War in Ukraine." Recorded Future, January 31, 2023. https://www.recordedfuture.com/dark-covenant-2-cybercrime-russian-state-war-ukraine.
66. Aslund, et al., *Russia after the Global Economic Crisis*, 123.
67. Satinsky, "The Growth of Russia's IT Outsourcing Industry: The Beginning of Russian Economic Diversification?".
68. Bajak, Frank. "How the Kremlin Provides a Safe Harbor for Ransomware." AP News, April 16, 2021. https://apnews.com/article/business-technology-general-news-government-and-politics-c9dab7eb3841be45dff2d93ed3102999.
69. Stephenson, "It Takes Two to Tango: The State and Organized Crime in Russia," 413.
70. Stephenson, "It Takes Two to Tango: The State and Organized Crime in Russia," 414.
71. Stephenson, "It Takes Two to Tango: The State and Organized Crime in Russia," 416.
72. Stephenson, "It Takes Two to Tango: The State and Organized Crime in Russia," 412.
73. Popov, Mikhail Yu., Andrey P. Mikhaylov, Ilya V. Pechkurov, Alexander A. Korovin, and Dmitriy N. Tishkin. "Relationship of Corruption and Organized Crime Groups in the Russian Society." In *Public Administration and Regional Management in Russia: Challenges and Prospects in a Multicultural Region*, edited by Elena G. Popkova and Konstantin V. Vodenko, 325. Contributions to Economics. (Cham: Springer International Publishing, 2020). https://doi.org/10.1007/978-3-030-38497-5_36.
74. Stephenson, "It Takes Two to Tango: The State and Organized Crime in Russia." 413.
75. Fleck, Anna. "Infographic: Cybercrime Expected To Skyrocket in Coming Years." Statista Daily Data, February 22, 2024. https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027.
76. Hill, Fiona. "Mr. Putin and the Art of the Offensive Defense: Approaches to Foreign Policy (Part Two)." Brookings, March 16, 2014. https://www.brookings.edu/articles/mr-putin-and-the-art-of-the-offensive-defense-approaches-to-foreign-policy-part-two/.
77. Reynolds, Maura. "'Yes, He Would': Fiona Hill on Putin and Nukes." *POLITICO*, February 28, 2022. https://www.politico.com/news/magazine/2022/02/28/world-war-iii-already-there-00012340.

NOTES

78. Wilde, Gavin, and Justin Sherman. "No Water's Edge: Russia's Information War and Regime Security." Carnegie Endowment for International Peace, January 4, 2023. https://carnegieendowment.org/2023/01/04/no-water-s-edge-russia-s-information-war-and-regime-security-pub-88644.
79. Connell, Michael, and Sarah Vogler. "Russia's Approach to Cyber Warfare." CNA, March 24, 2017. https://www.cna.org/reports/2017/russias-approach-to-cyber-warfare.
80. Whyte and Mazanec, *Understanding Cyber Warfare: Politics, Policy and Strategy,* 235.
81. Whyte and Mazanec, *Understanding Cyber Warfare: Politics, Policy and Strategy,* 234.
82. Whyte and Mazanec, *Understanding Cyber Warfare: Politics, Policy and Strategy,* 235.
83. Wilde, Gavin, and Justin Sherman. "No Water's Edge: Russia's Information War and Regime Security." Carnegie Endowment for International Peace, January 4, 2023. https://carnegieendowment.org/2023/01/04/no-water-s-edge-russia-s-information-war-and-regime-security-pub-88644.
84. Sukhodolov, Alexander P., Elena G. Popkova, and Irina M. Kuzlaeva. "Peculiarities of Formation and Development of Internet Economy in Russia," in *Internet Economy vs Classic Economy: Struggle of Contradictions. Studies in Computational Intelligence*, vol 714. (Cham: Springer, 2018), 66 accessed at https://link.springer.com/chapter/10.1007/978-3-319-60273-8_6
85. Wilde and Sherman, "No Water's Edge: Russia's Information War and Regime Security."
86. Maréchal, Nathalie. "Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy." Media and Communication 5, no. 1 (2017): 32. https://doi.org/10.17645/mac.v5i1.808.
87. Gritsenko, et al., "Digital Russia Studies: An Introduction." 7.
88. Sukhodolov,et al., "Peculiarities of Formation and Development of Internet Economy in Russia." 67.
89. Epifanova, Alena. "Deciphering Russia's 'Sovereign Internet Law,'" *German Council on Foreign Relations*, January 2020. https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law, 6.
90. Epifanova, "Deciphering Russia's "Sovereign Internet Law," 8.
91. Al Jazeera, "Shunned by the West, Russia's IT Sector Goes on the Defensive," November 21, 2022. https://www.aljazeera.com/news/2022/11/21/russias-it-sector-facing-ctrl-alt-delete-moment-in-midst-of-war.
92. Al Jazeera, "Shunned by the West, Russia's IT Sector Goes on the Defensive"
93. Chernova, Yuliya. "Departure of Tech Workers Weighs on Russian Economy." *WSJ*, November 13, 2022. https://www.wsj.com/articles/departure-of-tech-workers-weighs-on-russian-economy-11668172429.
94. Milmo, Dan. "Russia Blocks Access to Facebook and Twitter." *The Guardian*, March 4, 2022, sec. World news. https://www.theguardian.com/world/2022/mar/04/russia-completely-blocks-access-to-facebook-and-twitter.
95. Government of Russia, Federal Service for Supervision of Communications, Information Technology, and Mass Media, News of Roskomnadzor, "Retaliatory measures have been taken to restrict access to Russian media," March 4, 2022. https://rkn.gov.ru/news/rsoc/news74156.htm. Translated by Google.
96. Al Jazeera, "Shunned by the West, Russia's IT Sector Goes on the Defensive."
97. Van Noorden, Richard, "Data Hint at Russia's Shifting Science Collaborations after Year of War." *Nature* 615, no. 7951 (February 24, 2023): 199–200. https://doi.org/10.1038/d41586-023-00552-w.
98. Metz and Satariano. "Russian Tech Industry Faces 'Brain Drain' as Workers Flee." *The New York Times*, (New York), April 13, 2022, sec. Technology. https://www.nytimes.com/2022/04/13/technology/russia-tech-workers.html..
99. Champion, Marc, and Helena Bedwell. "Russia's Brain Drain Is Officially Underway." *Bloomberg.Com*, July 6, 2022. https://www.bloomberg.com/news/features/2022-07-06/russian-refugee-tech-workers-make-georgia-a-stepping-stone-for-global-career.