POLICY BRIEF

Exporting digital authoritarianism

Alina Polyakova and Chris Meserole

As Russia, China, and other states advance influence through forms of digital authoritarianism, stronger responses are needed from the U.S. and like-minded partners to limit the effects of their efforts.

EXECUTIVE SUMMARY

Digital authoritarianism — the use of digital information technology by authoritarian regimes to surveil, repress, and manipulate domestic and foreign populations — is reshaping the power balance between democracies and autocracies. At the forefront of this phenomenon, China and Russia have developed and exported distinct technology-driven playbooks for authoritarian rule. Beijing's experience using digital tools for domestic censorship and surveillance has made it the supplier of choice for illiberal regimes looking to deploy their own surveillance systems, while Moscow's lower-cost digital disinformation tools have proven effective in repressing potential opposition at home and undermining democracies abroad.

This policy brief examines the development and export of both the Chinese and Russian models. China pioneered digital age censorship with its "Great Firewall" of a state-controlled Internet and unprecedented high-tech repression deployed in Xinjiang in recent years, and has exported surveillance and monitoring systems to at least 18 countries. Russia relies less on filtering information and more on a repressive legal regime and intimidation of key companies and civil society, a lower-cost ad hoc model more easily transferable to most countries. The Russian government has made recent legal and technical moves which further tighten control, including legislation passed this year to establish a "sovereign Russian internet."

The authors recommend that the United States and other democracies should tighten export controls on technologies that advance digital authoritarianism, sanction regimes engaging in digital authoritarianism and firms that supply them, develop a competitive democratic model of digital governance with a code of conduct, and increase public awareness around information manipulation, including funding educational programs to build digital critical thinking skills among youth.

INTRODUCTION

In January 2010, Secretary of State Hillary Clinton delivered a landmark speech on internet freedom in which she argued that the spread of communications technology and free flow of information would ultimately lead to greater freedom and democracy.[1] In the years since, that view has come under increasing strain. Most notably, China and Russia have learned how to leverage both the internet and information technology in ways that have reduced rather than expanded human freedom. Worse, they have also begun to export their models of digital authoritarianism across the globe. Absent an effective democratic response, including an international rules of the road framework around surveillance technology exports, further advances in information technology may well yield a world of ever greater repression rather than liberalization.

Digital authoritarianism — the use of digital information technology by authoritarian regimes to surveil, repress, and manipulate domestic and foreign populations — is reshaping the power balance between democracies and autocracies. While China is driving innovation in high-tech social control, Russia has been more willing to weaponize information technologies as part of targeted influence operations. Both countries have developed and exported new tech-driven playbooks for authoritarian rule, but their strategies are quite distinct. The Chinese have long pioneered digital tools for domestic censorship and surveillance, dating back to the initial launch of its "Great Firewall" over two decades ago. More recently, Beijing's long experience building a robust digital surveillance architecture has started to pay dividends: China has increasingly become the supplier of choice for illiberal regimes looking to deploy surveillance systems of their own.

By contrast, Moscow is struggling to catch up with China's high-tech model of domestic control. Although the Russian government has sought to clamp down on internet freedom, gain access to citizens' personal data, and impose more control on the digital domain since the early 2000s, it has not been the "industry leader" in developing these tools. Rather, Moscow's domestic model is relatively low-tech when it comes to domestic surveillance. Its main focus has been the export of digital disinformation tools — a suite of information influence techniques easily bought and deployed by other state and non-state actors. Moscow's model of low-tech surveillance, due to its relative low cost and adaptability, is finding appeal among resource-poor governments that lack China's economic prowess, human capital capacities, and centralized state control.

Yet as different as the Chinese and Russian motivations and capabilities have been, the end result is remarkably similar: each country has developed a set of tools that enable rising authoritarians to repress potential opposition at home while undermining democracies abroad.

THE CHINESE MODEL

Beijing's approach to information technology dates back to the reformist era of Deng Xiaoping. In keeping with Deng's vision for opening China's economy while maintaining social stability, Zhongnanhai has consistently viewed digital technology as a key driver of economic development as well as a tool for preserving and even extending political control.[2] The strategy has largely been a success. China now boasts world-class technology and the second largest economy in the world,[3] yet the country's openness to global trade and information technology has not led to any meaningful political reform. The Chinese Communist Party (CCP) remains thoroughly entrenched in power, and Xi Jinping enjoys an extraordinary degree of political control.[4]

Beijing has leveraged information technology both online and offline. Email first arrived in China in 1987, and the commercial internet in 1994.[5] Not long after, Party leaders began insisting that the web would need to be used in accord with "Chinese characteristics."[6] In 1996, when only 150,000

Imams and Chinese government officials pass under security cameras as they leave the Id Kah Mosque in Kashgar, Xinjiang Uighur Autonomous Region, China, during a trip organized by the government for foreign reporters. January 4, 2019. REUTERS/Ben Blanchard

Chinese were online, State Council Order No. 195 explicitly brought the internet under state control. Within a year *Wired* was already referring to the "The Great Firewall of China."[7] In the twenty years since, Beijing's legal and technical architecture for web censorship and surveillance has grown dramatically. Although Xi centralized control over the internet in 2013, principally through the creation of a Cyberspace Administration that reports directly to him, the Chinese web is now overseen by over sixty agencies with vast legal and technical ability to monitor and regulate online activity.[8]

Far from sparking a political opening, within China the internet has been a valuable space for state censorship and surveillance.

Beijing's control over both the infrastructure and application layer of the web has had a profound impact on political behavior.[9] Although the CCP allows for some forms of criticism,[10] dissidents and human rights activists are nonetheless frequently detained for what they post on popular social media sites like Weibo and WeChat, both of which are aggressively monitored.[11] (Indeed, in Xinjiang, residents are only allowed to use WeChat, precisely because it is so widely monitored.)[12] Meanwhile, applications and websites that do not comply with Beijing's demands operate at considerable peril: in the first three weeks of 2019 alone, the Xi regime shut down over 700 websites and 9,000 mobile apps, including those owned by prominent companies like Tencent.[13] Far from sparking a political opening, within China the internet has been a valuable space for state censorship and surveillance.

Yet the Chinese are not just monitoring online activity. In 2005, the Ministry of Public Security (MPS) and Ministry of Industry and Information Technology (MIIT) jointly launched a program called SkyNet, which aimed to install a national network of CCTV feeds.[14] By 2010, Beijing alone was blanketed with 800,000 surveillance cameras, and by 2015 Beijing police boasted that the city was 100% covered. More than 20 million more cameras were

in use nationwide.[15] Based on the success of the SkyNet program, the National Development and Reform Commission (NDRC) in 2015 then set the ambitious goal of covering all of China's public spaces and leading industries in cameras by 2020, with the aim of creating an "omnipresent, fully networked, always working and fully controllable" surveillance system.[16] Although that goal is far-fetched, the resulting "Sharp Eyes" initiative is nonetheless extraordinary for its reach and scope. The project, whose title alludes to the CCP slogan "the people have sharp eyes,"[17] promises to link together smartphones and smart TVs as well as surveillance cameras, and has already produced smartphone apps individuals can use to monitor feeds and report suspicious activities.[18] As "Sharp Eyes" feeds are coupled with location data taken from smartphones and vehicles, Beijing will increasingly be able to monitor the movements and behavior of its citizens in unprecedented detail.[19]

However, China's vision for a real-time, nationwide surveillance network will require more than just ubiquitous video streams and sensor data. It will also need to leverage artificial intelligence (AI) to identify and track individuals across the network. As a result, Chinese companies like HikVision, the world's largest manufacturer of surveillance equipment, have moved aggressively to meet that demand,[20] while Beijing has invested heavily in domestic AI startups like Sensetime, Yitu, and Megvii, which received over $2 billion in government initiated investment in 2018.[21] SenseTime alone has the goal of creating a system that can monitor 100,000 high-resolution video feeds simultaneously and identify and track individuals across them in real-time.[22] Early efforts at such a network have illustrated its promise for local policing: during a concert in Jiangxi province in May 2018, a facial recognition software alerted concert security that one of the 60,000 concert goers was actually a suspected fugitive. The 31-year-old man was arrested within minutes,[23] and now represents one of thousands that state authorities claim SkyNet and similar programs have helped capture.[24]

Beijing is not just constructing separate surveillance systems for the web and real-world. It is also increasingly seeking to link the two. Most notably, in 2014 the State Council announced its goal to establish a national "social credit score" system by 2020.[25] As with "Sharp Eyes," that deadline will likely prove infeasible. A national system that can aggregate bank data, hospital records, real-world movements, online activity, and other records into a single "trustworthiness" score is still more an aspiration than a reality, as Jamie Horsely and others have noted.[26] But in mandating a system that will "allow the trustworthy to roam everywhere under heaven while making it hard for the discredited to take a single step," the State Council has nonetheless incentivized the creation of a suite of digital tools for algorithmic governance without meaningful due process.[27] By transforming online and offline data into a single measure that is then coupled with state power, the early social credit systems that have emerged promise to serve as a lever of social control that 20th century authoritarian regimes could only dream of.

China's development of "the autocrat's new toolkit," as Richard Fontaine and Kara Frederick have put it, will have a profound impact on the rights and liberties of all its citizens.[28] Yet that impact has already been felt far more acutely by one group in particular.

Xinjiang and the Strike Hard Campaign

Beijing has pioneered many of its most repressive surveillance technologies in the Muslim and Turkic-speaking provinces of western China.[29] In 2009, after two Uighurs were injured in fights with ethnically Han workers at a factory, rioting broke out in Urumqi, the capital of Xinjiang.[30] The resulting violence left more than 150 dead, and represented the worst unrest in China since the Tiananmen crackdown twenty years earlier.[31] Beijing's crackdown in response only sparked further, more deliberate violence: in 2013, militants from Xinjiang carried out a vehicle attack in Tiananmen square,

killing five;[32] in May 2014, five suicide bombers in Urumqi killed over 30 civilians;[33] in June 2014, at Kunming Station in Yunnan province, eight knife-wielding attackers from Xinjiang killed 29 more.[34]

As the violence escalated, Beijing grew impatient. In May 2014, China's national police ministry implemented a new "Strike Hard Campaign against Violent Terrorism."[35] As with prior "Strike Hard" campaigns in the region, the new campaign made extensive use of mass arrests and pre-trial detention centers. By the end of 2014, arrests in Xinjiang had doubled from the year before,[36] a figure that would soon rise three-fold.[37] Arrests and detentions have risen so dramatically in Xinjiang that up to 1 million individuals are now being held in various camps, centers, and prisons across Xinjiang.[38]

Yet the Strike Hard Campaign is unprecedented not just for its sheer scale, but also for its novel use and deployment of technology. Although authorities in Xinjiang have long used information technology to counter unrest—to quell the 2009 riots, for example, they shut down all internet and text-messaging in the region[39] — they had never previously used it with such precision and ubiquity. In August 2016, after Chen Quanguo was appointed Party Secretary in Xinjiang, he brought with him many of the securitization measures and surveillance technologies he introduced in Tibet.[40] By greatly expanding the number of police checkpoints in Xinjiang and outfitting them with biometric sensors, iris scanners, and access to nearby CCTV cameras, Chinese security services in Xinjiang have been able to monitor the movement and behavior of its residents in unparalleled detail, with Uighurs in particular being singled out. At police checkpoints, Uighurs frequently have their DNA collected and their eyes scanned,[41] and they may be forced to install spyware on their phones that tracks all of their online activity.[42] To cover Uighur movement between checkpoints, the CCP has also mandated all vehicles in Xinjiang to install a navigation system powered by Beidou, China's version of the Global Position System, or GPS.[43] In addition, security services in Xinjiang have also begun to deploy flocks of small bird-like surveillance drones to cover areas that CCTV feeds do not track.[44]

The Strike Hard Campaign in Xinjiang has created arguably the world's largest open air digital prison—and provided an early glimpse of what digital authoritarianism might have in store.

The Strike Hard Campaign in Xinjiang has created arguably the world's largest open air digital prison—and provided an early glimpse of what digital authoritarianism might have in store.

Exporting Digital Authoritarianism

China has sold information technology to foreign regimes for decades. From monitors and microprocessors to routers and radios, factories in Shenzhen and elsewhere have long manufactured communications technology used by states and security services abroad.

Yet China's export of information technology has changed recently in two ways. The first is that the products and services it sells are no longer low-cost knockoffs of high-tech products. Instead, Huawei, HikVision, Yitu, and others are now selling high-quality products that are not only produced in China but designed there too.[47] Although some Chinese surveillance products are still reliant on Western semiconductors and sensors, many reflect genuine innovation and are as competitive on quality as they are on cost. Second, Beijing no longer views information technology solely in terms of economic development, but also its value to Chinese foreign policy and strategy.[48] The Xi regime

has aggressively pushed Chinese information technology as part of its Belt and Road Initiative (BRI), the strategic investment vehicle China uses to finance major infrastructure projects abroad.[49] For Beijing, exporting its information technology is not only about securing important new sources of revenue and data, but also generating greater strategic leverage vis-à-vis the West.[50]

Beijing's efforts have already begun to pay dividends. In Southeast Asia, Malaysia has integrated Chinese facial-recognition technology into its armed services, while Singapore aims to deploy the technology across a network of street cameras, similar to Beijing's embrace of SkyNet.[51] In East Africa, Ethiopian security services relied on telecommunications equipment from ZTE to monitor and surveil opposition activists and journalists.[52] In Southern Africa, both Zimbabwe and Angola have signed partnerships with Chinese companies to provide AI for their ruling regimes, all under the auspices of BRI.[53] In Venezuela, the Maduro regime has contracted with ZTE to build a national ID card, payment system, and "fatherland database" that will track individuals' transactions alongside personal information such as birthdays and social media accounts. Opposition activists and human rights dissidents fear that Maduro's real aim is for ZTE to effectively implement China's "social credit system" within Venezuela.[54] Chinese surveillance systems, or a basic version of them, have also been implemented in Ecuador, where footage collected by the government's 4,300 cameras is transmitted to the intelligence services.[55] Meanwhile, in the Middle East, Dubai has already begun to deploy Chinese technology as part of its "Police without Policemen" program,[56] an ambitious project to reduce crime, replacing policemen with video surveillance and facial recognition technology.[57] Ecuador shows how technology built for China's political system is now being applied — and sometimes abused — by other governments. At least 18 countries currently use Chinese surveillance and monitoring systems, and at least 36 governments have held Chinese-led trainings and seminars on "new media" or "information management."[58]

As Chinese surveillance technology improves in quality and declines in cost, the global demand for Beijing's model of digital authoritarianism will likely only grow. With 5G networks on the horizon, illiberal and hybrid regimes throughout Asia, the Middle East, Africa, and Latin America will all build out the next generation of their domestic telecommunications and surveillance systems over the coming decade. If liberal democracies do not present a compelling and cost-effective alternative to the Chinese model of digital governance and infrastructure, the authoritarian toolkit that Beijing has long honed at home will increasingly spread abroad.

THE RUSSIAN MODEL

Compared to Beijing's early investment in developing content-blocking capabilities in the 1990s, Moscow was late to the game. As a result, as the internet penetrated Russian society, the digital domain remained, at least initially, relatively unencumbered and free. Unlike their Chinese neighbors, for example, Russians can access Facebook, Twitter, and Google — all of which are blocked in China. But Russia's unbridled net freedom was short-lived: by 1998, the government began to adapt Soviet era surveillance technology, known as the System of Operative-Search Measures (SORM), for the digital domain. To supplement technological surveillance, starting in the early 2000s, the Russian state began to implement a series of laws that *de facto* criminalize criticism of the government, legalize unfettered surveillance of citizens' online activities, and increase state control of the Russian internet or Runet.

Beginning in 2014, the government made legal and technical moves to establish a so-called Russian "sovereign internet" based on the Chinese model. Russian President Vladimir Putin signed the sovereign internet law in May 2019, allowing the government's media regulator, Rozkomnadzor, to seize the Russian internet if Russia were cut off from the global web.[59] If successful, which is

People shout slogans during a rally to protest against tightening state control over the internet in Moscow, Russia. March 10, 2019. REUTERS/Shamil Zhumatov

debatable, the Russian government would be able to isolate the Russian internet in whole or in parts from the global net. The law is set to come into effect on November 1, 2019,[60] and there is growing concern that Russia's efforts would accelerate the fracturing of the global internet, perhaps even surpassing China's initiative.[61]

In the long run, the Russian model may prove to be more adaptable globally as emerging authoritarian regimes that cannot afford China's high-tech model seek greater control over domestic populations and influence abroad.

Still, Russian surveillance technology relies less on filtering information before it reaches citizens (as is the case in China) and more on a repressive legal regime coupled with tightening information control and intimidation of internet service providers (ISPs), telecom providers, private companies, and civil society groups.[62] It is an ad hoc model utilizing legal, technical, and administrative means that is well-suited to diffusion across aspiring authoritarian regimes.[63] And across the world, there are far more countries that are similar to Russia in terms of capabilities, economic resources, and computing resources than China. For this reason, Russia's model may be an appealing, relatively low-tech and low-cost alternative to the Chinese model, because it does not necessitate high-tech information filtration capabilities and can be implemented without a pre-existing government firewall.[64] While Russian companies' main market for export of surveillance technologies has been the Russian "near abroad" — namely, some former Soviet states — Russian surveillance tech has appeared in the global south as well.[65] In the long run, the Russian model may prove to be more adaptable globally as emerging authoritarian regimes that cannot afford China's high-tech model seek greater control over domestic populations and influence abroad.

Ad-hoc Surveillance

SORM, the Russian government's surveillance system, was initially developed by the Soviet intelligence agency (KGB) to monitor phone calls. It expanded to the internet to monitor email traffic, web browsing activity, and other digital data under a new iteration known as SORM-2. By 2015, an updated version — SORM-3 — would encompass all telecommunications. Under Russian law (more on this below) ISPs and telecom providers are required to install SORM equipment providing the Russian Federal Security Services (FSB) access to all data shared online without companies' knowledge or control of which data are being shared and with whom. SORM works by basically copying all data flows on internet and telecom networks — sending one copy to the government and the other to the intended destination.[66] SORM is the FSB's "backdoor" to Russia's internet.[67]

Since Putin's return to the presidency in 2012, an increasing number of Russian state agencies have also been granted access to SORM surveillance and content moderation under the guise of "public safety" or counter-terrorism and extremism. In addition to the FSB, Roskomnadzor (the Russian media regulator), the Prosecutor General's Office, the Federal Service for Surveillance on Consumer Rights and Human Wellbeing (Rospotrebnadzor), and the Federal Drug Control Service were granted the ability to block content without court order in 2013.[68]

To extend the reach of the SORM-3 system, the Ministry of Communications plans to localize 99% of all internet data by 2020, which would require ISPs to store Russian citizens' personal data on Russian territory.[69] The Ministry also plans to require that more customer/client information be accessible to SORM in the next three years, including drafted text messages.[70] But the Russian government faces significant implementation challenges to effective surveillance. Most notably, the cost of mass surveillance related to all aspects of electronic tracking is high for the Russian government to implement — ranging from 130 to 10 trillion rubles (approximately 2 to 150 billion U.S. dollars per year).[71] Due to these high costs, the Russian government has invested more in targeting technologies that boost SORM's precision rather than an all-encompassing content-filtering system.[72]

In addition to SORM, Russia began to institute a video surveillance system in 2015 known as "Safe City." The system allows the automatic transfer of information, including facial/moving objects recognition, to government authorities.[73] This information is available to any executive or presidential body. The budget for "Safe City" implementation from 2012 to 2019 was an estimated $2.8 billion to cover all cities hosting the 2018 World Cup.[74] The city of Moscow has approximately 170,000 cameras, at least 105,000 of which have been outfitted with facial recognition technology developed by the Russian firm NTechLabs.[75]

Non-compliance by private companies has also been an obstacle for Moscow. The Russian government's battle with the messaging app "Telegram" illustrates the limits of the authorities' reach. Telegram, founded by Russian entrepreneur Pavel Durov, refused to allow government access to the platform's encrypted data, as required by Russian law. In April 2018, the government blocked Telegram, which in turn used various workarounds, including routing data through Amazon's and Google's cloud service, to still keep the app active. The Russian internet regulator found itself in the awkward position of having to block at least 18 million IP addresses, unintentionally disrupting banking, transportation, news sites, and other services.[76] Across Russian cities, Russians demonstrated in support of the app and internet freedom.[77] Google and Amazon conceded to the Russian government's demands to clamp down on "domain fronting," the technique that Telegram used to get around government monitoring. Still, the government's failure to block Telegram revealed the

limits of Moscow's capabilities, the importance of a free internet to Russian citizens, and the breadth of internet penetration across the country.

AI-powered Surveillance

Looking to China, Russia is eager to integrate artificial intelligence technologies into its system of surveillance. Speaking to Russian students in September 2017, Putin squarely positioned Russia in the technological arms race for AI when he declared that "whoever becomes the leader in [artificial intelligence] will become the ruler of the world."[78] Russia spends approximately $12.5 million a year on AI research[79] with hopes to grow the domestic Russian market for AI to $400 million by 2021.[80] In May 2019, the Russian Direct Investment Fund (RDIF) raised $2 billion from foreign investors to support domestic AI development.[81] Even with this new influx of investments, Russia would remain far behind China, which plans to grow its AI industry to $150 billion by 2030.[82] Still, the Russian government is ramping up its efforts to grow the AI sector. The Ministry of Defense, state-owned companies, and, to a much smaller extent, public-private partnerships and foreign investment are leading these efforts.

Following Putin's 2017 speech, the Russian Ministry of Defense took the lead in mobilizing the Russian government's approach, which includes building an AI-infrastructure for research and development, engaging the private and civilian sectors in government projects, and organizing major AI conferences in Russia.[83] The Ministry organized the first conference on AI in March 2018[84] and a second in April 2019 geared towards business solutions and AI technology optimization.[85] In January 2019, Putin issued an official decree instructing the government to produce a national security strategy on AI.[86] The decree tasks Sberbank, the state-controlled bank, with developing proposals for the AI strategy to be finalized in June 2019.[87] In a speech[88] on May 30, 2019, Putin previewed the forthcoming strategy that would include greater investment in STEM education, public-private partnerships, training, and an effort to protect intellectual property rights.[89] The strategy is part of the Russian government's larger "Digital Economy of the Russian Federation" program, which aims to implement AI technologies in other sectors such as e-governance and the judicial system.[90] The use of AI-driven predictive analytics in the Russian criminal system, for example, would allow the government to identify "potential offenders" and calibrate sentencing based on the threat they present to the regime.[91]

Legalizing Digital Authoritarianism

In 2016, a new package of laws, the so-called Yarovaya amendments, required telecom providers, social media platforms, and messaging services to store user data for three years and allow the FSB access to users' metadata and encrypted communications.[92] While there is little known information on how Russian intelligence agencies are using these data, their very collection is an opportunity for intimidation and harassment of private companies and civil society organizations.

Civil society groups and independent media have been the primary targets of legalized surveillance, repression, and censorship. The Russian government began blocking virtual private networks (VPNs) that allow access to banned content in July 2017. That fall, President Putin signed into law legislation allowing the Russian government to designate media organizations that receive funding from abroad as "foreign agents." The law also grants the Russian authorities an expansive mandate to block online content, including social media websites, whose activities are deemed "undesirable" or "extremist."[93] In January 2018, requirements went into effect preventing social media and communications platforms users from remaining anonymous. These have been difficult to enforce so far because of non-cooperation by private companies. Taken together, these measures and their subsequent countless amendments have set up a complex legal web of

repression. They have also granted the Russian government the power to block access to any distributed information appealing for public protest if it designates it extremist or undesirable.[94]

Creating a "Sovereign" Russian Internet

The Russian government began efforts to develop an internal internet "kill switch" in 2012, following anti-government protests over election fraud. The capability would go beyond blocking content or identifying potential dissenters — the aim is for the authorities to be able to switch off the country or specific regions from the global web while still maintaining the general operability of the internet.[95] In February 2019, legislation to establish the so-called "sovereign Russian internet" passed the first reading in the Russian parliament (the Duma) with 75% of the vote. President Putin signed it into law on May 1, 2019, and it is set to come into effect in November 2019.

With this new measure, the government aims to establish control of Russian internet traffic by routing it through domestic exchanges. The law requires internet providers to install "free" equipment to automatically block banned websites, monitor (and prohibit by discretion) communication across borders,[96] and allow Roskomnadzor to take centralized management at a "time of crisis."[97] In the long term, the bill has the potential to cut out small providers or control them, provide Roskomnadzor with a complete map of data exchange points, and restrict traditional bypass methods (VPNs, independent ISPs, etc.).[98] It also takes aim at Telegram, which remains accessible in Russia primarily through VPN use. Implementation of the legislation will prove to be costly if not impossible given Russia's high connectivity to the global web, which peaked in 2018, according to a Russian government index.[99] Moscow will also have to create its own Domain Name System (DNS) and ISPs will need to install the required monitoring equipment at an estimated cost of $320 million dollars to the Russian government.[100] The idea of a sovereign internet is also unpopular among Russians — only 23% support a sovereign internet model, while 52% believe that the internet in Russia should continue to develop in connection to the world.[101] Ultimately, the law may lead to greater segmentation of the World Wide Web — already segmented by China's sovereignty principles — as Russia restricts its citizens' access to global data.

Exporting the Russian Model

Countries in Russia's near abroad are importing SORM technologies and replicating the Russian legal framework supporting population surveillance. In Kazakhstan, a replica of SORM allows for the latest deep packet inspection (DPI), in line with Russian standards. In 2018, the Kazakh National Security Committee implemented new technical regulations for its SORM system to grant the government real-time access to operators' networks.[102] Belarus has had a SORM-style system since 2010.[103] Kyrgyzstan's surveillance network is also modeled on SORM and has matched Russian interception systems since 2012.[104] With the exception of the Baltic States, Armenia, and Georgia, all other former Soviet republics have instituted aspects of the Russian digital authoritarian model at various times in their post-Cold War histories.[105] Two Russian companies, Protei and Peter-Service, have become main SORM providers since the early-2010s. Some of Protei's customers are telecom companies in the Middle East (Bahrain, Iraq, Qatar, etc.) and Latin America (Cuba, Mexico, Venezuela). Peter-Service has customers in Belarus, Abkhazia, Georgia, and Ukraine.[106]

Beyond limited technology exports, the Russian state has invested significant resources in information manipulation — initially tested on domestic audiences and then deployed against other countries. In this space, Russian activities are not limited to its near abroad but take aim against Western democracies. Through overt state-sponsored media outlets, such as RT and Sputnik, and covert information operations in the digital

domain, Moscow seeks to influence the information environment on a global scale. Whereas China's efforts focus on promoting a positive view of China (or repressing negative views through various influence and intimidation techniques), the Russian approach aims to destabilize politics and polarize societies to weaken them from within. This zero-sum view of international relations has become part and parcel of Russian foreign policy.

CONCLUSIONS AND RECOMMENDATIONS

Responding to Digital Authoritarianism

As Russia, China, and other states advance influence through forms of digital authoritarianism, stronger responses are needed from the U.S. and like-minded partners to limit the detrimental effects of their efforts. An initial step involves designating regimes as digital authoritarians if they routinely and purposefully employ mass surveillance without adequate safeguards and protections. Firms that supply digital authoritarian regimes should be sanctioned heavily—not just those in Russia and the United States, but also companies based in Europe, Israel, and elsewhere. Concurrently, controls should be tightened over exports of sensitive technologies to China and other digital authoritarians.

Ultimately, the West will need to develop a democratic model of digital governance that can outcompete authoritarian ones. To do this, the technology sector and policymaking community in the United States and Europe will need to offer compelling models of digital surveillance that enhance security while still protecting civil liberties and human rights.

To advance this goal, a digital governance code of conduct is needed. A coalition of democratic governments, tech companies, and civil society should develop such a code, which would include an articulation of operating procedures for addressing social media manipulation, common terms of use across platforms, and shared rules on personal data use. Finally, greater public awareness of this challenge is needed. To build resilience against foreign influence operations in democratic societies, governments should invest in raising public awareness around information manipulation. This should include funding educational programs that build digital critical thinking skills among youth.

- **Export controls**. Although China can match the U.S. in software quality, it has yet to master semiconductor manufacturing. Some of the equipment that China relies on for mass surveillance systems incorporate advanced processors and sensors that are only produced in the west. The U.S. and Europe have already begun restricting the export of such technologies to China and should consider expanding the use of export controls.

- **Targeted sanctions**. The United States should designate regimes as "digital authoritarian" if they routinely and purposefully employ mass surveillance without adequate safeguards and protections. Firms that supply digital authoritarian regimes should be sanctioned heavily—not just those in Russia and the U.S., but also companies based in the United States and Europe.

- **Democratic models**. Where the export of digital authoritarianism is concerned, sanctions alone won't be enough to check its spread. Ultimately, the West will need to develop a democratic model of digital governance that can outcompete authoritarian ones. To do this, the technology sector and policymaking community in the United States and Europe will need to offer compelling models of digital surveillance that enhance security while still protecting civil liberties and human rights.

- **Digital governance code of conduct.** The U.S. and Europe should work to develop common practices, rules, and systems of digital governance. A coalition of democratic

governments, tech companies, and civil society should develop a code of conduct which should include an articulation of operating procedures for addressing social media manipulation, common terms of use across platforms, and shared rules on personal data use.

- **Public awareness.** To build resilience against foreign influence operations in democratic societies, governments should invest in raising public awareness around information manipulation. This should include funding of educational programs that build digital critical thinking skills among youth.

REFERENCES

1 Hillary Rodham Clinton, "Remarks on Internet Freedom," (speech, Washington, DC, January 21, 2010), https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

2 Chinese leaders were especially drawn to the technology's economic potential. In 1983, Zhao Zhiyang even claimed that, "The new technological revolution or information revolution … may help China skip over some of the stages of which have been experienced by other developing countries." Geoffry Taubman, "A Not-So World Wide Web: The Internet, China, and the Challenges to Nondemocratic Rule," *Political Communication* 15, no. 2 (1998): 262, https://www.tandfonline.com/doi/abs/10.1080/10584609809342369.

3 For more on China's cutting-edge technology sector, see *Testimony Before the House Permanent Select Committee on Intelligence: China's Threat to American Government and Private Sector Research and Innovation Leadership*, 115th Cong. (July 19, 2018) (statement of Elsa B. Kania, Adjunct Fellow, Center for a New American Security), https://docs.house.gov/meetings/IG/IG00/20180719/108561/HHRG-115-IG00-Wstate-KaniaE-20180719.pdf.

4 Most notably, in 2018 Xi managed to overturn the term limits Deng put in place in 1982. See James Doubek, "China Removes Presidential Term Limits, Enabling Xi Jinping To Rule Indefinitely," *NPR*, March 11, 2018, https://www.npr.org/sections/thetwo-way/2018/03/11/592694991/china-removes-presidential-term-limits-enabling-xi-jinping-to-rule-indefinitely.

5 Ironically, the first message sent from Beijing read, "Across the Great Wall we can reach every corner of the world." See Rongbin Han, *Contesting Cyberspace in China: Online Expression and Authoritarian Resilience* (New York: Columbia University Press, 2018), 29.

6 Geoffrey Taubman, "A Not-So World Wide Web: The Internet, China, and the Challenges to Nondemocratic Rule," 263.

7 Geremie R. Barme and Sang Ye, "The Great Firewall of China," *Wired*, June 1, 1997, https://www.wired.com/1997/06/china-3/.

8 Margaret E. Roberts, *Censored: Distraction and Diversion Inside China's Great Firewall* (Princeton, NJ: Princeton University Press, 2018), 106-107.

9 Paul Mozur, "China Presses Its Internet Censorship Efforts Across the Globe," *The New York Times,* March 2, 2018, https://www.nytimes.com/2018/03/02/technology/china-technology-censorship-borders-expansion.html.

10 Gary King, Jennifer Pan, and Margaret E. Roberts, "How Censorship in China Allows Government Criticism but Silences Collective Expression," *American Political Science Review* 107, no. 2 (May 2013): 1-18, https://gking.harvard.edu/files/gking/files/censored.pdf/. Rebecca MacKinnon, "Liberation Technology: China's "Networked Authoritarianism" *Journal of Democracy* 22, no. 2 (April 2011): 32-46, https://muse.jhu.edu/article/427159.

11 "China web users arrested over posts on Sina Weibo," *BBC News*, August 22, 2013, https://www.bbc.com/news/technology-23795294.

12 James A. Millward, "What It's Like to Live in a Surveillance State," *The New York Times*, February 3, 2018, https://www.nytimes.com/2018/02/03/opinion/sunday/china-surveillance-state-uighurs.html.

13 Cathy He, "China Purges 9,000 Mobile Apps, 700 Websites in Internet Crackdown," *The Epoch Times*, January 23, 2019, https://www.theepochtimes.com/china-purges-9000-mobile-apps-700-websites-in-internet-crackdown_2776207.html.

14 Zhang Zihan, "Beijing's guardian angels?," *Global Times*, October 10, 2012, http://www.globaltimes.cn/content/737491.shtml.

15 Frank Langfitt, "In China, Beware: A Camera May Be Watching You," *NPR*, January 23, 2013, https://www.npr.org/2013/01/29/170469038/in-china-beware-a-camera-may-be-watching-you.

16 "About Strengthening Public Safety Video Surveillance Construction Networking: Several opinions on application work," (Beijing: National Development and Reform Commission of the People's Republic of China, 2015), http://www.ndrc.gov.cn/zcfb/zcfbtz/201505/t20150513_691578.html.

17 Qiao Long, "China Aims For Near-Total Surveillance, Including in People's Homes," trans. and ed. Luisetta Mudie, *Radio Free Asia*, March 30, 2018, https://www.rfa.org/english/news/china/surveillance-03302018111415.html.

18 Oiwan Lam, "With 'Sharp Eyes', Smart Phones and TV Sets Are Watching Chinese Citizens," *Global Voices Advox*, April 3, 2018, https://advox.globalvoices.org/2018/04/03/with-sharp-eyes-smart-phones-and-tv-sets-are-watching-chinese-citizens/.

19 Simon Denyer, "Beijing bets on facial recognition in a big drive for total surveillance," *The Washington Post,* January 7, 2018, https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/?utm_term=.2183756975a9.

20 "Hikvision Launches Face Recognition Terminals," *HikVision*, July 2, 2018, https://www.hikvision.com/en/Press/Press-Releases/Product-Release/Hikvision-Launches-Face-Recognition-Terminals.

21 Kane Wu and Julie Zhu, "China's AI start-up Megvii raising $500 million at $3.5 billion valuation: sources," *Reuters*, December 9, 2018, https://www.reuters.com/article/us-megvii-fundraising/chinas-ai-start-up-megvii-raising-500-million-at-35-billion-valuation-sources-idUSKBN1O90AV.

22 "China Now Has the Most Valuable AI Startup in the World," *Bloomberg*, April 8, 2018, https://www.bloomberg.com/news/articles/2018-04-09/sensetime-snags-alibaba-funding-at-a-record-3-billion-valuation.

23 Amy B. Wang, "A suspect tried to blend in with 60,000 concertgoers. China's facial-recognition cameras caught him.," *The Washington Post*, April 13, 2018, https://www.washingtonpost.com/news/worldviews/wp/2018/04/13/china-crime-facial-recognition-cameras-catch-suspect-at-concert-with-60000-people/?utm_term=.e0ad09991412.

24 Eamon Barrett, "In China, Facial Recognition Tech Is Watching You," *Fortune*, October 28, 2018, http://fortune.com/2018/10/28/in-china-facial-recognition-tech-is-watching-you/.

25 "China outlines its first social credit system," *People China*, June 27, 2014, http://en.people.cn/n/2014/0627/c90785-8747863.html.

26 Jamie Horsley, "China's Orwellian Social Credit Score Isn't Real," *Foreign Policy,* November 16, 2018, https://foreignpolicy.com/2018/11/16/chinas-orwellian-social-credit-score-isnt-real/.

27 Simina Mistreanu, "Life Inside China's Social Credit Laboratory," *Foreign Policy*, April 3, 2018, https://foreignpolicy.com/2018/04/03/life-inside-chinas-social-credit-laboratory/.

28 Richard Fontaine and Kara Frederick, "The Autocrat's New Tool Kit," *The Wall Street Journal*, March 15, 2019, https://www.wsj.com/articles/the-autocrats-new-tool-kit-11552662637.

29 For a deeper history of conflict in the region, see Hodong Kim, *Holy War in China: The Muslim Rebellion and State in Chinese Central Asia, 1864-1877* (Stanford, CA: Stanford University Press, 2010).

30 Edward Wong, "Riots in Western China Amid Ethnic Tension," *The New York Times,* July 5, 2009, https://www.nytimes.com/2009/07/06/world/asia/06china.html.

31 "Is China fraying?," *The Economist,* July 9, 2009, https://www.economist.com/briefing/2009/07/09/is-china-fraying.

32 William Wan, "Chinese police say Tiananmen Square crash was 'premeditated, violent, terrorist attack'," *The Washington Post*, October 30, 2013, https://www.washingtonpost.com/world/asia_pacific/chinese-police-say-tiananmen-square-crash-was-premeditated-violent-terrorist-attack/2013/10/30/459e3e7e-4152-11e3-8b74-d89d714ca4dd_story.html?utm_term=.b8f8c1815a6a.

33 Michael Martina, "Chinese state media says five suicide bombers carried out Xinjiang attack," *Reuters*, May 22, 2014, https://www.reuters.com/article/us-china-blast/chinese-state-media-says-five-suicide-bombers-carried-out-xinjiang-attack-idUSBREA4L01K20140523.

34 "China charges four in Kunming attack, sentences 113 on terror crimes," *Reuters*, June 29, 2014, https://www.reuters.com/article/us-china-xinjiang/china-charges-four-in-kunming-attack-sentences-113-on-terror-crimes-idUSKBN0F507W20140630.

35 Charles Hutzler, "China's Police Ministry Orders Campaign Against Terrorism," *The Wall Street Journal,* May 25, 2014, https://www.wsj.com/articles/chinas-police-ministry-orders-campaign-against-terrorism-1401033223.

36 James T. Areddy, "Xinjiang Arrests Nearly Doubled in '14, Year of 'Strike-Hard' Campaign," *The Wall Street Journal,* January 23, 2015, https://blogs.wsj.com/chinarealtime/2015/01/23/xinjiang-arrests-nearly-doubled-in-14-year-of-strike-hard-campaign/.

37 Maya Wang, "'Eradicating Ideological Viruses': China's Campaign of Repression Against Xinjiang's Muslims," (New York: Human Rights Watch, September 9, 2018), https://www.hrw.org/report/2018/09/09/eradicating-ideological-viruses/chinas-campaign-repression-against-xinjiangs.

38 Lily Kuo, "China says UN criticism of human rights record is 'politically driven'," *The Guardian*, November 6, 2018, https://www.theguardian.com/world/2018/nov/06/china-un-criticism-human-rights-record.

39 "Timeline: Xinjiang unrest," *BBC News*, July 10, 2009, http://news.bbc.co.uk/2/hi/asia-pacific/8138866.stm.

40 Adrian Zenz and James Leibold, "Chen Quanguo: The Strongman Behind Beijing's Securitization Strategy in Tibet and Xinjiang," *The Jamestown Foundation China Brief* 17, no. 2 (September 21, 2017): 16-24, https://jamestown.org/program/chen-quanguo-the-strongman-behind-beijings-securitization-strategy-in-tibet-and-xinjiang/.

41 Benjamin Haas, "Chinese authorities collecting DNA from all residents of Xinjiang," *The Guardian*, December 12, 2017, https://www.theguardian.com/world/2017/dec/13/chinese-authorities-collecting-dna-residents-xinjiang.

42 Kieren McCarthy, "China crams spyware on phones in Muslim-majority province," *The Register*, July 24, 2017, https://www.theregister.co.uk/2017/07/24/china_installing_mobile_spyware/.

43 Edward Wong, "Western China Region Aims to Track People by Requiring Car Navigation," *The New York Times*, February 24, 2017, https://www.nytimes.com/2017/02/24/world/asia/china-xinjiang-gps-vehicles.html.

44 Stephen Chen, "China takes surveillance to new heights with flock of robotic Doves, but do they come in peace?," *South China Morning Post*, June 24, 2018, https://www.scmp.com/news/china/society/article/2152027/china-takes-surveillance-new-heights-flock-robotic-doves-do-they.

45 Megha Rajagopalan, "This Is What A 21st-Century Police State Really Looks Like," *BuzzFeed News*, October 17, 2017, https://www.buzzfeednews.com/article/meghara/the-police-state-of-the-future-is-already-here.

46 Maya Wang, "'Eradicating Ideological Viruses': China's Campaign of Repression Against Xinjiang's Muslims."

47 For more on this point, see Kai-Fu Li, *AI Superpowers: China, Silicon Valley, and the New World Order* (Boston: Houghton Mifflin Harcourt, 2018).

48 Whether Beijing *primarily* views technology as a vehicle for strategic gain is less straightforward, and relates to an ongoing debate over the extent to which China harbors aspirations for ideological expansion. For more, see Ryan Hass and Mira Rapp-Hooper, "Responsible competition and the future of U.S.-China relations," *The Brookings Institution*, February 6, 2019, https://www.brookings.edu/blog/order-from-chaos/2019/02/06/responsible-competition-and-the-future-of-u-s-china-relations/.

49 Andrew Chatzky and James McBride, "China's Massive Belt and Road Initiative," *Council on Foreign Relations*, May 21, 2019, https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative.

50 For more on the relationship between technology and BRI, see Daniel Kliman and Abigail Grace, "Power Play: Addressing China's Belt and Road Strategy," (Washington, DC: Center for a New American Security, September 20, 2018), 10-11, https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-Power-Play-Addressing-Chinas-Belt-and-Road-Strategy.pdf?mtime=20180920093003.

51 Stephen Feldstein, "The Road to Unfreedom: How Artificial Intelligence is Reshaping Repression," *Journal of Democracy* 30, no. 1 (January 2019): 40, https://www.journalofdemocracy.org/articles/the-road-to-digital-unfreedom-how-artificial-intelligence-is-reshaping-repression/.

52 "Ethiopia: Telecom Surveillance Chills Rights," *Human Rights Watch*, March 25, 2014, https://www.hrw.org/news/2014/03/25/ethiopia-telecom-surveillance-chills-rights.

53 Lynsey Chutel, "China is exporting facial recognition software to Africa, expanding its vast database," *Quartz*, May 25, 2018, https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-dominance-through-diversity/; Arthur Gwagwa, "Exporting Repression? China's Artificial Intelligence Push into Africa," *Council on Foreign Relations,* December 17, 2018, https://www.cfr.org/blog/exporting-repression-chinas-artificial-intelligence-push-africa.

54 Angus Berwick, "How ZTE helps Venezuela create China-style social control," *Reuters*, November 14, 2018, https://www.reuters.com/investigates/special-report/venezuela-zte/.

55 Paul Mozur, Jonah M. Kessel, and Melissa Chan, "Made in China, Exported to the World: The Surveillance State," *The New York Times*, April 24, 2019, https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html.

56 "Dubai rolls out 'Police without Policemen' initiative," *Gulf News*, March 12, 2018, https://gulfnews.com/uae/crime/dubai-rolls-out-police-without-policemen-initiative-1.2186841.

57 "UAE's Etisalat picks firms to develop AI, Blockchain solutions," *Arabian Business*, January 7, 2019, https://www.arabianbusiness.com/technology/410932-uaes-etisalat-picks-firms-to-develop-ai-blockchain-solutions.

58 Adrian Shahbaz, "Freedom on the Net 2018: The Rise of Digital Authoritarianism," (Washington, DC: Freedom House, 2018), https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism.

59 "Putin Signs 'Sovereign Internet' Law, Expanding Government Control of Internet," *Radio Free Europe/Radio Liberty*, May 1, 2019, https://www.rferl.org/a/putin-signs-sovereign-internet-law-expanding-government-control-of-internet/29915008.html.

60 "Путин подписал закон об изоляции Рунета" [Putin signed the law on the isolation of Runet], *Meduza Project*, May 1, 2019, https://meduza.io/news/2019/05/01/putin-podpisal-zakon-ob-izolyatsii-runeta.

61 Robert Morgus and Justin Sherman, "Is the Russian Internet a Lost Cause?," *Slate*, March 28, 2019, https://slate.com/technology/2019/03/russian-internet-runet-fragmentation-isolation.html.

62 Robert Morgus identifies four characteristics of Russian digital authoritarianism that distinguish it from the Chinese model: 1) Surveillance of internet traffic by the SORM system (and the opportunity for intimidation that FSB data access provides); 2) repressive legal structure that requires ISPs to install SORM black boxes without control over the information being collected; 3) intimidation and state capture of ISPs and other firms; 4) information manipulation (rather than content filtration). Robert Morgus, "The Spread of Russia's Digital Authoritarianism," in *AI, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives*, ed. Nicholas D. Wright, (Washington, DC: United States Department of Defense, 2018), 86.

63 On authoritarian diffusion of internet controls, see Jaclyn A. Kerr, "Information, Security, and Authoritarian Stability: Internet Policy Diffusion and Coordination in the Former Soviet Region," *International Journal of Communication* 12, (2018): 3,814–3,834, https://ijoc.org/index.php/ijoc/article/view/8542/2460.

64 Robert Morgus, "The Spread of Russia's Digital Authoritarianism," 85-86.

65 Andrei 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.

66 Robert Morgus, "The Spread of Russia's Digital Authoritarianism."

67 Andrei Soldatov and Irina Borogan, *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries* (New York: PublicAffairs, 2015), p.68

68 "Freedom on the Net 2018: Russia," (Washington, DC: Freedom House, 2018), https://freedomhouse.org/report/freedom-net/2018/russia.

69 "ФЕДЕРАЛЬНЫЙ ЗАКОН О внесении изменений в Федеральный закон «О связи»" [Federal Law "On the changes to the Federal Law 'On networks '"], (Moscow: Ministry of Economic Development of Russian Federation, October 11, 2016), http://regulation.gov.ru/projects#npa=58851. Also see: Juha Kukkola, Mari Ristolainen, Juha-Pekka Nikkarila, "Game Changer: Structural transformation of cyberspace," (Helsinki, Finnish Defence Research Agency, 2017), https://puolustusvoimat.fi/documents/1951253/2815786/PVTUTKL+julkaisuja+10.pdf/5d341704-816e-47be-b36d-cb1a0ccae398.

70 User's identifier; date and time of registration; date, time, and number of agreement (if any); nickname; date of birth; address; given name;, father's name and surname; passport details; identifiers of other personal documents; user's languages; details about relatives; information about accounts in other internet services; date and time of latest update of registration details; date and time of termination of user's registration; information about receiving, sending, and processing text messages; draft messages, images, sounds, other messages; addressees' details; monetary transactions, including details of payees, payment system, amounts, currency, paid goods (services), client software used; and geolocation data. For a brief description see (full report no longer available online) "Russia under surveillance 2017: How the Russian state is setting up a system of total control over its citizens," (Moscow: Agora International Human Rights Group, 2017), http://en.agora.legal/articles/Report-of-Agora-International-%E2%80%98Russia-under-surveillance-2017%E2%80%99/6.

71 "Russia under surveillance 2017: How the Russian state is setting up a system of total control over its citizens."

72 Andrei Zakharov and Svetlana Reiter, "Роскомнадзор внедрит новую технологию блокировок Telegram за 20 млрд рублей" [Roskomnadzor will establish a new technology for blocking Telegram for 20 billion rubles], *BBC News*, December 18, 2018, https://www.bbc.com/russian/features-46596673.

73 "Russia under surveillance 2017: How the Russian state is setting up a system of total control over its citizens."

74 "Russia Tests Facial Recognition Cameras in Moscow Ahead of World Cup," *Moscow Times*, April 18, 2018, https://www.themoscowtimes.com/2018/04/18/russia-tests-facial-recognition-cameras-moscow-ahead-world-cup-a61201.

75 Victoria Ryabikova, "Are you safe from Big Brother's prying eye in Moscow?" *Russia Beyond*, July 22, 2019. https://www.rbth.com/science-and-tech/330697-how-real-big-brother-operates-in-moscow.

76 Adrian Shahbaz, "Freedom on the Net 2018: The Rise of Digital Authoritarianism."

77 "Россияне запустили бумажные самолетики в поддержку свободного интернета. И пообещали убрать за собой" [The Russians launched paper airplanes in support of the free Internet. And they promised to clean up after themselves], *Meduza Project*, April 22, 2018, https://meduza.io/shapito/2018/04/22/rossiyane-zapustili-bumazhnye-samoletiki-v-podderzhku-svobodnogo-interneta-i-poobeschali-ubrat-za-soboy.

78 "Школьники на «Открытом уроке» рассказали Владимиру Путину о своих проектах. Он всем ответил одно и то же" [Schoolchildren at the 'Open lesson' told Vladimir Putin about their projects. He answered the same to everyone], *Meduza Project*, September 1, 2017, https://meduza.io/feature/2017/09/01/shkolniki-na-otkrytom-uroke-rasskazali-vladimiru-putinu-o-svoih-proektah-on-vsem-otvetil-odno-i-to-zhe.

79 Samuel Bendett, "In AI, Russia Is Hustling to Catch Up," *Defense One,* April 4, 2018, https://www.defenseone.com/ideas/2018/04/russia-races-forward-ai-development/147178/.

80 "Factsheet on Artificial Intelligence (AI) in Russia," (The Hague: Netherlands Worldwide, 2018), https://www.netherlandsworldwide.nl/documents/publications/2018/11/09/artificial-intelligence-in-russia.

81 Svetlana Yastrebova, Pavel Kantyshev, Alena Sukharevskaya, and Svetlana Bocharova, "Иностранные инвесторы дали РФПИ $2 млрд на искусственный интеллект" [Foreign investors gave RDIF $2 billion for artificial intelligence], *Vedemosti*, May 30, 2019, https://www.vedomosti.ru/technology/articles/2019/05/29/802828-inostrannie-investori.

82 Cade Metz, "As China Marches Forward on A.I., the White House Is Silent," *The New York Times*, February 12, 2018, https://www.nytimes.com/2018/02/12/technology/china-trump-artificial-intelligence.html.

83 See Samuel Bendett, "The Development of Artificial Intelligence in Russia," in *AI, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives*, ed. Nicholas D. Wright (Washington, DC: United States Department of Defense, 2018).

84 " Ministry of Defense of the Russian Federation, "Conference 'Artificial Intelligence: Problems and Solutions' – 2018,'" http://mil.ru/conferences/is-intellekt.htm.

85 "AI Conference," AI Conference, https://aiconference.ru/ru. The only proof that the conference took place is on Facebook ("AI Conference," Facebook, https://www.facebook.com/AIConference.ru/), LinkedIn ("AI Conference MSK," https://www.linkedin.com/showcase/ai-conference-msk/; and Instagram ("ai.conference," https://www.instagram.com/ai.conference/).

86 Samuel Bendett, "Putin Orders Up a National AI Strategy," *Defense One,* January 31, 2019, https://www.defenseone.com/technology/2019/01/putin-orders-national-ai-strategy/154555/.

87 At the time of writing, the strategy was not yet publically available; "Перечень поручений по итогам заседания наблюдательного совета Агентства стратегических инициатив" [The list of instructions following the meeting of the supervisory board of the Agency for Strategic Initiatives], Office of the President of Russia, January 30, 2019, http://kremlin.ru/acts/assignments/orders/59758.

88 "Совещание по вопросам развития технологий в области искусственного интеллекта" [Meeting on questions related to development of artificial intelligence], Office of the President of Russia, May 30, 2019, http://kremlin.ru/events/president/news/60630.

89 Samuel Bendett, "Putin Drops Hints about Upcoming National AI Strategy," *Defense One*, May 30, 2019, https://www.defenseone.com/ideas/2019/05/putin-drops-hints-about-upcoming-national-ai-strategy/157365/.

90 "'Digital Economy' Program Implementation," Analytical Center for the Government of the Federation of Russia, http://ac.gov.ru/en/projects/014097.html. For the original resolution see "Цифровая экономика Российской Федерации" [Digital Economy of the Russian Federation], (Moscow: Government of the Russian Federation, July 28, 2017), http://ac.gov.ru/files/content/14091/1632-r-pdf.pdf.

91 Vladimir Ovchinsky and Alexey Binetsky, "Судья с искусственным интеллектом" [AI Judge], *Zavtra*, February 13, 2019, http://zavtra.ru/blogs/sud_ya_s_iskusstvennim_intellektom.

92 "Overview of the Package of Changes into a Number of Laws of the Russian Federation Designed to Provide for Additional Measures to Counteract Terrorism," (Washington, DC: The International Center for Not-for-Profit Law, July 21, 2016), http://www.icnl.org/research/library/files/Russia/Yarovaya.pdf.

93 "Amendments to the law on information and the law on the media," Office of the President of Russia, November 25, 2017, http://en.kremlin.ru/acts/news/56179.

94 Alina Polyakova, "The Kremlin's Latest Crackdown on Independent Media: Russia's New Foreign Agent Law in Context," *Foreign Affairs*, December 5, 2017, https://www.foreignaffairs.com/articles/russia-fsu/2017-12-05/kremlins-latest-crackdown-independent-media.

95 Andrei Soldatov, "Bold steps on the Internet: Kremlin's capability to cut off Russia," *Raam op Rusland*, February 11, 2019, https://www.raamoprusland.nl/dossiers/media/1202-bold-steps-on-internet-kremlin-s-capability-to-cut-off-russia.

96 As of 2018, Roskomnadzor has already been testing how to prohibit passage of internet traffic, in conjunction with deep packet inspection (DPI) testing by the FSB: "Роскомнадзор тестирует новую технологию блокировки в интернете. Как она работает?" [Roskomnadzor is testing a new technology to block the internet. How does it work?], *BBC News*, August 31, 2018, https://www.bbc.com/russian/features-45368220.

97 In May 2019 the Ministry of Justice specified that times of crisis would occur after three types of threats: 1) to the "integrity" or connectivity of the network; 2) an attack or natural disaster jeopardizing the resilience of certain infrastructure; and 3) a threat to network security in the form of a hack. Matthew Luxmoore, "Russia Clarifies Threats That Would Lead It To Decouple RuNet From World Wide Web," *Radio Free Europe/Radio Liberty*, May 24, 2019, https://www.rferl.org/a/wholeness-resilience-security-russia-clarifies-threats-to-sovereign-internet-/29961306.html.

98 "Суверенный рунет: как он будет работать и чем это грозит пользователям" [Sovereign Runet: how it will work and how it threatens users], *The Bell*, December 19, 2018, https://thebell.io/suverennyj-runet-kak-on-budet-rabotat-i-chem-eto-grozit-polzovatelyam/.

99 ""Великий российский файрвол": что это такое и как будет работать" ['Great Russian firewall': what it is and how it will work], *BBC News*, December 14, 2018, https://www.bbc.com/russian/news-46566886.

100 Kirill Bulanov, "Путин подписал закон о «суверенном рунете»" [Putin signed the law on 'sovereign runet'] *Vedomosti*, May 1, 2019, https://www.vedomosti.ru/technology/articles/2019/05/01/800649-suverennom-runete.

101 Victor Khamraev, "В России настали цифровые времена" [Digital times have come to Russia], *Kommersant*, April 29, 2019, https://www.kommersant.ru/doc/3960049.

102 "Freedom on the Net 2018: Kazakhstan," (Washington, DC: Freedom House, 2018), https://freedomhouse.org/report/freedom-net/2018/kazakhstan.

103 "Freedom on the Net 2018: Belarus," (Washington, DC: Freedom House, 2018), https://freedomhouse.org/report/freedom-net/2018/belarus.

104 "Freedom on the Net 2018: Kyrgyzstan," (Washington, DC: Freedom House, 2018), https://freedomhouse.org/report/freedom-net/2018/kyrgyzstan.

105 Robert Morgus, "The Spread of Russia's Digital Authoritarianism."

106 Robert Morgus, "The Spread of Russia's Digital Authoritarianism," 89.

ABOUT THE AUTHORS

Alina Polyakova is the founding director of the Project on Global Democracy and Emerging Technology and a fellow in the Center on the United States and Europe at the Brookings Institution, where she leads the Foreign Policy program's Democracy Working Group. She is also adjunct professor of European studies at the Paul H. Nitze School of Advanced International Studies (SAIS) at Johns Hopkins University. Polyakova's writing and research is regularly featured in major outlets, such as the *The New York Times*, *Foreign Affairs*, and *Washington Post*, among others. Her book, *The Dark Side of European Integration*, examines the rise of far-right political parties in Europe. Prior to joining Brookings, Polyakova served as director of research and senior fellow for Europe and Eurasia at the Atlantic Council. Polyakova holds a doctorate from the University of California, Berkeley.

Chris Meserole is a fellow in Foreign Policy at the Brookings Institution and an expert on artificial intelligence, emerging technology, and international security. His current research is focused on developing democratic models of digital governance that can respond to the emerging threats of digital authoritarianism and online extremism. Meserole regularly briefs technology leaders and government officials in the United States and Europe, and his research has appeared or been featured in numerous publications, such as the *New Yorker*, *Time*, *Newsweek*, *Foreign Affairs*, and *Foreign Policy*.