

# Digital Authoritarianism and Implications for US National Security

---

Justin Sherman

## ABSTRACT

**D**igital authoritarianism, or the use of digital technologies to enhance or enable authoritarian governance, has received much attention due to its implications for human rights and global democracy. Yet, often overlooked are the implications of digital authoritarianism for US national security. This article explores the ways in which digital authoritarianism exposes US national security to risk on three fronts: consolidation of power in authoritarian regimes; increased incentives for authoritarians to promote diffusion of surveillance technologies; and potential insulation against foreign cyber attacks and lowered disincentives for authoritarians to conduct destabilizing cyber operations on the global Internet.

The US national security community increasingly is observing a phenomenon that for years has captured the interest of select academics, policy wonks, and human rights activists: “digital authoritarianism,” where undemocratic regimes routinely use digital tools to enhance or enable authoritarian governing practices.<sup>[1]</sup> While definitions of digital authoritarianism are sparse<sup>[2]</sup>—and terminology remains disputed<sup>[3]</sup>—used here it refers to such practices as pervasive Internet surveillance and the exercise of tight control over online information flows within a country’s borders. The Chinese and Russian governments have been the leading recipients of this “digital authoritarian” label, as they build out variously undemocratic practices, such as online censorship, using digital technologies.

Digital authoritarianism obviously impacts democracy and human rights. Controlling information flows within a country’s borders, for instance, can quite effectively enable a government to crack down on anti-regime speech, or suppress the online organization of political dissidents. Perhaps less intuitively, the impacts of digital authoritarianism extend beyond human rights and democracy, to include the global economy and US national security. This article focuses on the last of these categories of implications—analyzing why



**Justin Sherman** is a nonresident fellow at the Atlantic Council's Cyber Statecraft Initiative, a research fellow at the Tech, Law & Security Program at American University Washington College of Law, and a contributor at *WIRED* Magazine. He was previously a cybersecurity policy fellow at New America and a fellow at Duke Law School's Center on Law & Technology.

digital authoritarianism goes beyond human rights and democracy implications (which, normatively speaking, is already reason for concern), and can also undermine US national security and change the landscape of military and intelligence cyberspace operations.

First, digital authoritarianism allows authoritarian regimes to consolidate power—many of which already pose national security risks to the US, such as through malicious cyber activity and nuclear weapons. Second, digital authoritarianism may encourage certain technologically sophisticated governments, such as in China and Russia, to further encourage the global diffusion of tools and knowledge for digital surveillance. Third, digital authoritarianism, in the form of Internet isolation, could potentially insulate certain countries from foreign cyber attacks, thereby degrading disincentives to those that might create digital chaos on the global Internet. These main risks are addressed below.

## 1. AUTHORITARIANS CONSOLIDATING POWER

Digital authoritarianism, at its core, is a mechanism for exerting increased, unchecked control over one's population through digital technologies. Censorship, device hacking, and mass surveillance are all on the table. In this way, digital authoritarianism facilitates power consolidation—ensuring that challenges to a regime are outed in advance or quickly observed as they arise, and suppressed. This exposes US national security to risk.

In a world where citizen revolt tops the list of authoritarian fears, digital authoritarianism promises a set of solutions: Internet Protocol (IP) address lists used to block foreign online content; traffic header inspection to monitor online activity; legal control of Internet Service Providers (ISPs) whenever the government wants to shut down Internet services; and more. Sometimes, this is quite explicit. The Russian government, for instance, strongly promotes information control in domestic cyberspace for this reason.<sup>[4]</sup>

Other times, the suggestion is more subtle, for example when countries cite fake news and online disinformation as reasons to censor content deemed politically undesirable by those in power.<sup>[5]</sup>

In either case, authoritarian fears of protest and revolt have long driven such regimes to monitor their citizens. The difference today, however, is that digital technologies, like Internet packet inspection software and artificial intelligence (AI) facial recognition, are increasingly making it cheaper for dictators to do so. These technologies also make surveillance more scalable. They also reduce some of the risks caused by relying on massive networks of human spies and informants.<sup>[6]</sup> Steven Feldstein points out, for example, that the principal-agent problem, where, by empowering agents to spy and suppress, regimes empower them to act against the government, is a vulnerability that can be reduced by substituting automated surveillance technologies for human beings.<sup>[7]</sup> In turn, these technologies can heighten the speed, scale, and accuracy of authoritarian surveillance.

All of this matters for US national security because promoting democracy and contesting authoritarianism is in the US national interest—and digital authoritarianism helps authoritarian regimes consolidate power. Despite the sometimes resilient nature of online social movements, quashing political organization can be easier than ever before if aided by comprehensive digital surveillance and control technologies.<sup>[8]</sup> Governments can black out communications, such as Internet servers or mobile cell towers, during revolt. They can censor troubling posts before they bubble into something bigger. They can also censor foreign-originated information that could challenge regime narratives. Most importantly, they can continuously monitor their population, including during relatively stable times, to anticipate movements that could undermine government power. In the wake of a series of revolts in the Middle East that were informed, influenced, and/or aided in part by social media and the melding of online and offline mobilization, digital authoritarians, and those striving for such ends, are using digital technologies, often dual-use, to safeguard against such threats.<sup>[9]</sup> As the Russian General Valery Gerasimov offered in 2013, “The information space opens wide asymmetrical possibilities for reducing the fighting potential of the enemy,” making it “necessary to perfect activities in the information space, including the defense of our own objects [objectives].”<sup>[10]</sup>

Many of these governments like China, Russia, and Iran, are unaligned with the US on security issues. In the cyber domain, they might engage in everything from pervasive trade secret theft to cyber attacks on foreign countries’ electrical grids. In more traditional ways, they also pose national security risks through such vectors as nuclear weapons, military buildup, territorial aggression against US allies and partners, and disrupting the international order.<sup>[11]</sup> While US bilateral relationships are complex, often interconnected, and never zero-sum, elements of those relationships already pose national security risks.

Likewise, other countries pursuing digital authoritarian practices may be hostile to US interests (and democratic interests more broadly) or be aligned with other powers that threaten

national security. Power consolidation by these regimes poses national security risks in various dimensions. In some cases, the export and diffusion of digital surveillance tools, as part of digital authoritarianism, also pose additional national security risks, the point of focus in the next section.

## 2. INCENTIVES FOR AUTHORITARIANS TO ENCOURAGE DIFFUSION OF SURVEILLANCE CAPABILITIES

Private firms worldwide legally or illegally have long been selling dual-use digital technologies that can be used to monitor web traffic and to censor information. That there is a global market for digital surveillance tools is old news.

Companies incorporated in democracies heavily export these dual-use technologies worldwide, including, in many documented cases, to despots.<sup>[12]</sup> Likewise, companies incorporated in autocracies sell dual-use technologies, including those that can be used for censorship and surveillance, to other authoritarian regimes.<sup>[13]</sup> Some studies suggest that democracies account for a far greater volume of surveillance technology exports, including to despots, despite attempts to restrict such exports.<sup>[14]</sup>

The pursuit of digital authoritarianism to bolster state power magnifies incentives for some countries to acquire dual-use surveillance tools, and for others to encourage their spread. China's state leadership, for instance, consistently has advocated a sovereign and controlled Internet governance model on the global stage, with practices like censorship and surveillance, as opposed to a global and open model supported by many liberal democracies.<sup>[15]</sup>

In tandem with this global diplomatic messaging, the Chinese government has reportedly conducted trainings on new media or information management with representatives from dozens of countries, many on record as pursuing restrictive online practices.<sup>[16]</sup> This has coincided with countries targeted by the Belt and Road Initiative passing cybersecurity laws that sometimes mirror laws already enacted in China, such as Vietnam's recent establishment of data localization requirements.<sup>[17]</sup> Causality remains unclear in this situation, and empirical questions remain to be answered about the underlying drivers of digital authoritarianism in different countries. Nonetheless, these patterns and events, coupled with exports of surveillance technologies from China, raise questions about Beijing's intentions to spread digital authoritarianism globally, including through a greater focus on, and/or endorsement of, the sale of digital surveillance and control capabilities.

This could amplify the aforementioned national security risks, should authoritarian countries acquire the tools and/or knowledge needed to bolster their power through digital surveillance. National security analysts have already flagged these potential risks across Africa. Many countries China has engaged with through its Belt and Road investments have acquired Chinese surveillance technology, potentially usable for oppressive purposes. For instance, Chinese

company exports of surveillance technology to the Ethiopian government have occurred alongside Chinese government investments.<sup>[18]</sup> Given China's history of spying on and suppressing political dissidents, this is hardly a benign fact, and Ethiopia is but one of several examples. Should China's leadership be intent on spreading digital authoritarianism worldwide, to include diffusion of surveillance tools, this likely could include countries aligned with China's national security and/or economic interests.

Like China, Russia has long advocated for cyber sovereignty on the international stage,<sup>[19]</sup> with President Vladimir Putin repeatedly emphasizing the importance of information control within a country's sovereign borders.<sup>[20]</sup> As noted above, Russian companies export surveillance and hacking technologies, especially to post-Soviet states.<sup>[21]</sup> Andrei Soldatov and Irina Borogan actually suggest that Russian surveillance technology exports to some of these countries are a better fit than Western-made surveillance applications, because Russian laws and procedures governing traffic interception are more compatible for these countries, and the technologies are tailored accordingly.<sup>[22]</sup> In either case, these surveillance technology exports need further study, and they clearly serve as tools of political influence in Russia's near-abroad.

As with China, the extent of the Russian government's direct involvement in and support of such exports needs further study, because the Kremlin's direct hand in these exports, while visible, is hardly transparent. The desire to spread digital authoritarianism may well incentivize the Kremlin to better spread its surveillance technologies, or to at least look the other way when they occur, and thereby consolidate power in the hands of Russian-aligned countries at the expense of US government interests. This also could threaten vulnerable democracies worldwide, and facilitate the so-called fracturing of the global Internet, as countries build out technical and legal regimes that filter the global and open Internet touching and running through their borders.<sup>[23]</sup>

Again, the threat here is not only from governments in China and Russia. Companies incorporated in democracies also sell a high volume of dual-use surveillance technologies to despots, and this is something we are better able to monitor and correct. It is also important to reemphasize the existing incentives for countries to encourage or allow the spread of these capabilities to other countries (including the technologies and how to optimize them). But growing desires to spread digital authoritarianism globally not only undermine human rights and developing democracies; this also exposes US national security to increased risk.

### **3. INSULATION FROM FOREIGN CYBER ATTACKS AND LOWERED DISINCENTIVES TO DISRUPT GLOBAL INTERNET**

Growing digital authoritarianism is manifested in more countries cracking down on Internet freedom within their borders, as they develop or acquire technical mechanisms to spy on and censor online information. This aspect of broader state control of the Internet has been

referred to as “cyber sovereignty.”<sup>[24]</sup> Some countries have begun to alter cyberspace itself—for instance, how traffic flows from A to B, or what kinds of traffic can flow in the first place. This evolving global Internet landscape obviously impacts national cybersecurity and military cyber operations, by, among other ways, insulating certain actors from vulnerabilities, shifting the landscape of Internet connectivity in foreign countries, and potentially degrading foreign actors’ effective disincentives to hack others.

Russia recently pressed to establish a domestic Russian Internet—an objective Kremlin officials have discussed for years. This was spurred in part, according to supporters, by an “aggressive” 2018 US cybersecurity strategy, referring to the White House’s new cyber strategy published in the fall of 2018.<sup>[25]</sup>

There are undoubtedly other motivations for a domestic internet; in particular, the Kremlin leadership has sought more than ever, over the past few years, to control online traffic flows into, out of, and within Russia’s borders.<sup>[26]</sup> Absent the scaled and sophisticated censorship infrastructure of its Chinese counterparts, isolating the Internet may be an easier Internet control solution for Russian leadership. Together, though, these motivations for Internet control and defense against foreign cyber threats have fueled the Kremlin’s pursuit of a domestic internet that can be cut off from the rest of the world and still function under state management.

Russia’s plans for isolating its Internet include granting the country’s Internet regulator enhanced control over key “traffic exchange points,” and allowing that same regulator to centralize the management of the Russian Internet in cases where its “integrity, stability, and security” appear at risk. These plans also include building a national Domain Name System (DNS) for Russia, thereby centralizing management and control of Internet traffic routing into and out of Russian territory.<sup>[27]</sup> Clearly, this is no easy lift; political and technical challenges remain for implementation.<sup>[28]</sup> In part, this may explain why a purportedly planned “disconnection test” of the Russian Internet<sup>[29]</sup> has yet to go forward. Yet, should this plan for a domestic Internet ultimately even partly succeed (e.g., the state consolidates more control over traffic routing, or Internet companies in Russia fall even more directly under Kremlin control), it is possible that Russia could better insulate itself from foreign cyber activity, both malicious and benign.

Enhanced control over Internet infrastructure and traffic flow and domination of the Internet within a country to reduce vulnerability to foreign cyber attacks has a potentially troublesome side effect, and that could be to reduce the Russian government’s disincentives to attack or manipulate the more open Internet systems of others.

On the first point, vulnerability, US vulnerability to cybercrime, nation-state computer network operations, and other undesirable or malicious cyber behavior stems not only from issues like poor device security-by-design, but also from our relatively open Internet connectivity. The open connectedness of the US to the global Internet means myriad paths into US-based devices, networks, and infrastructure exist, and also, that operations targeting internet routing protocols can have a greater adverse impact on the US. For instance, manipulations of the Border



Gateway Protocol, which routes global Internet traffic, already have caused notable volumes of US Internet traffic to be unexpectedly routed through other countries, including China.<sup>[30]</sup> This could have serious economic and national security implications depending on the attack scenario.

Apart from other reduced vulnerabilities, if a country like Russia is far less dependent upon global Internet routing protocols, because it has built out its own DNS—that country may also be less susceptible to attacks that target protocols on the global side. As cyberspace within certain borders changes, other countries may have to alter exactly how cyber operations relating to that country must be conducted. This obviously impacts US military and Intelligence Community cyberspace operations, and that of our allies and partners, in ways often more drastic than mere routine additions, disconnections, updates, and relocations of devices and systems on the target country Internet. (Note: This need not be a negatively impactful change; centralizing management of the DNS within Russia, for instance, could actually make that country more vulnerable to Internet hijackings should a foreign country or criminal entity desire it.<sup>[31]</sup>)


On the second point, disruption of incentives, the Kremlin already views its domestic internet plans in the context of decreased reliance on the global Internet, which President Putin casts as a CIA project,<sup>[32]</sup> and which the Kremlin continually tries to prove untrustworthy to justify its ever tightening Internet control.<sup>[33]</sup> The Russian government, which professes to be a victim of US cyber aggression, itself is a major destabilizing actor in cyberspace: conducting extensive online influence operations, from Ukraine to Turkey to Germany to the US;<sup>[34]</sup> launching large-scale global attacks like the NotPetya ransomware that caused billions of dollars in damage to the global economy;<sup>[35]</sup> and hacking and turning off the power grid in Ukraine.<sup>[36]</sup> Clearly, strong incentives drive the Kremlin to order, support, and allow cyber and information operations that use the Internet for destabilizing purposes abroad.

If Russia becomes increasingly less reliant on global networks, and hence perceives itself less vulnerable to foreign cyber-attacks, whether or not that perception is reality, this could reduce the disincentives for the Russian government to conduct even more destabilizing cyber operations.<sup>[37]</sup> Manipulating the Internet protocols of others, for instance, may present a more compelling option to sow chaos abroad and to undermine trust in the global Internet if the Kremlin feels insulated from retaliation in kind. Hence, growing digital authoritarianism on the Internet in the form of web isolation, therefore stands to impact global cybersecurity and US national security not only in how it changes the nature of the domain, but also the perceived consequences and incentives at play for state actors.

## CONCLUSION

If and as other countries move in a direction similar to Russia—such as Iran, which continues to pursue its goal of a completely domestic Iranian Internet<sup>[38]</sup>—digital authoritarianism increasingly will implicate the layout and behavior of cyberspace itself. This also may diminish

disincentives against malicious cyber behavior, and change how cyber operations are conducted against such actors. Despite a concerted US focus on norm-development in cyberspace, the tracking and management of these changes to the layout and behavior of cyberspace (for example, which cables are cut, and how are protocols designed and redesigned?) are equally, if not more, important to encouraging reduced offensive cyber behavior by bad faith actors.

The risks that digital authoritarianism will bolster the power of authoritarian states, encourage the diffusion of dual-use surveillance and computer penetration technologies, insulate some regimes from foreign cyber-attacks, and degrade disincentives for certain regimes to engage in offensive cyber operations all impact US national security. Digital authoritarianism also obviously has serious implications for human rights and global democracy. This, normatively speaking, is more than reason enough for top leadership in the US to devote serious attention and resources to the issue. But the US military, including the entire national security establishment, increasingly will also find itself impacted by the worldwide spread of digital authoritarianism around the world, and should be proactively focused on this threat now. 



## NOTES

1. The author would like to thank Robert Morgus and Deb Crawford for their comments on an earlier draft of this article.
2. I first offered this general definition in Justin Sherman, “India’s Digital Path: Leaning Democratic or Authoritarian?” *Just Security*, February 4, 2019, <https://www.justsecurity.org/62464/indias-digital-path-leaning-democratic-authoritarian/>. Other prominent uses of this phrase can be found in Freedom House, “Freedom on the Net 2018,” October 2018, <https://freedomhouse.org/report/freedom-net/freedom-net-2018>; and Nicholas Wright, “How Artificial Intelligence Will Reshape the Global Order,” *Foreign Affairs*, July 10, 2018, <https://www.foreignaffairs.com/articles/world/2018-07-10/how-artificial-intelligence-will-reshape-global-order>.
3. For instance, there is a consideration that the “authoritarianism” element of “digital authoritarianism” is an imprecise way to characterize digitally undemocratic or digitally illiberal practices that may be spread across, and occur differently in, various regime types that are not necessarily, by a very academic definition, “authoritarian.”
4. Justin Sherman, “Russia’s Tightening Control of Cyberspace Within Its Borders,” *Just Security*, December 24, 2018, <https://www.justsecurity.org/62023/russias-tightening-control-cyberspace-borders/>.
5. Freedom House, “Freedom on the Net 2018,” October 2018, <https://freedomhouse.org/report/freedom-net/freedom-net-2018>.
6. Justin Sherman, “Digital authoritarianism and the threat to global democracy,” *Bulletin of the Atomic Scientists*, July 25, 2019, <https://thebulletin.org/2019/07/digital-authoritarianism-and-the-threat-to-global-democracy/>.
7. Steven Feldstein, “The Road to Digital Unfreedom: How Artificial Intelligence is Reshaping Repression,” *Journal of Democracy*, Vol. 30, Issue 1 (Jan., 2019), 40-52.
8. Zeynep Tufekci, *Twitter and Teargas: The Power and Fragility of Networked Protest*, Yale University Press: New Haven, CT (2017).
9. Ibid.
10. Valery Gerasimov, “The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations,” *Military Review*, January-February 2016, [https://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview\\_20160228\\_art008.pdf](https://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art008.pdf) 27. Translated from Russian into English by Robert Coalson on June 21, 2014, from *Military-Industrial Kurier*, February 27, 2013.
11. Several of these points on more “traditional” threat vectors are pulled from Amy Zegart, “The President’s National Security In-Box,” Stanford University, October 11, 2016, <https://medium.com/@election2016stanford/the-presidents-national-security-inbox-cl220944acf5>.
12. Robert Morgus and Justin Sherman, “How U.S. surveillance technology is propping up authoritarian regimes,” *The Washington Post*, January 17, 2019, <https://www.washingtonpost.com/outlook/2019/01/17/how-us-surveillance-technology-is-propping-up-authoritarian-regimes/>.
13. Among many other news stories and analyses about companies incorporated in the likes of China and Russia exporting dual-use surveillance and digital control technologies, see Daniel Benaim and Hollie Russon Gilman, “China’s Aggressive Surveillance Technology Will Spread Beyond Its Borders,” *Slate*, August 9, 2018, <https://slate.com/technology/2018/08/chinas-export-of-cutting-edge-surveillance-and-facial-recognition-technology-will-empower-authoritarians-worldwide.html>; and Samuel Woodhams, “How China Exports Repression to Africa,” *The Diplomat*, February 23, 2019, <https://thediplomat.com/2019/02/how-china-exports-repression-to-africa/>.
14. Privacy International, “The Global Surveillance Industry,” Privacy International, July 2016, [https://www.privacyinternational.org/sites/default/files/2017-12/global\\_surveillance\\_0.pdf](https://www.privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf), cited in Steven Feldstein, “Can a U.N. Report Help Rein in Expansive and Abusive Digital Surveillance?” *World Politics Review*, July 9, 2019, <https://www.worldpoliticsreview.com/articles/28016/can-a-u-n-report-help-rein-in-expansive-and-abusive-digital-surveillance>.
15. Robert Morgus, Jocelyn Woolbright, and Justin Sherman, “The Digital Deciders: How a group of often overlooked countries could hold the keys to the future of the global internet,” *New America*, October 23, 2018, <https://www.newamerica.org/cybersecurity-initiative/reports/digital-deciders/>.
16. Freedom House, “Freedom on the Net 2018,” Freedom House, October 2018, [https://freedomhouse.org/sites/default/files/FOTN\\_2018\\_Final%20Booklet\\_11\\_1\\_2018.pdf](https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf), 8.
17. Ibid.

## NOTES

18. Human Rights Watch, “Ethiopia: Telecom Surveillance Chills Rights,” March 25, 2014, <https://www.hrw.org/news/2014/03/25/ethiopia-telecom-surveillance-chills-rights>; Xinhua, “Upcoming Belt and Road forum to inject new momentum to Ethiopia infrastructure dev’t drive,” *Xinhua*, April 19, 2019, [http://www.xinhuanet.com/english/2019-04/19/c\\_137988653.htm](http://www.xinhuanet.com/english/2019-04/19/c_137988653.htm); and Amy Hawkins, “Beijing’s Big Brother Needs African Faces,” *Foreign Policy*, July 24, 2018, <https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/>.
19. Robert Morgus, Jocelyn Woolbright, and Justin Sherman, “The Digital Deciders: How a group of often overlooked countries could hold the keys to the future of the global internet,” *New America*, October 23, 2018, <https://www.newamerica.org/cybersecurity-initiative/reports/digital-deciders/>.
20. This extends far beyond just the Internet, although that is the focus here. For instance, see Jill Dougherty, “How the Media Became One of Putin’s Most Powerful Weapons,” *The Atlantic*, April 21, 2015, <https://www.theatlantic.com/international/archive/2015/04/how-the-media-became-putins-most-powerful-weapon/391062/>. Also see later footnotes for sources on “information security” in Russia.
21. Peter Bourgelais, “Commonwealth of Surveillance States: On the Export and Resale of Russian Surveillance Technology to Post-Soviet Central Asia,” *Access Now*, 2013, [https://www.accessnow.org/cms/assets/uploads/archive/docs/Commonwealth\\_of\\_Surveillance\\_States\\_ENG\\_1.pdf](https://www.accessnow.org/cms/assets/uploads/archive/docs/Commonwealth_of_Surveillance_States_ENG_1.pdf).
22. Andrei Soldatov and Irina Borogan, “In Ex-Soviet States, Russian Spy Tech Still Watches You,” *Wired*, December 21, 2012, <https://www.wired.com/2012/12/russias-hand/>.
23. Justin Sherman and Robert Morgus, “Authoritarians Are Exporting Surveillance Tech, and With It Their Vision for the Internet,” *Council on Foreign Relations*, December 5, 2018, <https://www.cfr.org/blog/authoritarians-are-exporting-surveillance-tech-and-it-their-vision-internet>.
24. For instance, see a discussion of cyber sovereignty by a member of the Cyberspace Administration of China: Lu Wei, “Cyber Sovereignty Must Rule Global Internet,” *The Huffington Post*, February 14, 2015, [https://www.huffpost.com/entry/china-cyber-sovereignty\\_b\\_6324060](https://www.huffpost.com/entry/china-cyber-sovereignty_b_6324060).
25. Robert Morgus and Justin Sherman, “Analysis: Russia’s Plans for a National Internet,” *New America*, February 19, 2019, <https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/russias-plans-for-a-national-internet/>.
26. Justin Sherman, “Russia’s Tightening Control of Cyberspace Within Its Borders,” *Just Security*, December 24, 2018, <https://www.justsecurity.org/62023/russias-tightening-control-cyberspace-borders/>.
27. Robert Morgus and Justin Sherman, “Analysis: Russia’s Plans for a National Internet,” *New America*, February 19, 2019, <https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/russias-plans-for-a-national-internet/>.
28. Among other analyses of the challenges at hand for Russia, see Charlotte Jee, “Russia wants to cut itself off from the global internet. Here’s what that really means,” *MIT Technology Review*, March 21, 2019, <https://www.technologyreview.com/s/613138/russia-wants-to-cut-itself-off-from-the-global-internet-heres-what-that-really-means/>; and Robert Morgus and Justin Sherman, “Is the Russian Internet a Lost Cause?” *Slate*, March 28, 2019, <https://slate.com/technology/2019/03/russian-internet-rune-fragmentation-isolation.html>.
29. Catalin Cimpanu, “Russia to disconnect from the internet as part of a planned test,” *ZDNet*, February 11, 2019, <https://www.zdnet.com/article/russia-to-disconnect-from-the-internet-as-part-of-a-planned-test/>.
30. Chris C. Demchak and Yuval Shavitt, “China’s Maxim – Leave No Access Point Unexploited: The Hidden History of China Telecom’s BGP Hijacking,” *Military Cyber Affairs*, Vol. 3 (Issue 1), 2018, 1-9, <https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1050&context=mca>.
31. This is not to advocate for the position of manipulating others’ Internet protocols, but merely to clarify that the drastic changes to a country’s Internet that may occur with Internet isolation policies could be harmful, beneficial, or benign to a foreign military’s cyber operations against said country..
32. Ewan MacAskill, “Putin calls internet a ‘CIA project’ renewing fears of web breakup,” *The Guardian*, April 24, 2014, <https://www.theguardian.com/world/2014/apr/24/vladimir-putin-web-breakup-internet-cia>.

## NOTES

33. Kremlin efforts on the international stage over the past several years emphasize Internet insecurity and, as a direct consequence, the need for the state to tightly control the Internet as opposed to solutions to cybersecurity that have been proposed in more democratic countries. For discussion of this fact and motivations at play, see, among others: Alex Grigsby, “Will China and Russia’s Updated Code of Conduct Get More Traction in a Post-Snowden Era?” Council on Foreign Relations, January 28, 2015, <https://www.cfr.org/blog/will-china-and-russias-updated-code-conduct-get-more-traction-post-snowden-era>; Sarah McKune, “An Analysis of the Information Code of Conduct for Information Security,” The Citizen Lab, September 28, 2015, <https://citizenlab.ca/2015/09/international-code-of-conduct/>; David Ignatius, “Russia is pushing to control cyberspace. We should all be worried,” *The Washington Post*, October 24, 2017, [https://www.washingtonpost.com/opinions/global-opinions/russia-is-pushing-to-control-cyberspace-we-should-all-be-worried/2017/10/24/7014b-cc6-b8f1-11e7-be94-fabb0f1e9ffb\\_story.html](https://www.washingtonpost.com/opinions/global-opinions/russia-is-pushing-to-control-cyberspace-we-should-all-be-worried/2017/10/24/7014b-cc6-b8f1-11e7-be94-fabb0f1e9ffb_story.html); and Geoff Van Epps, “Common Ground: U.S. and NATO Engagement with Russia in the Cyber Domain,” 2013, <https://www.jstor.org/stable/26326340>, 27.
34. Alina Polyakova, “Want to know what’s next in Russian election interference? Pay attention to Ukraine’s elections,” Brookings Institution, March 28, 2019, <https://www.brookings.edu/blog/order-from-chaos/2019/03/28/want-to-know-whats-next-in-russian-election-interference-pay-attention-to-ukraines-elections/>; Katherine Costello, “Russia’s Use of Media and Information Operations in Turkey,” RAND Corporation, 2018, <https://www.rand.org/pubs/perspectives/PE278.html>; Michael Carpenter, “Undermining Democracy: Kremlin Tools of Malign Political Influence,” Testimony before the U.S. House of Representatives Subcommittee on Europe, Eurasia, Energy, and the Environment, May 21, 2019, <https://docs.house.gov/meetings/FA/FA14/20190521/109537/HHRG-116-FA14-Wstate-CarpenterM-20190521.pdf>; and Erik Brattberg and Tim Maurer, “Russian Election Interference: Europe’s Counter to Fake News and Cyber Attacks,” Carnegie Endowment for International Peace, May 23, 2018, <https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435>.
35. Andy Greenberg, “The Untold Story of NotPetya, the Most Devastating Cyber Attack in History,” *Wired*, August 22, 2018, <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>.
36. Donghui Park, Julia Summers, and Michael Walstrom, “Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks,” University of Washington, October 11, 2017, <https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/>.
37. This discussion of insulation from foreign cyber attacks is a build-out of a point briefly made in: Justin Sherman, “Russia and Iran Plan to Fundamentally Isolate the Internet,” *Wired*, June 6, 2019, <https://www.wired.com/story/russia-and-iran-plan-to-fundamentally-isolate-the-internet/>.
38. *Ibid.*, and BBC, “Iran rolls out domestic internet,” *BBC*, August 29, 2016, <https://www.bbc.com/news/technology-37212456>.