SPECIAL REPORT

NO. 499 | JULY 2021 UNITED STATES INSTITUTE OF PEACE www.usip.org

Digital Authoritarianism and Nonviolent Action: Challenging the Digital Counterrevolution

By Matthew Cebul and Jonathan Pinckney

People shine the lights of their smartphones at a demonstration in Hong Kong on June 16, 2019, to commemorate the death of a fellow protester. (Photo by Lam Yik Fei/New York Times)

Contents

Summary

- Nonviolent action campaigns, in which ordinary citizens use tactics such as protests, strikes, and boycotts to put pressure on power holders, have been one of the most effective ways of peacefully bringing about change in nonresponsive autocratic countries.
- These campaigns are increasingly shaped by emergent technologies—the internet, social media, artificial intelligence, and facial recognition—that offer significant benefits to nonviolent action. At the same time, these technologies are increasingly advantaging authoritarian regimes, which use them to suppress dissent and sustain oppressive political systems.
- These technologies present two key challenges: they make public life more legible to the state and reduce opportunities for nonviolent action to spark defections from among regime loyalists.
- The challenges are illustrated in the ways two authoritarian regimes, China and Russia, have developed tools of censorship, propaganda, and surveillance using newer technologies.
- As authoritarian regimes use these technologies to an ever-greater extent, it is crucial for policymakers and activists to respond to the challenges of increased legibility and decreased defection.

United States Institute of Peace
Making Peace Possible

SPECIAL REPORT

NO. 499 | JULY 2021

NONVIOLENT ACTION

ABOUT THE REPORT

This report examines how use of newer and emergent technologies affects nonviolent action campaigns. It identifies two significant related challenges and presents evidence of these dynamics at work in two digital autocracies, China and Russia. It was funded through an interagency agreement between the United States Institute of Peace (USIP) and the US Agency for International Development's Center for Democracy, Human Rights, and Governance.

ABOUT THE AUTHORS

Matthew Cebul is a research officer with the Program on Nonviolent Action at USIP, where he conducts multimethod research on nonviolent action and its implications. Jonathan Pinckney is a senior researcher with the Program on Nonviolent Action at USIP and the author of *From Dissent to Democracy: The Promise and Peril of Civil Resistance Transitions*, which was published by Oxford University Press in 2020.

The views expressed in this report are those of the authors alone. They do not necessarily reflect the views of the United States Institute of Peace. An online edition of this and related reports can be found on our website (www.usip.org), together with additional information on the subject.

United States Institute of Peace
2301 Constitution Avenue NW
Washington, DC 20037

Phone: (202) 457-1700
Fax: (202) 429-6063
E-mail: usip_requests@usip.org
Web: www.USIP.org

Special Report No. 499. First published 2021.

ISBN: 978-1-60127-859-3

UNITED STATES
INSTITUTE OF PEACE PRESS

People shine the lights of their mobile phones during a rally in support of jailed opposition leader Alexei Navalny in Moscow, Russia, on April 21, 2021. (Photo by Alexander Zemlianichenko/AP)

Introduction

In 2019, citizens of Hong Kong took to the streets over a new law that would further enable the Chinese government in Beijing to extradite Hong Kongers to the Chinese mainland. Over the following months, the protests escalated to demanding greater democracy and even the secession of Hong Kong from China. The protests attracted mass participation and their youthful, creative tactics, following martial arts star Bruce Lee's advice to "be water," inspired movements around the world.

The Hong Kong and Beijing governments responded with a range of tactics, from tear gas and batons to arrests and mass firings. Yet perhaps the most critical front in the war between the pro-democracy protesters and the mainland government was fought online. Hong Kong has long enjoyed more flexible rules about freedom of expression than mainland China and is ostensibly outside Beijing's Great Firewall of censorship. Beijing, however, deployed an increasingly sophisticated set of repressive tools, including facial recognition cameras, invasive online surveillance, and a draconian security law to stifle the movement.[1] Activists fought back, coordinating resistance through encrypted messaging systems such as Signal and Telegram, and posting videos online about how to fool facial recognition cameras using lasers and creative face-covering hairstyles.

In early 2021, demonstrations broke out across Russia following the arrest of opposition leader Alexei Navalny, with protesters braving subzero temperatures to express their opposition to

Hong Kongers hold up blank sheets of paper at a demonstration on July 3, 2020, protesting the government's slogan ban. (Photo by Lam Yik Fei/ New York Times)

President Vladimir Putin. The protests were fueled by a YouTube video posted by Navalny's party presenting evidence that Putin illicitly owned a huge estate on the Black Sea. The Russian government arrested thousands and likely intimidated thousands more. It also, however, fought back online with virtual disinformation and an increasingly aggressive censorship and surveillance regime.[2]

Nonviolent action campaigns like these—which involve tactics such as protests, strikes, and boycotts to achieve political goals—are one of the most common ways citizens seek to peacefully change nonresponsive political systems.[3] Campaigns are often fought to increase equity, fight corruption, and ensure good governance. They are a powerful way to transform social and political fragility into long-term stability, providing the disaffected and aggrieved a way of effecting change without violence. Because global authoritarianism is on the rise, the ability of ordinary people to wage nonviolent resistance is crucial to building a peaceful, democratic world.

Yet as these case studies make clear, recently developed and emergent technologies are transforming the nature of contentious interactions between activists and authoritarian governments. Although a wide range of factors influence whether movements succeed or fail, the technological landscape is an increasingly important one. Dissidents have used social media to rally support and coordinate resistance activities. Yet dictators, too, are deploying new technologies more and more frequently, using automation to flood online forums with disinformation and identifying dissidents with sophisticated algorithms based on the newest artificial intelligence (AI). These interactions are not random or haphazard. They are instead coordinated strategies by authoritarian governments to preserve their rule in the changing environment of the twenty-first century.

Democratic governments have also employed many of these technologies, and many of the underlying technologies originate in American technology companies. Yet the most egregious uses of emergent technology to surveil and suppress dissent come directly from authoritarian regimes seeking to maintain themselves without the consent of their populations.[4]

Two Challenges for Nonviolent Action

Emergent technologies pose two particular challenges for nonviolent action. The first is increasing legibility of social and political life through digital surveillance, which eliminates free space for coordinating collective action. The second is diminishing opportunities for activists to induce regime defections, a product of more effective preemptive repression and the increased centralization of the repressive apparatus. Both challenges go to the heart of how nonviolent action works. Both speak to the immediate need for policy responses to enable nonviolent action campaigns to effectively counter digital authoritarians.

INCREASED LEGIBILITY

The first major challenge is the way in which digital information and communications technologies are shifting interpersonal communication, interaction, and mobilization into information environments that are more directly "legible" to the state, that is, those the state can readily access and interpret.

Mobilizing nonviolent action campaigns typically requires "free spaces" beyond state control in which action and attitudes can be coordinated and a "revolutionary ideology" developed.[5] Free spaces allow for the frank exchange of ideas that would otherwise provoke repression. Such spaces take many forms, from religious institutions like the East German churches that fostered protests for peace in the 1980s to marketplace associations like the Bazaaris that helped organize the Iranian revolution in the 1970s. Their key characteristic is that what goes on within them is not subject to government oversight or control.

Authoritarian governments, particularly totalitarian dictatorships, have long sought to scrutinize free spaces using comprehensive networks of informants and surveillance, or by absorbing independent civil society structures into their governing coalitions. Yet the complexity of modern society makes total information control close to impossible. Even in situations of extreme repression, "weapons of the weak," such as mockery of those in power or shirking government-mandated responsibilities, can provide the foundation for undermining authoritarian myths and sparking collective action.[6] Even a moderately free space in which to express dissent can have powerful consequences. Authoritarian regimes incorporate a comprehensive "preference falsification," in which people, fearing repression, hide their true attitudes toward the government. Yet even a small number of vocal dissenters can spark revolutionary cascades as others observe that opposition to the regime is more widespread than they imagined.[7]

In its early days, the internet, and especially social media, appeared to be near-ideal free spaces. Activists and international observers hailed the internet's lack of gatekeepers, the ability of individuals across a wide range of contexts to communicate directly, and the practical tools that digital organizing provided for under-resourced movements.[8] The benefits of technology for movements are real. In the internet era, mobilizing a protest of millions is feasible in a way unimaginable to prior generations.[9] These advantages have made digital activism a core part of

> Twenty-first-century technologies have granted regimes a tremendous advantage by shifting an ever-growing proportion of civic life . . . into a world of digital communication that is by design easily legible.

many movements' strategies, a trend only heightened by the COVID-19 pandemic.[10]

Yet while social media is a powerful tool for organizing dissent, the virtual commons are perilous territory for nonviolent activists. Digital technologies not only ease communication, but also make communications more accessible and legible, both to the companies that produce them and to the state. Digital autocracies can directly censor online information that threatens to foster collective action, inundate online discourse with counternarratives and disinformation, map the social media ties of disruptive users to better understand opposition networks, and pry into dissidents' ostensibly private communications. Even if their techniques are relatively crude, the regime's presence on such platforms, and citizens' knowledge of this surveillance, can encourage self-censorship and stifle free discourse.[11]

When citizens seek to organize despite government surveillance, technology provides a way for authoritarian regimes to preemptively suppress opposition. AI-enhanced surveillance, from social media–scouring algorithms to advanced facial imaging systems, is making mobilization processes that were previously opaque to the state increasingly legible and predictable, empowering autocrats to quickly identify the warning signs of coordinated protests and target disruptive activists. Armed with notice, regimes can preemptively enact measures to forestall mobilization, locking down trouble spots and locking up dissidents before large-scale mobilization occurs. As preemptive repression becomes more efficient, regimes have less need to use physical violence to disperse protests. This is highly consequential in that one of the main drivers of regime defections is popular backlash to visible episodes of repression against unarmed demonstrators.[12] Increased legibility is taking repression increasingly out of sight and mind.

In short, twenty-first-century technologies have granted regimes a tremendous advantage by shifting an ever-growing proportion of civic life away from the complex, often inscrutable world of face-to-face human interaction and into a world of digital communication that is by design easily legible. Indeed, insofar as online communication substitutes for in-person networking, it may even indirectly stifle the development of other free spaces as citizens abandon real-world activities once beyond government control.

REDUCING REGIME DEFECTION

The second major challenge for nonviolent action campaigns is that emergent technologies can help autocrats prevent major regime defections in two ways. First is to enhance preventive repression that enables regimes to avoid risky episodes of large-scale violent repression. Second is to shift much of the everyday burden of repression away from a large group of police and soldiers and into the hands of a small number of specialists, whose loyalty can be better monitored and ensured and whose propensity for defection is low.

When all else fails, autocracies rely on violent repression to keep their populations in line. The logic of nonviolent action recognizes that autocrats' ability to repress requires the cooperation of complex, extensive "pillars of support."[13] Ruling elites rely on a security apparatus (and in some cases, pro-regime civilians) to identify threats and, when necessary, use violence to deter them.

This reliance presents authoritarian leaders with several challenges. First, repression comes at a direct high cost. Secret police must be paid, surveillance equipment must be purchased and maintained, and security forces must be mobilized. Second, repression creates a significant hazard for the state's political elite in that the institutions to which it outsources its repressive capacity may one day use that capacity to seize power for themselves.[14] Last, in the context of a nonviolent action campaign, security forces may shirk their responsibilities, refuse to repress peaceful protesters, or defect from the state and embrace calls for change. Defection is common in nonviolent action campaigns and significantly increases the odds of campaign success.[15] Defections often start from the bottom tiers of security forces and work their way up. When top security officials defect, it is typically because they fear that their rank-and-file will not obey orders to repress on the ruler's behalf. This pillar of support then extricates itself from the regime, facilitating its collapse.

Numerous factors influence security sector defections during nonviolent action campaigns.[16] One of the most crucial is when security forces are called on to repress in ways they believe excessive or unjustified. For example, in the 2020 protests against President Alexander Lukashenko in Belarus, many police officers publicly took off their uniforms and refused to obey orders, rejecting the government's demand that they use deadly force against peaceful protesters. Similarly, a key turning point in the 2010–2011 Tunisian uprising came when President Zine El Abedine Ben Ali called on the military to violently suppress the revolution. Military leaders refused, precipitating Ben Ali's flight from the country.

A related factor facilitating defection involves personal connections with security forces.[17] For example, in the 2004 Ukrainian Orange Revolution, opposition figures used family ties to create a vast network of bottom-up contacts and informal agreements within the Ukrainian military that soldiers would not use violence against peaceful protesters.[18] In Nepal, a lack of such connections led to the emergence of an armed insurgency.[19]

Emergent technologies, particularly artificial intelligence, undermine both these mechanisms, thereby reducing the likelihood of regime defections. To start, these technologies increase the efficiency of preventive repression, permitting regimes to keep their populations in check without resorting to episodes of egregious violence that might prompt security force defections. AI provides authoritarian governments with computational tools that significantly enhance their capacity to censor and surveil their populations. As the case studies clarify, this capacity enables regimes to identify dissenters and snuff out resistance before activists can orchestrate the dramatic visuals and appeals to conscience that may trigger defections, either from security forces or among regime supporters more generally.[20]

Automating repression allows rulers to place repression in the hands of a small number of regime loyalists.[21] Because automated algorithms now do the day-to-day work, a certain degree of surveillance, propaganda, and censorship that previously required large numbers of the relatively less skilled—soldiers, police, informants, and intelligence agents—can now be achieved with a relatively small number of the highly skilled, those tasked with designing and overseeing the automated systems. These managers, programmers, and engineers, typically members of the political and social elite, can then in turn be more closely and easily monitored, and their loyalty ensured. And at the lower levels of these apparatuses, artificial intelligence may remove even the possibility of human interaction or compassion, in much the same way that automated traffic cameras remove human agency from the enforcement of traffic laws.

China Revolutionizes Digital Autocracy

China is pushing the boundaries of digital authoritarianism. Although the internet has empowered Chinese civil society in some ways, emergent technologies have empowered the Chinese Communist Party (CCP) still further, allowing it to manipulate information, identify dissidents, and efficiently preempt mass mobilization. Enhanced censorship, propaganda, and surveillance have made Chinese civil society more legible to the CCP than ever before, mitigating the prospects for either antiregime mobilization or significant regime defections.

CENSORSHIP

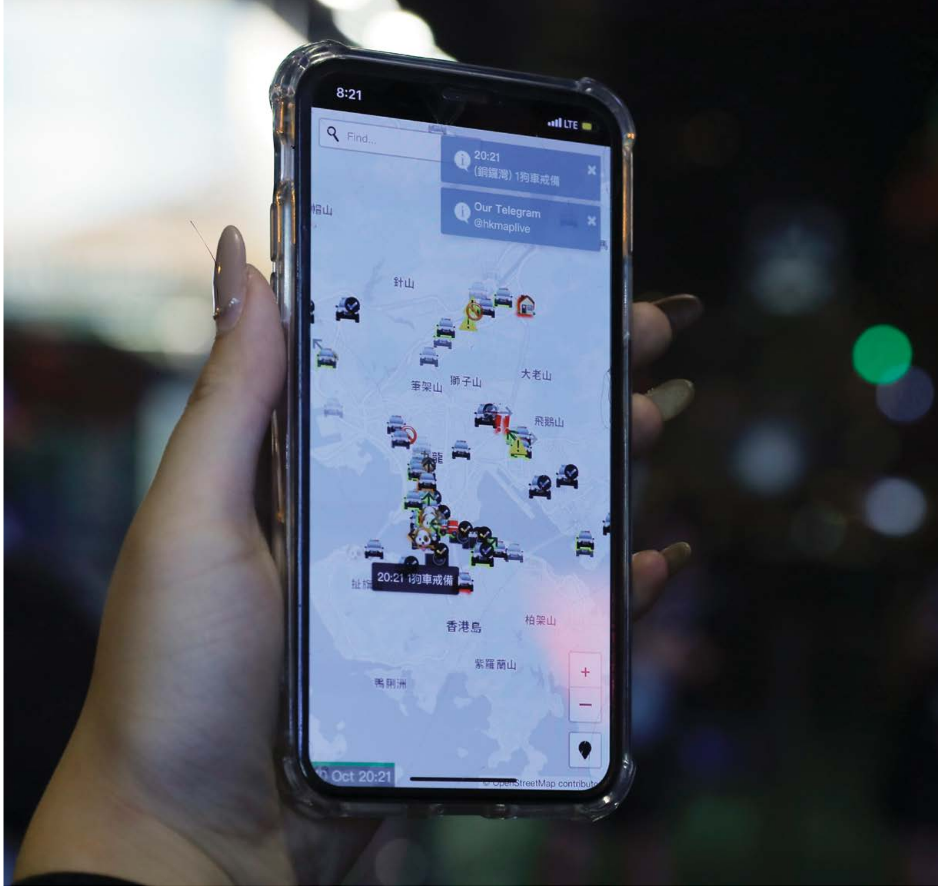
China's censorship regime is the most comprehensive in the world. Famously, the Great Firewall blocks Chinese users from accessing many websites, from Google and Twitter to the *New York Times*. The CCP also keeps a firm grip on internet gatekeepers, supervising news media while holding both ISPs and content providers like Sina Weibo (China's Facebook equivalent) liable for online content. To avoid prosecution, these companies employ armies of censors in coordination with the CCP's Propaganda Department. Censorship laws ban any content that "disseminates rumors, disturbs the social order or damages social stability."[22] The censors, though, focus on content that encourages collective action or challenges CCP legitimacy.[23]

Chinese censorship is far from airtight. Internet users can jump the Great Firewall with a VPN and evade automated keyword blocks with simple wordplay. Weibo users have written millions of posts criticizing local governance failures.[24] And though enforcement under Xi Jinping appears to be tightening, criminal punishment for content violations is rare, largely reserved for high-profile dissidents such as Nobel laureate Liu Xiaobo.[25]

Still, "porous censorship" is effective. Most users are unwilling to invest the effort to access censored content: throttling web pages, reordering search results, and limiting VPNs introduces enough friction to subtly nudge users away from banned content without triggering backlash.[26] Only an estimated 3 to 15 percent of China's more than nine hundred million internet users avail themselves of VPNs to jump the Great Firewall.[27] The rest are content to stay within a restricted but vibrant Chinese internet ecosystem.[28] Thus, Chinese internet users are largely blinded to the CCP's worst excesses. Many Chinese university students do not even recognize iconic imagery from the 1989 Tiananmen Square protests.[29]

PROPAGANDA

The CCP also generates its own content, using online platforms to manipulate national discourse. Hundreds of thousands of CCP agents, known colloquially as the 50 Cent (50c) Party because of their apocryphal pay per post, regularly flood social media with comments lauding the regime and its policies, generating around 450 million posts annually.[30] This helps the CCP bury bad press while discreetly nudging citizens toward favorable content, relative to more overt propaganda from traditional news agencies widely understood to be state organs.[31] CCP propaganda especially



An app on a person's mobile phone shows the location of protesters and police in the Tsim Sha Tsui district in Hong Kong on October 10, 2019. (Photo/Kin Cheung/AP)

highlights court-provided restitution for local abuses, encouraging citizens to air grievances through institutional channels rather than mass protests.[32]

The 50c Party is relatively low-tech. Government employees are asked to generate pro-regime propaganda as a term of their employment; pro-CCP volunteers can contribute as well. Newer and emergent technologies, though, promise to enhance this online Party propaganda. Bot programs can efficiently spew coordinated waves of it on command, distracting users from unsavory current events such as Hong Kong protests or the COVID-19 pandemic . Similarly, advances in AI will likely allow the CCP to identify trends and abuse social media content algorithms to more prominently display pro-regime content.[33] As these technologies evolve, China's mass data-gathering and surveillance may even enable tailoring propaganda to individuals, such as using targeted online ads.[34]

SURVEILLANCE

Perhaps most important, the CCP has exploited advances in big data and facial imaging technology to create a comprehensive surveillance state. To start, it is rapidly developing the capacity to analyze the vast troves of social media data on user associations, preferences, and behavior. Online trends can be used to identify real-world disturbances, facilitating preemptive repression. For example, government officials in Chengdu responded to online efforts to organize a Saturday demonstration by preemptively extending the work week through the weekend.[35] A social media early warning system can also be efficiently automated, given that algorithms already constantly search for trends that portend collective action and flag threatening activity.

Beijing also uses online surveillance to identify opposition sympathizers. Per the 2016 Cyber Security Law, internet providers are required to collect identifying information. ID is required to access social media, make purchases through WeChat Pay, or use other ubiquitous applications.[36] As virtual anonymity withers, the CCP can pry into private communications, map virtual networks of dissenters, and readily link online criticism to real-world identities. The Great Firewall can also track user requests for access to censored websites, another indicator of anti-regime sentiment.[37] In turn, the regime can more efficiently target suspected dissidents for "invitations to tea" with security, leaving other citizens unmolested and oblivious.

Over the past decade, Beijing has massively expanded its surveillance program, installing hundreds of millions of cameras in a bid to achieve 100 percent coverage of public spaces.

Further, CCP surveillance follows internet users into their daily lives even after they have gone offline. The regime has made major strides in facial imaging technology, developing an unparalleled video surveillance system to identify and track individuals in real time.[38] Over the past decade, Beijing has massively expanded its surveillance program, installing hundreds of millions of cameras in a bid to achieve 100 percent coverage of public spaces.[39] It is now commonplace for citizens to be photographed or recorded in public areas, especially in major cities. This expansion has increased the number of political arrests.[40]

The abusive implications of the CCP's behemoth surveillance apparatus are difficult to overstate. Consider the ongoing work on China's social credit system (SCS), first announced in 2014. Ostensibly intended to foster social trust, the SCS will assign each Chinese citizen a social credit score, rewarding those who behave "virtuously" with preferential access to public goods and denying these goods to citizens with low scores. What distinguishes China's SCS from other credit systems is its potential to incorporate an astounding array of both financial and personal data. Pilot SCS programs have factored in not just whether citizens' bills are paid, but also what they buy, what they post on social media, who they socialize with online—even how long they spend playing video games.[41] Although the SCS pilots and data are currently fragmented across cities, regions, and companies, Beijing intends to develop a unified national system. And, as facial recognition grows ever more ubiquitous, it is hardly a stretch to envision the inclusion of location or other behavioral data as well.

Looming on the horizon, then, is a world in which China can maintain personalized dossiers tracking where its citizens go, what they do, and what they say, in both virtual and physical space, using AI to identify patterns in these data in ways unimaginable just a few years ago. Many in China welcomed pilot SCS programs, which the CCP brands as a rewards system for good behavior.[42] The SCS, however, will ultimately grant Beijing incredible leverage to punish whoever it deems to engage in subversive behavior. As research scientist Xiao Qiang stresses, "Once fully operative, the SCS—premised on a massive invasion of citizens' privacy through large-scale monitoring—will provide the state with a range of new mechanisms by which it can exert control over China's people."[43]

Last, Beijing also uses social media to improve government performance. Typically, repressive autocracies have a principal-agent problem, in which unaccountable local officials exaggerate their performance to central elites. Social media allows the CCP to crowdsource more accurate information about local grievances, creating a new accountability mechanism.[44] For this reason, the CCP tolerates vehement online criticism of local-level corruption: Party elites can use that information to sanction local officials, taking credit for addressing local concerns while staving off demands for systemic change.[45] This mechanism is imperfect because local officials may not report online complaints to their superiors when they are directly implicated in wrongdoing.[46] Yet these complaints are usually visible online, and online grievances have led to top-down accountability in a number of cases. The Communist Party also actively solicits citizen feedback through various e-government platforms, enhancing regime legitimacy while further channeling citizens toward institutional forms of redress rather than regime-threatening mass mobilization.

IMPLICATIONS FOR NONVIOLENT ACTION

As others have observed, the internet has transformed how Chinese citizens interact with the state. Online forums are far more critical than traditional media, and virtual campaigns have forced the CCP to adjust policies on several prominent occasions.[47] For decades, protests in China have numbered in the tens of thousands annually, on issues of taxation, land seizure, and labor abuse, among others.[48] These movements have been enhanced by internet activism, which has empowered Chinese civil society to forge online communities, voice grievances, and draw national attention to local governance failures.[49]

However, emergent technologies have empowered the CCP still further. Chinese civil society is more legible than ever before. The regime can track trends in cyberspace, snoop through virtual conversations on WeChat, manipulate social media narratives, and monitor citizens' everyday behavior. Its ability to do so is only increasing. Chinese social media has seen explosive growth, but this vibrant civic engagement is circumscribed within tightly controlled virtual space. In China, online political discourse is hardly free, let alone risk free.

Moreover, opportunities to provoke regime defections are limited. As the CCP improves its ability to preemptively quash mobilization, it has less need for high-profile physical repression, meaning fewer chances for mass movements to generate defections. Further, repression is increasingly automated and difficult to disrupt. Virtual surveillance on social media platforms is highly efficient, enabling the CCP to replicate a Stasi-like intelligence operation with a fraction of the manpower and a less overbearing public footprint.[50] Once established, the SCS can be automated and devoid of personal interaction, such that citizens experience punishment for "deviant" behavior without ever seeing a state agent and without recourse. Journalist Liu Hu recounts as much from his experiences after being placed on a Dishonest Persons blacklist: "There was no file, no police warrant, no official advance notification. They just cut me off from the things I was once entitled to. What's really scary is there's nothing you can do about it. You can report to no one. You are stuck in the middle of nowhere."[51]

In short, Beijing has effectively adapted to the internet age. Whereas online activism has fueled mass uprisings in other autocracies, China has not experienced any regime-threatening mobilization since 1989. Protests in the country are reformist and occur exclusively around non-ideological concerns. Civic engagement and investigative journalism are rising, but online users avoid challenging the CCP directly.[52] The regime keeps a tight grip on the media and has imprisoned a number of prominent human rights activists.[53] The resulting chilling effect is increasingly leading democracy-minded Chinese citizens to self-censor.[54] Fear of censorship is on full display in Hong Kong, where opposition sympathizers frantically scrubbed their virtual lives of revolutionary content in the aftermath of the new security law.[55] In these circumstances, the likelihood of a large-scale nonviolent campaign triggering significant regime defections seems slim.

Yet even as organized dissent is suffocated, many Chinese appear less fearful of the regime. Many are blissfully ignorant of the scope of repression, enjoy virtual life within the Great Firewall's subtle constraints, and appreciate the convenience of a networked society under the CCP's watchful eye.[56] In other words, China's digital autocrats are having their cake and eating it too.

Russia Wages Information Warfare

Russia initially embraced a laissez-faire approach to the internet and was forced to react defensively to online activism. The Kremlin lacks the technical capacity to fully emulate Beijing's repressive toolkit. To compensate, Russia has developed a vigorous online disinformation machine and an increasingly oppressive blend of legal restrictions, surveillance, and coercion. Although effective, this system does not fully exploit the repressive potential of emerging technologies. Because of this the legibility and defection challenges for nonviolent action are less severe than in China. Thus, whereas China illustrates the frontiers of possibility for a high-capacity digital autocracy, Russia illustrates how even moderate-capacity autocracies can use emergent technologies to thwart nonviolent action campaigns.

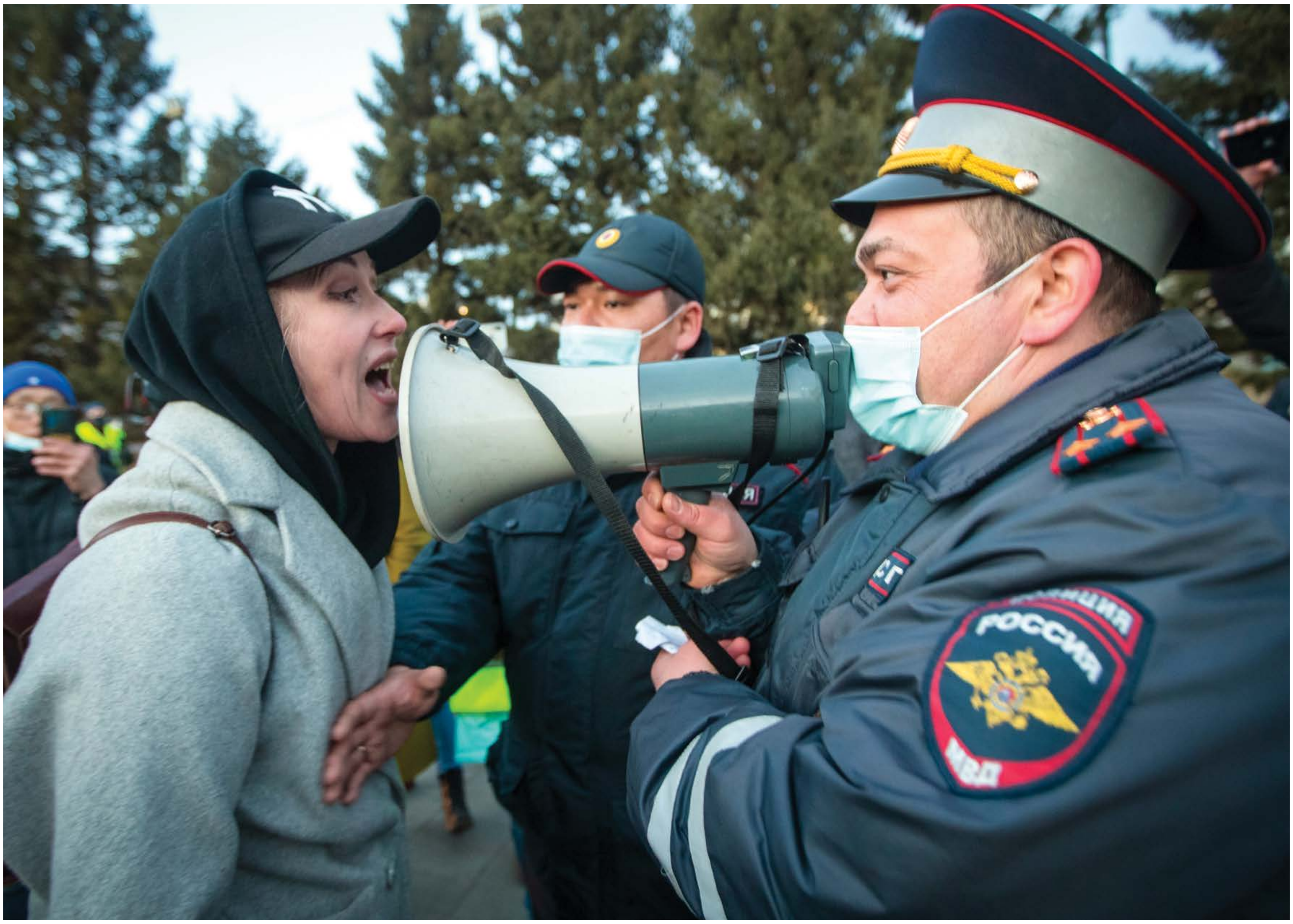
CENSORSHIP

For much of its existence, Russia's internet ecosystem (RUNET) was remarkably free.[57] President Putin curtailed media freedoms following his election in 2000, but left the nascent internet unregulated, rejecting Chinese-style censorship. As a result, RUNET flourished—Yandex and VKontakte (VK, InContact) outcompeted Google and Facebook among Russian users, who cultivated a vibrant blogosphere.[58] Yet as internet penetration soared, the Kremlin reevaluated its approach. Control over traditional media did nothing to stop online mobilization, a reality punctuated by the 2011–2012 protests. After returning to the presidency in 2012, Putin made it a priority to rein in RUNET.[59]

To start, Russia is building a quasi-legal censorship regime backed by state coercion. In 2012, the Duma established a blacklist of so-called extremist websites, maintained by the censorship agency Roskomnadzor. Soon thereafter, the Duma granted the prosecutor general the authority to block sites without a court order and expanded the blacklist to include sites publicizing unsanctioned mass events. Other legislation compels popular content producers to register with the government and holds them liable for site content (the Blogger's Law), and fines ISPs that fail to block VPNs. In turn, the Kremlin has used this veneer of legality to harass, intimidate, and even capture content providers. For instance, VK founder Pavel Durov was forced to flee Russia in 2014 after he refused to block alleged extremist accounts associated with the Euromaidan movement. Durov was replaced by Kremlin loyalists, ensuring that VK remains pliant to the Kremlin.[60]

Still, Russian censorship is belated and crude. Whereas the CCP built censorship into China's internet infrastructure from its infancy, twenty years of unfettered private development thoroughly entangled RUNET with the global internet. For now, it would be prohibitively challenging for Russia to isolate RUNET via a national firewall. As Artem Kozlyuk, founder of the digital freedoms NGO Roskomsvoboda, put it, "Russia separating itself from the World Wide Web would be like closing down its airspace."[61] Russians are accustomed to global internet access, and blocking widely used services like Facebook and Google would likely prompt backlash.

Moreover, Russian censorship is unsophisticated, banning websites at the IP address rather than filtering based on keywords. This means that Roskomnadzor must manually identify sites to block. Pro-Kremlin users can help crowdsource this information, but censorship is hardly



A woman argues with a police officer during a protest in support of opposition leader Alexei Navalny in Ulan-Ude, the regional capital of Buryatia, a region near the Russia-Mongolia border, on April 21, 2021. (Photo by Anna Ogorodnik/AP)

airtight.[62] And because websites often share IP addresses, IP blocks can cause collateral damage, as evidenced by Russia's failed attempt to block Telegram, which disrupted many online services.[63] International companies often ignore Russia's censorship demands and evade IP blocks, and Russian users circumvent censorship with VPNs. In short, whereas CCP censorship is vast yet subtle, the Kremlin's efforts are limited yet ham-fisted—or as one Russian blogger put it, Roskomnadzor is staffed by "monkeys with grenades."[64]

That said, Russia is improving its censorship capacities. The 2019 sovereign internet law forces ISPs to install equipment that could allow the Kremlin to temporarily sever global internet access in particular regions without affecting Russian national domains.[65] Russia is also growing more aggressive with foreign companies and is currently throttling Twitter for censorship violations.[66] Nevertheless, Russia's road to comprehensive censorship is long.

DISINFORMATION

To compensate for these deficiencies, Russia has leaned into disinformation campaigns. As in China, the Kremlin pays pro-regime youth groups and bribes influential bloggers to cheerlead for the regime, lauding Putin while smearing his opponents.[67] The effect is to derail opposition narratives of regime abuses, foster cynicism about political engagement, and signal the regime's unassailable strength—in short, to sow "distortion, confusion, and discouragement" in cyberspace.[68]

Putin has used bot and troll farms to "flood the zone" with disinformation, polluting online discourse with meaningless conspiracies and rumors. . . . On some days, more than half of Russian Twitter posts about politics are generated by bots.

This strategy has been supercharged by automated technology. Putin has used bot and troll farms to "flood the zone" with disinformation, polluting online discourse with meaningless conspiracies and rumors. This effectively taxes users curious about the opposition, who are forced to sift through the garbage before encountering real information about government performance.[69] On some days, more than half of Russian Twitter posts about politics are generated by bots.[70] This is a cheap but effective strategy, enabling the Kremlin to muddy the waters about corruption while branding the opposition as a Western-sponsored fifth column. Bots also decrease online activism's persuasive impact. Some bots are easy to spot, but sophisticated troll accounts are not always obvious, enabling them to infiltrate and hijack online opposition discourse.[71] Opposition engagement with paid regime supporters is at best fruitless.

In addition, Russia has also weaponized online disinformation and troll operations as a potent tool of foreign policy. Russia has unleashed targeted waves of disinformation on multiple foreign policy fronts, using virtual propaganda to justify Russia's war in Ukraine and annexation of Crimea and to substantially interfere in the 2016 US elections.[72] These propaganda campaigns are both less overt than traditional news propaganda and remarkably sophisticated.[73]

SURVEILLANCE

Last, Russia has exploited social media to upgrade its surveillance. Although Russian telecommunications surveillance (the SORM system) has been in operation since the 1990s, emerging technologies are enhancing these tools.[74] The 2016 Yarovaya amendments require all "organizers of information dissemination" to archive user data for three years on Russian servers and to grant the Federal Security Service (FSB) access to these communications and any encryption codes. In 2017, the Duma legislated that social media companies must identify users by cell phone number and banned anonymous access to such services via VPN. The 2019 sovereign internet law requires ISPs to install deep packet inspection technology, enabling the FSB to surveil the content of online traffic in addition to the metadata and without ISP knowledge or consent.[75] The combined effect of these laws is to grant the Kremlin sweeping access to digital communication in Russia.

As in China, online surveillance enables the Kremlin to monitor and suppress dissent. Charges of online extremism are rising, facilitated in part by VK's cooperation with FSB requests for user data.[76] Still, Russia's surveillance system remains limited. The Kremlin does not have the technical capacity to process the oceans of data generated by the new storage laws. This limits it to targeted surveillance rather than comprehensive monitoring, although Russia is working with China to improve its AI data processing abilities.[77] Many Russians use messaging applications with end-to-end encryption such as Telegram that are not easily surveilled (these are not commonly available in China).[78] Russian users can also circumvent social media ID requirements through SIM card loaning programs.[79] They can do so as well by noncompliance from international content providers, which Russia struggles to deter. And though Russia has invested in facial imaging surveillance at major transportation hubs, it cannot come close to replicating China's nationwide video surveillance.[80]

IMPLICATIONS FOR NONVIOLENT ACTION

Newer and emergent technologies have provided Russia with repressive benefits similar to those of China, but to a lesser degree. Unlike Beijing, the Kremlin cannot fully exploit the internet's repressive potential—its censorship is more porous and its surveillance less omniscient. The CCP is leveraging emerging technologies to analyze previously incomprehensible quantities of data, rendering Chinese society ever more legible to the repressive apparatus. The Kremlin cannot match this system, so online activism remains a liability. Russia has compensated by leaning on reactionary disinformation, intimidation, and occasional assassinations to disrupt opposition coordination, obfuscate bad press, and sideline dissenters.[81] This resembles a more traditional, low-tech mode of authoritarian repression, albeit enhanced by digital surveillance. Ironically, whereas the Chinese regime is undoubtedly more oppressive, the Russian regime appears more thuggish and violent.

This distinction has important implications for nonviolent action in Russia. Most pointedly, Putin's ability to preemptively repress mass mobilization remains limited, as evidenced by the recent anti-regime protests. News of Alexei Navalny's arrest and show trial was shared among millions of online viewers on YouTube, TikTok, and Instagram, and Navalny's call for action prompted mass protests across Russia. Roskomnadzor pressured companies to remove related content, but the damage was already done: TikTok's #FreeNavalny and #23January hashtags generated more than two hundred million views within days of Navalny's arrest, and Navalny's supporters continue to wage his anti-corruption campaign online.[82] Such content would be exceedingly short-lived on the Chinese internet. In contrast, Putin can only distort reality, not erase it.

In turn, the Kremlin's inability to preempt mobilization matters for the possibility of regime defections. The Kremlin continues to rely on physical repression to keep protesters in check—Russian police arrested thousands of demonstrators at the recent protests. Abusive episodes like this increase the risk of backlash, in which excessive repression only stokes further outrage. Moreover, crackdowns expose the security apparatus to one of the opposition's most powerful tools to encourage regime defections: unjustified suffering at their own hands. Anonymous online trolls may be immune to persuasion, but in-person opposition fraternization with security forces can win converts. Indeed, some anecdotal evidence indicates this in recent protests, including one Moscow police captain who chose to retire rather than repress protesters, proclaiming, "I am ashamed to wear this uniform because I realize it is covered in blood."[83]

To be sure, these inroads are limited. Putin remains popular, the formal Russian opposition is weak and fragmented, and the Kremlin is improving its ability to monitor online activism. Russia may not be a likely case for successful democratic transition. Yet Russia's brand of digital autocracy has vulnerabilities that could be exploited by a determined and disciplined nonviolent movement.

Recommendations for Policymakers and Activists

Few regimes have reached the level of sophistication that China and even Russia exhibit in their use of newer and emergent technologies, and most lack the technical and bureaucratic proficiency required to fully exploit the kinds of tools described here.[84] Nevertheless, many others, such as Saudi Arabia and Iran, have long used their own advanced censorship and filtering apparatuses.[85] Regimes that do not have these capacities are rapidly moving to acquire them.[86]

Both China and Russia are accelerating these moves as part of their grand strategies. China is providing dozens of countries across the globe with AI-enhanced surveillance technology, from Pakistan and Malaysia to Argentina and Venezuela. Russia too is exporting its SORM surveillance technology into its near abroad.[87] Nor are Western countries exempt from responsibility for the spread of digital authoritarianism. Tech firms in the United States, Israel, Italy, and elsewhere are playing a significant role in building the infrastructure of the digital authoritarian state.[88] If current trends continue, the spread of repressive technologies will only accelerate. The challenges to nonviolent action of increased legibility and decreased defection will grow in severity at the same time.

The policy conversation on great-power competition over newer and emergent technologies, particularly artificial intelligence, is robust. The recent capstone report of the National Security Commission on Artificial Intelligence documented accelerating competition between China and the United States on AI, and emphasized the importance of "build[ing] privacy-protecting standards into AI technologies and advance[ing] democratic norms to guide AI uses."[89] The findings in this report reinforce well-worn recommendations to better control the export of technologies that facilitate digital repression, advocate for an internet less subject to government surveillance, and develop global standards to promote ethical AI.

Focusing on the core challenges of legibility and defection suggests several unique recommendations as well. Regarding legibility, three are especially important:

External actors should increase support for free spaces based on traditional institutional structures. Optimism about the democratizing impact of emergent technology led to a wave of outside funding for diffuse, often youth-based networks that relied heavily on social media. Even after that initial optimism, a preference for supporting digital activism remains, as does a fascination with the potential for social media–fueled mobilization in authoritarian settings. There are some grounds for continued optimism, given that in many countries online mobilization continues to outmaneuver even dedicated efforts at repression. Yet technological trends are not encouraging. The development and spread of AI alongside ever-increasing computing power will increase the ease with which the tools described here can be deployed to suppress nonviolent action, even in states without China's capacity and experience. Donors would do well to shift their attention toward the day-to-day networks of work, recreation, and faith that build underlying civic capacity for future mobilization without relying on increasingly legible online space.

A Chinese national flag flutters near surveillance cameras mounted on a lamppost in Tiananmen Square in Beijing, China, on March 15, 2019. (Photo by Andy Wong/AP)

Activists should preemptively build offline redundancy for online activism. Considering how deeply engrained the internet and social media have become in daily life, activists cannot simply abandon digital space. Yet overemphasizing online activism is likely to be a major weakness by making movements more legible to repression. Many movements have learned this lesson the hard way, belatedly building less vulnerable offline networks in response to repression. For example, in Ethiopia, young activists in the 2015–2016 protests, originally organized almost entirely digitally, were forced to adapt to the government's control of the internet by building in-person networks in prison after mass arrests.[90] Activists can avoid this pitfall by building offline redundancy for their communication, organization, and networking before a crisis occurs. Indeed, this type of civil society development is almost certainly beneficial for movements regardless of concerns about digital authoritarianism.

Both donors and activists should facilitate training in advanced digital security. As many activists are well aware, digital security is crucial to ensuring movement viability and success. Numerous resources exist to introduce activists to the basics of digital security, such as how to use VPNs, end-to-end encryption, and air-gapped computers.[91] However, the rapidly changing nature of this space makes it important that activists frequently update their awareness of digitally enhanced repression and avoid relying on a single curriculum or set of resources. Regular strategic analysis of the digital landscape and potential vulnerabilities are a critical part of any twenty-first-century nonviolent action movement. Outside actors can support such training and strategic thinking, both by supporting initiatives that develop training resources, helping provide movements with the (often prohibitively) technical equipment to increase their security, and by publicizing research on advances in digital authoritarianism.

On the reduced potential for defection, three additional recommendations are important.

External actors should promote training and professional development in the ethical use of newer and emerging technologies. Many of the professional and technical elites who operate the systems underlying digital authoritarianism have few connections to the activists advocating for nonviolent change in their countries. Yet these same elites are often trained and socialized in democracies, particularly the United States.[92] This provides an opportunity to include ethical training and build the kinds of interpersonal networks and professional socialization that may make these elites more hesitant to engage in digital repression.

Activists should use creative nonviolent tactics to expose the injustice of preemptive repression. Prompting defection is challenging when preemptive repression makes the injustice of oppressive systems less visible, as in China. Tactics that both reveal the preemptive repressive apparatus at work while humorously mocking its absurdity may help.[93] For example, in 2013 the Chinese government censored images of rubber ducks after a blogger posted a photoshopped version of the famous image of Tank Man at the 1989 Tiananmen Square protests, replacing the tanks with giant rubber ducks. More recently, the CCP has scrubbed the cartoon bear Winnie-the-Pooh from its internet in response to mocking comparisons between Pooh and President Xi Jinping. Such light mockery may seem inconsequential in the face of the CCP's might. Yet, as many past campaigns show, subtle humorous actions that reveal the injustice and absurdity of repression can be important precursors to future mobilization.[94]

Activists should also build networks with the scientists and engineers building and maintaining the infrastructure of digital authoritarianism. Activists have long emphasized the importance of building networks between activists and members of the security forces to reduce repression and facilitate defections.[95] Yet as repression of nonviolent action is increasingly mediated through digital information and communications technology, the most influential defectors will more and more frequently be those responsible for running the state's digital infrastructure. Activists can redirect their efforts accordingly, given that the same careful networking and relationship building that movements have used to thwart physical repression can be used to thwart digital repression.

Along these lines, activists across many contexts are developing creative strategies to respond to the challenges of digital authoritarianism, using emergent technologies to advance social and political change. Nonviolent action has been one of the most potent forces for peaceful and progressive political change in recent decades. As the technological ground on which nonviolent action movements struggle shifts, tactics and strategies to ensure success will also have to shift if grassroots activists are to counter rising authoritarianism and peacefully advocate for a better world.

Notes

1. Paul Mozur, “In Hong Kong, a Proxy Battle over Internet Freedom Begins,” *New York Times*, July 7, 2020, www.nytimes.com/2020/07/07/business/hong-kong-security-law-tech.html.
2. Alexy Gorbachev, “New Generation of Russian Protesters Harnesses Social Media,” Voice of America, February 4, 2021, www.voanews.com/press-freedom/new-generation-russian-protesters-harnesses-social-media.
3. Erica Chenoweth, “The Future of Nonviolent Resistance,” *Journal of Democracy* 31, no. 3 (2020): 69–84.
4. Steven Feldstein, *The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance* (New York: Oxford University Press, 2021).
5. On free spaces, Sharon Erickson Nepstad, *Nonviolent Struggle: Theories, Strategies, and Dynamics* (New York: Oxford University Press, 2015), 91; on revolutionary ideology, John Foran and Jean-Pierre Reed, “Political Cultures of Opposition: Exploring Idioms, Ideologies, and Revolutionary Agency in the Case of Nicaragua,” *Theory and Society* 28, no. 3 (2002): 1–38.
6. James C. Scott, *Weapons of the Weak: Everyday Forms of Peasant Resistance* (New Haven, CT: Yale University Press, 1985).
7. Timur Kuran, “Now Out of Never: The Element of Surprise in the East European Revolution of 1989,” *World Politics* 44, no. 1 (1991): 7–48.
8. Clay Shirky, *Here Comes Everybody: The Power of Organizing Without Organizations* (New York: Penguin, 2008); Manuel Castells, *Networks of Outrage and Hope: Social Movements in the Internet Age* (Hoboken, NJ: John Wiley & Sons, 2015); and Wael Ghonim, *Revolution 2.0: The Power of the People Is Greater Than the People in Power* (New York: Houghton Mifflin Harcourt, 2012).
9. Zeynep Tufekci, *Twitter and Tear Gas: The Power and Fragility of Networked Protest* (New Haven, CT: Yale University Press, 2017).
10. Jonathan Pinckney and Miranda Rivers, “Sickness or Silence: Social Movement Adaptation to COVID-19,” *Journal of International Affairs* 73, no. 2 (2020).
11. Elvin Ong, “Online Repression and Self-Censorship: Evidence from Southeast Asia,” *Government and Opposition* 56 (2021): 141–62.
12. Gene Sharp, *The Politics of Nonviolent Action* (Boston, MA: Porter Sargent, 1973).
13. Gene Sharp, *Waging Nonviolent Struggle: 20th Century Practice and 21st Century Potential* (Boston, MA: Porter Sargent, 2005); and Robert L. Helvey, *On Strategic Nonviolent Conflict: Thinking About the Fundamentals* (Boston, MA: Albert Einstein Institute, 2004).
14. Milan W. Svolik, *The Politics of Authoritarian Rule* (New York: Cambridge University Press, 2012).
15. Erica Chenoweth and Maria J. Stephan, *Why Civil Resistance Works: The Strategic Logic of Nonviolent Conflict* (New York: Columbia University Press, 2011).
16. Sharon Erickson Nepstad, “Mutiny and Nonviolence in the Arab Spring: Exploring Military Defections and Loyalty in Egypt, Bahrain, and Syria,” *Journal of Peace Research* 50, no. 3 (2013): 337–49; Jaclyn Johnson and Clayton L. Thyne, “Squeaky Wheels and Troop Loyalty: How Domestic Protests Influence Coups d’État, 1951–2005,” *Journal of Conflict Resolution* 62, no. 3 (2018): 597–625; and Holger Albrecht and Dorothy Ohl, “Exit, Resistance, Loyalty: Military Behavior During Unrest in Authoritarian Regimes,” *Perspectives on Politics* 14, no. 1 (2016): 38–52.
17. Chenoweth and Stephan, *Why Civil Resistance Works*; and Kevin Koehler, Dorothy Ohl, and Holger Albrecht, “From Disaffection to Desertion: How Networks Facilitate Military Insubordination in Civil Conflict,” *Comparative Politics* 48, no. 4 (2016): 439–57.
18. Anika Locke Binnendijk and Ivan Marovic, “Power and Persuasion: Nonviolent Strategies to Influence State Security Forces in Serbia (2000) and Ukraine (2004),” *Communist and Post-Communist Studies* 39, no. 3 (2006): 419.
19. Ches Thurber, “Social Ties and the Strategy of Civil Resistance,” *International Studies Quarterly* 63, no. 4 (2019): 974–86.
20. Feldstein, *Rise of Digital Repression*.
21. Andrea Kendall-Taylor, Erica Frantz, and Joseph Wright, “The Digital Dictators: How Technology Strengthens Autocracy,” *Foreign Affairs*, March/April 2020, www.foreignaffairs.com/articles/china/2020-02-06/digital-dictators.
22. Xiaoyan Chen and Pen Hwa Ang, “The Internet Police in China: Regulation, Scope and Myths,” in *Online Society in China: Creating, Celebrating, and Instrumentalising the Online Carnival*, ed. David Kurt Herold and Peter Marolt (New York: Routledge, 2011), 45.
23. 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 (2013): 326–43.
24. Jonathan Sullivan, “China’s Weibo: Is Faster Different?,” *New Media & Society* 16, no. 1 (2014): 24–37; and Bei Qin, David Strömberg, and Yanhui Wu, “Why Does China Allow Freer Social Media? Protests versus Surveillance and Propaganda,” *Journal of Economic Perspectives* 31, no. 1 (2017): 117–40.
25. Elizabeth C. Economy, “The Great Firewall of China: Xi Jinping’s Internet Shutdown,” *The Guardian*, June 29, 2018, www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown; Freedom House, “China: Freedom on the Net 2020 Country Report,” Freedom House, www.freedomhouse.org/country/china/freedom-net/2020; and Qin, Strömberg, and Wu, “Why Does China Allow Freer Social Media?”

26. Margaret E. Roberts, *Censored: Distraction and Diversion Inside China's Great Firewall* (Princeton, NJ: Princeton University Press, 2018).
27. William R. Hobbs and Margaret E. Roberts, "How Sudden Censorship Can Increase Access to Information," *American Political Science Review* 112, no. 3 (2018): 621–36; and Yuyu Chen and David Y. Yang, "The Impact of Media Censorship: 1984 or Brave New World?," *American Economic Review* 109, no. 6 (2019): 2294–2332.
28. Margaret Roberts also observes that by permitting some VPN usage, the CCP bifurcates elites operating beyond censorship and the masses living within it. In this way, the CCP "drives a wedge between the elite and the masses," preventing core-periphery linkages that could generate regime-threatening collective action (*Censored*, 8).
29. Rebecca MacKinnon, "China's 'Networked Authoritarianism,'" *Journal of Democracy* 22, no. 2 (2011): 32–46.
30. Gary King, Jennifer Pan, and Margaret E. Roberts, "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument," *American Political Science Review* 111, no. 3 (2017): 484–501.
31. Rongbin Han, "Manufacturing Consent in Cyberspace: China's 'Fifty-Cent Army,'" *Journal of Current Chinese Affairs* 44, no. 2 (2015): 105–34.
32. Daniela Stockmann and Mary E. Gallagher, "Remote Control: How the Media Sustain Authoritarian Rule in China," *Comparative Political Studies* 44, no. 4 (2011): 436–67.
33. Steven Feldstein, "The Road to Digital Unfreedom: How Artificial Intelligence Is Reshaping Repression," *Journal of Democracy* 30, no. 1 (2019): 40–52.
34. Roberts, *Censored*.
35. Qin, Strömberg, and Wu, "Why Does China Allow Freer Social Media?"
36. Paul Triolo and Samm Sacks, "Shrinking Anonymity in Chinese Cyberspace," Center for Strategic and International Studies, September 26, 2017, www.csis.org/analysis/shrinking-anonymity-chinese-cyberspace.
37. Roberts, *Censored*, 109–10.
38. Joyce Liu and Xiqing Wang, "In Your Face: China's All-Seeing State," BBC News, 2017, www.bbc.com/news/av/world-asia-china-42248056.
39. Josh Chin and Clément Bürge, "Twelve Days in Xinjiang: How China's Surveillance State Overwhelms Daily Life," *Wall Street Journal*, December 9, 2017, www.wsj.com/articles/twelve-days-in-xinjiang-how-chinas-surveillance-state-overwhelms-daily-life-1513700355; and Xiao Qiang, "The Road to Digital Unfreedom: President Xi's Surveillance State," *Journal of Democracy* 30, no. 1 (2019): 53–67.
40. Xu Xu, "To Repress or To Co-Opt? Authoritarian Control in the Age of Digital Surveillance," *American Journal of Political Science* 65, no. 2 (2020): 309–25.
41. Triolo and Sacks, "Shrinking Anonymity in Chinese Cyberspace"; Qiang, "Road to Digital Unfreedom: President Xi's Surveillance State"; and Kendall-Taylor, Frantz, and Wright, "Digital Dictators."
42. Genia Kostka, "China's Social Credit Systems and Public Opinion: Explaining High Levels of Approval," *New Media & Society* 21, no. 7 (2019): 1565–93.
43. Qiang, "Road to Digital Unfreedom: President Xi's Surveillance State," 60.
44. Seva Gunitsky, "Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability," *Perspectives on Politics* 13, no. 1 (2015): 42–54.
45. Xiao Qiang, "The Battle for the Chinese Internet," *Journal of Democracy* 22, no. 2 (2011): 47–61; Peter Lorentzen, "China's Strategic Censorship," *American Journal of Political Science* 58, no. 2 (2014): 402–14; Nele Noesselt, "Microblogs and the Adaptation of the Chinese Party-State's Governance Strategy," *Governance* 27, no. 3 (2014): 449–68; and Sullivan, "China's Weibo."
46. Jennifer Pan and Kaiping Chen, "Concealing Corruption: How Chinese Officials Distort Upward Reporting of Online Grievances," *American Political Science Review* 112, no. 3 (August 2018): 602–20.
47. Ashley Esarey and Xiao Qiang, "Digital Communication and Political Change in China," *International Journal of Communication* 5 (2011): 298–319.
48. Teresa Wright, "Protest as Participation: China's Local Protest Movements," *World Politics Review*, April 6, 2013, www.worldpoliticsreview.com/articles/12877/protest-as-participation-chinas-local-protest-movements; and Teresa Wright, *Handbook of Protest and Resistance in China* (Northampton, MA: Edward Elgar, 2019).
49. Guobin Yang, *The Power of the Internet in China: Citizen Activism Online* (New York: Columbia University Press, 2009).
50. As Ronald Deibert quips, "Why would a government bother building its own surveillance machine when the private sector already provides one?" "The Road to Digital Unfreedom: Three Painful Truths About Social Media," Journal of Democracy 30, no. 1 (January 2019): 35.
51. Nicole Kobie, "The Complicated Truth About China's Social Credit System," *Wired UK*, July 2019, www.wired.co.uk/article/china-social-credit-system-explained.
52. Qiang, "Battle for the Chinese Internet"; and Lorentzen, "China's Strategic Censorship."

53. Human Rights Watch, “World Report 2021: Rights Trends in China,” January 2021, www.hrw.org/world-report/2021/country-chapters/china-and-tibet.

54. MacKinnon, “China’s ‘Networked Authoritarianism’”; Darrel Robinson and Marcus Tannenberg, “Self-Censorship of Regime Support in Authoritarian States: Evidence from List Experiments in China,” *Research & Politics* 6, no. 3 (July 1, 2019); and Freedom House, “China: Freedom on the Net 2020 Country Report.”

55. Sarah Wu Zhou Joyce, “Editing History: Hong Kong Publishers Self-Censor Under New Security Law,” Reuters, July 14, 2020, www.reuters.com/article/us-hongkong-security-publishers-idUSKCN24F09P.

56. MacKinnon, “China’s ‘Networked Authoritarianism,’” 33.

57. Ronald J. Deibert et al., eds., *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (Cambridge, MA: MIT Press, 2010); Karina Alexanyan et al., “Exploring Russian Cyberspace: Digitally-Mediated Collective Action and the Networked Public Sphere,” Research Publication no. 2012-2, Berkman Klein Center for Internet & Society, Harvard University, March 2012, https://cyber.harvard.edu/publications/2012/exploring_russian_cyberspace; and Sergey Sanovich, Denis Stukal, and Joshua A. Tucker, “Turning the Virtual Tables: Government Strategies for Addressing Online Opposition with an Application to Russia,” *Comparative Politics* 50, no. 3 (2018): 435–54.

58. Sanovich, Stukal, and Tucker, “Turning the Virtual Tables,” appendix.

59. Andrei Soldatov and Irina Borogan, *The Red Web: The Struggle Between Russia’s Digital Dictators and the New Online Revolutionaries*, reprint ed. (New York: PublicAffairs, 2015).

60. Human Rights Watch, “Online and On All Fronts: Russia’s Assault on Freedom of Expression,” July 18, 2017, www.hrw.org/report/2017/07/18/online-and-all-fronts/russias-assault-freedom-expression; Sanovich, Stukal, and Tucker, “Turning the Virtual Tables”; and Human Rights Watch, “Russia: Growing Internet Isolation, Control, Censorship,” June 18, 2020, www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship.

61. Jan Lindenau, “Russia’s Sovereign Internet Law Comes into Force,” *Moscow Times*, November 1, 2019, www.themoscowtimes.com/2019/11/01/russias-sovereign-internet-law-comes-into-force-a68002. See also Anton Troianovski, “China Censors the Internet. So Why Doesn’t Russia?,” *New York Times*, February 21, 2021, www.nytimes.com/2021/02/21/world/europe/russia-internet-censorship.html.

62. Soldatov and Borogan, *Red Web*, 195–205.

63. Alina Polyakova and Chris Meserole, “Exporting Digital Authoritarianism: The Russian and Chinese Models” (Washington, DC: Brookings Institution, August 2019); and Human Rights Watch, “Russia: Growing Internet Isolation, Control, Censorship.”

64. *Moscow Times*, “Twitter, Facebook Blacklisted in Russia’s Telegram Ban,” April 27, 2018, www.themoscowtimes.com/2018/04/27/twitter-facebook-blacklisted-in-russias-telegram-ban-a61281.

65. Polyakova and Meserole, “Exporting Digital Authoritarianism”; Kendall-Taylor, Frantz, and Wright, “Digital Dictators”; and Human Rights Watch, “Russia: Growing Internet Isolation, Control, Censorship.”

66. Grigory Levchenko, “Slow Down, Twitter Roskomnadzor Throttles Twitter over Failure to Remove ‘Illegal Content,’” Meduza, March 10, 2021, www.meduza.io/en/feature/2021/03/10/slow-down-twitter.

67. Miriam Elder, “Hacked Emails Allege Russian Youth Group Nashi Paying Bloggers,” *The Guardian*, February 7, 2012, www.theguardian.com/world/2012/feb/07/hacked-emails-nashi-putin-bloggers; Adrian Chen, “The Agency,” *New York Times*, June 2, 2015, www.nytimes.com/2015/06/07/magazine/the-agency.html; and Gunitsky, “Corrupting the Cyber-Commons.”

68. Sanovich, Stukal, and Tucker, “Turning the Virtual Tables.” See also Peter Pomerantsev, “The Kremlin’s Information War,” *Journal of Democracy* 26, no. 4 (2015): 40–50; and Kendall-Taylor, Frantz, and Wright, “Digital Dictators.”

69. Denis Stukal et al., “For Whom the Bot Tolls: A Neural Networks Approach to Measuring Political Orientation of Twitter Bots in Russia,” *SAGE Open* 9, no. 2 (2019); and Denis Stukal et al., “Bots for Autocrats: How Pro-Government Bots Fight Opposition in Russia” (working paper, University of Sydney, 2019), www.denisstukal.com/uploads/8/4/7/0/84708866/stukal_et_al__2020__bots_for_autocrats.pdf.

70. Denis Stukal et al., “Detecting Bots on Russian Political Twitter,” *Big Data* 5, no. 4 (2017): 310–24.

71. Anton Sobolev, “How Pro-Government ‘Trolls’ Influence Online Conversation in Russia” (paper presented at the NYU Jordan Center for the Advanced Study of Russia, New York, February 12, 2021).

72. On Crimea, Soldatov and Borogan, *Red Web*, 278–85. On the United States, Chen, “The Agency”; and US Senate Select Committee on Intelligence, “Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Vol. 2,” Report 116–290 (Washington, DC: Government Publishing Office, 2020), www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

73. Todd C. Helmus et al., *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe* (Santa Monica, CA: RAND Corporation, 2018), www.rand.org/pubs/research_reports/RR2237.html.

74. Deibert et al., *Access Controlled*; and Andrei Soldatov and Irina Borogan, “Putin Trolls Facebook: Privacy and Moscow’s New Data Laws,” *Foreign Affairs,* November 3, 2015, www.foreignaffairs.com/articles/russian-federation/2015-11-03/putin-trolls-facebook.

75. Soldatov and Borogan, *Red Web*, 216–20; Polyakova and Meserole, “Exporting Digital Authoritarianism”; and Human Rights Watch, “Russia: Growing Internet Isolation, Control, Censorship.”
76. Human Rights Watch, “Online and On All Fronts.”
77. Andrei Soldatov and Irina Borogan, “Putin Brings China’s Great Firewall to Russia in Cybersecurity Pact,” *The Guardian*, November 29, 2016, www.theguardian.com/world/2016/nov/29/putin-china-internet-great-firewall-russia-cybersecurity-pact.
78. Human Rights Watch, “Online and On All Fronts.”
79. Although directly identifying information is theoretically required to acquire the cell phone numbers used for social media verification, in practice this requirement can be skirted.
80. Polyakova and Meserole, “Exporting Digital Authoritarianism.”
81. Valentin Weber, “Why China’s Internet Censorship Model Will Prevail Over Russia’s,” Council on Foreign Relations, December 12, 2017, www.cfr.org/blog/why-chinas-internet-censorship-model-will-prevail-over-russias.
82. Anton Troianovski et al., “Russia Protesters Defy Vast Police Operation as Signs of Kremlin Anxiety Mount,” *New York Times*, January 31, 2021, www.nytimes.com/2021/01/31/world/europe/russia-protests-navalny-live-updates.html; and Kat Lonsdorf, “Social Media Fueled Russian Protests Despite Government Attempts to Censor,” NPR, January 24, 2021, www.npr.org/2021/01/24/960113653/social-media-fueled-russian-protests-despite-government-attempts-to-censor.`
83. Joshua Yaffa, “The Russians Protesting Putin in Their Personal Lives,” *New Yorker*, March 4, 2021, www.newyorker.com/news/a-reporter-at-large/the-russians-protesting-putin-in-their-personal-lives.
84. Feldstein, *Rise of Digital Repression*.
85. Freedom House, “Iran: Freedom on the Net 2019 Country Report,” www.freedomhouse.org/country/iran/freedom-net/2019; and Freedom House, “Saudi Arabia: Freedom on the Net 2019 Country Report,” www.freedomhouse.org/country/saudi-arabia/freedom-net/2019.
86. Adrian Shahbaz, “The Rise of Digital Authoritarianism,” Freedom House, 2018, www.freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism; and Feldstein, *Rise of Digital Repression*.
87. Steven Feldstein, “The Global Expansion of AI Surveillance,” Carnegie Endowment for International Peace, September 2019, https://carnegie endowment.org/files/WP-Feldstein-AISurveillance_final1.pdf; and Polyakova and Meserole, “Exporting Digital Authoritarianism.”
88. Feldstein, “Global Expansion of AI Surveillance.” For a specific example, see Bill Marczak et al., “Champing at the Cyberbit: Ethiopian Dissidents Targeted with New Commercial Spyware,” Research Report no. 102, The Citizen Lab, University of Toronto, December 6, 2017, www.citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware.
89. *Final Report of the National Security Commission on Artificial Intelligence* (Washington, DC: National Security Commission on Artificial Intelligence, 2021), https://reports.nscai.gov/final-report/table-of-contents.
90. Feldstein, *Rise of Digital Repression*, 201.
91. See resources such as the “Surveillance Self-Defense,” Electronic Frontier Foundation (www.ssd.eff.org), or “Security-in-a-Box,” Front Line Defenders (www.securityinabox.org/en).
92. China and Russia are increasing their domestic capacity in this regard, but elite US programs continue to significantly outperform them. Prashant Loyalka et al., “Computer Science Skills across China, India, Russia, and the United States,” *PNAS* 116, no. 14 (2019): 6732–36.
93. Majken Jul Sorensen, “Humor as a Serious Strategy of Nonviolent Resistance to Oppression,” *Peace & Change* 33, no. 2 (2008): 167–90.
94. Srdja Popovic, *Blueprint for Revolution: How to Use Rice Pudding, Lego Men, and Other Nonviolent Techniques to Galvanize Communities, Overthrow Dictators, or Simply Change the World* (New York: Spiegel & Grau, 2015).
95. Binnendijk and Marovic, “Power and Persuasion.”

ABOUT THE INSTITUTE

The United States Institute of Peace is a national, nonpartisan, independent institute, founded by Congress and dedicated to the proposition that a world without violent conflict is possible, practical, and essential for US and global security. In conflict zones abroad, the Institute works with local partners to prevent, mitigate, and resolve violent conflict. To reduce future crises and the need for costly interventions, USIP works with governments and civil societies to help their countries solve their own problems peacefully. The Institute provides expertise, training, analysis, and support to those who are working to build a more peaceful, inclusive world.

BOARD OF DIRECTORS

Members Ex Officio

THE UNITED STATES INSTITUTE OF PEACE PRESS

Since its inception in 1991, the United States Institute of Peace Press has published hundreds of influential books, reports, and briefs on the prevention, management, and peaceful resolution of international conflicts. All our books and reports arise from research and fieldwork sponsored by the Institute's many programs, and the Press is committed to expanding the reach of the Institute's work by continuing to publish significant and sustainable publications for practitioners, scholars, diplomats, and students. Each work undergoes thorough peer review by external subject experts to ensure that the research and conclusions are balanced, relevant, and sound.

OTHER USIP PUBLICATIONS

- *Processes of Reintegrating Central Asian Returnees from Syria and Iraq* by William B. Farrell, Rustam Burnashev, Rustam Azizi, and Bakhtiyar Babadjanov (Special Report, July 2021)
- *Democracy in Afghanistan: Amid and Beyond Conflict* by Anna Larson (Special Report, July 2021)
- *Nonviolent Action and Transitions to Democracy: The Impact of Inclusive Dialogue and Negotiation* by Véronique Dudouet and Jonathan Pinckney (Peaceworks, July 2021)
- *National Dialogues in Peacebuilding and Transitions: Creativity and Adaptive Thinking* edited by Elizabeth Murray and Susan Stigant (Peaceworks, June 2021)
- *Nigeria's State Peacebuilding Institutions: Early Success and Continuing Challenges* by Darren Kew (Special Report, June 2021)

UNITED STATES
INSTITUTE OF PEACE PRESS

2301 Constitution Avenue NW
Washington, DC 20037
(202) 457-1700
www.USIP.org