SPECIAL REPORT

NO. 506 | FEBRUARY 2022 UNITED STATES INSTITUTE OF PEACE www.usip.org

Nonviolent Action in the Era of Digital Authoritarianism: Hardships and Innovations

By Matthew Cebul and Jonathan Pinckney

Rohingya Muslim refugees look at a phone in Bangladesh in January 2018. Unrestricted hate speech on Facebook fueled ethnic cleansing in Myanmar. (Photo by Manish Swarup/AP)

Contents

Summary

- Although emergent technologies and online activism initially empowered nonviolent campaigns, activists are now challenged by authoritarian regimes armed with enhanced digital repression technologies.
- Interviews in nine countries reveal how activists are adapting to the new reality of sophisticated digital authoritarianism. Activists have made significant technical and organizational innovations, from routinizing end-to-end encryption and virtual private networks to adopting decentralized movement structures.
- Nevertheless, significant obstacles remain. Activists struggle with the trade-off between digital security and convenience, the difficulty in movement-level coordination, and the digital landscape's ever-increasing technical complexity.
- Nonviolent activists are also struggling to confront powerful international technology companies that aid, whether through indifference or incompetence, digital autocrats in their repressive efforts.
- International supporters must both accelerate the pace of activists' digital adaptations and obstruct autocratic innovation. Priority issues include rectifying geographic inequities in access to training, building cross-national activist networks, and tightening regulation to prevent the further diffusion of digital repression technologies.

United States Institute of Peace
Making Peace Possible

SPECIAL REPORT

NO. 506 | FEBRUARY 2022

ABOUT THE REPORT

This report examines how activists engaged in nonviolent action are adapting to the use of emergent technologies by authoritarian regimes. Based on interviews with twenty-five leading activists from nine countries, 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*, 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.

© 2022 by the United States Institute of Peace

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. 506. First published 2022.

ISBN: 978-1-60127-887-6

UNITED STATES
INSTITUTE OF PEACE PRESS

Belarusian opposition supporters shine smartphone lights during a rally in Independence Square in Minsk, Belarus, on August 20, 2020. (Photo by Dmitri Lovetsky/AP)

Introduction

Emergent technologies have transformed twenty-first-century nonviolent action. Following breathtaking advances in digital communication and the global expansion of internet access, activists have embraced emergent technologies to mobilize, organize, and amplify their demands. These technologies have enabled activists to rapidly coordinate decentralized, leaderless movements linked to both national peripheries and international audiences, to dramatically expose human rights abuses previously cloaked in plausible deniability, and to nurture vibrant civic discourses in online ecosystems liberated from traditional media gatekeepers.[1] One is hard pressed to identify a contemporary nonviolent campaign that does not have a sizable online footprint. From Hong Kong to South Sudan to Venezuela and beyond, virtual space is a defining arena for nonviolent action.

These advantages of online activism were especially pronounced in the period surrounding the Arab Spring—early, youthful adopters quickly mastered the digital domain, leaving autocrats scrambling to contain unexpected outbursts of dissent.[2] Some persist. Yet these euphoric early days gave way to digital repression, restricted online freedoms, and democratic backsliding. As documented in an earlier report by the US Institute of Peace and in a growing literature on digital authoritarianism, most activists now confront technologically savvy regimes armed with digital censorship, surveillance, and misinformation techniques.[3] These more sophisticated digital autocracies are muzzling online critics, infiltrating opposition forums, monitoring activists both online and offline, and crafting legal and pseudo-legal architectures to coerce tech companies to facilitate repression.

Problems of convenience, movement-level coordination, and uncertainty about the ever-evolving digital security landscape leave activists vulnerable to digital repression. These problems are exacerbated by significant inequality of access to digital security training.

The world's autocracies are rapidly adapting to the digital era, evidenced by a steady drumbeat of arrests for online activism and diminishing digital rights across the globe.[4]

How are nonviolent activists weathering this storm, and what can they do to emerge stronger on the other side? This report documents how activists are adapting to new forms of digital repression, drawing on interviews with twenty-five activists from nine countries.[5] These activists are mobilizing around a wide variety of issues and with different levels of experience—some are young digital rights activists, others seasoned advocates of democratization struggles, still others local-level peacebuilders.[6] Their accounts illuminate the challenges activists face across a range of digital autocracies, from high-capacity regimes such as Russia and China to countries such as South Sudan or Bangladesh where the government has only recently adopted some of the key elements of digital repression.

The interviews highlighted three key trends:

- Activists have discovered many creative adaptations to the new reality of digital authoritarianism. Digital security measures are more common and better understood among activists today than even just a few years ago. More activists have adopted technologies, organizational structures, and community practices to communicate more securely, remain resilient in the face of digital repression, and continue to push for change. Some are even using advanced emergent technologies to further their activism in innovative ways.

- However, activists confront stubborn difficulties in adapting to digital authoritarianism and struggle to keep pace with sophisticated security regimes. Problems of convenience, movement-level coordination, and uncertainty about the ever-evolving digital security landscape leave activists vulnerable to digital repression. These problems are exacerbated by significant inequality of access to digital security training: activists in high-priority countries and urban areas enjoy easy access, whereas similarly at-risk activists in more marginal settings are neglected.

- Activists are fighting on multiple fronts, against not only repressive regimes but also tech companies that often prove indifferent or even hostile to their needs. Social media is an indispensable asset for activists, yet identity requirements and nontransparent, algorithmic content moderation stifle activism on such platforms. Likewise, tech companies profit from the sale of counterterror surveillance technology yet cynically shirk responsibility when autocrats wield these tools to silence dissidents.

To meet these challenges, activists and their international supporters need to accelerate the pace of activist innovation and obstruct the proliferation of digital repression technologies. Doing so will help tip the technological balance away from autocrats and back toward the nonviolent action campaigns that challenge them, thereby promoting the peace, democracy, and social justice that those movements aim to achieve.

Activists Adapt to Digital Repression

The digital authoritarian toolkit, in which authoritarian regimes use emergent technologies to engage in censorship, surveillance, and misinformation, initially caught many activists by surprise. Flush with optimism over the ways in which digital technology empowered activists to reach millions with a keystroke, most spoke of their initial assessments of these technologies as strictly positive. As one Russian activist put it, "Without the internet, we wouldn't have a civil society."

This appreciation for digital activism stemmed in large part from repressive regimes' lack of technical expertise. Many approached the internet not just with indifference but also with active disdain, an attitude that left some of their ground-level personnel comically incompetent. For instance, an activist from Iran told a story about a friend who about a decade ago was interrogated for hours by police over the identity of a mysterious conspirator named Sarvar whom, they alleged, he had been discussing with a friend. After much confusion, the police produced the ostensibly incriminating emails, and the arrested activist realized that the interrogators had mistaken the term *server* for a female Persian name.

Yet, as documented extensively, most autocrats quickly learned from their early blunders, often in the aftermath of social media–fueled mass uprisings.[7] The 2009 Green Revolution in Iran, Arab Spring uprisings in 2010 and 2011, and protests in Russia after the 2011 legislative elections were particularly prominent wake-up calls. China, which developed a high degree of technical capacity and control early on, was the innovative pioneer that other high-capacity autocrats sought to emulate. States such as Russia and Iran have leveraged new technology to enact comprehensive regimes of censorship, surveillance, and misinformation. High-profile arrests brought home the necessity of adaptation to nearly all activists from these countries.

In countries with less-developed digital repression infrastructure, the necessity for adaptation has been less apparent. Unconcerned by their governments' rudimentary technical capacity, many activists continued to neglect even the basics of online digital hygiene, let alone comprehensive digital security protocols. Yet even in these countries, recent changes have given many activists cause to rethink their practices. An environmental activist from Bangladesh reported that few of their colleagues had previously thought seriously about online security. Passage of the country's Digital Security Act in September 2018 and several instances in which regimes surveilled and publicized embarrassing private content from prominent activists has led these colleagues to radically change how they interact with the internet. Similarly, activists from South Sudan reported that they had only recently shifted to more secure digital platforms after instances of hacking smartphones and social media accounts.

Major revelations of advanced surveillance technologies have also shaped the adaptation conversation. In particular, many activists expressed concern about the Pegasus Project, which exposed the Israeli security firm NSO Group's sale of their signature software to many authoritarian governments, which used it to surveil activists and opposition politicians.[8] Whereas most phishing attacks require that the target click a link or open an email, Pegasus infects private electronic devices without any user action. Many activists mentioned Pegasus, and though most expressed confidence that their governments did not have the resources to widely deploy exploits like it, they pointed to it as an example of the increasingly pernicious tools of digital repression that autocrats have at their disposal.

Some activists also resisted the idea of responding to digital repression by implementing improved security practices, and a few pushed back against the idea of countering government surveillance at all. One digital security trainer pointed to a culture of martyrdom, or a feeling that evading surveillance was tacitly admitting to doing something wrong, and stressed the need to shift the conversation among activists from one focused on not having done anything wrong to one focused on how digital security preserves activist resilience for the long term. Yet even those who resented the necessity of doing so pointed to a slow adoption of specific tools to thwart digital repression.

The result of these processes has been a major uptick in interest in digital security and an evolving set of innovative adaptations to digital authoritarianism. The extent of their behavioral changes varied significantly, but all activists acknowledged the importance of adapting to new tools of digital repression and identified ways they have done so. As one interviewee put it:

> Before, say you had a workshop for activists and had two breakout sessions, one on fundraising and one on digital security. Back then, you'd have everybody in fundraising and nobody in digital security. But now, because this is increasingly a matter of life and death, you really see people learning about digital tools. Today, that workshop would maybe be 70 percent of people in fundraising and 30 percent in digital security.

TECHNICAL ADAPTATIONS

The first set of adaptations entails technical shifts in the tools, platforms, and devices that activists use to mobilize and coordinate their actions. Much of this process seeks to address the challenge of legibility—communications that "the state can readily access and interpret."[9] Emergent technology makes the social and political world legible to authoritarian regimes, enabling them to comprehensively observe it with ease. Activists have thus sought to shift their technical practices into avenues that are illegible to potential government observers.

One key step is to transition from social media and communications platforms that can be easily censored or surveilled toward those that are kept private through robust encryption. Forms of online communication that employ end-to-end encryption (E2EE) are standard practice for most activists in more challenging environments, though they remain relatively rare in environments with less extreme government repression. Activists reported that many of the most prominent E2EE tools, such as the messaging platform Signal or the email service ProtonMail, are common among activist circles in their countries. Many activists report switching back and forth between these platforms for sensitive internal communications and more popular platforms such as WhatsApp or Facebook Messenger for less sensitive external communications.

Another important adaptation has been more consistent use of virtual private networks (VPNs). When a user connects to the internet through a VPN, the user's data goes from their computer to a third-party server via an encrypted connection. The third-party server then connects to the website or service the user wants to access and sends the data back to the user through that same encrypted connection. It thus prevents external parties from surveilling or censoring a user's web traffic. Because VPN servers are often located in other countries, they can also help users access international websites that their government censors domestically. All the Russian activists interviewed for this report, for instance, consider using a VPN to be basic standard

Protesters look at their smartphones in Hong Kong on June 12, 2019. Virtual space is a defining arena for nonviolent action, and open anonymous online forums such as LIHKG have served as crucial organizing platforms. (Photo by Kin Cheung/AP)

practice and do so every time they connect to the internet. An Iranian activist reported that "inside Iran, 99 percent of activists use a VPN."

A third common technical adaptation has been in changing data storage practices. Activists reported that their most serious vulnerability was if the security forces detained them or one of their activist colleagues and thus gained possession of their phone or computer. With the physical device in hand, security forces were typically able to coerce activists into unlocking devices and subsequently access sensitive communication records and organizational documents. Activists reported several technical avenues to address this situation. One activist in Russia reported that they fully wiped their device of all messages and data every three days. This is an extreme approach, but many activists reported similar adaptations, turning on settings on messaging apps that would automatically delete messages, storing data solely on encrypted cloud servers rather than on physical devices, and fully wiping their device if they felt themselves to be in any imminent danger of arrest. Software that permitted remote deletion or codes to quickly delete data from the lock screen were also important.

NONTECHNICAL ADAPTATIONS

Perhaps even more important than technical adaptations have been nontechnical adaptations—modifications in movement-level practices and patterns of action that make activists more resilient to the challenges that digital authoritarianism poses.

For instance, the pro-democracy movement in Hong Kong, in addition to adopting many of the technical adaptations described, has also radically reshaped the movement's structure. Whereas early communication moved outward from a small set of well-identified leaders to the broader movement, the need to guard against digital repression has led to a more diffuse, decentralized structure. Now, most movement activity takes place in open anonymous online forums such as the Reddit-like LIHKG. These discussions use in-group language and tricks of Cantonese phrasing to distinguish movement participants from government saboteurs attempting to infiltrate the discussion. This shift has led to a radically horizontal movement structure in which tactics and strategy must be generally accepted by all participants. It has also enabled continued (though reduced) activism even in the face of severe government physical and digital repression.[10]

Although activists are becoming more conscientious about online security, interviewees frequently expressed reservations about their efforts to adapt to digital authoritarianism.

Hong Kong activists have blended this decentralized, anonymous online discussion board structure with an increase in in-person local activism as well, building networks in their neighborhoods that do not rely on digital mediation and thus are more difficult for the government to observe.

Several activists similarly described a meticulous focus on having "nothing to hide" as one of their key nontechnical adaptations. They take all the technical steps they can to frustrate government surveillance and censorship efforts but treat any online communication, even on the most secure channels, as something that could be surveilled and used against them.

Another key nontechnical adaptation is increasing social pressure among activist groups about the importance of digital security. Many groups, particularly those working against the most sophisticated digital autocrats, discussed developing detailed security protocols, which were a common topic of conversation among themselves and their activist colleagues. "It's the first thing I think about when I wake up in the morning," one democracy activist and digital security trainer said. An activist from Russia reported that they kept up their digital security protocols using a combination of lighthearted social shaming and hard professional consequences. "The first time we see somebody breaking the security protocol, usually by leaving a laptop open when they're not using it, then they have to buy everybody in the office pizza. The second time, they get fired."

Ongoing Challenges of Digital Security

Although activists are becoming more conscientious about online security, interviewees frequently expressed reservations about their efforts to adapt to digital authoritarianism. Four general and persistent challenges that movements face in the digital era emerge from their concerns.

SECURITY-CONVENIENCE TRADE-OFF

The first challenge is an issue commonly known as the *security-convenience trade-off*. More effective security measures tend to be more cumbersome and less user-friendly, and therefore less likely to be widely adopted by volunteer movement participants.

Perhaps the clearest example of the trade-off is the use of VPNs. As described earlier, many activists in especially repressive contexts use VPNs religiously. Others, however, neglected VPNs because they were difficult to access, slow, and seemingly unnecessary for "nonsensitive" online activity.[11] Similarly, many activists report that although Signal is more secure than Telegram and WhatsApp, they still prefer WhatsApp's functionality and have yet to fully migrate from older services. Several respondents also observed that anonymous chat groups are safer than identifiable ones, yet make participants more uncomfortable and less trusting, which discourages their use. These concerns pale in comparison to the rigors of a comprehensive security protocol, which can include routine data wipes, disposable "burner" phones, complex passwords,

encrypted drives, careful separation of activist and non-activist online personas, and plans for remote data destruction in the event of arrest, among other measures.

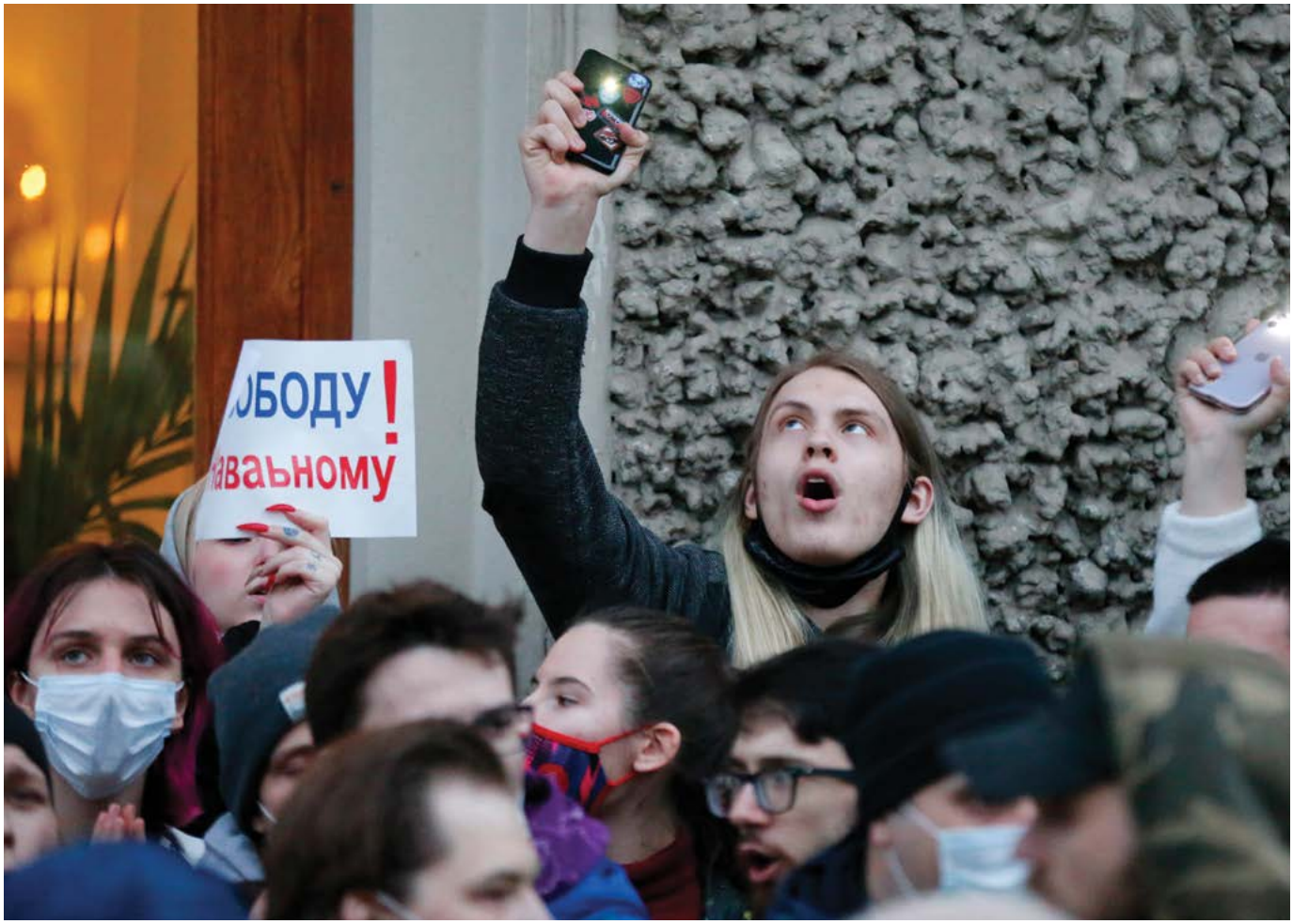
Some of the reluctance to adopt effective security protocols stems from group-level path dependency—activists need to engage with mass audiences and thus cannot easily transition from established platforms toward newer, more secure options that have yet to develop large user bases. But much of the problem is simple convenience. For instance, one Russian activist bemoaned the fact that some of his colleagues continue to use Mail.ru and Yandex, Russian-owned email and internet search providers with clear ties to the Kremlin, even though secure options like ProtonMail are readily available. Others discussed their efforts to convince friends and fellow activists to embrace new platforms or security practices, sometimes to little avail—as one digital security trainer from Iran quipped, "Activists just want to push a button and have everything solved." User desire for convenience continues to hinder the adoption of best security practices.

MOVEMENT-LEVEL COORDINATION

Closely related to the security-convenience trade-off is the problem of *movement-level coordination*: although digital security starts with individuals, campaign security is a collective endeavor, and activists may be only as secure as their least-secure colleague.

The heart of this concern is the aforementioned legibility challenge. As we live more and more of our lives online, civic processes that were previously too subtle to notice or too complex to parse are now faithfully documented in friend lists, group memberships, geolocated photos, chat records, and search histories. Repressive regimes, especially those armed with advanced surveillance and automated data processing technologies, can exploit this data to identify and penetrate entire activist networks. One unwitting user's unlocked phone or hacked account may compromise many activists—as one Hong Kong activist grimly joked, "If I drop my phone, everyone on my team can go to hell." Interviewees recounted harrowing episodes of regimes detaining activists, compelling them to unlock their devices, and then using the acquired information to build cases and track down more activists. One activist described the hacking of the Facebook group he co-administered, which temporarily gave police control over the group even though the other administrators were secure. These anecdotes help explain some respondents' frustration with others' failure to effectively safeguard their data. As the same Hong Kong activist asserted, careless colleagues are effectively "committing a team kill."

Unfortunately, this coordination problem has no quick solutions. Widespread public adoption of best security practices would improve collective movement security, but in many countries digital hygiene standards are still lacking and slow to change. Within movements, activists can compartmentalize their contacts to limit the damage from any one breach, forging disconnected local networks within cities or neighborhoods. Indeed, decentralized mass movements naturally lend themselves toward this structure, though compartmentalization imposes coordination problems of its own and interviewees did not often mention it. More recently, many activists have embraced self-deleting messages in Signal, Instagram, and other platforms to avoid leaving a record on others' devices. These measures are helpful, but ultimately can only partially mitigate the risks of interconnected online activism.



People hold signs reading "Freedom for Navalny!" and shine smartphone lights during a rally in support of jailed opposition leader Alexei Navalny in Moscow on April 21, 2021. (Photo by Alexander Zemlianichenko/AP)

COMPLEXITY AND UNCERTAINTY

A third challenge is the inherently complex and evolving nature of digital technology, which generates uncertainty among both activists and the public, and leaves activists struggling to understand and implement best practices.

Digital technology develops rapidly, often behind closed corporate doors, and the legal landscape remains murky. Apps and programs that are safe one day are compromised or blocked the next; regimes acquire new surveillance and censorship capabilities; apps change their privacy settings or terms of service; and companies grow more willing to cooperate with new local cybersecurity laws. Several Russian activists noted that the legal aspect is especially challenging because the Kremlin is rapidly reforming laws governing online speech, leaving activists uncertain about how they will be enforced in practice. Digital security basics can be found in many online guides, such as those provided by the Electronic Frontier Foundation (EFF), the Citizen Lab, Paradigm Initiative, and Security First's Umbrella app.[12] Yet these guides are often not translated for local languages and contexts and may not be accessible or even known to activists in countries where they are most needed. Moreover, the technical complexity of digital privacy techniques and the sheer volume of material can impose a steep learning curve on activists without a background in computer science.

Lacking authoritative sources on these matters, activists may struggle to stay up to date. Uncertainty and disagreement among activists about best security practices is common. For example, some respondents reported concerns about WhatsApp's lack of security and data sharing practices even as others contended that the platform is encrypted and safe.[13] An Iranian digital rights activist explained that confusion over even basic computer jargon made it difficult to assist Iranian activists trying to connect to a secure server.

A key aspect of this uncertainty is that activists usually learn that their security measures are vulnerable only after they have failed. In this respect, activists are often unfortunately reactive, not proactive. For instance, respondents learned to distrust Facebook groups or abandon infiltrated Telegram or WhatsApp groups only after those group's administrators (in some cases their own accounts) had been hacked. By the same token, because activists usually cannot directly observe covert regime surveillance or hacking attempts in real time, they can never be fully confident that they have done enough to protect themselves from surveillance. The cognitive burden of uncertainty weighs heavily even on those activists who take all the recommended precautions.

One common response to this lack of knowledge is education and training programs. Some respondents had participated in digital security training and mastered the basics. Yet such training has limited reach—untrained respondents expressed concerns about their relative ignorance on the subject, and almost everyone wanted more guidance. Moreover, digital security training tended to reinforce inequities in activist access to the international community. Well-known groups in high-priority countries such as Russia can access training essentially at will, but those in countries such as South Sudan only rarely had access to digital security guidance. These access problems are exacerbated by worsening repression in that local digital rights groups restrict their outreach to activists they know and can vet to protect in-country trainers from regime surveillance.

INCREASING GOVERNMENT CAPACITY

Last, the challenges described are all magnified by steadily growing regime capacity for digital repression. Despite significant variation in technical competence across countries, most regimes are making up for lost time, increasing the pressure on a generation of digitally native activists that were once accustomed to nearly free rein over virtual space.[14] Today's Iranian activists—in stark contrast to a decade ago, when the regime was unfamiliar with digital tech—fear its cunning and devious digital surveillance program, which targets both local and diaspora activists. An Iranian activist living abroad described how Iranian officials had sought to entrap her with messages from her detained brother's phone. In late 2020, Iran also engaged in advanced phishing efforts in Sweden with a malware app ostensibly designed to help Persian speakers obtain a local driver's license.[15]

Nor is this escalating digital crackdown limited to Iran. A Russian activist recounted that, ten years ago, Russians of all stripes fearlessly posted on Facebook about anti-Putin protests. Now, he and other activists worry about the Kremlin's tightening enforcement of digital speech and censorship laws, facilitated by ubiquitous SORM (System of Operational-Investigatory Measures) surveillance that has essentially unfettered access to unencrypted Russian internet traffic, alongside the regime's growing capacity to block or throttle traffic from both international websites

and even VPNs. In Nicaragua, physical repression is coupled with a new (January 2021) cybercrimes law, which criminalizes any purportedly false or distorted news spread online, forcing activists underground. In South Sudan, to avoid National Security Service surveillance, activists do not speak about sensitive matters over the phone.[16] Repressive regimes are also learning how to undermine common digital security tools, such as by blocking VPN providers or by intercepting two-factor authentication codes sent via SMS message. Still, the most worrisome repressive tool remains the most low-tech as regimes forcibly compel detained activists to unlock their devices and then identify other activists to target for arrest.

In sum, truly free online civic space is growing scarce, inducing a chilling effect among activists. The most glaring recent example is Hong Kong, where activists in 2020 frantically scrubbed their social media accounts in response to a new security law. Many Russian activists have fled the country. Although diaspora activists still operate online, they cannot join physical in-country protests, and some even limit their contact with activists remaining in Russia out of security concerns. Regardless, few of the activists interviewed expressed confidence that they could protect themselves online, and most are resigned to the idea that their governments could eventually break into their private lives if they decided to do so. Nor do regimes need to enact total crackdowns to trigger this chilling effect, as one Hong Kong activist explained: just one arrest per month is enough to scare activists into self-censorship. That many courageously accept the risks as a necessary sacrifice for activism makes them no less concerning.

Big Tech: Ally or Adversary?

Beyond hostile governments, activists also face challenges from international tech companies. These firms wield immense power to shape the possibilities of online activism, a reality that looms large in the minds of almost all those interviewed. As one activist and digital security trainer profanely put it, "The first thing I think when I wake up in the morning is what the f—— did Facebook do today?" Big Tech has historically prioritized its profits over activists' safety and aspirations, and its actions are often harmful to nonviolent campaigns.

Others have written extensively on human rights and Big Tech in the digital era.[17] The following section highlights two main difficulties for activists: social media content moderation and the rapid proliferation of digital surveillance technologies.

SOCIAL MEDIA CONTENT MODERATION

Who is permitted to say what online is of vital importance for twenty-first-century nonviolent action. In this respect, social media companies have become governments unto themselves, delimiting freedom of speech across a diversity of social and political contexts but with little accountability in place for even egregious mistakes. Although content moderation poses an exceptional challenge under the best circumstances, Silicon Valley tech entrepreneurs have been—and largely remain—tragically ill-equipped to manage the ethical and moral responsibilities associated with content moderation.

Paradoxically, social media companies engage in both too little and too much content moderation. On the former, Facebook has rapidly expanded to many countries about which the company

Social media companies often accede to regime demands to remove opposition content, making them directly complicit in autocratic repression. This practice is shockingly routine and often occurs in response to private requests.

lacks even rudimentary cultural awareness, let alone dedicated staff fluent in local languages. As a result, Facebook consistently fails to police genuinely violent content. For instance, it failed to restrict a deluge of anti-Rohingya hate speech in Myanmar that fueled the ethnic cleansing campaign there, and to control hate speech in Ethiopia during an ongoing civil war, in both cases because the company lacked local language support and despite repeated internal warnings. Ethiopian activists sent Excel spreadsheets full of offending posts to Facebook for removal, often receiving no response or, in some cases, replies asking for English translations.[18]

On the latter, examples of unjustifiable censorship are so numerous as to defy comprehensive recording.[19] The problem has only worsened as social media giants, overwhelmed by the enormous volume of daily posts, shift to algorithmic content moderation that incorporates systematic biases. Facebook has blocked pro-Palestinian posts that its censors mistakenly associate with terrorism; meanwhile, YouTube's anti-violence censors are purging video evidence, posted by activists, of the Assad regime's war crimes.[20] Recently, Facebook empowered a new body, the Oversight Board, that has reversed some of its censorship decisions. Yet the millions of wrongful removals that go unresolved dwarf the Oversight Board's limited time and resources for appeals.[21]

Moreover, social media companies often accede to regime demands to remove opposition content, making them directly complicit in autocratic repression. This practice is shockingly routine and often occurs in response to private requests. For instance, Facebook CEO Mark Zuckerberg personally authorized censoring opposition content ahead of Vietnam's party congress in January, and Google and Apple recently succumbed to pressure to remove opposition leader Alexei Navalny's Smart Voting app on the day of Russia's 2021 elections.[22] That such censorship is antithetical to liberal democratic values is indisputable. Yet social media companies frequently bend to respect local law (thereby preserving market access), even when local law is plainly at odds with international human rights law.

Content moderation at scale is a challenge with no straightforward solution. Automated censorship may curtail outbursts of hate speech but also inadvertently censor genuine activist content. For that reason, the European Union's ongoing efforts to hold social media companies liable for content may backfire: companies may impose egregiously strict censorship to avoid legal exposure, thereby curtailing activists' global reach.[23] What is clear, however, is that social media giants have leapt into new markets with too little regard for potential safety concerns and all too often put their desire for profits ahead of the human rights of their activist users. That the Santa Clara Principles for content moderation—a relatively low bar—have been fully met only by Reddit suggests that activists' fundamental mistrust of Big Tech is well-placed.[24]

SURVEILLANCE TECHNOLOGIES

Another major concern is the sale of dual-use technologies to regimes that directly facilitate violent repression. The most prominent recent example is Israel's NSO Group and its Pegasus spyware, which is ostensibly sold for counterterrorism purposes but is actually linked to the illicit surveillance of thousands of noncriminal targets by repressive regimes.

That said, the root of the problem is more mundane than bleeding-edge zero-click exploits. For years, the dual-use technology required for basic content filtering and surveillance has been sold by private corporations to brutal dictatorships, in some cases with the direct endorsement of the United States and other liberal Western democracies.[25] This has enabled regimes that have no domestic tech industry to nevertheless develop enhanced digital repressive capacity. Among many other examples, the military regime in Myanmar has used Western surveillance equipment to crush ongoing opposition to the recent coup.[26] South Sudan relies on Israeli surveillance technology to monitor its citizens.[27] And Belarus used deep-packet inspection technology from the Canadian company Sandvine to blacklist opposition websites during its 2020 presidential election.[28]

In most of these democracies, trade in dual-use technology is purportedly regulated under existing law. Yet, as evidenced by the rapid spread of Western surveillance technology to the world's autocracies, these regulations are weak, easily bypassed, and poorly enforced.[29] Private industry has thus facilitated the global proliferation of digital repressive technologies, to activists' detriment.

ADVOCATING FOR DIGITAL RIGHTS

In response to these challenges, activists have embraced the need for transnational advocacy in defense of digital rights. Modern social movements cannot abandon online activism, so activists are investing considerable effort to push back against Big Tech's complicity with digital authoritarianism.

To start, activists work to appeal unjustified content moderation. Sometimes activists leverage personal ties with well-connected individuals in the tech industry or with journalists acting as conduits between activists and social media teams. For instance, in 2010, Google employee Wael Ghonim was able to use his clout as an employee of a major tech firm to quickly undo Facebook's block on the "We Are All Khaled Saeed" page he administered, a major forum for discussing politics and police violence in Egypt, named after a young man beaten to death by police earlier that year.[30] Similarly, one South Sudanese activist reported that he routinely communicates with Facebook to identify malicious users and help activists resolve problems. In other cases, broad transnational advocacy campaigns emerge to contest systematic abuse, often mobilizing on the offending platforms themselves, such as Palestinian campaigns against Facebook censorship.[31]

This system of redress is hardly ideal in that it privileges well-connected users with both English fluency and ties to US tech firms. One South Sudanese activist reported that he had been unable to get Facebook to either restore access to or remove his old account that regime agents had hacked. As mentioned, most user appeals of erroneous algorithmic censorship go unprocessed, and Facebook's failures in Myanmar and Ethiopia further evidence the limits of activist outreach to social media companies. Nevertheless, persistent crowdsourced feedback is an essential tool in defense of users' rights.

At a broader level, the need to advocate for digital rights has encouraged newfound specialization among activists around these issues. Some of the respondents interviewed for this report self-identified as digital rights activists and have dedicated themselves to preserving the internet as a space for free expression and social change. Those who did not have specialized technical skills often reported knowing someone or some group who did to whom they could turn

Wael Ghonim, center, walks into Tahrir Square in Cairo after Egyptian President Hosni Mubarak's televised statement to the nation on February 10, 2011. Ghonim used his tech firm connections to quickly undo a Facebook block. (Photo by Tara Todras-Whitehill/AP)

for assistance. Their efforts are paralleled by the activities of international organizations such as the EFF, Citizen Lab, the Paradigm Initiative, and many others that have formed durable working partnerships with activist communities, offering technical advice and training, documenting the global spread of spyware and other abusive practices, and lobbying both Big Tech and global governments for needed reforms.

These are welcome developments, suggesting that activist communities are steadily developing the knowledge, capacity, and international linkages required to combat digital authoritarianism. However, the playing field is still far from level because activists are competing against comparatively well-resourced repressive governments that also lobby Big Tech. These companies have demonstrated a willingness to comply with takedown requests and access restrictions to preserve market share despite activist outcry. Others knowingly sell advanced surveillance equipment to dictatorships for profit and cynically shirk responsibility when that technology is inevitably used to repress peaceful activists. As discussed in the following recommendations, public pressure has had some notable successes in compelling tech companies to change their behavior. Many of their dealings occur outside public view, however, and isolated victories absent broader regulation are an inadequate check on Big Tech's excesses.

Policy Recommendations: Accelerating Activist Innovations

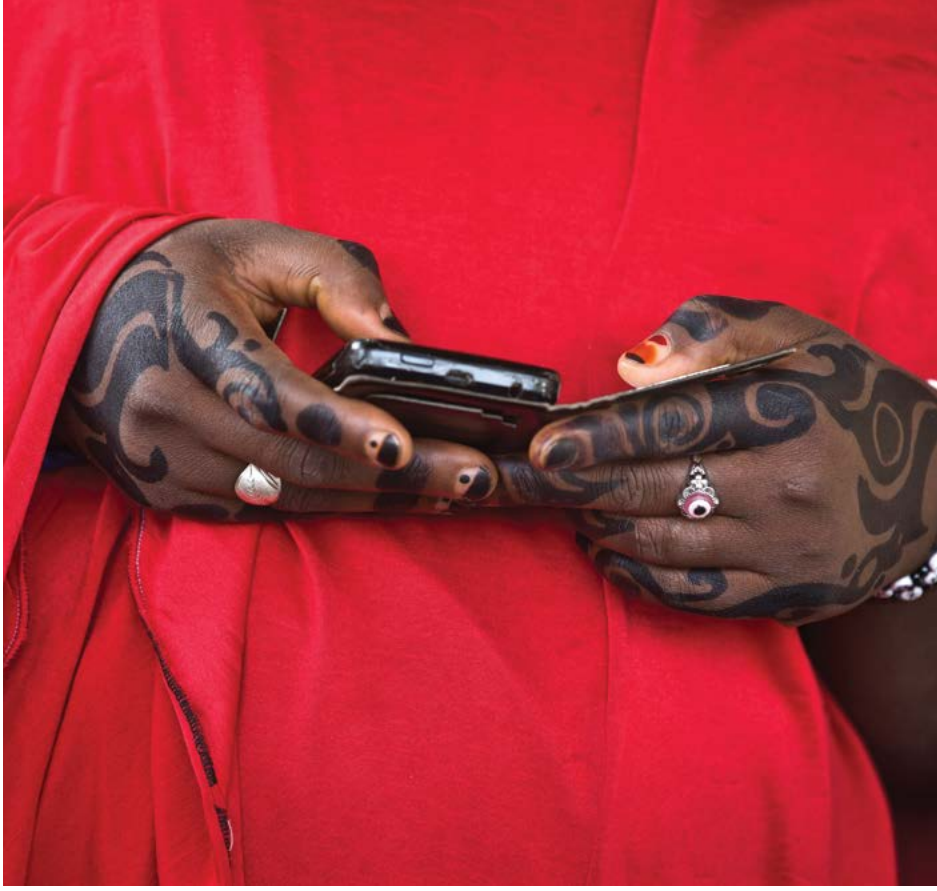
The dynamics described here are a snapshot in time of a broader process, that of the ever-changing balance of digital capabilities between activists and autocrats. In account after account, activists describe how the rapid pace of technological change has both favorably and unfavorably shifted this balance of power. Activists are highly motivated to innovate and often the first to recognize the advantages of new technologies. Authoritarian opponents may only belatedly appreciate this potential; yet once they recognize the threat, they marshal superior resources to erase activists' initial advantage, requiring a new cycle of tactical and technological innovation for activists to regain parity, if not the upper hand. This technological balance between activists and autocrats is constantly evolving. Thus, the rise of digital authoritarianism is not a one-and-done event, but is instead an ongoing process of interaction and learning among activists, autocrats, and tech companies.

In this light, rising to the challenge of digital authoritarianism requires action on two parallel fronts. First, activist communities and their international backers should strive to quicken the pace of movement innovation in response to digital opportunities and constraints. Second, the United States and other liberal democracies should make it a priority to obstruct, punish, and otherwise slow the pace of autocratic innovation in digital repressive technologies.

ACCELERATING ACTIVIST ADAPTATIONS TO EMERGENT TECHNOLOGY

An essential response to increasingly sophisticated digital authoritarianism is to improve activists' ability to quickly innovate and adapt to new challenges. Notably, short-term recommendations or technical fixes for immediate problems are necessary but inadequate. Certain standard recommendations are uncontroversial, such as using end-to-end encryption, password managers, and reliable VPNs that do not log traffic and regularly shift across servers. Yet even these come with contextual caveats. One digital security expert highlighted that their activist training always begins with a careful contextual analysis, a holistic view of how that group operates. A myopic focus on technical recommendations can come dangerously close to victim blaming, criticizing activists for not adopting specific tools yet eliding the many political, social, and psychological pressures that shape their choices.

Moreover, any specific recommendations will inevitably be made obsolete by events, in this realm even more rapidly than most. Even in the short term, autocrats are taking steps to counter the technical adaptations described in this report, for instance, by seeking to regulate VPN usage, as a 2017 Russian VPN law does, or by isolating their domestic internet from the global internet, as Iran does. In the longer term, technological advances just over the horizon will almost certainly disrupt the balance of power between autocrats and activists. Scalable quantum computers, which could emerge within the next decade, would likely render existing encryption obsolete overnight, imperiling activists' digital security but also empowering activists seeking to uncover hidden evidence of



A woman from the Hausa tribe looks at her smartphone on March 28, 2015, at a polling station in Daura, Nigeria. In response to violence across Nigeria's northwest and central states, governors blocked telecommunications in many areas across five states to enable military operations. (Photo by Ben Curtis/AP)

government abuse.[32] Advances in artificial intelligence may soon allow authoritarian governments to sift through enormous volumes of surveillance data, identifying patterns that reveal activists. Improvements in blockchain technology could make cryptocurrency (currently unavailable to most activists because of technical barriers) an easy way of fundraising outside government surveillance. Easily accessible, low-latency satellite internet service could decentralize internet access points, thereby crippling autocratic censorship and surveillance.

A more detailed examination of these new technologies is beyond the scope of this report. Any one of these innovations has the potential to radically shift the technological ground on which activists and autocrats compete in multiple, unpredictable ways.[33] Instead, this report emphasizes that what activists need is not a specific technical response to today's challenges, but rather shifts in the activist ecosystem to accelerate learning and adaptation to the rapid pace of technological change, for both today and the days to come.

One way to achieve this acceleration is greater diffusion of training in basic digital security and strategic thinking about digital threats. Various forms of digital repression will eventually come to prominence in almost every country, yet, as noted, global inequities in who can access digital security training are significant. International efforts have focused on a handful of high-profile countries, such as Russia and Iran, whose activist communities are now saturated with digital security knowledge, even as activists in more peripheral or lower capacity autocracies have little to no access. A Western and English-speaking bias in the digital activism and security space is also a major hindrance to the spread of digital innovation through activist communities.

In this vein, international efforts should focus on expanding training beyond "priority" countries most closely associated with digital authoritarianism and to countries where this challenge is still latent. A concerted effort to translate digital security knowledge into more languages would go far toward accelerating the pace of activist learning. Moreover, these efforts should move beyond a simple "information dump" training model. A crash course on digital security basics is only one small part in a larger strategy of accelerating activist adaptation to digital authoritarianism. Instead, international actors should pursue holistic training that not only covers the fundamentals of good digital hygiene but also considers how digital activism connects with

Digital activism and repression are both largely made possible by technology companies based in Western democracies. . . . Decisions made in Silicon Valley boardrooms have spillover effects from Moscow to Managua.

real-world activism, critically interrogates current trends in digital activism and how they might change over time, and offers support for the psychological burdens associated with digital activism, among other valuable topics.

Another wise long-term investment for international actors is to facilitate the growth of robust transnational activist networks. As a Belarusian activist put it, "What we need is knowledge management and knowledge sharing. . . . When we were creating solutions in Belarus, we didn't even know where to ask. We had to build everything from scratch. If we could have gotten experience from other countries it would have saved us a lot of time and effort." As another activist and digital security trainer put it, "Knowing other activists' stories helps us know our mistakes faster and helps us strategize. It's a powerful motivator to know you're not alone."

Evidence is abundant that convening activists from a broad range of contexts to share stories and lessons learned is one of the most effective forms of external support.[34] Transnational activist networks have been crucial to many of the most important strategic developments in nonviolent action in recent decades.[35] The international community can help forge such networks, providing forums for discussion and learning about activism and digital security. The more comprehensive these networks, and the more readily information flows within them, the more likely it is that relevant innovations generated in one context can be rapidly adopted in another.

Separately, international donors and supporters of nonviolent action should better incorporate digital security as an essential component of all projects conducted in potentially repressive contexts. Several activists said that it was difficult to convince international funders to seriously consider the operational costs associated with basic digital security measures such as VPN licenses, secure computers and phones, or encrypted cloud storage. Funders should carefully assess the digital landscape with as much care as they would a country's political or economic landscape when choosing partners and designing programming. As a matter of course, external supporters for nonviolent action campaigns should scrutinize their own digital security to identify potential weak spots that leave their activist partners vulnerable.

STIFLING AUTOCRATIC INNOVATION

At the same time, international actors should also strive to restrain digital authoritarianism by denying autocrats access to the tools, technologies, and knowledge required to innovate new repressive techniques. Here, democratic states hoping to support the free, peaceful expression of grievances through nonviolent action have a crucial role to play. Digital activism and repression are both largely made possible by technology companies based in Western democracies, the most influential of which are in the United States. Decisions made in Silicon Valley boardrooms have spillover effects from Moscow to Managua.

In turn, intergovernmental coordination around strict, extensive, and well-enforced controls on the distribution of dual-use surveillance technology are essential. On this count, states have already taken some steps in the right direction. The European Union is working with clear determination to tighten its regulation of tech companies, most prominently through the Digital Services Act, which will likely become law in 2022.[36] The United States has also begun to take export

controls on dual-use technology more seriously, recently adding more tech companies (including Israel's NSO Group) to the Commerce Department's Entity List, which prohibits US companies from exporting technology to included parties, and adopting new regulations that bar the export of intrusion software and other cybersecurity technology without an approved license.[37]

Beyond aligning tech companies' financial incentives with basic human rights, tougher export controls could also launch a much-needed normative shift in US cybersecurity policy. For most of the past two decades, the United States has embraced privacy-invading tools in the name of counterterrorism, and at activists' expense. Moving forward, Washington should strive to cultivate new global norms of privacy and encryption, investing resources to improve access to encryption and anti-surveillance technology while conditioning foreign aid on state guarantees to abide by foundational principles of digital privacy. It should also engage with social media companies to encourage them to resist autocratic regimes' demands to remove critical content or provide users' identifying information in almost all circumstances. Although fully examining available policy measures is beyond the scope of this report, in general, the United States will ultimately be better off pursuing new norms of privacy and online freedom than in maintaining a status quo wholly incompatible with the pursuit of human rights in the digital era.

Last, public pressure is also an important source of leverage against obstinate corporations and repressive regimes alike. For example, recent public outcry about Sandvine's filtering technology enabling internet shutdowns in Belarus successfully pressured the company to end its contract with the Belarusian government.[38] Similarly, the combination of public outrage and government pressure in response to revelations about NSO Group's misdeeds led Israel to slash its permitted cyber export list to exclude a number of violent autocracies.[39] Various forms of external pressure can also be wielded directly against offending autocracies themselves, magnifying the "dictator's digital dilemma," in which digital repression leads to significant public backlash and loss of reputation.[40]

As the front lines of emergent technology shift in the coming years, the digital balance of power between repressive autocrats and the nonviolent activists who oppose them will change in unpredictable ways. Whatever new technologies the future brings, international actors can help tip the scales in favor of nonviolent activists, both by bolstering activists' strategic capacity to respond to technological advances and by hindering autocrats' ability to use emerging technologies to repress peaceful change. Following such a determined and coordinated effort, digital technologies may finally live up to their promise as the tools of mass liberation.

Notes

1. For an introduction to the literature on digital technology and mass protest, see Larry Diamond, "Liberation Technology," *Journal of Democracy* 21, no. 3 (2010): 69–83; Marc Lynch, "After Egypt: The Limits and Promise of Online Challenges to the Authoritarian Arab State," *Perspectives on Politics* 9, no. 2 (June 2011): 301–10; Jennifer Earl and Katrina Kimport, *Digitally Enabled Social Change: Activism in the Internet Age* (Cambridge, MA: MIT Press, 2013); Andrew T. Little, "Communication Technology and Protest," *Journal of Politics* 78, no. 1 (January 2016): 152–66; Nils B. Weidmann and Espen Geelmuyden Rød, *The Internet and Political Protest in Autocracies* (New York: Oxford University Press, 2019); Killian Clarke and Korhan Kocak, "Launching Revolution: Social Media and the Egyptian Uprising's First Movers," *British Journal of Political Science* 50, no. 3 (July 2020): 1025–45; Ruben Enikolopov, Alexey Makarin, and Maria Petrova, "Social Media and Protest Participation: Evidence From Russia," *Econometrica* 88, no. 4 (2020): 1479–514.
2. Wael Ghonim, *Revolution 2.0: The Power of the People Is Greater Than the People in Power* (New York: Houghton Mifflin Harcourt, 2012).
3. Matthew Cebul and Jonathan Pinckney, "Digital Authoritarianism and Nonviolent Action: Challenging the Digital Counterrevolution," Special Report no. 499, United States Institute of Peace, July 2021, www.usip.org/publications/2021/07/digital-authoritarianism-and-nonviolent-action-challenging-digital; Andrea Kendall-Taylor, Erica Frantz, and Joseph Wright, "The Digital Dictators," *Foreign Affairs*, February 2, 2020, www.foreignaffairs.com/articles/china/2020-02-06/digital-dictators; Steven Feldstein, *The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance* (New York: Oxford University Press, 2021).
4. Freedom House, "Freedom on the Net 2021: The Global Drive to Control Big Tech," 2021, www.freedomhouse.org/report/freedom-net/2021/global-drive-control-big-tech.
5. These include Bangladesh, Belarus, China (Hong Kong), Iran, Nicaragua, Nigeria, Russia, South Sudan, and Vietnam.
6. Given travel restrictions imposed by the COVID-19 pandemic, interviews were conducted over encrypted Zoom sessions. These interviews were conducted following Health Media Lab Institutional Review Board approval (Review #950USIP21). To protect the safety of the interviewees, all quotations are anonymous. Interviewees are identified only by nonspecific descriptions of their country and role.
7. Feldstein, *Rise of Digital Repression*; Adrian Shahbaz, "The Rise of Digital Authoritarianism," Freedom House, 2018, www.freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism; Cebul and Pinckney, "Digital Authoritarianism and Nonviolent Action."
8. Stephanie Kirchgaessner et al., "Revealed: Leak Uncovers Global Abuse of Cyber-Surveillance Weapon," *The Guardian*, July 18, 2021, www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus.
9. Legibility of digital communications is one of the two main challenges posed by emergent technologies for nonviolent movements. See Cebul and Pinckney, "Digital Authoritarianism and Nonviolent Action," 5–7.
10. See also Rachel Yeo, "What Is LIHKG and How Did It Become Go-to Forum for Hong Kong's Protesters?," *South China Morning Post*, August 3, 2019, www.scmp.com/news/hong-kong/society/article/3021224/hong-kong-protests-how-citys-reddit-forum-lihkg-has-become; or Nicolle Liu and Sue-Lin Wong, "How to Mobilize Millions: Lessons from Hong Kong," OZY, July 7, 2019, www.ozy.com/around-the-world/how-to-mobilize-millions-lessons-from-hong-kong/95354.
11. Interestingly, the spur to VPN adoption often appears to be government attempts to fully ban popular online content, such as Instagram or YouTube—see William R. Hobbs and Margaret E. Roberts, "How Sudden Censorship Can Increase Access to Information," *American Political Science Review* 112, no. 3 (August 2018): 621–36.
12. EFF, "Surveillance Self-Defense," https://ssd.eff.org/en; The Citizen Lab, "Security Planner," www.citizenlab.ca/category/research/tools-resources/security-planner; Security First, "What is Umbrella?," www.secfirst.org/umbrella; Paradigm Initiative, "Ayeta: A proactive toolkit for African digital rights actors," www.paradigmhq.org/programs/digital-rights/ayeta.
13. Facebook asserts that all WhatsApp messages are end-to-end encrypted, but media reports highlight previously undisclosed breaches of this encryption. See, for example, Peter Elkind, Jack Gillum, and Craig Silverman, "How Facebook Undermines Privacy Protections for its 2 Billion WhatsApp Users," *ProPublica*, September 8, 2021, www.propublica.org/article/how-facebook-undermines-privacy-protections-for-its-2-billion-whatsapp-users.
14. The rise of digital autocracies is explained in Cebul and Pinckney, "Digital Authoritarianism and Nonviolent Action."
15. Check Point Research, "Rampant Kitten: An Iranian Espionage Campaign," September 18, 2020, https://research.checkpoint.com/2020/rampant-kitten-an-iranian-espionage-campaign.
16. See also Amnesty International, "These Walls Have Ears: The Chilling Effect of Surveillance in South Sudan," February 2021, www.amnesty.org/en/documents/afr65/3577/2021/en/.
17. For helpful primers, see Rebecca MacKinnon, *Consent of the Networked: The Worldwide Struggle For Internet Freedom*, reprint edition (New York: Basic Books, 2013); Ronald J. Deibert, "The Road to Digital Unfreedom: Three Painful Truths About Social Media," *Journal of Democracy* 30, no. 1 (January 2019): 25–39; Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight*

for a Human Future at the New Frontier of Power (New York: PublicAffairs, 2019); Jillian C. York, *Silicon Values: The Future of Free Speech Under Surveillance Capitalism* (London: Verso, 2021).

18. See Euan McKirdy, "Facebook: We didn't do enough to prevent Myanmar violence," CNN, November 6, 2018, https://edition.cnn.com/2018/11/06/tech/facebook-myanmar-report/index.html; Eliza Mackintosh, "Facebook knew it was being used to incite violence in Ethiopia. It did little to stop the spread, documents show," CNN, October 25, 2021, www.cnn.com/2021/10/25/business/ethiopia-violence-facebook-papers-cmd-intl/index.html; Rishi Inyengar, "Facebook has language blind spots around the world that allow hate speech to flourish," CNN, October 26, 2021, www.cnn.com/2021/10/26/tech/facebook-papers-language-hate-speech-international/index.html.
19. York, *Silicon Values*.
20. Elizabeth Dwoskin and Gerrit De Vynck, "Facebook's AI Treats Palestinian Activists Like It Treats American Black Activists. It Blocks Them," *Washington Post*, May 28, 2021, www.washingtonpost.com/technology/2021/05/28/facebook-palestinian-censorship; Human Rights Watch, "Israel/Palestine: Facebook Censors Discussion of Rights Issues," October 8, 2021, www.hrw.org/news/2021/10/08/israel/palestine-facebook-censors-discussion-rights-issues.
21. Facebook likely makes hundreds of thousands of incorrect removal decisions every day. See Kristen Grind, "Inside 'Facebook Jail': The Secret Rules that Put Users in the Doghouse," *Wall Street Journal*, May 4, 2021, www.wsj.com/articles/inside-facebook-jail-trump-the-secret-rules-that-put-users-in-the-doghouse-11620138445.
22. Anton Troianovski and Adam Satariano, "Google and Apple, Under Pressure from Russia, Remove Voting App," *New York Times*, September 17, 2021, www.nytimes.com/2021/09/17/world/europe/russia-navalny-app-election.html; Elizabeth Dwoskin, Tory Newmyer, and Shibani Mahtani, "The case against Mark Zuckerberg: Insiders say Facebook's CEO chose growth over safety," *Washington Post*, October 25, 2021, www.washingtonpost.com/technology/2021/10/25/mark-zuckerberg-facebook-whistleblower.
23. Christopher Schmon, "European Parliament's Plans of a Digital Services Act Threaten Internet Freedom," Electronic Frontier Foundation, November 10, 2021, www.eff.org/deeplinks/2021/11/european-parliaments-plans-digital-services-act-threaten-internet-freedoms.
24. The Santa Clara Principles on Transparency and Accountability in Content Moderation, https://santaclaraprinciples.org.
25. See Steven Feldstein, "Governments Are Using Spyware on Citizens: Can They Be Stopped?," Carnegie Endowment for International Peace, July 21, 2021, www.carnegieendowment.org/2021/07/21/governments-are-using-spyware-on-citizens.-can-they-be-stopped-pub-85019; Siena Anstis, Sharly Chan, Adam Senft, and Ronald J. Deibert, "Annotated Bibliography: Dual-Use Technologies: Network Traffic Management and Device Intrusion for Targeted Monitoring," The Citizen Lab, September 2019, www.citizenlab.ca/wp-content/uploads/2019/09/Annotated-Bibliography-Network-Traffic-Management-and-Device-Intrusion-for-Targeted-Monitoring.pdf.
26. Hannah Beech, "Myanmar's Military Deploys Digital Arsenal of Repression in Crackdown," *New York Times*, March 1, 2021, www.nytimes.com/2021/03/01/world/asia/myanmar-coup-military-surveillance.html.
27. Amnesty International, "These Walls Have Ears."
28. Ryan Gallagher, "U.S. Company Faces Backlash After Belarus Uses its Tech to Block Internet," Bloomberg, September 11, 2020, www.bnnbloomberg.ca/u-s-company-faces-backlash-after-belarus-uses-its-tech-to-block-internet-1.1492656.
29. For more on companies marketing cyber-intrusion technologies to NATO adversaries, see Winnona DeSombre, Lars Gjesvik, and Johann Ole Willers, "Surveillance Technology at the Fair: Proliferation of Cyber Capabilities in International Arms Markets," Atlantic Council, November 2021, www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf.
30. Zeynep Tufekci, *Twitter and Tear Gas: The Power and Fragility of Networked Protest* (New Haven, CT: Yale University Press, 2017); York, *Silicon Values*.
31. For example, see Tell Facebook: Stop Silencing Palestine, www.stopsilencingpalestine.com.
32. See William Barker, William Polk, and Murugiah Souppaya. "Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms," NIST Cybersecurity White Paper, National Institute of Standards and Technology, April 28, 2021, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04282021.pdf.
33. See, for example, the many potential scenarios described in Miles Brundage et al., "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation," *ArXiv Preprint*, February 2018.
34. Erica Chenoweth and Maria J Stephan, *The Role of External Support in Nonviolent Campaigns: Poisoned Chalice or Holy Grail?* (Washington, DC: ICNC Press, 2021); Ray Salvatore Jennings, "Serbia's Bulldozer Revolution: Evaluating Internal and External Factors in Successful Democratic Breakthrough in Serbia," *CDDRL* working paper no. 105 (Stanford, CA: Sanford University, Center on Democracy, Development and the Rule of Law, 2009), https://cddrl.fsi.stanford.edu/publications/serbias_bulldozer_revolution_evaluating_internal_and_external_factors_in_successful_democratic_breakthrough_in_serbia.

35. Margaret E. Keck and Kathryn Sikkink, *Activists Beyond Borders: Advocacy Networks in International Politics* (Ithaca, NY: Cornell University Press, 1998); Valerie J. Bunce and Sharon L. Wolchik, *Defeating Authoritarian Leaders in Postcommunist Countries* (New York: Cambridge University Press, 2011).
36. Eliska Pirkova, "How the Digital Services Act Could Hack Big Tech's Human Rights Problem," Access Now, October 15, 2020, www.accessnow.org/eu-digital-services-act.
37. Drew Harwell, Ellen Nakashima, and Craig Timberg, "Biden Administration Blacklists NSO Group over Pegasus Spyware," *Washington Post*, November 3, 2021, www.washingtonpost.com/technology/2021/11/03/pegasus-nso-entity-list-spyware; Ellen Nakashima, "Commerce Department announces new rule aimed at stemming sale of hacking tools to Russia and China," *Washington Post*, October 20, 2021, www.washingtonpost.com/national-security/commerce-department-announces-new-rule-aimed-at-stemming-sale-of-hacking-tools-to-repressive-governments/2021/10/20/ecb56428-311b-11ec-93e2-dba2c2c11851_story.html.
38. Ryan Gallagher, "Francisco-Backed Sandvine Nixes Belarus Deal," *Bloomberg News*, September 15, 2020, www.bloomberg.com/news/articles/2020-09-15/sandvine-says-it-will-no-longer-sell-its-products-in-belarus.
39. Meir Orbach, "Israeli Defense Ministry slashes cyber export list, drops Saudi Arabia, UAE," *Calcalist*, November 25, 2021, www.calcalistech.com/ctech/articles/0,7340,L-3923361,00.html.
40. Feldstein, *Rise of Digital Repression*.

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

George E. Moose (Chair), Adjunct Professor of Practice, The George Washington University, Washington, DC • Judy Ansley (Vice Chair), Former Assistant to the President and Deputy National Security Advisor under George W. Bush, Washington, DC • Eric Edelman, Roger Hertog Practitioner in Residence, Johns Hopkins University School of Advanced International Studies, Washington, DC • Joseph Eldridge, Distinguished Practitioner, School of International Service, American University, Washington, DC • Stephen J. Hadley, Principal, Rice, Hadley, Gates & Manuel LLC, Washington, DC • Kerry Kennedy, President, Robert F. Kennedy Human Rights, Washington, DC • Ikram U. Khan, President, Quality Care Consultants, LLC, Las Vegas, NV • Stephen D. Krasner, Graham H. Stuart Professor of International Relations, Stanford University, Palo Alto, CA • John A. Lancaster, Former Executive Director, National Council on Independent Living, Potsdam, NY • Jeremy A. Rabkin, Professor of Law, Antonin Scalia Law School, George Mason University, Arlington, VA • J. Robinson West, Former Chairman, PFC Energy, Washington, DC • Nancy Zirkin, Executive Vice President, Leadership Conference on Civil and Human Rights, Washington, DC

Members Ex Officio

Antony J. Blinken, Secretary of State • Lloyd J. Austin III, Secretary of Defense • Michael T. Plehn, Lieutenant General, US Air Force; President, National Defense University • Lise Grande, President and CEO, United States Institute of Peace (nonvoting)

THE UNITED STATES INSTITUTE OF PEACE PRESS

Since 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. The Press is committed to advancing peace by publishing significant and useful works for policymakers, practitioners, scholars, diplomats, and students. In keeping with the best traditions of scholarly publishing, each work undergoes thorough peer review by external subject experts to ensure that the research, perspectives, and conclusions are balanced, relevant, and sound.

OTHER USIP PUBLICATIONS

- *China's Security Force Posture in Thailand, Laos, and Cambodia* by John Bradford (Special Report, December 2021)
- *Removing Sanctions on North Korea: Challenges and Potential Pathways* by Troy Stangarone (Special Report, December 2021)
- *Engaging with Muslim Civil Society in Central Asia: Components, Approaches, and Opportunities* by Sebastien Peyrouse and Emil Nasritdinov (Peaceworks, December 2021)
- *Advancing Global Peace and Security through Religious Engagement: Lessons to Improve US Policy* by Peter Mandaville and Chris Seiple (Special Report, November 2021)
- *Young and Angry in Fezzan: Achieving Stability in Southern Libya through Greater Economic Opportunity* by Mary Fitzgerald and Nate Wilson (Peaceworks, November 2021)

UNITED STATES
INSTITUTE OF PEACE PRESS

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