# TABLE OF CONTENTS

EXECUTIVE SUMMARY ........................................................................................................ III

BACKGROUND ...................................................................................................................... 6

METHODOLOGY .................................................................................................................... 6

STUDY QUESTIONS ................................................................................................................ 7

LITERATURE REVIEW .......................................................................................................... 7

INTRODUCTION ..................................................................................................................... 7

SECTION I: THE DIGITAL REPRESSION TOOLKIT ................................................................ 9

HOW AUTHORITARIAN REGIMES ARE USING DIGITAL TOOLS ........................................ 9

THE POLITICAL CONSEQUENCES OF DIGITAL REPRESSION ........................................... 16

SECTION II: UNDERSTANDING TRENDS AND VARIATION IN DIGITAL REPRESSION .... 19

DATA ..................................................................................................................................... 19

BASIC DATA TRENDS ......................................................................................................... 20

SECTION III: EXTERNAL FACTORS: STATES AND PRIVATE SECTOR ROLE IN SPREADING...

DIGITAL AUTOCRACY AUTHORITARIANISM ...................................................................... 25

STATE-LED SPREAD OF DIGITAL AUTHORITARIANISM ................................................... 25

UNDERSTANDING THE ROLE OF THE PRIVATE SECTOR IN DEMOCRACIES ............... 31

SYNTHESIS OF SUGGESTED POLICY RECOMMENDATIONS ........................................ 32

ANNEX I ............................................................................................................................... 37

TABLES AND FIGURES ....................................................................................................... 37

REFERENCES ......................................................................................................................... 41
## ACRONYMS

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AI</td>
<td>Artificial Intelligence</td>
</tr>
<tr>
<td>CCP</td>
<td>Chinese Community Party</td>
</tr>
<tr>
<td>CNAS</td>
<td>Center for a New American Security</td>
</tr>
<tr>
<td>DRG</td>
<td>Democracy, Human Rights, and Governance</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>LER</td>
<td>Learning, Evaluation, and Research</td>
</tr>
<tr>
<td>NORC</td>
<td>National Opinion Research Center at the University of Chicago</td>
</tr>
<tr>
<td>PRC</td>
<td>People’s Republic of China</td>
</tr>
<tr>
<td>SORM</td>
<td>System for Operative Investigative Activities</td>
</tr>
</tbody>
</table>
EXECUTIVE SUMMARY

The digital age changed the context in which authoritarian regimes operate. New technologies such as the Internet and social media reduced barriers to coordination, making it easier for ordinary citizens to mobilize and challenge unresponsive and repressive governments. Research shows that in the post-Cold War era protests have surpassed coups as the most common way that authoritarian leaders are ousted from office (Kendall-Taylor and Frantz, 2014). Authoritarian regimes, however, have adapted to this new challenge and learned to co-opt digital tools in ways that significantly shape political dynamics in their regimes.

First, autocracies that use digital repression face a lower risk of protests than do those autocratic regimes that do not employ these same tools. Digital repression not only decreases the likelihood that a protest will occur but also reduces the chances that a government will face large, sustained mobilization efforts. Second, dictatorships harness technology not only to suppress protests but also to enhance older methods of control. Data show that dictatorships that increase their use of digital repression also tend to increase their use of violent forms of repression “in real life,” particularly torture and the killing of opponents. This indicates that authoritarian leaders do not replace traditional repression with digital repression. Instead, by making it easier for authoritarian regimes to identify their opposition, digital repression allows them to fine-tune targeted repression. Finally, as autocracies have learned to co-opt new technologies, they have become a more formidable threat to democracy. Not only has the rising tide of technology seemingly benefited all dictatorships, but Kendall-Taylor, Frantz and Wright (2020) show that those authoritarian regimes that rely more heavily on digital repression are among the most durable. Between 2000 and 2017, 37 of the 91 dictatorships that had lasted more than a year collapsed; those regimes that avoided collapse had significantly higher levels of digital repression, on average, than those that fell.

There are myriad ways that digital tools support and, in many cases, enhance authoritarian regimes’ survival tactics. While in some cases digital tools supercharge long standing authoritarian strategies, in other cases these tools can have a transformative effect on a regime’s repressive capacity. We identify the following ways that autocrats are using digital repression:

Monitor citizens and identify dissidents. The advancement of AI-powered surveillance is the most significant evolution in digital authoritarianism. High-resolution cameras, facial recognition, spying malware, automated text analysis, and big-data processing have opened a wide range of new methods of citizen control, including those outside a government’s borders through transnational repression. Although surveillance has been a long-standing practice in authoritarian systems (and is present in democracies too given that surveillance can be used for legitimate as well as for coercive purposes), digital autocrats are using new technologies to monitor citizens and identify dissidents in a timely — and sometimes even preemptive — manner.

Monitor performance of regime elite, root out underperforming members. New technologies also afford authoritarian leaders greater control over members of the government. Authoritarian regimes are always vulnerable to threats from within, including coups and high-level elite defections. With the new digital tools, leaders can keep tabs on government officials, gauging the extent to which they advance regime objectives and rooting out underperforming officials who over time can tarnish public perception of the regime.
**Enhance ability to co-opt support.** Today’s technologies not only make it easier for governments to repress critics; they also make it easy to co-opt supporters. Technology-powered integration between government agencies allows the regime in the People’s Republic of China (PRC), for example, to more precisely control access to government services so that it can calibrate the distribution — or denial — of everything from bus passes and passports to jobs and access to education. In this way, new technologies help authoritarian regimes fine-tune their use of reward and refusal, blurring the line between co-opt and coercive control.

**Censorship.** Digital tools have supercharged authoritarians’ capacity for censorship. Recent advances in automated text analysis, machine learning techniques, and high-powered computing have reduced the costs of identifying critical users and censoring messages. While censorship allows leaders to regulate information flows, it is not without costs. Censorship can signal to citizens that the government has something to hide, reducing perceptions of legitimacy. It can also limit the regime’s ability to monitor the Internet and social media in ways that provide information about potential sources of discontent.

**Internet shutdowns.** Even if censorship fails and dissent escalates, digital autocracies have an added line of defense: they can block all citizens’ access to the Internet (or large parts of it) to prevent members of the opposition from communicating, organizing, or broadcasting their messages.

**Social manipulation and disinformation.** New technologies have improved their ability to do so. Tactics include trolling and harassing, including deliberately posting offensive content to provoke or disrupt conversations, and flooding. In the world of autocracies, the ability to manipulate the information environment is critical because it shapes citizens’ willingness to participate in protests and anti-regime activity (Kuran 1987). Technology increases the efficiency of autocrats’ efforts to drown out criticism and inflate perceptions of regime support, lowering the prospects for protest.

**Mimic elements of democracy.** Digital tools might even help regimes make themselves appear less repressive and more responsive to their citizens. In some cases, authoritarian regimes have deployed new technologies to mimic components of democracy, such as participation and deliberation, which could mitigate the bottom-up pressure that can destabilize authoritarian systems.

**Increase legibility of society.** Technology is also useful in preventing protest because it improves autocrats’ access to information about their citizens — historically a critical vulnerability in authoritarian systems. Known as the “dictator’s dilemma,” leaders in authoritarian systems typically have limited insight into the sentiment and views of their citizens because their use of repression reduces people’s willingness to communicate their beliefs. In many ways, technology alleviates this dilemma, allowing autocrats to identify and respond to (even cosmetically) sources of discontent before they spiral into something more threatening.

Although digital repression is more prevalent in authoritarian regimes than in democracies, its use has grown significantly in both settings since 2000. That said, political system type is one of the biggest predictors of where we will see digital repression: as states grow more democratic, their usage of digital repression declines. The relationship between levels of democracy and digital repression is linear and holds using a variety of measures of political system type.
Existing literature suggests that among state actors, the PRC and to a lesser extent Russia are the major players contributing to the spread of digital repression. Scholars are divided over the factors that drive the proliferation of the PRC’s digital tools. Existing assessments underscore that the drivers of this trend are complex, stemming from the expansion of the PRC geopolitical interests, the increasing market power of its technology companies, and conditions in recipient states, including high crime rates, that make PRC technology an attractive choice despite concerns about security and privacy. And while Russia’s brand of digital authoritarianism is not as technologically savvy as the PRC, it could prove to be readily adaptable and enduring. Many autocracies more closely resemble Russia than the PRC in that they did not build censorship into their systems from the start and lack the resources and in many cases the capacity to filter data and block content like Beijing. Likewise, many regimes prefer to uphold at least a veneer of democracy and prefer less overt approaches to digital repression, making Russia’s example of social manipulation and disinflation attractive.

All signs indicate that digital authoritarianism is likely to deepen around the globe, as more dictatorships obtain new technologies and grow more sophisticated in their ability to use them for repressive purposes. There are no easy answers for how to effectively push back against these developments. That said, existing literature emphasizes the importance of intensifying regulation of private companies, developing an international framework for dealing with the proliferation of dual-use digital technologies, strengthening civil society actors, developing products that protect human rights by design, and promoting a democratic model for managing the digital era.
BACKGROUND

USAID’s Center of Excellence on Democracy, Human Rights, and Governance (the DRG Center) is committed to advancing learning and evidence-based programming around all aspects of DRG policy, strategy, program development, implementation, and evaluation. Since 2015, the DRG Center has commissioned research through the Democratic Theories of Change Research Initiative to better understand democratic backsliding, democratic openings in authoritarian systems, and democratization as a means to build peace in conflict states.

Building on the insights from this initiative, this literature review will summarize key findings from the academic and gray literatures on the use of digital tools by authoritarian regimes. The lessons drawn from this literature review will be used to inform strategic planning, project and activity design, and implementation within the DRG community.

METHODOLOGY

This literature review summarizes key findings from existing academic and gray literature that focus on the digital tools, techniques, and tactics that autocracies1 employ to deepen and expand their control, as well as the role of external state and non-state actors. It includes country examples to illustrate any broader claims made. Lastly, it identifies gaps not addressed in the current literature regarding the study questions.

To ensure the literature review is comprehensive and includes all relevant studies, we adopted a multi-pronged strategy. First, we relied on the subject-matter expertise of the evaluation team, consisting of Dr. Andrea Kendall-Taylor and Dr. Erica Frantz, both of whom have written widely on topics related to how autocratic regimes use digital technologies to consolidate their rule. As a first pass, Dr. Kendall-Taylor and Dr. Frantz identified relevant studies pertaining to each of the key study questions that they were already familiar with. Second, from this set of initial “seed studies”, the authors reviewed i) the studies that they have been cited by, and ii) the studies that they cite, to identify potentially relevant research. (Note that the literature review does not include relevant studies if the research was not deemed academically rigorous.) The final strategy consisted of ad hoc searches through Google Scholar and other academic databases based on insights that emerged during the literature review and writing process. This was complemented with broader searches to flag any news and policy pieces that did not appear in academic outlets but are informative for understanding the study questions. Areas where these processes failed to identify studies and other work pertaining to the key study questions and outline below are identified as important gaps for future research to address.

In addition to reviewing the academic and gray literatures on digital authoritarianism, the study authors documented trends and variation in digital repression using data from the Digital Society Project, which produces a survey consisting of 35 questions, measuring a wide variety of aspects of the Internet’s intersection with politics around the world. The resulting data cover 179 countries from 2000 to 2019. Further details on the analysis of these data are provided below in “Section II: Understanding Trends and Variation in Digital Repression”.

---

1 For the purposes of this literature review, countries under analysis include those that are deepening autocracy or nominally democratic but backsliding into or towards autocracy.
STUDY QUESTIONS

The literature review addresses the following set of study questions:

1. **Types:** What digital tools, techniques, and tactics do authoritarian regimes use to deepen and expand their control?
   - a. How do these strategies vary by type of authoritarian regime (e.g. consolidated autocracy, electoral autocracy, authoritarian democracy)?
   - b. What is the universe of technologies that could be included under the “digital authoritarianism” heading?

2. **Internal Factors:** What factors influence the selection of digital tools, techniques, and tactics?
   - a. Do the types of technologies and tactics differ across actors (e.g. military, police, elected officials, or other entities in a position of power or authority)?
   - b. What other factors explain variation in the types of technologies and tactics used by authoritarian regimes to strengthen their rule? What is the role of a country’s legal/regulatory environment, income level, population, and level of local tech/engineering capacity? What is the role of regional trade and security alliances? Does the use of technologies and tools differ according to the type of extent to which a society, for instance is open or closed versus open societies?
   - c. Are actor motivations the same for every type of state actor?
   - d. How are actor motivations different in relatively open versus relatively closed societies?

3. **External Factors:** What role do external state and non-state actors (including private sector companies) play in enabling these techniques and tactics?
   - a. To what extent and how is technology, financial assistance, or in-kind support being used to support digital authoritarianism?
   - b. What safeguards are in place to prevent the technology from being used for these ends; how effective are they?

LITERATURE REVIEW

INTRODUCTION

Digital authoritarianism defines authoritarian regimes’ use of digital tools to supercharge longstanding survival tactics. In many cases this entails autocrats’ use of digital repression to control their citizens more effectively. But digital autocracies also use digital tools in ways that co-opt support, by enhancing regime performance, mimicking elements of democracy, and increasing the legibility of society to allow leaders to cosmetically respond to citizen demands in an effort to preempt discontent. Digital authoritarianism, therefore, is a broader concept than digital repression. At the same time, digital repression is not restricted to authoritarian settings. It can be employed by both democratic and autocratic governments, although democracies use digital repression less than their autocratic counterparts.
For the purposes of this discussion, digital repression refers to the use of new technologies — namely the Internet, social media, and Artificial Intelligence (AI) — to repress citizens and maintain political control (Frantz, Kendall-Taylor, and Wright, 2020). Feldstein (2021) similarly defines it as “the use of information and communications technology to surveil, coerce, or manipulate individuals or groups in order to deter specific activities or beliefs that challenge the state” (p. 25). It comes in a variety of forms, including simple tactics (such as Internet shutdowns) and more sophisticated techniques (such as disinformation campaigns on social media to discredit opponents, or AI-powered surveillance to track their activities).

On many fronts, digital repression is similar to traditional repression. The goal of both is to increase the costs of disloyalty and assist leaders in identifying their opponents and restricting their ability to mobilize against the regime. Digital repression differs from traditional repression, however, in important ways (Kendall-Taylor, Frantz, and Wright, 2020). Notably, digital repression decreases the costs of longstanding repressive tactics, while increasing their effectiveness. It supercharges traditional tactics for maintaining control by allowing governments to broaden their repressive approach so that they can target their opponents in a more precise fashion. Digital repression also differs from traditional repression in the speed with which governments can develop the capacity to execute it. In the past, cultivating an effective repressive apparatus with widespread boots-on-the-ground surveillance capacity entailed recruiting, training and arming thousands of loyal cadres. With digital tools, however, this sort of extensive manpower is no longer necessary to surveil and monitor citizens. Governments can simply import the capacity to digitally repress by buying desired technologies and training a small number of individuals in how to use them. In the digital age, developing an effective repressive apparatus is no longer restricted to a handful of competent dictatorships, suggesting that the repressive capabilities of today’s authoritarians are likely to expand in the years to come.

In this report, we review the existing literature on digital authoritarianism. We start by identifying how authoritarian regimes are using digital tools. In many ways, technology is supercharging longstanding authoritarian tactics. In other cases, these technologies and tools can have a transformative effect on a state’s capacity for repression. Building on our understanding of authoritarian regimes’ survival strategies, we document how digital tools can enhance their ability to maintain power. We include discussion of known effects of digital repression, including how it shapes a dictatorship’s repressive strategy (namely by enhancing the ability to fine-tune and target repression), reduces a dictatorship’s chances of being ousted in protest, increases the durability of dictatorships, and facilitates democratic backsliding in weak democracies.

In the second section, we offer data to illustrate the digital repression landscape. Here we show which countries in the world have the capacity for digital repression, as well as which countries are relying most on it. We examine the relationship between political system type and digital capacity and repression, before delving into how authoritarian regimes differ in their reliance on digital tools. We also explore whether indicators such as population, urbanization, and level of development are linked with digital capacity and repression.

Finally, we discuss how digital authoritarianism is spreading. We review the role of state actors, especially the PRC and Russia, which are the primary state drivers of the spread of digital authoritarianism. We also examine the role of private companies in democracies. We close by
summarizing existing policy recommendations proposed for dealing with the digital authoritarianism challenge.

SECTION I: THE DIGITAL REPRESSION TOOLKIT

The digital age changed the context in which authoritarian regimes operate. New technologies such as the Internet and social media reduced barriers to coordination, making it easier for ordinary citizens to mobilize and challenge unresponsive and repressive governments. Data from the Mass Mobilization Project and the Autocratic Regimes dataset, for example, reveal that between 2000 and 2017, 60 percent of all dictatorships faced at least one anti-government protest of 50 participants or more. Although many of these demonstrations were small and posed little threat to the regime, their sheer frequency underscores the continuous unrest that many authoritarian governments face from below.

Many of these movements are succeeding in bringing about the downfall of authoritarian regimes. In fact, protests have surpassed coups as the most common way that authoritarian leaders exit office (Kendall-Taylor and Frantz, 2014). Between 2000 and 2017, protests unseated ten autocracies, or 23 percent of the 44 authoritarian regimes that fell during the period. Another 19 authoritarian regimes lost power via elections. And while there were nearly twice as many regimes ousted by elections as by protests, many of the elections had followed mass protest campaigns.

The growing threat of protests has not been lost on today’s autocrats. In the past, when they feared coups, most such leaders relied on “coup proofing” tactics, such as overpaying the security services to win their loyalty or rotating elites through positions of power so that no one could develop an independent base of support. As protests have increased, however, authoritarian regimes have adapted their survival tactics to focus on mitigating the threat from mass mobilization. Data compiled by Freedom House reveal that since 2000, the number of restrictions on political and civil liberties globally has grown. A large share of this increase has occurred in authoritarian countries, where leaders impose restrictions on political and civil liberties to make it harder for citizens to organize and agitate against the state.

Beyond narrowing the space for civil society, authoritarian states are also learning to use digital tools to quell dissent. Although technology has helped facilitate protests, today’s digitally savvy authoritarian regimes are using some of the same technological innovations to push back against dangerous popular mobilizations. Digital tools allow autocrats to monitor personal communications, disrupt political organizing, and manipulate public conversations. In many ways, today’s digital autocracies are using technology — the Internet, social media, and AI — to supercharge long-standing authoritarian survival tactics. They are harnessing a new arsenal of digital tools to counteract what has become the most significant threat to the typical authoritarian regime today: the physical, human force of mass anti-government protests.

HOW AUTHORITARIAN REGIMES ARE USING DIGITAL TOOLS

Authoritarian regimes — as well as some aspiring autocrats — are using technology to accomplish a number of objectives that aid their survival strategies. We review the various ways that autocrats are using digital tools here.
Monitor citizens and identify dissidents

The advancement of AI-powered surveillance is the most significant evolution in digital authoritarianism. High-resolution cameras, facial recognition, spying malware, automated text analysis, and big-data processing have opened up a wide range of new methods of citizen control. Although surveillance has been a long-standing practice in authoritarian system (indeed, in democracies too given that surveillance can be used for legitimate as well as for coercive purposes), digital autocrats are using new technologies to monitor citizens and identify dissidents in a timely — and sometimes even preemptive — manner.

Feldstein (2021) identifies four broad surveillance strategies commonly used by governments: passive surveillance, targeted surveillance, AI and big-data approaches, and surveillance laws and directives. We review these strategies here.

Feldstein (2021) defines passive surveillance as “communications surveillance that is made up of hundreds of instruments that directly monitor, collect, intercept, and retain data that has been ‘communicated, relayed or generated over communications networks to a group of recipients by a third party’” (p. 27-28). This category encompasses everything from mobile phone tapping and location monitoring to network interception (which allows governments to intercept Internet traffic that meets specific criteria, based on things like user identify, location, or content) and deep packet inspection (which enables governments to examine the content of Internet network transmissions, such as email communications).

According to Feldstein (2021), targeted surveillance comprises “intrusion operations that manipulate software, data, computer systems, or networks in order to gain unauthorized access to user information and devices” (p. 28). Targeted surveillance is more focused on specific individuals than passive surveillance and typically relies on specific deployment of malware or spyware to collect information. Citizen Lab (2014) classifies targeted intrusion operations into three types. The first is national in-house operations or advanced persistent threat (APT), which describe “threat actors have capabilities and resources to develop their own customized malware and conduct wide scale operations” (p. 8). This level of capacity is difficult to develop and is generally restricted to well-resourced actors like states, although “cyber militia” that have direct or tacit support from governments can also carry out these types of operations. The second type is repurposed crimeware, which tends to be based on remote access trojans (RATS). Finally, commercial spyware “relies on the procurement of commercial ‘lawful intercept’ products and services that provide actors with turnkey surveillance solutions” (p. 10). Firms such as NSO Group, FinFisher, and Hacking Team are examples of players providing these capabilities. O’Neill (2019) suggests that these tactics are “designed to silently infect and invisibly surveil even paranoid targets who might have a high level of digital security awareness. In his research, Feldstein (2021) finds that at least 61 countries worldwide are deploying spyware in support of their objectives.

We note that observers have expressed concerns about the potential for COVID-19 smartphone applications (intended for contact tracing, enforcing quarantines, assessing health statuses, and other public health goals) to be misused for government surveillance purposes (Shahbaz and Funk, 2020; Powers-Riggs, 2020). Though to date there is not extensive evidence that these applications are being applied in this way, there are at least 54 countries around the world that have deployed COVID-19
related smartphone applications, few of which have appropriate checks and balances in place to ensure that such abuses do not occur.

Governments in the PRC and Russia, for example, have required social media companies to store data within the country so that security agencies can access information (Shahbaz, 2018). Data localization requirements for tech firms are also in effect in Vietnam, Nigeria, and Pakistan. Importantly, authoritarian governments are not only using digital tools to identify and monitor dissidents within their own borders, but increasingly they are using these tools to mitigate risks from dissidents outside their borders, contributing to the documented rise of transnational repression. Citizen Lab (2021) published an annotated bibliography on “digital transnational repression,” which they define as those instances in which “states seek to exert pressure — using digital tools — on citizens living abroad in order to constrain, limit, or eliminate political or social action that threatens regime stability or social and cultural norms within the country” (p. 5). They note that while transnational repression itself is not a new phenomenon, “there has been limited research on how such repression is enabled and expanded by digital tools” (p. 5).

Their early conclusions highlight a number of important dynamics. First, media reports published in the past few years show that countries such as Saudi Arabia, the PRC, Rwanda, and others use a range of digital tools in order to silence human rights activists, political dissidents, and journalists living abroad. These are in addition to traditional mechanisms of repression, such as in-person harassment and surveillance or threats to family. Second, the sophistication of digital techniques utilized varies, from phishing campaigns dependent on savvy social engineering to the deployment of sophisticated and expensive spyware to social media harassment. While attention to this problem of the use of digital tools to refine repression outside of a state’s borders is gaining attention, efforts to fully understand and address it are still nascent.

**Monitor performance of regime elite, root out underperforming members**

New technologies also afford authoritarian leaders greater control over members of the government. Authoritarian regimes are always vulnerable to threats from within, including coups and high-level elite defections. With the new digital tools, leaders can keep tabs on government officials, gauging the extent to which they advance regime objectives and rooting out underperforming officials who over time can tarnish public perception of the regime. For example, research has shown that Beijing avoids censoring citizens’ posts about local corruption on Weibo (the PRC equivalent of Twitter) because those posts give the regime a window into the performance of local officials (Qin, Strömberg and Wu, 2017).

**Enhance ability to co-opt support**

Today’s technologies not only make it easier for governments to repress critics; they also make it easy to co-opt supporters. Co-optation — where regimes extend benefits to potential challengers in exchange for their loyalty — is a critical component of the authoritarian survival toolkit. New technologies are enhancing authoritarians’ ability to do so. Technology-powered integration between government agencies allows the PRC regime, for example, to more precisely control access to government services, so that it can calibrate the distribution — or denial — of everything from bus passes and passports to jobs and access to education (Hoffman 2019). The nascent social credit system in the PRC has the effect of punishing individuals critical of the regime and rewarding loyalty. Citizens with good social credit scores benefit from a range of perks, including expedited overseas travel
applications, discounted energy bills, and less frequent audits. In this way, new technologies help authoritarian regimes fine-tune their use of reward and refusal, blurring the line between co-optation and coercive control (Hoffman 2019).

The Chinese Communist Party (CCP) collects an incredible amount of data on individuals and businesses: tax returns, bank statements, purchasing histories, and criminal and medical records. The regime then uses AI to analyze this information and compile “social credit scores,” which it seeks to use to set the parameters of acceptable behavior and improve citizen control. Individuals or companies deemed “untrustworthy” can find themselves excluded from state-sponsored benefits, such as deposit-free apartment rentals, or banned from air and rail travel. Although the CCP is still honing this system, advances in big-data analysis and decision-making technologies will only improve the regime’s capacity for predictive control, what the government calls “social management” (Hoffman 2019).

_Censorship_

Digital tools have supercharged authoritarians’ capacity for censorship. Feldstein defines online censorship as “the laws, regulations, or actions a government takes to restrict Internet content and circumscribe access to information” (p. 30). Roberts (2018) identifies three censorship techniques: fear, frictions, and flooding. Flooding describes efforts by governments to inject information into the information ecosystem designed to deliberately drown out legitimate sources of information. We describe this tactic at greater length below as social manipulation and disinformation.

Fear tactics are designed to deter individuals or the media from distributing, collecting, or creating certain content by raising the costs of such actions through threats, arrests, fines, and closures. Many countries have created legal frameworks that allow them to selectively apply deliberately vague laws (much as they do in the traditional media space) to encourage self-censorship and content suppression. We discussed above how governments are using robust but often vague laws to enhance their latitude for digital repression. There are examples abound, including in hybrid regimes and weak democracies. Pakistan created new guidelines in May 2017, for example, to restrict online anonymity and increase the government’s ability to censor unfavorable speech and punish the individuals who said it. Guinea passed Law No. 037, as well, which was enacted in July 2016, allowing for online censorship and making whistleblowing illegal.

Friction tactics describe efforts designed to deter people from accessing prohibited content. Such actions include making it hard to find and download virtual private network technologies, for example. In Russia, a 2018 law introduces fines for search engines providing access to proxy services, such as VPNs, that allow a user access to banned content or provide instructions for gaining access to such content.

In addition to fear, friction and flooding, additional censorship tactics include distributed denial of service attacks (DDOS) and infrastructure restrictions, such as setting up closed national Internet networks where government monitors have free reign to restrict content. DDOSs render computer networks or websites inoperative by flooding them with data simultaneously sent from multiple computers. Examples of sovereign Internets include the PRC’s great firewall and Iran’s National Information Network, or “halal net.” Russia is also taking steps to advance its RuNet. It passed a “sovereign Internet” law that envisages the full transfer of control over online communication networks to a government agency, from shutting down networks within certain areas of Russia, through cutting Russia off from the World...
Wide Web. If carried out as planned, the sovereign Internet law will also enable the government to directly block whatever content it deems undesirable, according to Human Rights Watch.

Recent advances in automated text analysis, machine learning techniques, and high-powered computing have reduced the costs of identifying critical users and censoring messages.

While censorship allows leaders to regulate information flows, it is not without costs. Censorship can signal to citizens that the government has something to hide, reducing perceptions of legitimacy. It can also motivate citizens to seek out restricted content. Hobbs and Roberts (2018) find that the PRC’s blocking of Instagram motivated users to bypass other blocks and spurred political interest and critical online discourse. More specifically, when the PRC government blocked Instagram, millions of PRC users obtained virtual private networks and then joined censored websites (Twitter and Facebook). Even if they were initially apolitical, they then began looking at political pages that had been blocked too and discussed highly political topics. Censorship can also limit the regime’s ability to monitor the Internet and social media in ways that provide information about potential sources of discontent (as we describe below in the section on legibility). Moreover, censorship carries economic costs. Efforts to constrain digital communications can impede innovation, negatively affecting economic outcomes.

**Internet shutdowns**

Even if censorship fails and dissent escalates, digital autocracies have an added line of defense: they can block all citizens’ access to the Internet (or large parts of it) to prevent members of the opposition from communicating, organizing, or broadcasting their messages. In Iran, for example, the government successfully shut down the Internet across the country amid widespread protests. Broadly speaking, Internet shutdowns are a blunt tool, affecting every citizen in the country regardless of their views on the regime. In some cases, including Hosni Mubarak’s decision to cut off Internet in Egypt in 2011, Internet shutdowns can inflame public sentiment and paradoxically push more people on to the street to find out what was happening. Internet shutdowns can also blind the regime to protesters’ developing plans, making it more difficult to thwart or even preempt their moves. Finally, Internet shutdowns can be costly. Research by Samuel Woodhams and Simon Migliano finds that since 2019 there have been 228 major internet shutdowns in 41 countries, creating an accumulated cost to the global economy of approximately $15 billion. In 2021 alone there have been 23 internet shutdowns in 14 countries (as of July 2021) costing $3 billion to date this year.

In addition to shutdowns – including those that temporarily disconnect access for parts of or the whole population – governments have other means to calibrate country-wide access. Those include tampering with digital communication by throttling bandwidth to the extent that browsing of either the Internet or specific applications becomes nearly impossible. The question often becomes, why do private companies comply with state orders to shutdown Internet access? In one study, Mare (2020) argues that governments often deploy political, regulatory, and lawfare strategies to force state-ordered Internet shutdowns. In her study of Zimbabwe, Mare argues that “private telecommunications operators comply with government partly to abide by their licensing obligations, for fear of political harassment and victimization and threats of arbitrary imprisonment.” Similarly, in Pakistan (a democracy, albeit a weak one), the government can impose heavy fines on telecommunication companies that do not comply with
government shutdown orders, and these companies are not permitted to challenge or scrutinize such decisions (Wagner, 2018).

**Social manipulation and disinformation**

Authoritarian regimes have long produced propaganda and sought to manipulate their information environments. Such strategies help authoritarians shape perceptions about the popularity and legitimacy of their regimes, both by advancing regime-friendly narratives and distracting from those that are unfavorable. Authoritarian regimes can exert influence by spreading disinformation, trolling and harassing (including deliberately posting offensive content to provoke or disrupt conversations), and flooding. In the world of autocracies, the ability to manipulate the information environment is critical because it shapes citizens’ willingness to participate in protests and anti-regime activity (Kornbluh 1987). An average citizen is only willing to participate in a protest if he or she believes that others share their discontent. Technology increases the efficiency of autocrats’ efforts to drown out criticism and inflate perceptions of regime support, lowering the prospects for protest.

There is evidence of state-sponsored trolling in a number of dictatorships. Many of these activities target journalists in particular. Governments hire activists or low-paid subcontractors to levy campaigns seeking to discredit and criticize journalists and spread propaganda. These include “Vietnamese cyber-soldiers, the Russian troll factories, the Chinese ‘little pinks,’ Narendra Modi’s ‘yoddhas’ in India, Erdogan’s ‘white trolls’ in Turkey, Iran’s cyber-guardians of the revolution for a halal Internet,” and in the Philippines, poor workers earning 10 dollars a day to post fake news on social networks favorable to the president (Reporters Without Borders, 2018). Doxing is a subcomponent of trolling that involves the public release of personal information to compromise individual safety and intimidate people to prevent them from engaging in certain actions. Doxing is a technique that has been used by both protesters (including in Hong Kong where protesters routinely dox unbadged police officers) and state agents.

Automated methods also serve to amplify regime narratives. Automated accounts (or “bots”) on social media can amplify influence campaigns and produce a flurry of distracting or misleading posts that crowd out opponents’ messaging. This is an area in which Russia has played a leading role. The Kremlin floods the Internet with pro-regime stories, distracting online users from negative news, and creates confusion and uncertainty through the spread of alternative narratives.

Maturing technologies such as so-called microtargeting and deepfakes — digital forgeries impossible to distinguish from authentic audio, video, or images — are likely to further boost the capacity of authoritarian regimes to manipulate their citizens’ perceptions (Fontaine and Fredrick 2019).² Microtargeting will eventually allow autocracies to tailor content for specific individuals or segments of society, just as the commercial world uses demographic and behavioral characteristics to customize advertisements. AI-powered algorithms will allow autocracies to microtarget individuals with

---

² Microtargeting is also cited as troubling for democracies, particularly its use during political campaigns. Many observers have called for social media platforms to limit microtargeting of political advertisements, due to its role in disinformation campaigns (Kornbluh and Goodman, 2020). Others have suggested that social media platforms should publish more data about microtargeting (including information about the identity of who purchases such advertisements) and offer users greater control over the types of ads that target them (KACEDDA, 2020).
information that either reinforces their support for the regime or seeks to counteract specific sources of discontent. Likewise, the production of deepfakes will make it easier to discredit opposition leaders and will make it increasingly difficult for the public to know what is real, in turn sowing doubt, confusion, and apathy.

Examples of authoritarian regimes’ use of social manipulation and disinformation abound. Bradshaw and Howard (2018) found that from 2017 to 2019 there was a 150 percent increase in countries using organized social media manipulation campaigns (from 28 in 2017 to 70 in 2019). In particular, cyber troops used computational propaganda to attack political opposition (89 percent), followed by spreading pro-government propaganda (71 percent), and lastly spreading polarizing messages to divide society (34 percent). Facebook remains the dominant platform for cyber troop activity. After this it is Twitter, then to a much lesser degree WhatsApp, YouTube, and Instagram.

In one interesting study, Tan (2020) describes how the authoritarian regime in Singapore learned to use digital marketing and computational propaganda tools to strengthen its hold over public opinion and compete with opposition parties. The regime adapted digital marketing strategies in innovative ways to add a softer touch to extend its online influence, including by hiring digital media consultants, an “Internet brigade” and influencers to engage in “guerrilla-type activism” to shape public opinion and soft-sell controversial policies in a friendly way. Rather than blocking, censoring, and suppressing communications, Singapore’s regime learned to use social media tools and a blend of control, co-optation, and manipulation to influence public opinion, underscoring how authoritarian learning and innovation can occur in subtle, covert ways to maintain hegemonic party dominance.

Unlike censorship, social manipulation and disinformation come with fewer costs to the regime. These tactics offer many of the same benefits as censorship, such as inhibiting the free flow of information and suppressing alternative viewpoints, but without the same reputational or economic costs. Many illiberal democracies, such as Brazil, Nigeria, and the Philippines have deployed social manipulation tools to great effect (Feldstein 2021).

**Mimic elements of democracy**

Digital tools might even help regimes make themselves appear less repressive and more responsive to their citizens. In some cases, authoritarian regimes have deployed new technologies to mimic components of democracy, such as participation and deliberation. Some local PRC officials, for example, are using the Internet and social media to allow citizens to voice their opinions in online polls or through other digitally based participatory channels. Truex’s research (2014) suggests that such online participation enhanced public perception of the CCP among less educated citizens. Consultative sites, such as the regime’s “You Propose My Opinion” portal, make citizens feel that their voices matter without the regime having to actually pursue genuine reform. These outlets can also allow citizens to express their grievances, relieving pent up discontent that they might otherwise express on the street or through more active approaches. In other words, digital autocracies are learning to use digital tools to emulate elements of democracy in ways that could mitigate the bottom-up pressure that can destabilize authoritarian systems.
**Increase legibility of society**

Technology is also useful in preventing protest because it improves autocrat’s access to information about their citizens — historically a critical vulnerability in authoritarian systems. Known as the “dictator’s dilemma,” leaders in authoritarian systems have had limited insight into the sentiment and views of their citizens because their use of repression reduces people’s willingness to communicate their beliefs. In contrast to democracies where free speech and elections serve as accurate information gathering mechanisms, dictators face the difficulty of obtaining accurate information about citizens even if they hold elections because citizens have an incentive to misrepresent their anti-regime sentiments when faced with the prospect of repression (Kuran 1991). In many ways, technology alleviates this dilemma, allowing autocrats to identify and respond to (even cosmetically) sources of discontent before they spiral into something more threatening. Gunitsky’s research (2015) suggests that ICTs provides authoritarian governments with new opportunities for political control by enabling them to use ICTs to collect information about citizens’ preferences. King, Pan, and Roberts (2013, 2014) argue that the PRC government tentatively allows public criticism against the governments for the reason of collecting citizens’ preference.

Similarly, another study shows that the PRC government uses digital tools to anticipate events that could create focal points for protest and then uses preventive repression to reduce dissent beforehand (Truex 2019). And while digital autocracies may not currently be able to use all the data they collect, advances in big data analysis and decision-making technologies will enhance their ability to read the public mood and respond accordingly.

**THE POLITICAL CONSEQUENCES OF DIGITAL REPRESSION**

In this section, we focus on digital repression in authoritarian regimes and review the literature discussing the ways in which it influences political outcomes. We also discuss digital repression’s role in democratic backsliding.

**Repression**

The evidence suggests that the use of digital repression in dictatorships influences the broader repressive strategy. Specifically, those dictatorships that increase their reliance on digital repression subsequently increase their reliance on high-intensity repression (Frantz, Kendall-Taylor, and Wright, 2020). High-intensity repression refers to easily observable acts of violence, such as the Tiananmen Square massacre in 1989, which saw the Communist regime in the PRC kill hundreds of student protestors, or – more recently – mass shootings of protestors in Myanmar this year, where security forces have killed more than 300 citizens following protests against the military coup in early 2021. This form of repression usually targets well-recognized individuals and groups. It contrasts with low-intensity repression, which is subtler in nature, including tactics such as surveillance and short detainments of opponents. The data reveal that digital repression – which falls in the category of low-intensity repression – complements the use of high-intensity repression. Dictatorships are therefore not using digital repression to replace high-intensity repression, but instead leveraging it to hone their ability to execute it. By providing dictatorships with more information about their opponents, digital repression enables regimes to use violence more precisely and efficiently. This is advantageous given the potential for indiscriminate government violence to trigger a political backlash.
Several studies confirm the finding that digital repression is allowing governments to fine tune and increase targeted repression. Xu (2020) shows that digital surveillance allows dictators to more easily identify their political opposition and therefore substitute targeted repression for non-exclusive co-optation to forestall coordinated uprisings. Using a difference-in-differences design that exploits temporal variation in digital surveillance systems among PRC counties, Xu finds that surveillance increases local governments’ public security expenditure and arrests of political activists but decreases public goods provision. Xu writes that, in this way, improved government access to information decreased citizen well-being in the PRC. (Though future research is needed to evaluate whether this relationship holds in other authoritarian contexts, this finding suggests that policy makers could potentially generate pushback against acquisitions of digital surveillance technologies by flagging the ways in which they are associated with reduced investments in public goods for citizens.)

Likewise, Ghodes (2020) from her study in Syria finds that where governments offer Internet access, they use surveillance of digital information to gather intelligence and improve their ability to use targeted repression (particularly in areas of contestation). Where they limit access to the Internet, they can hurt the opposition’s ability to organize, but at the cost of having less information leading to greater untargeted repression.

Similarly, Feldstein (2021) suggests that digital tools not only augment existing repression but can transform the state’s ability to track and monitor the opposition, quell protest movements, and consolidate control. Feldstein argues, however, that this is really only the case in countries with already high levels of repressive capacity. In lower capacity countries, he writes, “acquiring digital tools does not bring the same transformative repression effect” (p. 40). He does not offer quantitative evidence that this is true, and we see this as a question that merits further research.

Protest

As discussed above, protests have become the most significant threat to 21st century autocrats. In fact, protests have now replaced coups as the one of the greatest threats to authoritarian rule. Although the rise of digital tools initially increased the incidence and success of protests, research shows that authoritarian governments are beginning to adapt to the rising threat of protest by leveraging digital technologies (Frantz, Kendall-Taylor, and Wright, 2020). In fact, the data reveal that digital repression decreases the chance of protests in dictatorships, even when controlling for a variety of potentially confounding factors. As the use of digital repression goes up, the chance of protest declines. Today’s dictatorships are therefore countering the most challenging threat they face to their control by ratcheting up reliance on digital repression.

Xu (2019) finds similar results. In his dissertation, Xu finds that digital surveillance, like informant-based surveillance, deters political expression and protest participation but this digital repression, unlike human informants, does so without lowering interpersonal trust and regime legitimacy.

We note that research in this field is in the early stages. Therefore, we do not know the extent to which digital repression influences the likelihood of protest in other political contexts, such as in fragile or backsliding democracies.
**Authoritarian regime survival**

Today’s dictatorships govern for longer than their predecessors. The data show that whereas the typical dictatorship from 1946 to 2000 ruled for about ten years, from 2001 to 2019 this number increased to 25 years. This greater durability corresponds to the advent of digital tools. Research suggests that this is not coincidental: those dictatorships that rely on digital repression to a greater degree last longer in power than those that do not (Frantz, Kendall-Taylor, and Wright, 2020). The evidence reveals that rather than fall victim to technological change, as many optimists envisioned at the start of the 21st century, authoritarian regimes are instead using new technological tools to prolong their rule.

A study by Dragu and Lupu (2021) is consistent with this finding. Using a game theoretic model, the authors show that technological developments are not going to hurt authoritarians but rather help them by improving their ability to abuse human rights. Innovations are used to prevent opposition groups from mobilizing, thereby increasing human rights abuses. The basic message is that digital tools are not going to harm authoritarians; they are going to bolster their rule.

**Democratic backsliding**

Research on the relationship between digital tools and democratic backsliding is nascent. Early research suggests that in addition to increasing the durability of autocracies, digital tools are also associated with an elevated risk of democratic decline in fragile democracies (Kendall-Taylor, Frantz, and Wright, 2020). From 2001 to 2017, there were 18 cases of democratic erosion. In countries such as Mali and Zambia, the government’s use of digital repression preceded democratic decline. In a handful of other countries, including Brazil and Ecuador, rising digital repression occurred concurrently with democratic decline. And in some cases, such as South Korea and Sri Lanka, the uptick in digital repression began just after respect for democracy began to deteriorate. While it is too soon to conclude that digital repression is causing the backsliding, it is clear that these dynamics are moving together. In other words, new technologies are now part of the process in which democracies are sliding into authoritarianism.

New technologies pose a particular danger to weak democracies because many of them are dual use: the very tools that can help governments more efficiently deal with challenges such as crime can also be used to target opponents. In other words, democracies may acquire digital tools for valid reasons, but at any moment would-be autocrats governing them may use them for repressive means.

Newer research also suggests that digital repression is associated with the increasing personalization of democratic politics (Kendall-Taylor, Frantz, and Wright, 2021). In this context, personalization describes those systems where leaders hold more power relative to their political parties than nonpersonalist leaders do, such that politics more strongly reflect the leader’s preferences than a bargaining process among multiple actors and institutions. As digital repression grows, we see an increase in personalism the following years. This suggests that technology lowers costs for leaders seeking to consolidate power.

---

3 Frantz, Kendall-Taylor, and Wright (2020) find that the evidence is mixed with respect to whether this is a causal relationship (i.e., whether digital repression causes greater authoritarian survival). In cross-national, time-series statistical tests that consider confounding factors, they find little evidence that when autocratic regimes increase their use of digital repression it influences their risk of collapse. At the same time, they find that those autocratic regimes that rely on digital repression more, are less likely to fall from power. The mixed evidence may be due to the small number of years for which there are digital repression data. That said, the correlation between reliance on digital repression and authoritarian survival is strong.
Greater control of the narrative may enable them to lessen resistance to power grabs, mitigating the extent to which they must rely on repression to concentrate control and personalize the political system. In this way digital repression creates an environment more conducive to the personalization of power. This same research suggests that personalization, in turn, raises the risk of democratic decline, including gradual incumbent power grabs, democratic erosion, and total democratic collapse.

While this research suggests that digital repression can facilitate leaders’ efforts to roll back democracy, far more work is needed to understand the mechanisms at play. We still do not understand how leaders use these tools to dismantle democracy, obscuring clear evidence-based policy interventions that would increase democracy’s resilience in the face of growing technological threats.

SECTION II: UNDERSTANDING TRENDS AND VARIATION IN DIGITAL REPRESSION

DATA

In this section, we use data to shed light on the digital repression landscape. We begin by explaining our data sources. For information on governments’ reliance on digital tools, we use data from the Digital Society Project’s “Digital Society Survey.” The data are coded from 2000 to 2020 for more than 180 countries. For information on political system and authoritarian regime type, we use data from Geddes, Wright, and Frantz (2014) (and updated by Frantz) unless otherwise noted. These are only available through 2019, however, so the analyses are limited to the 2000 to 2019 timeframe.

To measure digital repression, we follow Frantz, Kendall-Taylor, and Wright (2020), who create a digital repression index. The digital repression index includes the variables below from the “Digital Society Survey.” The question included with each variable offers the information provided in the codebook regarding what it is seeking to capture. Note that few additional details beyond this are offered.

- Government social media censorship in practice
  - “To what degree does the government censor political content (i.e., deleting or filtering specific posts for political reasons on social media in practice?)”
- Government social media monitoring
  - “How comprehensive is the surveillance of political content in social media by the government or its agents?”
- Government social media shut down in practice
  - “How often does the government shut down access to social media platforms?”
- Government Internet shut down in practice
  - “How often does the government shut down domestic access to the Internet?”

---

4 This data set classifies political systems as democracies or dictatorships, primarily based on whether leaders are selected through a free and fair electoral process. The classifications largely overlap with more gradated measures of political system type (that distinguish hybrid systems, for example), such as Freedom House or combined Polity scores, though there are occasionally disagreements over classification of hybrid cases (such as Botswana). The Geddes, Wright, and Frantz data are advantageous for our purposes because they also include measures of the start and end dates of authoritarian regimes, which are necessary for evaluating authoritarian regime duration and collapse. The basic messages offered here, however, hold regardless of the political system type measure used.
- Government Internet filtering in practice
  - “How frequently does the government censor political information (text, audio, images, or video) on the Internet by filtering (blocking access to certain websites)?”
- Government social media alternatives
  - “How prevalent is the usage of social media platforms that are wholly controlled by either the government or its agents in this country?”

Like Frantz, Kendall-Taylor, and Wright (2020), we also measure digital capacity (which captures a government’s capacity to carry out digital repression, not its application). The digital capacity index, also from the survey, includes the variables below.

- Government cyber security capacity
  - “Does the government have sufficiently technologically skilled staff and resources to mitigate harm from cyber-security threats?”
- Government Internet shut down capacity
  - “Independent of whether it actually does so in practice, does the government have the technical capacity to actively shut down domestic access to the Internet if it decided to?”
- Government Internet filtering capacity
  - “Independent of whether it actually does so in practice, does the government have the technical capacity to censor information (text, audio, images, or video) on the Internet by filtering (blocking access to certain websites) if it decided to?”
- Government capacity to regulate online content
  - “Does the government have sufficient staff and resources to regulate Internet content in accordance with existing law?”

We analyze one additional variable from the survey as well: government online content regulation. This variable captures the “government uses its own resources and institutions to monitor and regulate online content,” as opposed to distributing “this regulatory burden to private actors such as Internet service providers.”

**BASIC DATA TRENDS**

*The digital repression landscape*

Using the digital repression and digital capacity indices, we can get a perspective of what the digital landscape looks like. Figure 1 and Figure 2 in Annex 1 provide a map that displays average levels of these two indicators from 2000 to 2019 for all countries with data. It reveals that there is substantial variation across countries in their capacity and application of digital repression, with the PRC standing out as high on both indices.
Trends over time

Figure 3 shows trends over time in digital repression and digital capacity by political system type. Both digital repression and digital capacity have increased during the period. Looking at the six variables in the digital repression index, the data show that both democracies and dictatorships have increased their reliance on all six over time. Democracies tend to feature less digital repression and digital capacity than dictatorships do. That said, the difference between the two political systems is less pronounced with digital capacity, suggesting that many democracies have the capacity to use digital repression but opt not to do so. In other words, autocracies digitally repress more than their capabilities indicate. This suggests that autocracies are making up the gap either by frequently using relatively crude approaches (like Internet shutdowns) or through access to external sources of technology. On the flip side, future research is needed to better understand whether specific triggers (such as protests) cause governments with high digital capacity to subsequently ratchet up digital repression.

There have been few changes over time in states’ approaches to regulating online content (either in democracies or dictatorships). Unfortunately, we know little about state approaches to regulating surveillance, given the absence of data to capture it.

Digital tools and political system type

The data show that digital repression decreases as states grow more democratic.\(^5\) The relationship is fairly linear and holds regardless of whether the political system measure is electoral democracy, liberal democracy, or combined polity scores. The basic message is that as states grow more democratic, their usage of digital repression declines. This is consistent with research by Feldstein (2021), whose work reaffirms the tight negative correlation between electoral democracy and digital repression. Feldstein suggests that democracies perform worse across the board on all digital repression measurements than democracies.

Feldstein (2021) suggests several reasons for the difference in levels of digital repression between democracies and authoritarian regimes. The first is the net benefits of digital repression. Autocracies have fewer constraints on their ability to deploy these tools, and the benefits are vast (as described in the section above). For democracies, the deployment of digital repression can prompt backlash (costs), reducing the net benefits. Second, Feldstein argues that traditional repression is closely linked to digital repression strategies. More specifically, he finds that a government’s restriction of civil liberties is a big predictor of digital repression.

There are a handful of electoral democracies that use digital repression substantially more than expected given their level of democracy. These include Burkina Faso, France, Mauritius, Nepal, and Taiwan. Likewise, there are a handful of dictatorships that use digital repression substantially less than expected given their level of authoritarianism (these are Belarus, Laos, and Thailand).\(^6\) Future research is needed to better understand whether there are common patterns underlying these deviations and if they offer unique opportunities for policy interventions.

---

\(^5\) Here we use a variety of continuous measures of political system type offered by Varieties of Democracy (V-Dem) and the Polity Project.  
\(^6\) Note that these data run through 2019 and therefore do not capture political developments in 2020 that may have led to changes in digital repression, such as the protests in Belarus.
When looking at digital capacity, the data reveal a nonlinear relationship with levels of democracy. Digital capacity tends to be highest among states that are the least democratic. It then declines among hybrid states, before increasing as states become highly democratic. The message that emerges here is highly autocratic states tend to have high levels of digital capacity, followed by highly democratic states, and lastly hybrid states.

Looking at the state’s approach to regulating online content, dictatorships are more likely than democracies to have the government take the lead, suggesting that democracies rely more on private actors to regulate online content than dictatorships do.

**The preferred digital tools of democracies and dictatorships**

While both autocracies and flawed democracies use digital repression, they do so differently. Our analysis (presented in Table 1. Average reliance on digital tools by political system type (in 2019)Table 1) shows that among the variables in the digital repression index, democracies currently (as of 2019) rely most heavily on social media monitoring, followed by social media censorship, although the level of social media censorship (and reliance on all digital tools discussed here) in democracies is significantly lower than in authoritarian regimes. In their study, Meserve and Pemstein (2020) find that democracies are most likely to increase Internet censorship amid increases in terrorist attacks. Today’s democracies rely least on shutting down or filtering the Internet or social media than on other digital tools.

As Feldstein (2019a) points out, even though liberal democracies (i.e., highly democratic states) are major users of certain digital technologies (such as AI-based surveillance), this does not necessarily mean that they are abusing them. One of the biggest factors for predicting whether a state will use digital tools for repression is their level of democracy. This is consistent with research from Greitens (2020b), who looks at the effect of COVID-19 and the spread of health-related surveillance technology. She finds that “a large number of consolidated democracies have employed surveillance, but have managed to navigate the initial stages of crisis without significantly compromising democratic standards. In these cases, surveillance technology has been fenced in by democratic institutions and rule of law, and norms, institutions, and public opinion have worked together to facilitate pandemic responses that are (on balance) proportional, limited in time and scope, and subject to democratic oversight.”

Among the tools in the digital repression index, dictatorships currently (as of 2019) rely the most on social media monitoring, followed by Internet filtering. They rely least on shutting down the Internet or social media.

Looking at the four variables in the digital capacity index, the data show that both democracies and dictatorships have increased their abilities in all four areas, though for dictatorships this only began starting around 2008. Among the capacity variables, democracies are highest in the areas of capacity for cyber security and to regulate content; they are lowest in the capacity to shut down the Internet. Dictatorships currently have a high capacity to filter the Internet, followed by the ability to shut it down; they rank lowest in the capacity variables when it comes to cyber security.

It is worth nothing that Feldstein (2021) looks at the same data as we do here but incorporates two additional concepts (also from the “Digital Society Survey” data): government and party dissemination of false information domestically (which he refers to as “social manipulation and disinformation”) and
arrests of citizens for posting political content online. He looks at these data for the 2010 to 2019 period. Consistent with what we report above, he finds that dictatorships rely heavily on social media monitoring; he finds that they rely heavily, as well, on social manipulation and disinformation and arresting online users for political content in the period. He finds that democracies also rely heavily on social manipulation and disinformation, such that the gap between democracies and dictatorships in their use of digital repression tools is smallest when looking at social manipulation and disinformation. He also finds that among democracies, reliance on social media monitoring is a preferred digital tactic (as we report above), second only to social manipulation and disinformation.

In our own analysis looking at these two additional measures, the trends that Feldstein identifies hold if we look explicitly at 2019: dictatorships’ reliance on social manipulation and disinformation and arrests of citizens for posting political content remain high, comparable to their reliance on social media monitoring and Internet filtering. Likewise, democracies continue to rely quite a bit on social manipulation and disinformation, slightly more so than they do on social media monitoring.

**Digital tools and authoritarian regime type**

Looking at different types of authoritarian regimes, there are also clear patterns in digital capacity and repression. Military dictatorships rely on digital repression the most, whereas personalist dictatorships rely on it the least. Monarchies and party-based dictatorships are in the middle, though party-based dictatorships exhibit sizable variance. Monarchies have the most digital capacity, whereas personalist dictatorships have the least. Again, there is the widest variance among party-based dictatorships.

The interesting takeaway here is that though personalist dictatorships are known to rely quite a bit on traditional forms of repression (Frantz, 2018), they are the least likely of all dictatorships to use digital repression and to have the capacity to do so in a sophisticated fashion.

A ranking of authoritarian regimes in terms of their reliance on digital repression is provided in

*Figure 4* (note that many authoritarian regimes in the data set are no longer in power as of 2020, as indicated by the regime end date). This figure reveals that North Korea, Turkmenistan, Eritrea, and the PRC are the four dictatorships in power today that use digital repression the most. On the flip side, Mozambique, Botswana, Belarus, and Tanzania are the four authoritarian regimes in power today that use digital repression the least.

In many instances, levels of digital capacity match levels of digital repression in dictatorships. That said, there are cases where there are sizeable differences. A list of authoritarian regimes that use digital repression less than we would expect given their capacity to do so is offered in Table 2. A list of those that rely substantially more on digital repression than we would anticipate given their capacity is offered in Table 3. As Frantz, Kendall-Taylor, and Wright (2020) point out, the latter likely occurs where

---

7 These data capture activities by the government, its agents, and major political parties and candidates for office.
dictatorships use rudimentary tactics to repress, such as Internet shut-downs, which do not require substantial capacity.

Future research is needed to better understand the meaning of these trends and whether they provide opportunities for policy interventions. For example, are dictatorships that rely little on digital repression instead using other survival tools to maintain power? Are the threats they face different than in other authoritarian contexts? These and other basic questions about the digital repression landscape remain unanswered in the literature.

**Digital tools and population**

There is little relationship between population size and reliance on digital repression. Looking solely at the size of the urban population (as a percentage of the total population), there is a slight pattern: as states grow more urban, they are less likely to use digital repression. This relationship appears to be conditioned on political system type: there is little link between urbanization and digital repression in dictatorships; in democracies, however, as urbanization increases, levels of digital repression decline.

In terms of digital capacity, states with larger populations are slightly more likely to have high digital capacity than those with smaller populations. If we look at the urban population (as a percentage of the total population), however, a clearer picture emerges. Digital capacity increases as states grow more urban.

**Digital tools and levels of development**

States rely less on digital repression as they increase in their levels of wealth (measured as GDP per capita). That said, this relationship only holds in democracies; there is little connection between levels of wealth and reliance on digital repression in dictatorships. However, when looking only at surveillance, Feldstein argues that surveillance is “most relevant for wealthy autocratic regimes that are less concerned about public backlash and have sufficient capacity to operate advanced systems,” (2021, p. 44) including in countries such as the PRC, Russia, the Gulf states, Turkey, and Iran.

States increase their digital capacity as they increase in their levels of wealth. This relationship holds in both democracies and dictatorships.

This suggests that in democracies, as states grow richer, they obtain greater digital capacity but use digital repression less. In dictatorships, however, wealth is associated with greater digital capacity but not with changes in reliance on digital repression. Future research is needed to better understand the ways in which changes in levels of development influence government decisions to adopt digital tools and use them for repression purposes.

It is worth mentioning that a state’s military spending is positively correlated with its use of AI-based surveillance systems (Feldstein, 2019a). Though this does not mean states with high military spending are using such systems for repression, among the fifty states with the highest military spending, 80 percent use AI-based surveillance technology.
SECTION III: EXTERNAL FACTORS: STATES AND PRIVATE SECTOR ROLE IN SPREADING DIGITAL AUTHORITARIANISM

STATE-LED SPREAD OF DIGITAL AUTHORITARIANISM

Our review of the literature suggests that two authoritarian states play a major role in the spread of digital authoritarianism: the PRC and Russia. This does not mean that other dictatorships are not also active in this domain. For example, Syria is using Iran’s methods of online surveillance and Internet filtering to monitor its opponents. That said, the PRC and Russia are clearly at the forefront of these behaviors, with the PRC substantially in the lead.

Both the PRC and Russia have crafted distinct technology models for authoritarian rule (Polyakova and Meserole, 2019). The PRC has developed digital tools for censorship and surveillance and is the major exporter of these tools to other authoritarians wishing to improve their own ability to surveil. Russia, on the other hand, has lower cost tools which can be used for disinformation campaigns. These tools are effective in improving the ability to repress opponents, as well as adversaries abroad in democracies.

In what follows, we highlight the basic ways in which the PRC and Russia use digital repression themselves, before turning to a discussion of how they are proliferating it. We include in this discussion a review of debates over the PRC’s motivations regarding the spread of digital technologies.

Digital authoritarianism in the People’s Republic of China (PRC)

The PRC model of digital authoritarianism has AI-powered surveillance at the center (Kendall-Taylor, Frantz, and Wright, 2020). The regime uses high-resolution cameras, facial recognition, spying malware, automated text analysis, and big-data processing in ways that give it substantial capacity to monitor citizens and identify opponents quickly (Kendall-Taylor, Frantz, and Wright, 2020). An example of this is the regime’s compilation of “social credit scores” (Kendall-Taylor, Frantz, and Wright, 2020). The PRC government collects an enormous amount of data on ordinary citizens – ranging from tax returns to purchasing histories – which is then used to determine an individual’s score. Those who are seen as falling short on regime standards of acceptable behavior often lose access to government benefits and can even be banned from travel. This system is still a work in progress but given the speed with which big data and decision-making technologies are advancing, it is likely to improve its capacity to manage society in ways that conform to its goals.

Another example of the regime’s sophisticated use of AI-based surveillance technology is the installation of facial recognition software all over neighborhoods in the Xinjiang (Kendall-Taylor, Frantz, and Wright, 2020). This software is used to determine which individuals can and cannot pass through neighborhoods; individuals who are flagged are immediately detained. More than one million Uighurs have been detained and sent to “reeducation camps” as a result. In this way, digital tools are enabling physical human rights abuses. Beyond facial recognition, the regime is also gathering a vast amount of data on the Uighur population, which it is using to try to assess actions it deems threatening.

Beijing is also using AI technologies to improve its ability to censor online content (Kendall-Taylor, Frantz, and Wright, 2021). With such tools it can sift through large swaths of text and images, filter and
censor content, and ensure unfavorable information about the regime is not available to users. When the protest movement in Hong Kong gained steam in 2019, for example, the PRC reinforced its “Great Firewall” and instantly removed negative content online from those on the mainland.

To summarize, the PRC model of digital dictatorship leverages extremely sophisticated capabilities in AI technologies to automate surveillance and censor extensively. In these ways, it is a digital authoritarianism trailblazer.

**How the PRC is spreading digital technologies**

The PRC is the world leader in the export of digital technologies that can be used to violate human rights (Feldstein, 2019a). It is providing technologies to at least 63 countries. It is exporting high-quality products that are made and designed in the PRC, relying less and less on Western components (Polyakova and Meserole, 2019). Huawei is the big leader in PRC technology exports. It supplies AI-based surveillance technology to at least 50 countries; other companies pale in comparison (Feldstein, 2019a). PRC technology companies (including Huawei and ZTE) have taken the lead in the development and implementation of fifth generation (5G) telecommunications infrastructure, as well (Democratic Staff Report, 2020). As of now there are few alternatives to PRC-made 5G technologies. Huawei is at the forefront, owning more patents for 5G infrastructure than any of its competitors (Rahn, 2019). Some observers have expressed concerns that PRC dominance in the 5G market will not only increase countries’ dependence on the PRC for their Internet, but also expose them to PRC monitoring and diverting of their data traffic, in turn “feeding China’s intelligence collection and technological advances in areas such as AI” (Rahn, 2019).

One key way that the PRC is spreading digital technologies is through the Belt and Road Initiative, which is a trillion dollar development plan for investing in infrastructure projects that help PRC trade and broaden its influence in the target countries (Shahbaz, 2018). Among those countries receiving PRC technologies, 36 are signatories to the Belt and Road Initiative (Feldstein, 2019a). The plan includes a “digital Silk Road,” with PRC-made fiber-optic networks that could enable monitoring of Internet traffic by PRC intelligence agencies. As part of the digital Silk Road, PRC companies have laid down fiber-optic links to Myanmar, Kyrgyzstan, and Nepal, to name a few countries (Shahbaz, 2018). The PRC has used Belt and Road investments to sell surveillance technology as well. It exported such tools to Ethiopia, for example, in conjunction with PRC government investments (Sherman, 2021). The PRC often sells its products with soft loans to incentivize governments to purchase them. Loan recipients include Kenya, Laos, Mongolia, Uganda, and Uzbekistan (Feldstein, 2019a).

The PRC has also organized forums to share its practices with countries at events such as the 2017 World Internet Conference in Wuzhen (Shahbaz, 2017). It has held events and training sessions on new media and information management with representatives from at least 36 other countries. While it is unknown what occurs during these events, Saudi Arabia and Vietnam had PRC Internet experts demonstrate to them how to block Western websites (Gunitsky, 2015). And it is notable that Vietnam followed up its training session with the introduction of a law closely mirroring PRC cybersecurity law. The same sort of mimicking of restrictive digital laws also occurred in Uganda and Tanzania (Shahbaz, 2018; Brannen, Haig, and Schmidt, 2020). Tanzania passed a law to regulate online content, for example, that is said to mirror the PRC model — Tanzania justified it as a crackdown on “moral decadence,” just as the PRC said it had banned “decadent” things on social media (Hawkins, 2018).
Many African countries rely on the PRC for their telecom and digital services, as Hawkins (2018) reports. The number one smartphone company in Africa in 2017, for example, was Transsion Holdings, which is based in the PRC. Ethiopia uses PRC telecoms company ZTE to monitor citizen communications, as well. And PRC company Hikvision, which is a leading global manufacturer of surveillance cameras, now has an office in South Africa. There is evidence of some of these relationships leading to digital repression. Uganda hired the PRC company Huawei, for example, to help it hack into a WhatsApp group that was spreading dissent about the government (Brannen, Haig, and Schmidt, 2020). And Zambia—a democracy, albeit a fragile one—hired the same company to help it hack into the phones of known opposition leaders (Brannen, Haig, and Schmidt, 2020). Outside of Africa, Iran signed a deal with the PRC company ZTE to build a comprehensive surveillance apparatus for its entire telecom sector. This has forced citizens to resort to VPNs and other forms of masking software to maintain secrecy in their activities (Berman, 2015).

The PRC government is funding a number of AI projects in Africa too. Part of this appears to be because PRC companies are more willing to accept the risks of investing and doing business in volatile environments. There are indications that some of these systems are being used for repressive purposes (Hawkins, 2018). Globally, PRC companies (such as Yitu, Hikvision, and CloudWalk) are leveraging artificial intelligence and facial recognition technologies to create digital systems that can identify threats to “public order” in at least 18 countries (Shahbaz, 2018).

Many have flagged the PRC’s relationship with Zimbabwe as particularly troubling for human rights (Shahbaz, 2018; Cave et al., 2019). The PRC is deeply involved with Zimbabwe, with links to the government and the state’s telecom companies. It is Zimbabwe’s main source of foreign investment (due to sanctions on the country by the West for its human rights violations) (Cave et al., 2019). The PRC telecom giant Huawei has multi-million-dollar contracts with Zimbabwe’s state cellular network, NetOne. The PRC company ZTE and the Chinese Development Bank also loaned the Zimbabwean telecom company Econet $500 million. The PRC company CloudWalk signed an agreement with that country to build a monitoring database, with no citizen ability to opt out (Shabaz, 2018). Zimbabwe was then supposed to send the data back to the PRC as part of the deal, so that CloudWalk could improve its ability to recognize faces with darker skin tones, which had been difficult for its algorithm.

Is the PRC exporting digital tools as part of a strategy to spread digital authoritarianism?

That the PRC is the global leader in the spread of digital tools with the potential to abuse human rights is undisputed in the literature. Debates persist, however, over what the PRC regime’s motivations are. Existing assessments underscore that the drivers of this trend are complex, stemming from the expansion of the PRC’s geopolitical interests, the increasing market power of its technology companies, and conditions in recipient states that make PRC technology an attractive choice despite concerns about security and privacy (Greitens, 2020a).

On the one hand, some assert that PRC behavior is simply a reflection of its economic incentives. According to this line of thought, there are numerous “pull” factors that lead governments to seek out the PRC’s digital tools. In many cases, demand for PRC digital tools is high, particularly among countries that face security concerns. In her research, Greitens (2020a) finds that countries with high crime rates are comparatively more likely to adopt these technologies. From this perspective, there is no concerted PRC effort to export their model with the goal of undermining democracy (Weiss, 2019). Countries are obtaining PRC technologies not because the PRC is persuading them to do so, but rather because they
see it as in their interest. Moreover, many of the products that the PRC is criticized for exporting have uses beyond repression (Weiss, 2019). The PRC donated $14 million worth of AI equipment to Ecuador in 2016, for example, whose, the government said helped it cut crime (Hawkins, 2018). In fact, the majority (51 percent) of users of AI-based surveillance technologies are liberal democracies, which are not necessarily using them in abusive ways (Feldstein, 2019a). Whether these technologies are applied in ways that violate human rights depends on domestic factors (Feldstein, 2021). It is also worth noting that many democracies also sell the same products (Weiss, 2019).

On the other hand, others argue that the PRC is proactively trying to export its model of digital authoritarianism. In 2017, for example, PRC President Xi Jinping stated that he intended to turn the PRC into a “cyber superpower,” and offer the PRC model as “a new option for other countries and nations that want to speed up their development while preserving their independence” (Shahbaz, 2018). From this perspective, the PRC uses its geopolitical Belt and Road Initiative to push its technologies. A report by Feldstein (2019a) notes that over half of the countries in which PRC-sourced AI technology was used were signatories to the Belt and Road Initiative, and there are indications that PRC government loans may be used to subsidize countries’ acquisition of repressive technologies. Polyakova and Meserole (2019) note that Beijing views information technology not just in terms of economic development but “its value to Chinese foreign policy and strategy… exporting its information technology is not only about securing important new sources of revenue and data, but also generating greater strategic leverage vis-à-vis the West.”

PRC-sponsored events and training sessions on the use of digital tools are also part of an effort to teach other countries how to copy the PRC model of digital dictatorship, not simply provide guidance on the use of digital technologies for harmless reasons. The more that the PRC can get other countries’ models of governance to mirror its own, the less risk those countries pose to PRC power (Feldstein, 2019b).

It is unlikely that outside observers will ever know the true motivations underlying the PRC’s global digital strategy. The assertion that the PRC is intentionally spreading digital tools to deepen global authoritarianism is likely overstated (Feldstein, 2021, p. 48); where we see PRC digital technologies adopted and whether they are likely to be used for repressive purposes likely has more to do with each country’s domestic environment than a PRC grand strategy.

Moreover, it is possible that countries may seek to mimic the PRC model absent any PRC pressures to do so. Tanzania’s deputy minister for transport and communications commented in 2017, for example, “Our Chinese friends have managed to block such media [Facebook, Twitter, and Instagram] in their country and replaced them with their homegrown sites that are safe, constructive, and popular. We aren’t there yet, but while we are still using these platforms, we should guard against their misuse” (Weiss, 2019).

Likewise, Vietnam created a system of rating its citizens based on “ethical standards” that is very similar to the PRC’s social credit system. Major cities in Vietnam have adopted smart city policies, as well, including using facial recognition to track crime and potentially monitor dissent. The government has

---

8 Greitens (2020a) points out that analysts debate the extent to which the PRC’s access to large amounts of global data will enhance its algorithms and machine learning processes to such a degree that it will influence security and military competition with the United States, enabling it, for example, to generate valuable insights on key countries and populations.
also sponsored an initiative to implement 5G, which could prove useful for pursuing future repressive actions (Le, 2019).

Regardless of motivations, the impact of the spread of PRC digital tools across the globe is the same. As more and more countries purchase PRC digital products, 1) their potential misuse for repression expands, and 2) PRC companies grow richer and the PRC’s economic and political leverage over those countries grows stronger. In other words, even if the PRC is not the direct driver of the spread of digital repression, it is still using its expertise in digital tools to exert greater global influence (Feldstein, 2021). The more that recipient countries grow dependent on the PRC for these technologies, the more the PRC can pressure them to pursue policies in line with PRC interests (Feldstein, 2019a). The PRC’s leading role in the digital market, therefore, enables it to leverage its economic ties to further its foreign policy might (Polyakova and Meserole, 2019).

Feldstein (2021) highlights three approaches that underlie PRC activities. First, the PRC is using its digital capabilities to tighten economic ties with other countries thereby strengthening its political influence over recipients. Second, it is trying to mold international rules related to digital technology so that they are favorable to the PRC, particularly in terms of pushing a vision of cyber sovereignty. Third, the PRC is showing other countries how to use digital repression tools to meet their political needs, through things such as training and exchanges, also deepening PRC influence.

To summarize, regardless of the precise nature of the PRC’s motivations, it is likely to continue to be at the forefront of the proliferation of digital technologies globally given that it has substantial incentive to do so.

**Digital authoritarianism in Russia**

Compared to the PRC, Russia relies less on highly technical methods in its model of digital authoritarianism, such as filtering information and surveillance. Instead, it emphasizes a repressive legal regime and tight controls on the Internet (Polyakova and Meserole, 2019). Since the 2011-2012 protests in Russia, the regime sees information flows as dangerous to its rule and seeks to control them. Rather than using overt censorship, however, Russia uses legal rules, discrete online surveillance, and online information manipulation to gain the upper hand over the information environment (CNAS, 2021).

In terms of legal tools, Russia has frameworks in place that put heavy burdens of liability on content intermediaries, thereby incentivizing self-censorship (CNAS, 2021). The Ministry of Communications and Mass Media’s Federal Service for Supervision of Communications, Information Technology, and Mass Media (referred to as Roskomnadzor) is in charge of blocking web sites and online posts with content deemed offensive. Censorship powers lie with the government, but Internet service providers (ISPs) are held legally responsible for content their users can access that is forbidden. This results in ISPs under-censoring to minimize the chance they will face heavy fines or lose their licenses (CNAS, 2021). Russia also has a bevy of laws in place to control the media environment, most of which are applied indiscriminately generating uncertainty and fear.

This legal framework is buttressed by an intense surveillance system that monitors all Internet traffic (CNAS, 2021). Russia uses a system called SORM (System for Operative Investigative Activities), which allows it to intercept and view all network content (Polyakova and Meserole, 2019). ISP and telecommunication providers are legally required to install SORM equipment (CNAS, 2021). The regime
then uses information from SORM equipment to target its opponents, including members of civil society and the media.

Russia is working to establish a sovereign Internet, as well, which means that all Russian Internet traffic would be controlled by the government and function cut off from the rest of the world (Polyakova and Meserole, 2019). If fully achieved, such a sovereign Internet would allow the regime to more easily control the information environment (CNAS, 2021).

Russia is using these strategies in conjunction with its own efforts to spread propaganda and misinformation, which are a key feature of the Russian model of digital dictatorship (CNAS, 2021). Instead of fully restricting information, it overwhelms citizens with pro-government messages and misleading stories. This strategy is effective because it distracts citizens from negative coverage of the regime and generates confusion.

While Russia is seeking to expand its abilities to surveil its citizens – it started a Safe City surveillance network in 2018 and is delivering surveillance systems to Russian schools, for example – its current surveillance capabilities pale in comparison to the PRC’s (CNAS, 2021).

Lastly, a key component of the Russian brand of digital authoritarianism is countering perceived threats outside of Russia’s borders (CNAS, 2021). Russia has used a variety of digital tools, including paid human trolls and social media bots, to generate discord and uncertainty in the information environments of other countries. Its goal is to weaken confidence and trust among citizens in democracies, as a means of protecting the Russian regime (CNAS, 2021).

**How Russia is spreading digital tools**

Russia plays a lesser role in the spread of digital tools than the PRC, but its activities in this regard are still important to highlight. Importantly, Russia is keen to establish itself as a leader in the digital economy (CNAS, 2021). Russian President Vladimir Putin stated in 2017, for example, “Artificial intelligence is the future, not only for Russia, but for all of humankind… Whoever becomes the leader in this sphere will become the ruler of the world” (CNAS, 2021). Russia sees its expansion in the digital market as important for its economy, helping to generate investment, spur growth, and garner prestige, as well as critical to its ability to free itself from dependence on Western products. It faces greater constraints to fulfilling its technological goals than the PRC does (with problems such as brain drain and corruption), but it is likely to continue to be a key player in the spread of digital technologies (CNAS, 2021).

Whereas the PRC tends to focus on the export of digital tools for surveillance and content filtering and blocking, Russia focuses primarily on providing disinformation and electoral manipulation services (Feldstein, 2021). It is worth mentioning that, interestingly, Russia is increasingly relying on PRC technology to upgrade its own surveillance capabilities (Feldstein, 2021). This cheaper model may be desirable for those countries that lack substantial capabilities and resources (Polyakova and Meserole, 2019).

Russia is primarily engaging in digital activities with former-Soviet countries (Polyakova and Meserole, 2019). For example, in 2012, following the Arab Spring protests, Russia leveraged the Collective Security Treaty Organization (CSTO) – a Russian-led regional defense alliance with Belarus, Armenia,
Kazakhstan, Kyrgyzstan, and Tajikistan – to share technology developing a joint strategy to try to deal with protests following the Arab spring (Soldatov and Borogan, 2012). That same year, the Commonwealth of Independent States commissioned Russia’s leading research center in communications (VNIIPVTI) to train experts in information security. There were also efforts in 2012 for CIS countries to establish a Center of Cybersecurity to cooperate on those issues. Many of the ideas proposed have stalled, but regardless similar efforts persist for cooperation on the use of digital technologies.

Russian companies also sell surveillance and hacking technologies, particularly to post-Soviet states (notable examples include Belarus, Ukraine, and Kyrgyzstan). Such exports are sometimes a better fit for countries than Western-made tools because Russian laws and rules for traffic interception are more compatible for them and the technologies are tailored as such (Sherman, 2021).

There are indications that Russia may be intentionally trying to export a model of digital authoritarianism. At the Russia-Africa Forum in September 2019, for example, Russia talked about offering “disinformation as a service” to other countries looking to control their domestic information environment, through things such as locally hired staff and “troll farm” offices (Brannen, Haig, and Schmidt, 2020). That said, as with the PRC, it is difficult to disentangle whether this is part of a larger political strategy or simply a way for increasing economic and political influence. Regardless, a number of dictatorships with close ties to Russia, including regimes in Belarus, Azerbaijan, and Central Asia, have adopted elements of the Russian model of digital authoritarianism (CNAS, 2021).

UNDERSTANDING THE ROLE OF THE PRIVATE SECTOR IN DEMOCRACIES

The private sector in democracies is actively participating in the proliferation of technologies used for repressive actions, as Penney, McKune, and Deibert report (2018). The Italian surveillance company Hacking Team and Israeli software company Nice Systems, for example, assisted the Thai military dictatorship in the development of a “cyber warfare” unit, which it has applied to secretly monitor citizens (McDermott, 2021). U.S. companies – such as IBM, Palantir, and Cisco – are exporting digital technologies to at least 32 countries around the globe (Feldstein, 2019a). Companies in France, Germany, Israel, and Japan are playing a major role, as well.

It is impossible to know whether private companies in democracies are actively trying to proliferate digital repression or simply acting out of their economic interests. As one member of the technology industry in Israel commented, “Everyone in this field knows that we are manufacturing systems that invade people’s lives and violate their most basic rights. It’s a weapon – like selling a pistol. The thing is that in this industry people think about the technological challenges, not about the implications” (Shezaf and Jacobson, 2018). That said, when the recipient government is autocratic (and therefore more likely to abuse human rights in the first place), the chances that these products will be applied for repressive purposes are simply higher. Exports of dual-use technology products to authoritarian countries with troubling repression records should therefore be seen as a red flag. And yet these markets are quite active. For example, one-third of European Union licenses to export surveillance products were intended for countries Freedom House determined “not free” (Hawkins, 2018).

Examples of authoritarians’ misuse of dual-use technologies purchased from private companies operating in democracies abound (Penney, McKune, and Deibert, 2018). For example, the Canadian technology company Netsweeper’s products are being used to filter online content in authoritarian regimes such as
UAE, Bahrain, and Sudan. There are many other similar companies, such as Sandvine, FinFisher, Hacking Team, NSO Group, and BlueCoat, which sell products that should be used for intelligence and law enforcement officials to protect citizens but are instead being used by autocracies. Penney, McKune, and Deibert (2018) point out that when there are pressures for these companies to do something, they typically respond with vague statements and take little action.

Experience from Israel is illustrative of the challenge. According to an investigation by the news outlet Haaretz, Israel has become a major exporter of tools used to spy on civilians, with testimonials from individuals in 15 countries revealing that these tools have been used to violate human rights (Shezaf and Jacobson, 2018). Israeli-based company NSO Group, for example, has a tool called Pegasus which can be used to surveil individual citizens using their cell phones in total secrecy. An additional investigation by the Washington Post (in conjunction with 16 media partners and the nonprofit group Forbidden Stories) was even more damaging to the NSO Group (Washington Post, 2021). It found that the Pegasus tool had been used by governments to hack 37 smartphones belonging to journalists, human rights activists, and business executives, as well as those of the two women who were very close to Jamal Khashoggi, the murdered Saudi journalist. As Haaretz reported, demand for such tools is high, and Pegasus has been extremely profitable for the company. The investigation found that Israeli firms continued to export their products even when public reports revealed that they were being used for repression. Private Israeli companies have sold surveillance products to authoritarian regimes in Bahrain, Angola, Mozambique, Swaziland, Azerbaijan, and Nicaragua, to name a few, where testimonials reveal that they were indeed used to commit human rights abuses. The exports are legal and – from the private companies’ perspective – there is little they can do to prevent abuses once their products are sold.

SYNTHESIS OF SUGGESTED POLICY RECOMMENDATIONS

A number of policy papers and briefs address the issue of what should be done to deal with the rise of digital authoritarianism. All of these papers share the perspective that the international community should be doing more in this domain and that existing efforts are falling short. They also share the concern that the issue is pressing, given that digital authoritarianism is only continuing to spread and intensify.

In these ways, the debate over how to deal with the spread of dual-use digital technologies is similar to longstanding international concerns with the spread of dual-use nuclear technologies. As Shahbaz (2018) points out, the ethical and moral concerns are comparable. Democracies want to secure these technologies for security reasons, making it difficult for them to adopt the moral high ground. Likewise, countries can also justify their purchasing of such technologies as benign, given their dual-use nature.

The global COVID-19 pandemic has created a new opportunity for the potential technological misuse. As discussed earlier, at least 54 countries around the world that have deployed COVID-19 related smartphone applications — intended for contact tracing, enforcing quarantines, assessing health statuses, and other public health goals (Shahbaz and Funk, 2020). Few of these applications, however, have protections in place to ensure that governments do not abuse them for surveillance purposes.

We summarize some of the common themes and debates in the recommendation literature here. We emphasize that these suggestions (to our knowledge) are not necessarily grounded in the findings of empirical research. That said, they do represent what experts in this area contend should be pursued.
Regulation

Most observers assess that greater regulation of private companies that sell digital products with the potential to be used for repression is needed. That said, there is little consensus about what should be done (Yayboke and Brannen, 2020). Some argue that businesses should self-regulate, but most assess that governments need to get involved and play a stronger role.

The problem with self-regulation is that many companies just will not do it on their own, particularly due to fears over market losses absent a coordinated effort (Yayboke and Brannen, 2020). Moreover, self-regulation is often ineffective. Technology companies frequently put in place ethical guidelines to prevent the harmful use of their products, which is an easy option for companies so that they can appear proactive (Bacciarelli). Yet, these guidelines typically have little substance and, once in place, there are few mechanisms for holding companies accountable for any breaches (Bacciarelli, 2019). In the area of AI, most “codes of ethics” emphasize commitments to fairness and justice, as opposed to ensuring protections of human rights (Pizzi, Romanoff, and Engelhardt, 2021). Very little that is in them is substantively in line with the guidelines of the Universal Declaration of Human Rights; few have any guidelines in place to deal with accountability. There needs to be a much clearer articulation of what rights companies will protect and how they will ensure it (Pizzi, Romanoff, and Engelhardt, 2021).

At the same time, government regulation can have unintended consequences by favoring those companies that have the resources to comply. And, even with regulations, it is often difficult to punish companies that have broken the rules. Observers note that it is very difficult to make corporations liable (Zerk, 2012). Loopholes and roadblocks are a serious problem, which make prosecuting complicit companies extremely challenging. This results in a situation where there is little oversight or accountability over the private sector. Reforms are therefore needed to make it harder for companies to avoid prosecution.

International frameworks

Most observers support democracies doing more to push for international frameworks to deal with digital repression. The United Nations Guiding Principles on Business and Human Rights is highlighted as a good template for considering this (Feldstein, 2019b). Likewise, Pizzi, Romanoff, and Engelhardt (2021) argue that existing international human rights law already provides an organizational framework for how governments and companies can avoid using digital tools to violate human rights. Frameworks are in place, in other words, that should be leveraged. Digital technologies simply need to be folded into them. Donahoe and MacDuffee Metzger (2019) concur that the best strategy may be integrating the global digital environment into existing human rights frameworks. In a similar vein, Allen and West (2021) put forth that global treaties are urgently needed to deal with the security ramifications of artificial intelligence. They argue that such treaties could build off key principles (discussed in detail in their piece) prevalent in earlier global treaties on nuclear, biological, and chemical weapons.

Strengthening civil society

Most observers assert that civil society will play a critical role in holding actors (both governments and private companies) accountable for digital repression. For this reason, some advocate democracies dedicating more resources to strengthening civil society and better equip those within it to understand how to push back against repressive acts or breaches of existing regulations (Feldstein, 2019b). Wright
(2020) argues that civil society needs to do better to anticipate what the dangers of certain paths are and be aware of the value of data silos, which should be preserved to better protect individual rights. See Shahbaz (2018) for an in-depth discussion of how governments can work with civil society to better protect against digital manipulation.

**Human rights by design**

Some observers assess that the international community should do more to encourage companies to think about how a new technology could be used to abuse human rights as it is being developed (Donahoe and MacDuffee Metzger, 2019). This would entail training developers in human rights norms so that they can build ethical AI applications. Adopting principles of human rights by design would be a marked improvement over existing efforts at self-regulation (Penney, McKune, Gill, and Deibert, 2018). The goal would be for tools and technologies that are sold to protect human rights as a default. For a deeper discussion of this and other related strategies, see Penney, McKune, Gill, and Deibert (2018).

**Promotion of a democratic model for managing the digital era**

A number of observers argue that democracies need to show the world’s countries that they have a better model for managing the Internet — including dealing with social media manipulation, data misuse, and other problems — that shows respect for human rights while allowing a free Internet (Shahbaz, 2018). Wright (2020) likewise argues that democracies need to adapt in the face of contemporary changes and develop a model for the use of digital tools that is in line with democratic norms. In the field of AI, for example, the democratic model needs to improve security while also protecting civil liberties and human rights (Polyakova and Meserole, 2019). Democracies should work with tech companies and civil society to establish a digital governance code of conduct (Polyakova and Meserole, 2019).

Observers note that democracies’ efforts to push for standards to protect against digital repression are unlikely to be effective if democracies themselves are not abiding by them. The United States, Brazil, and India, for example, are identified as democracies that have engaged in efforts to censor material posted and searched for online (Hughes, 2012). Hughes (2012) argues that the increasing prevalence and use of platforms such as Google and Twitter have led some democracies to attempt repressive measures. In 2012, India had the most non-court backed requests for taking down posts, according to Google Transparency Reports, while the United States and Brazil had the most court-backed requests. A Twitter transparency report showed that the United States was the country with the most demands for information about individual users (Hughes also notes that the transparency reports are a good example of company-level safeguards that can be used to prevent technology abuses).

There are other examples of democracies toeing if not crossing the line. Spain asked the software development platform GitHub to remove files from an app that Catalan protestors were relying on to mobilize their movement (a move both Russia and the PRC have also done in the past) (Brannen, Haig, and Schmidt, 2020). In addition, Brazil is developing a far-reaching facial recognition system for its police forces, reportedly to deal with urban crime. The potential for repressive abuses is very real, however, given its security forces’ track record. The technology also has close links with the PRC, creating fears that Brazilian officials will try to copycat PRC repression tactics (Ionova, 2020).

**Other recommendations:**
• **Import/export controls.** Observers recommend tightening import and export controls to limit the spread of digital tools that can be used for repressive purposes (Shahbaz, 2018; Polyakova and Meserole, 2019).

• **Sanctions.** Most observers contend that there need to be stricter sanctions in place for those technology companies and governments that use and export repressive digital technologies (Shahbaz, 2018; Polyakova and Meserole, 2019).

• **Development of a ranking and reporting framework:** The international community could better keep technology companies accountable for how they sell their products to by implementing a ranking and reporting system (George, 2017). The system would track companies’ sales and activity across the globe and measure how frequently companies comply with requests to hand over data to different governments. Companies could then be ranked according to how compliant they are. This would better equip the public to put pressure on those companies with poor track records. The idea is that companies value their public image enough that they would avoid enabling repression if they were likely to get called out for it. The Ranking Digital Rights Corporate Accountability Index (Ranking Digital Rights, 2021) offers a start. It ranks 26 companies (14 digital platforms and 12 telecommunications firms) based on their disclosed commitments, policies, and practices to protect freedom of expression and privacy of Internet users worldwide.

• **Require social media platforms to remove hate speech.** For the problem of state-sponsored trolling, the recommendation is that governments require social media platforms to remove hate speech and implement this in a transparent way (in the United States, potentially using the First Amendment to build upon existing hate speech prohibitions) and work with technology companies to detect and identify state-sponsored accounts (Nyst and Monaco, 2018).

• **Address the demand for dual-use digital technologies.** Many countries seek out digital tools for legitimate reasons, even though these tools have the potential to be used for repressive purposes. Addressing the demand for dual-use technologies, therefore, has the potential to limit the spread of digital repression (Yayboke and Brannen, 2020), particularly in countries that are still democratic. Research shows, for example, that demand for dual-use technologies is particularly high among countries with high crime rates (Greitens, 2020a). And PRC technology companies often tout this as justification for the export of dual-use products. One tactic for limiting the spread of digital repression, therefore, would be to help such countries reduce their crime rates (or other challenges), without having to rely on dual-use technologies.

**CONCLUDING REMARKS**

The consensus among experts is that digital authoritarianism is on the rise worldwide, and there are few indications that this trend is likely to reverse course anytime soon. For supporters of democracy and global freedom, these trends are alarming. Protests from below are currently the most frequent way that contemporary dictatorships collapse, and yet digital repression is shown to lower their onset. Likewise, digital repression in authoritarian regimes is associated with more durable authoritarian rule. Even in democracies, digital repression appears to go hand in hand with democratic backsliding. Future
research is needed to assess whether the latter are causal relationships, but regardless they paint a dim picture of the future of democracy.

At the same time, all is not lost. It is worth remembering that even the highly repressive and tightly controlled Soviet Union eventually collapsed from within, along with the bulk of its satellite regimes. Opportunities for opposition mobilization can emerge in unlikely moments and places. Moreover, opposition tactics can and do evolve in unanticipated ways. It is possible that ordinary citizens will develop innovative and effective techniques for pushing back against digital authoritarianism; it is also possible that we will see the emergence of “liberation” technologies that actually deliver.

In the meantime, observers have put forth a handful of strategies policy makers could pursue that have the potential to be effective at slowing digital authoritarianism’s spread, which we highlighted here. Existing literature emphasizes the importance of intensifying regulation of private companies, developing an international framework for dealing with the proliferation of dual-use digital technologies, strengthening civil society actors, developing products that protect human rights by design, and promoting a democratic model for managing the digital era.

Unfortunately, these suggestions are not tightly wedded to findings from academic research in this area, which has struggled to catch up to the rapidly evolving digital repression landscape. For this reason, we see dedicating greater resources toward academic research on digital authoritarianism as an additional suggestion worthy of pursuit. As this literature review has made clear, future research is needed in a variety of domains. Filling in these holes will not only improve understanding of digital authoritarianism, but also the efficacy of strategies pursued to limits its diffusion.
ANNEX I

TABLES AND FIGURES

Figure 1. Average digital repression by country: 2000-2019

Description: Figure 1 depicts a world map with a color scale to indicate a country’s average digital repression score from 2000-2019.

Figure 2. Average digital capacity by country: 2000-2019

Description: Figure 2 depicts a world map with a color scale to indicate a country’s average digital capacity score from 2000-2019.
Table 1. Average reliance on digital tools by political system type (in 2019)
(Higher values equal greater reliance)

<table>
<thead>
<tr>
<th>Category</th>
<th>Digital tool</th>
<th>Democracies</th>
<th>Dictatorships</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital repression</td>
<td>Government social media censorship in practice</td>
<td>-0.81</td>
<td>1.11</td>
</tr>
<tr>
<td></td>
<td>Government social media monitoring</td>
<td>-0.61</td>
<td>1.35</td>
</tr>
<tr>
<td></td>
<td>Government social media shut down in practice</td>
<td>-1.11</td>
<td>0.75</td>
</tr>
<tr>
<td></td>
<td>Government Internet shut down in practice</td>
<td>-1.02</td>
<td>0.67</td>
</tr>
<tr>
<td></td>
<td>Government Internet filtering in practice</td>
<td>-1.10</td>
<td>1.23</td>
</tr>
<tr>
<td></td>
<td>Government social media alternatives</td>
<td>-0.86</td>
<td>0.86</td>
</tr>
<tr>
<td>Digital Capacity</td>
<td>Government cyber security capacity</td>
<td>0.22</td>
<td>0.19</td>
</tr>
<tr>
<td></td>
<td>Government Internet shut down capacity</td>
<td>-0.26</td>
<td>0.98</td>
</tr>
<tr>
<td></td>
<td>Government Internet filtering capacity</td>
<td>0.02</td>
<td>1.10</td>
</tr>
<tr>
<td></td>
<td>Government capacity to regulate online content</td>
<td>0.30</td>
<td>0.87</td>
</tr>
<tr>
<td>Other</td>
<td>Government online content regulation (as opposed to</td>
<td>-0.66</td>
<td>0.63</td>
</tr>
<tr>
<td></td>
<td>regulation by private actors)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 2. Dictatorships that repress less than their capacity

<table>
<thead>
<tr>
<th>Country</th>
<th>Years</th>
</tr>
</thead>
<tbody>
<tr>
<td>Armenia</td>
<td>1999-2018</td>
</tr>
<tr>
<td>Belarus</td>
<td>1995-</td>
</tr>
<tr>
<td>Botswana</td>
<td>1967-</td>
</tr>
<tr>
<td>Hungary</td>
<td>2019-</td>
</tr>
<tr>
<td>Kuwait</td>
<td>1962-</td>
</tr>
<tr>
<td>Malaysia</td>
<td>1958-2018</td>
</tr>
<tr>
<td>Russia</td>
<td>1994-</td>
</tr>
<tr>
<td>Singapore</td>
<td>1966-</td>
</tr>
</tbody>
</table>

Table 3. Dictatorships that repress more than their capacity

<table>
<thead>
<tr>
<th>Country</th>
<th>Years</th>
</tr>
</thead>
<tbody>
<tr>
<td>Burundi</td>
<td>2011-</td>
</tr>
<tr>
<td>Cambodia</td>
<td>1980-</td>
</tr>
<tr>
<td>Chad</td>
<td>1991-</td>
</tr>
<tr>
<td>Congo/Zaire</td>
<td>1998-</td>
</tr>
<tr>
<td>Eritrea</td>
<td>1994-</td>
</tr>
<tr>
<td>Ethiopia</td>
<td>1992-</td>
</tr>
<tr>
<td>Guinea Bissau</td>
<td>2013-2014</td>
</tr>
<tr>
<td>Guinea</td>
<td>1985-2008; 2009-2010</td>
</tr>
<tr>
<td>Korea North</td>
<td>1949-</td>
</tr>
<tr>
<td>Laos</td>
<td>1976-</td>
</tr>
<tr>
<td>Libya</td>
<td>1970-2011</td>
</tr>
<tr>
<td>Madagascar</td>
<td>2010-2013</td>
</tr>
<tr>
<td>Nepal</td>
<td>2003-2006</td>
</tr>
<tr>
<td>Nicaragua</td>
<td>2017-</td>
</tr>
<tr>
<td>South Sudan</td>
<td>2012-</td>
</tr>
<tr>
<td>Sudan</td>
<td>1990-2019</td>
</tr>
<tr>
<td>Tajikistan</td>
<td>1992-</td>
</tr>
<tr>
<td>Turkmenistan</td>
<td>1992-</td>
</tr>
</tbody>
</table>
Figure 3. Digital repression and capacity in democracies and dictatorships over time: 2000-2019

Description: Figure 3 depicts two side-by-side line graphs showing average scores of digital repression and capacity in democracies and dictatorships 2000-2019. The line graph in the left depicts digital repression scores, while the graph in the right depicts digital capacity scores.
Figure 4. Ranking of digital repression by authoritarian regime

(Blue dots represent the regime’s average digital repression during the period; bars represent their range of scores)

Description: Figure 4 depicts a chart indicating each authoritarian regimes’ average digital repression score.
REFERENCES


Citizen Lab, “Communities @ Risk: Targeted Digital Threats Against Civil Society,” 2014. Available at: https://targetedthreats.net/media/1-ExecutiveSummary.pdf.


Feldstein, Steven, “When It Comes to Digital Authoritarianism, China is a Challenge—But Not the Only Challenge,” Carnegie Endowment for International Peace, 2020. Available at:


Geddes, Barbara, Joseph Wright, and Erica Frantz, “Autocratic Regime Data,” Pennsylvania State University, 2014. Available at: https://sites.psu.edu/dictators.


