Innovators and Emulators: China and Russia's Compounding Influence on Digital Censorship

Catherine Andrzejewski, Ana Horigoshi, Abigail I. Maher, and Jonathan A. Solis

May 2023

AIDDATA
A Research Lab at William & Mary

INTERNATIONAL REPUBLICAN INSTITUTE
Advancing Democracy Worldwide

Executive Summary

Authoritarian governments, like those of Russia and China, increasingly serve as role models for autocratizing states and export their tools of repression globally. These tools include methods and tactics used to limit and restrict free expression and press. As digital citizen engagement and online media grow, authoritarians seek new models, tools, and strategies to censor and restrict these forms of expression. Ultimately, the scale of digital media and speed at which new frameworks emerge means that even high-capacity states cannot monitor and censor all information, authoritarian regimes seek to induce citizen self-censorship in the digital information space.

This report seeks to develop an understanding of how both autocratic regimes and backsliding democracies are learning from and emulating the established authoritarian powers of China and Russia. The report maps out common authoritarian tools of digital censorship used by China and Russia. Then, the degree to which five "emulator" countries have been influenced and implemented these tools is examined. These five countries - Azerbaijan, Nicaragua, Serbia, Turkey, and Uganda - were chosen for their geographic diversity along with their differing degrees of autocratization. All five are also battlegrounds for influence among China, Russia, and the West. Finally, the report summarizes which lessons emulator countries may be learning from the "innovators" along with key findings and takeaways.

Principal Conclusions

- Digital censorship is broadly on the rise in countries featured in this study.
- China is the premier innovator in digital censorship with the most advanced tools and deepest "censorship ecosystem." While still an innovator relative to other countries, Russia's censorship regime is less sophisticated than China's.
- China and Russia use institutional tools which include legislation and regulatory bodies that are given wide latitude to censor. Legislation on digital censorship is intentionally kept vague to provide the state a broad range of actions and to adjust to rapidly shifting online trends and platforms. Some autocratizing countries in our study copied these laws nearly verbatim.
- Censorship regimes also use technological tools to target content directly or the software and hardware that enables the provision of content. Objectionable content can be targeted via human moderators, blocking social media accounts, keyword filtering along with other specific targeting methods. Software can also be censored via Distributed Denial of Service (DDoS) attacks, Domain Name System (DNS) poisoning, blocking Virtual Private Networks (VPN), Deep Packet Inspection (DPI), and blocking specific websites.
- When digital censorship regimes began to be developed by the state matters. China began to implement robust online restrictions as internet and mobile access began to proliferate in East Asia. This allowed China to develop advanced tools and strategies over time as well as set in place norms and expectations around digital expression.
- There are potential, but limited, action points to limit digital censorship. Democratic states can coordinate to set standards on Internet freedom and digital information protocols. Democracies are also on the forefront of many digital technologies that can be used by authoritarian powers, which may necessitate careful monitoring and export restrictions.

Emulator Countries

Azerbaijan

Azerbaijan has emulated both Russia and China in developing their institutional tools of censorship, particularly in the legislative arena. Following China's approach, Azerbaijan has increasingly codified previously ad hoc censorship, passing several major laws regarding content regulation in the 2010's. The COVID-19 pandemic and the ongoing armed conflict with Armenia have been used as opportunities to expand information censorship laws. Azerbaijan has also censored digital content directly through frequent bans of opposition and independent media websites along with restricting access to these organizations' social media presence. While there is limited evidence of Azerbaijan deploying more technically sophisticated methods of censorship, the Azerbaijani government has purchased equipment with DPI capabilities from Israeli and Canadian firms. Expert interviews also suggest

that Azerbaijan has deployed Pegasus software, an advanced spyware technology, with China's support.

Nicaragua

Nicaragua has mirrored Russian legislation on content regulation with one interviewed expert describing a recent law as "basically [a] copy-paste from Russia." Nicaraguan law has followed the template of vague descriptions of objectionable digital content coupled with harsh punishments for violations. Telecommunications regulatory bodies in Nicaragua are also under close control of the government and often under direct control of the President. Nicaragua rarely deploys technological tools to censor content, primarily due to a lack of technical sophistication within the government. Instead, traditional tools such as arrests and imprisonment of journalists are used to induce self-censorship.

Serbia

Serbia is less autocratic and experiences greater judicial, legislative, and regulatory independence than the preceding countries studied. Serbian laws on digital content are broadly in-line with European Union standards and do not enable broad government censorship of information. However, the report finds that Serbian "response-to-crisis" laws that provide the government broader power to regulate information in specific circumstances resembles related Russian laws. Serbia also emulates Russia and China the least in the regulatory space. Direct content targeting is relatively rare in Serbia and there is little evidence to suggest that the Serbian government engages in any form of software censorship.

Turkey

Turkey's legislative and regulatory systems do not directly enable explicit government censorship of digital information, but other regulatory structures are applied to both offline and online content. Broad anti-terror laws are used to target online journalists with criminal and civil penalties. Recent laws have increased registration requirements for social media and streaming services and have increased the ability of Turkish regulators to remove content based on the protection of "family values" and "morality" issues. Expert interviews suggest that these laws indicate that Turkey is not only emulating Russia and China, but also parts of the West. The Turkish government has the technical ability to deploy advanced technological tools such as DPI and VPN blocking. Turkey also has a more advanced domestic telecommunications industry which allows the government more direct access to infrastructure and hardware such as mobile phone sim cards. The Turkish government's technical sophistication and history of offline censorship position Turkey as both an innovator and emulator in the digital censorship space.

Uganda

Uganda's laws on digital content also feature vague wording that provides the government with broad discretion to remove content and arrest posters and journalists. Additionally, Uganda levies a tax on Internet data use which serves as a significant deterrent and burden to Internet use in a developing economy. Similarly to Nicaragua's government, the Ugandan government lacks the technical ability to deploy sophisticated technological tools. However, China is establishing an extensive presence in Uganda's digital infrastructure which may open opportunities for Uganda to emulate Chinese censorship techniques especially as Internet penetration and use remains relatively limited in the country. Huawei has already assisted the Ugandan government in penetrating the communications of opposition politicians and organizers.

1. Introduction 1
2. Key Concepts and Approach 2
    2.1. Digital Censorship 2
    2.2. Data Collection 2
3. Innovators: China and Russia 3
    3.1. Paths to Digital Censorship 3
    3.2. Institutional and Technological Environment 4
    3.3. Digital Censorship Toolkit 5
        3.3.1. Institutional Tools 6
        3.3.2. Technological Tools 9
        3.3.3. The Ultimate Aim: Self-Censorship 10
4. Emulators 12
    4.1. Institutional and Technological Environment 12
    4.2. Compounding Influence? Comparison and Analysis 14
        4.2.1. Institutional Tools 14
        4.2.2. Technological Tools 16
        4.2.3. Self-Censorship 19
5. Key Takeaways 24
6. Conclusion 26
7. References 27
8. Appendix 35

Acknowledgements

The authors would like to acknowledge invaluable contributions to this report by Rodney Knight and our International Republican Institute counterparts Caitlin Dearing Scott and Lukasz Kondraciuk. John Custer and Sarina Patterson contributed editing, formatting, and supporting visuals. We also thank Emily Elston, Morgan King, Marianna Bonilla, Kaya Lee, and Emma Williams for excellent research assistance.

1. Introduction

Illiberalism is on the rise in countries around the world, as once-promising democratic countries have regressed into more authoritarian ones. The share of the global population now living in autocratic countries has increased dramatically over the past decade, from 49% in 2011 to 70% in 2021 (Boese et al.). Varieties of Democracy (V-Dem) declared "autocratization has turned viral" in their 2021 report on democratic trends worldwide (Alizada et al.). Governments now poised to remain in power against the will of their citizenry are beginning to mirror the illiberal practices of authoritarian regimes, such as China and Russia, that project their power regionally and throughout the globe.

As authoritarian institutions deepen, governments are using more methods and strategies to solidify their hold on power, including but not limited to threats to freedom of expression and restrictions on the press. While popular consumption of traditional media such as radio, newspapers, and television declines, citizen engagement with digital and social media is on the rise as internet and smartphone access increases among individuals in developing countries (Boulianne). This has forced authoritarian leaders to rethink and repurpose older approaches to controlling the narrative (Puyosa). They have developed new tools to censor and restrict this newer, growing form of media.

In response to this alarming trend, development practitioners keen to fund programs to counteract authoritarian influence are often left with analyses that focus on the influence of a single authoritarian regime in a country or region. However, rising autocrats may take guidance from multiple foreign governments, and the compounding effects of two or more authoritarian actors in a single country remains understudied by researchers, leaving a crucial knowledge gap for practitioners.

This project begins to fill this gap. In partnership with the International Republican Institute (IRI), AidData has mapped the common tools of digital censorship utilized by China and Russia—two established, authoritarian governments keen to influence and spread illiberalism to vulnerable countries. These vulnerable countries are often backsliding in democracy or entrenching their autocratic institutions. Using reports from media watchdogs and key informant interviews, this study maps the tools used by both authoritarian and autocratizing governments for digital censorship, focusing on domestic digital censorship. The report then supplements these findings with quantitative data examining trends of digital censorship and key democracy variables over time. Finally, the study analyzes the overlap in use of censorship tools and assesses the compounding influence that China and Russia have on five specific autocratizing countries: Azerbaijan, Nicaragua, Serbia, Turkey, and Uganda. These countries vary by democracy level, ranging from Azerbaijan as the most autocratic to Serbia as the least.[1]

The report first defines key concepts like "digital censorship" and a "tool of digital censorship," which guide the data collection approach. The report then describes the data collection efforts, which include both qualitative and quantitative data. Subsequently, it evaluates the tools of digital censorship in two "innovator" countries—Russia and China—before comparing and contrasting the use of these tools in five "emulator" countries. Finally, the report provides key takeaways and policy recommendations

[1] The five case study countries range from countries that are still largely democratic, like Serbia, to those that are firmly non-democratic. Serbia in particular is not considered autocratic, though a recent report from the Varieties of Democracy (V-Dem) Institute suggests that it is one of the top autocratizing countries worldwide over the last ten years (Papada et al.). See Appendix Figure A1 for more data on each country's democracy levels over time.

2. Key Concepts and Approach

2.1. Digital Censorship

This report defines digital censorship as "actions taken by a government to remove or obscure internet content from its citizens or to limit the ability of someone to digitally transmit information to a broad audience" (Meserve and Pemstein). Implicit in this definition is that digital censorship is often not a singular act and usually does not occur in a vacuum. Governments may take several actions—such as passing laws or utilizing surveillance—that enable and/or precede the actual removal or restriction of content. This study is interested in both direct digital censorship and the enabling actions that create a "censorship ecosystem." Government acts of digital censorship also include measures to induce self-censorship, such as penalties for posting certain content or harassment and physical threats.

Specifically, this report maps the tools governments use in digital censorship. It defines a tool as *an instrument used in performing an operation or that aids in accomplishing a task*. In this study, the "operation" or "task" is censorship of digital content. Therefore, anything that allows a government to censor digital content is a tool of digital censorship. As noted above, more than one tool could be used by a government to perform digital censorship. For example, a law may allow for greater surveillance, which gives one or more regulatory bodies (usually invested with powers through a law) the intelligence to either block content or request that the content be removed. A court may affirm the government's action if it is challenged in the legal system. In some cases, the knowledge of regulations and surveillance is enough to induce self-censorship and prevent individuals from posting content, if they fear the government will take actions to censor it or punish them. Therefore, the report argues that it is more useful to consider tools as part of a larger, digital "censorship ecosystem" rather than separate, self-contained instruments.

While censorship can come from different avenues, this report focuses on government censorship. The report includes subnational actors (such as provincial courts or local officials), as long as they appear to be in concert with the national government. This includes government-directed or government-encouraged digital censorship, such as government regulation that penalizes private companies if they do not censor certain content. This study does not include digital censorship from illegal non-state actors censoring digital media, such as criminal organizations or terrorist groups, although it tries to capture contexts in which a government directs and/or works in concert with such actors.

2.2. Data Collection

This report uses both qualitative and quantitative analysis and relies on three main sources of data: desk research, key informant interviews, and quantitative democracy and censorship index data. For the desk research, AidData's research team reviewed recent (2015 or later) reports from media watchdog groups to develop a censorship profile of tools and tactics that each government in the report's sample uses to censor internet content and restrict the freedom of online expression. These media watchdogs include Freedom House, the Committee to Protect Journalists (CPJ), IFEX, the US Department of State, and Reporters without Borders (RSF).

In addition to the desk research, AidData conducted key informant interviews (KIIs) with experts in digital censorship in each country who were identified through contact with IRI or through AidData's own searches.[2] Next, AidData interviewed at least one expert from each target country (18 experts in total).[3] The key informant interviews update and fill in any areas not covered by the desk research to generate a more robust and contextualized censorship profile of each country. Finally, AidData researchers analyzed quantitative data on democracy and digital censorship over time from the Varieties of Democracy (V-Dem) dataset and Freedom House's Freedom in the World reports.

The following sections present three key features of the analysis: (i) China's digital censorship profile; (ii) Russia's digital censorship profile (and Russia's similarities and differences with China); and (iii) censorship profiles of five diverse countries from different regions, in different stages of autocratization, and with varying degrees of foreign, authoritarian influence from Russia and/or China. These five countries—Azerbaijan, Turkey, Nicaragua, Serbia, and Uganda—serve as pilots and were selected with input from IRI.

[2] This study was approved by the College of William & Mary's Protection of Human Subjects Committee (PHSC) prior to conducting the KIIs. The research was approved by the PHSC under protocol number: #PHSC-2022-04-11-15602-ahorigoshireis.
[3] Table A1 in the Appendix provides a detailed list of the number of key informant interviews per country.

3. Innovators: China and Russia

3.1.Paths to Digital Censorship

A key starting point in understanding digital censorship is the fact that it involves a larger ecosystem beyond the simple utilization of censorship tools. While this study categorizes both China and Russia as similar authoritarian malign actors, China's censorship regime is considerably more advanced and further entrenched in its society than Russia's. Moreover, Russia appears to be learning directly from China, which is often characterized as a pioneer in the use of most of the digital censorship tools this report identified. For example, in 2016, Russia hosted a forum with the founder of the Chinese Great Firewall (Schearf). Russia has also looked to China for digital censorship techniques, such as blocking Western media sites among others (Parker; Troianovski; Yuan).

China and Russia's recent histories diverge in important ways regarding digital censorship. China was already deeply authoritarian in the 1990s when it began implementing its "Golden Shield'' regime to regulate the internet, a precursor to the "Great Firewall" currently in use. Beijing recognized at the dawn of the internet its potential power and strove to exert greater control over the internet content its citizens were able to see (Hoffman 44-45). Furthermore, the collapse of the Soviet Union, along with the Tiananmen Square protests, left China in a vulnerable position as the only remaining major communist state. Attributing in large part the demise of the Soviet Union to the relaxation of the state's vigilance about Western influence through information and ideology, the People's Republic of China was determined not to make the same mistakes (French).

Russia, by contrast, exited the Soviet Union in the early 1990s with somewhat genuine intentions to open and democratize. While not a perfect democracy, the Yeltsin administration was not nearly as prone to censorship as China. Russia, perhaps due to its proximity to the European Union (EU) and involvement in some European institutions such as the Council of Europe, perpetuated a veneer of the rule of law. However, new measures passed since the 2022 invasion of Ukraine—and Russia's subsequent removal from the Council of Europe over this act of war—show Russia moving firmly away from these Western influences.

One notable distinction between how the two countries implement digital censorship is Russia's reliance on its courts. Russian courts, which do not operate independently from the Russian government, often rubber stamp media freedom restrictions and buttress digital censorship efforts. For example, Freedom House reported that in April 2018 a Russian district court ordered Telegram—a popular social media platform—to be blocked for refusing to comply with the Yarovaya Law, which requires apps to provide encryption keys to the government upon request (see Box 2 below for further detail).

The internet in Russia, often referred to as the "RuNet," played an important role as an alternative media source in its early years. On the political front, it was sometimes seen as a space for opposition political actors. In the late 1990s, when his Minister of Communication pressed for the inclusion of some form of internet regulation, Putin opposed it, stating that "We are not going to look for a balance between freedom and regulation. We will always choose freedom" (Gritsenko et al. 289). By the late 2000s, the use of digital platforms for social mobilization and civic action in Russia was growing (Alexanyan et al. 2-3).

It was not until more recently that, triggered by the identification of a political threat associated with the 2011-2012 election, Putin's regime sought to entrench digital censorship in Russia. However, Russians already had widespread access to the internet by that point (Troianovski). In retrospect, the cases of Russia and China suggest it is easier for a government to ensure internet censorship if these efforts began when the internet was not yet widespread, as was the case with China. As internet access grew, China was able to adapt its censorship efforts to the growing market (Troianovski). Moreover, and as confirmed in expert interviews, Chinese companies will often voluntarily censor to avoid running afoul with the government, in such a manner that while there is not necessarily direct coordination, the model is more nimble to changes in what the government wants to censor.

In contrast, by the time Moscow committed to engaging in widespread digital censorship, it was more difficult to wrangle such a large population already accustomed to a somewhat free internet. Russia's digital censorship regime also appears to be a reaction to periods of political or social instability,

beginning with the Chechen-Russian conflict, which occurred intermittently between 1994 and 2009 (Krushelnycky). Qualitative research further identified additional waves of increased Russian digital censorship—for example, following mass protests in 2012, the invasion of Crimea in 2014, and during the Covid-19 pandemic in 2020—although the internet was relatively uncensored until the 2022 invasion of Ukraine (Troianovski and Safronova).

In contrast to Russia (which only emphasized "cyber sovereignty" more recently), Beijing has constructed its censorship apparatus grounded on the belief that a state exerts complete control over the digital network within its borders (Mueller 779-80). With this policy, Beijing strives to create the institutional conditions to ensure digital sovereignty within its borders and has actively campaigned for "cyber sovereignty" at the United Nations for several years (Mueller 787). The key elements to achieve these institutional conditions are: (i) legislation regulating digital content; (ii) regulatory bodies that police content in the digital space; and (iii) authoritarian governance.

Legislation and regulatory bodies give censorship an air of legitimacy, while authoritarian governance ensures the state can control these processes without any further obstructions, such as citizens who elect other leaders or a judiciary that may rule against their actions. These conditions allow the state to control the more technical aspects needed to censor digital media, such as controlling telecommunications infrastructure like internet service providers (ISPs) either directly or by proxy. With its "Great Firewall" in place, Beijing can censor digital content in several ways; the report discusses this in more detail below. However, and as noted by one of key informant interviews, Beijing's ultimate aim is for individuals, the media, journalists, and businesses to self-censor.

3.2. Institutional and Technological Environment

Autocratic Governance

Autocratic governance and suppression of the opposition allow China and Russia to implement legislation and empower regulatory bodies to restrict digital freedom. Governance in both China and Russia exhibits two key features: a lack of both electoral democracy and judicial independence. Chinese and Russian citizens are unable to vote out their national leaders, and challenges to the legality of any censorship measures are usually upheld by courts that lack any independence in decision-making.[4] For example, the Russian Supreme Court rejected an appeal by the editors of Russian website *Batenka* in 2020 and upheld a 2018 decision by Kremlin censors to remove an article about a model struggling with addiction (Mediazona, "My Friend"). In the case of China, legal challenges are considerably more limited, since the media has been kept under stricter control. One prominent example of a legal challenge to censorship was a 2018 case in which a member of the public took China's media watchdog to court over new regulations describing gay relations as "abnormal" (Siu).

In sum, Russia and China's digital censorship profiles feature a "digital censorship ecosystem" that begins with the concept of "cyber sovereignty," is made possible by digital censorship legislation and regulatory bodies, and is maintained by their autocratic political environments.

Internet Infrastructure

While institutional features create the conditions that enable digital censorship, technology allows the state to directly implement censorship measures. Here, the report details the technological infrastructure that not only enables governments to monitor their citizens but also creates alternative digital worlds.

A key feature of China's internet is the creation of digital platforms within the Chinese sovereign domain that do not interact with individuals outside of China or only do so minimally.[5] To this end, controlling telecommunications companies remains a key goal for Beijing. Three ISPs dominate the market: China Mobile, China Unicom, and China Telecom (Freedom House, "Freedom on the Net 2021: China"). China Mobile and China Unicom control most of the broadband market, and these two ISPs, along with China Telecom, also control most of the mobile market. China no longer allows foreign social media and messaging services in

[4] Autocratic institutions have deepened in Russia and China over time. Freedom House describes Russia and China's legal environment in its 2016 report on Freedom on the Net. See Freedom House, "Freedom on the Net 2016: Russia" (C. Violations of User Rights: Legal Environment) and Freedom House, "Freedom on the Net 2016: China" (C. Violations of User Rights: Legal Environment). Figure A1 in the Appendix presents data for Russia and China on digital censorship and three democracy indicators from 2010 to 2021, including electoral democracy, judicial independence, and Freedom House's Freedom in the World's democracy measure. The Appendix describes the data in more detail.

[5] Freedom House notes, however, that it is essential for the government and businesses in China to use virtual private networks (VPNs) to interact with the outside world. This had led to much regulation but not banning of VPNs (Freedom House, "Freedom on the Net 2020: China").

favor of those created within its borders that it can control. For example, WeChat is an app created by Chinese tech company Tencent that includes messaging, several aspects of social media, and mobile payment capabilities. It includes many features of banned Western apps like Facebook and Twitter.

Similarly, Russia's Information and Communication Technology (ICT) infrastructure remains concentrated within a few companies that are government controlled or heavily influenced. The state-owned Rostelecom controls 41% of the fixed broadband market by revenue, while ER Telecom and MTS hold 11% and 8% of the market, respectively (Freedom House, "Freedom on the Net 2021: Russia"). Smaller companies control the remaining shares. Four ISPs control the vast majority of Russia's mobile market: MTS (30%), MegaFon (28%), VEON (20%), and Tele2 (19%) (Freedom House, "Freedom on the Net 2021: Russia"). Furthermore, there is evidence of telecom companies aiding the government in stifling the opposition. For example, members of Russian opposition activist groups have claimed their Telegram accounts were hacked by a state security agency enabled by internet provider MTS (Telesoft).

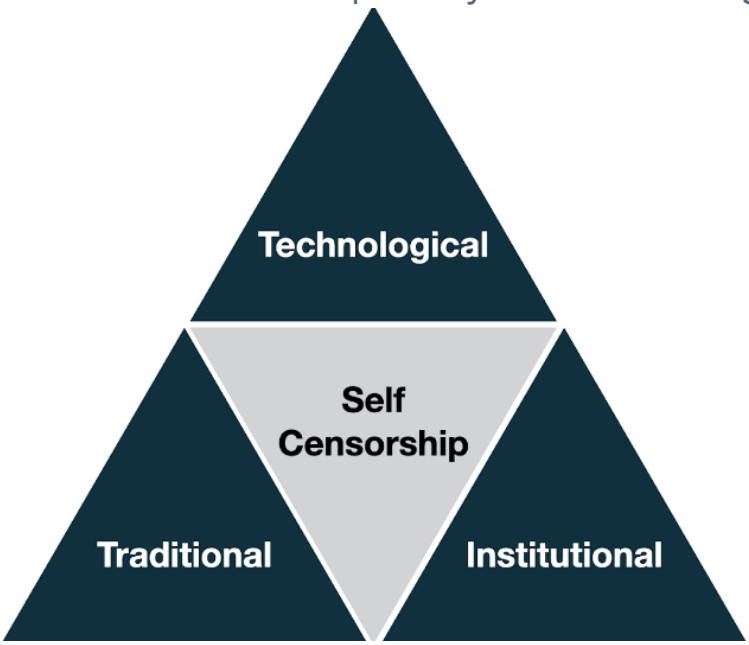
Russia's most popular social media platform is the Russian-owned and -based VK. However, while attempts to create other Russian social media platforms exist, a key informant expert confirmed they are not as popular as Western-based platforms such as YouTube (which is still very popular and used in Russia as a platform of dissent, although this may change as recent laws restrict the use of virtual private networks (VPNs) needed to access it). This speaks to how entrenched the internet and Western platforms were in Russia prior to serious censorship efforts (Troianovski). Moreover, since the start of the war in Ukraine, Russia has blocked several Western social media websites, such as all Meta platforms (except for WhatsApp) and Twitter. These efforts may further change the social media landscape in Russia, as the conflict is ongoing, but so far Russians have still been able to access them.

3.3. Digital Censorship Toolkit

As noted above, digital censorship does not occur in a vacuum. Rather, it grows in a "censorship ecosystem"—an environment that features traditional censorship, an authoritarian institutional context, and the technological means to censor, all with the goal of achieving citizens' self-censorship. Figure 1, below, illustrates this censorship ecosystem.

China and Russia use a full suite of tools and resources to implement digital censorship to different degrees. The sections below elaborate on the following categories of tools: institutional tools, technological tools, and traditional tools that promote self-censorship.

Figure 1: Components of a "Censorship Ecosystem" Fostering Self-Censorship



Box 1: Major Digital Censorship Legislation in China Since 2015

Article 84 of the 2015 Counter-Terrorism laws has implications for digital content, including fines and up to 15-day detentions for telecommunications firms and internet service providers that failed to restrict "terrorist or extremist content." It also prevents social media users from sharing content about acts of terrorism that could promote copycat attacks. In addition, this law requires companies to help decrypt information at the request of authorities.

The 2017 Cybersecurity Law includes further direction for fines and detention for sharing content, but also identifies the Cybersecurity Administration of China (CAC) as the agency responsible for implementing the legislation. The CAC reports directly to the Central Cyberspace Affairs Commission. The extensive law has many implications for internet companies. It increases censorship requirements, enforced data localization, requires real-name registration, and forces them to comply with any government investigations. Due to this law, a 2018 CAC regulation obliges internet companies "of public-opinion nature" or that have "the capacity for social mobilization" to undergo "voluntary" assessments of their ability to prevent "security risks." Further requirements include mandated on-site inspections, as well as for companies to maintain data on personal information, including real names, IP addresses, activity logs, and the type of device used. Finally, the 2017 law mandates that internet companies must store the data of Chinese users on domestic servers, making it more accessible to the government.

The 2020 Encryption Law allows the CAC to review critical information, namely infrastructure providers' encryption technologies, based on their ability to impact national security.

The 2021 Data Security Law obliges organizations to manage data activities both within and outside of China that could harm China's national security or the public interest of Chinese citizens or organizations. It also requires businesses to obtain state approval to share data with a foreign government authority.

3.3.1. Institutional Tools

Legislation

Both China and Russia use legislation to foster and encourage digital censorship. The section below provides a brief overview of the legal context in China and Russia and details a few of the major pieces of legislation passed in the two countries since 2015.[6]

In China, much digital censorship initially occurred on an *ad hoc* basis, with existing practices later consolidated into official legislation to lend legitimacy to how the government censored digital content.[7] That legal transition largely took place around the 2018 party-state restructuring, in which the most sweeping digital censorship legislation was crafted. However, the prioritization of control over the information sphere, in an attempt to forestall challenges to the Chinese Communist Party's (CCP) legitimacy, is linked with Xi Jinping since his ascension to power in 2012 (Qiang 53).

One feature of these laws is that they are often vague and widely encompassing. One of the most comprehensive pieces of legislation from this period in China was the 2017 Cybersecurity Law, which is still used as the baseline for China's current guidelines (Maranto). The law provides further direction to officials for fines and detention for sharing content undesirable to the CCP, but also identifies the Cybersecurity Administration of China (CAC) as the agency responsible for implementing the legislation. Box 1 above presents more detail about the 2017 Cybersecurity Law as well as other examples of major digital censorship legislation in China since 2015. Once this legislation was passed, the CCP was able to issue regulations that both citizens and companies must follow.

In the case of Russia, the proliferation of digital technologies coincided with the "authoritarian turn" observed under President Putin in the 2010s (Smyth 339). Until 2012, there were no specific regulations regarding online content, and the Russian internet was regulated through more general laws, such as the Law on Mass Media. In 2012, digital censorship regulation kicked off with the creation of the Unified Register of banned web pages and sites through an amendment to the Federal Law "On the Protection of Children from Information Harmful to their Health and Development." Since 2015, Moscow has passed several major pieces of legislation that

[6] The Appendix provides a more detailed list.
[7] Key informant expert and Freedom House, "Freedom on the Net 2017: China."

make digital censorship easier. A notable example is the 2019 Sovereign Net Law. This sweeping and extensive legislation proposes to allow the Russian internet to operate independently of the global DNS servers. This law is based on the same "cyber sovereignty" philosophy that is at the root of China's Great Firewall. Russia has also amended a 2012 law on "foreign entities" to require journalists and media outlets with funding outside of Russia to register as foreign entities. The law is often a precursor to large fines and government harassment, such as when a Moscow court used the law to fine *The New York Times* 22.3 million rubles ($338,000 USD) in 2018 (CPJ, "Russia uses 'foreign agents' law") and to harass Roman Dobrokhotov, founder and editor of investigative website *The Insider* in 2021 (CPJ, "Russian authorities harass family"). Before the 2022 Russian invasion of Ukraine, independent news website *Mediazona* and human rights news website *OVD-Info* were also declared "foreign agents" (CPJ, "Russia labels Mediazona"). Box 2 below explains this law in more detail, and gives other examples of major Russian digital censorship legislation since 2015. As in China, Russian laws are intentionally vague to allow for broad application (Kravchenko 174).

Responses observed from the tech industry varied according to each piece of legislation. In the case of Telegram, when the company failed to provide Russia's security services with backdoor encryption keys, the app was blocked in Russia. The blocking lasted from 2018 until 2020 but was mostly unsuccessful, as Telegram routes traffic through Amazon's and Google's cloud services and blocking those services entirely resulted in several malfunctions of online banking and retail services that also used those cloud services across the country.[8] The ban has since been lifted following requests from Telegram's founder who cited ongoing efforts to improve the removal of extremist propaganda without violating users' privacy (Sherman). In China's case, Apple has had to compromise in multiple instances to remain operating in China. It has aided in government censorship of the Chinese version of Apple's App store and built a data center in China to store the information of its Chinese customers and comply with the Cybersecurity Law (Nicas et al.). The CAC has also applied the law to domestic companies, including fines levied at Weibo and Douban in 2021 (Lin).

Regulatory Bodies

Both China and Russia have passed legislation that either established regulatory bodies or assigned greater responsibility to existing bodies. The vagueness of the legislation remains key, as it usually results in the assigned regulatory bodies being vested with significant leeway to enforce digital censorship.

Beijing relies on several regulatory bodies to implement digital censorship legislation. While not an exhaustive list, Box 3 below highlights several key bodies. The most important body in China is the Cyberspace Administration of China (CAC). The CAC oversees the telecommunications sector and regulates content online in China. It reports to the CCP's Central Cyberspace Affairs Commission, which is headed by President Xi Jinping. Much of its authority comes from the 2017 Cybersecurity Law. In 2020, the CAC implemented additional measures that further restricted internet freedom. A draft version of new measures in 2022 moved further in that direction by making all online comments subject to a pre-review before being published (Yang).

Russia also has several bodies it utilizes to censor digital content, detailed below in Box 4. The most important is the Federal Service for Supervision of Communication, Information Technology, and Mass Media (Roskomnadzor). Roskomnadzor was formed in 2008 via a presidential decree[9] but its censorship power dramatically increased in 2019 with the Sovereign Internet Law described in Box 2 above.

[8] As Vlad Savov predicted in *The Verge* when the Kremlin initially initiated the ban (Savov).

[9] By Decree No. 1715 issued December 3, 2008 (Roskomnadzor).

Box 2: Major Digital Censorship Legislation in Russia Since 2015

The 2016 Yarovaya Law makes widespread amendments to existing laws and further limits internet freedom in Russia. One of these amendments was to Article 205.2 of the Criminal Code, which imposes prison terms of up to seven years for inciting or justifying terrorism on the internet. The altered laws are vaguely worded and feature strong penalties for actions online, both of which can be used to censor legitimate speech online. The Yarovaya Law also requires internet service providers to install equipment to collect and retain the network traffic data of their users and requires social media companies to provide their encryption keys to the government.

The 2019 Sovereign Internet Law establishes Russia's "cyber sovereignty." Key features of the bill include establishing a domain name system (DNS) specific for Russia, severing Russia from the global DNS. The law also includes provisions for data localization; when a user in Russia uses any website or mobile application, their data from these online engagements must be stored in Russia. Cyber sovereignty is intended to give the Kremlin greater control over narratives in digital content and the ability to control coordination efforts.

The 2020 COVID-19 Fake News Law further expands on the 2019 Fake News Law to increase fines for fake news regarding COVID-19 and anything that poses a "danger to the health and safety of citizens." Individuals can be fined up to 700,000 rubles for sharing information online or up to 2 million rubles if authorities deem the content as leading to someone's death under Articles 207.1-2 of the Criminal Code. Organizations can be fined up to 5 million rubles under Article 13.15 of the Administrative Code. The Fake News Law can even lead to imprisonment if false information led to a person's death and if individuals knew the information was false but wrongly presented it as true.

The Foreign Agents Law passed in 2012, amended in 2019, and amended again in 2020 has been increasingly used to censor individuals and organizations that criticize the government. The law initially required organizations (such as non-governmental organizations) that receive any amount of foreign funding and engage in vague "political activities" in Russia to register as "foreign agents." In 2019, legislators expanded the law to apply to individuals as well who share online information and receive foreign funding, allowing the government to block the websites and social media accounts of these "foreign agents." The law was expanded again in 2020 to label any individual or organization as a foreign agent if it was not registered as a legal entity. The law also requires media outlets to label foreign agents by their status when mentioned in any publication.

The 2021 Law on Blocking Defamatory Information allows the Prosecutor General's Office to block "inaccurate information that discredits the honor and dignity of a citizen or undermines his reputation and is associated with the accusation of this person of committing a crime." The law increases the ability of the Prosecutor General's Office to extrajudicially block content.

Box 3: Top Digital Censorship Regulatory Bodies in China

The Ministry of Industry and Information Technology (MIIT) regulates China's telecommunications industry and oversees the gateway operators, which all service providers must subscribe to as part of the Great Firewall. Like many Chinese agencies, it also has the ability to issue regulations on digital censorship.

The State Council enforces digital censorship via its State Council Information Office. The State Council restricts who can share news on the Chinese internet and manages Chinese media. It can also approve business measures regarding the use of virtual private networks (VPNs) for foreign companies in the country.

The Cyberspace Administration of China (CAC) reports to the CCP's Central Cyberspace Affairs Commission, which is headed by President Xi Jinping. The CAC oversees the telecommunications sector and regulates content online. Under the 2017 Cybersecurity Law, the CAC became the primary regulatory body responsible for implementing the law and the digital censorship efforts it outlined. The agency can restrict access to social media platforms and apps that contain banned content.

The Central Cyberspace Affairs Commission is China's highest authority on internet policy and a CCP entity led directly by Xi Jinping. Working mostly through the CAC, it regulates the internet and telecommunications sector.

Box 4: Top Digital Censorship Regulatory Bodies in Russia

The Federal Service for Supervision of Communication, Information Technology, and Mass Media (Roskomnadzor) has steadily increased in power, jurisdiction, and prestige over the course of the report's period of study. Culminating with legislation passed since the 2022 Russian invasion of Ukraine, it is the main enforcement wing of digital censorship in Russia. For example, it maintains a list of blocked websites and makes requests for blacklisted websites to be blocked or content to be removed and taken down. It is also tasked with implementing the "Sovereign RuNet."

The Federal Security Service (FSB) engages in electronic surveillance of both journalists and regular internet users. It also has the ability to restrict access to encrypted services, such as requesting telecommunications providers to block messaging services such as ProtonMail without needing permission from Roskomnadzor.

The Prosecutor General's Office can block content online, such as restricting access to the popular social media site Telegram. The Prosecutor General's Office blocks so-called "extremist" content and posts that call for mass protests. Under the Law on Blocking Defamatory Information, the Prosecutor General's office was authorized to block "inaccurate information that discredits the honor and dignity of a citizen or undermines his reputation and is associated with the accusation of this person of committing a crime."

The Federal Financial Monitoring Service (RosFinMonitoring) maintains a list of individuals who have been investigated for "extremist" activities, even if they were never convicted of a crime, and can cause them to be banned from certain professions and have their bank accounts frozen.

3.3.2. Technological Tools

Direct Content and Software Censorship

This section details how digital censorship can be applied explicitly to content online or the software that provides the content. In China, the "Great Firewall" enables two forms of digital censorship: (i) techniques that target digital content directly and (ii) software censorship tools and techniques that target the technologies that deliver digital content. China pursues the following digital content censorship: blocking websites via widespread HTTP usage,[10] filtering for words and subsequently blocking that content, shutdowns/blackouts, closing social media accounts, disabling posts and comment sections, and removal of digital content by human moderators. For example, several key informant experts noted that China (and Russia) use middleboxes, the physical structures used to intercept and censor internet transmissions.

China also uses a number of software censorship technologies, including: cyberattacks, distributed denial-of-service (DDoS) attacks, deliberate throttling (slowing the load time of webpages), DNS poisoning (e.g., returning fake pages or replacing the requested site with content retrieved from an unrelated IP address), blocking VPN technologies, and Deep Packet Inspection (DPI, a method of examining data files through monitor checkpoints). These tools are more malicious in nature and are generally done under the radar rather than out in the open via legislation and regulatory bodies. For example, GitHub experienced a large DDoS attack in 2015 that security researchers at Insight Labs indicated originated in China: "...[T]he DDoS specifically target[ed] two GitHub projects that are designed to combat censorship in China: GreatFire, and cn-nytimes, a Chinese language version of *The New York Times*" (Anthony).

Russia, like China, also utilizes multiple methods of digital content and software censorship. For example, Russia blocks specific websites to censor digital content. Roskomnadzor maintains a list of websites it requires to be blocked, and companies that fail to do so are subject to fines. For example, Freedom House reports that *Meduza*—an award-winning Russian and English media outlet that is blocked in Russia and currently registered in Latvia—no longer appeared in search results in Yandex, a Russian search engine.[11] Russia also filters digital content for specific words and subsequently blocks that content. Yandex filters results based on Roskomnadzor's blacklist of websites (RSF). Russia also uses internet shutdowns and blackouts; before the country's September 2019 regional elections, part of Moscow experienced a disruption of fixed and mobile internet connections related to protests (US Department of State, "2019: Country Reports on Human

[10] A key informant expert explained that the purpose of HTTP use over HTTPS was that the lack of security allows easier site-specific blockings. This makes monitoring and censoring web pages easier in general.

[11] Several other websites were also blocked, including (but far from limited to) BBC News and Deutsche Welle (RFE/RL).

Rights Practices: Russia"). Other censorship tools used by Russia include closing social media accounts and removing digital content. For example, Freedom House reported that Roskomnadzor has removed several hundred pieces of digital content since the "Fake News" bill took effect in 2019 (Freedom House, "Freedom on the Net 2021: Russia").

Additionally, Russia has also resorted to blocking apps. The case of Smart Voting is one example. The app, developed by associates of opposition leader Alexei Navalny, was built to help Russian voters choose the candidate more likely to beat the ruling United Russia in each polling district. The Russian government blocked the website after Navalny's organization was classified an "extremist" organization. Upon pressure from the government, Google and Apple both removed the app from their respective app stores in Russia. Moreover, Russia also restricted access to YouTube videos and Google Docs files containing the names of the suggested candidates (Lokot and Wijermars).

China has also doubled efforts to automate censorship using AI technology. According to employees of Bytedance Ltd., TikTok's parent company, AI can accurately identify and remove content related to the 1989 crackdown in Tiananmen Square (Cadell). Chinese researchers have also developed an AI text censor that is 91% accurate, in comparison to traditional machine censors who rely on keywords and reach only 70% accuracy (Chen).

3.3.3. The Ultimate Aim: Self-Censorship

As one key informant interview noted, it is impossible for any government to see everything in the digital space. While China and Russia do employ technology and people to monitor and censor digital content, the ultimate goal appears to be inculcating self-censorship throughout society. If the state can create sufficient conditions conducive to censorship, then it can rely on the combination of customs, legislation, and social pressure to induce businesses and individuals to self-censor what they post and share online. Reducing users' anonymity online and deploying pro-government trolls also contribute to self-censorship. This section discusses digital censorship tools used in Russia and China (beyond the ones described above) that are not direct digital censorship tools but rather inculcate self-censorship.

Given the staggering amount of digital content from over a billion people in China, it is not possible for Beijing to monitor and potentially censor all citizens' content. Similarly, in Russia it is not possible for the Kremlin to censor all citizens' content from over 140 million people. Both Beijing and Moscow rely on tools—technological as well as traditional—to encourage self-censorship. Some are classic methods to suppress media and restrict press freedom that existed long before the internet. These include jailing, imprisoning, detaining, and physically harassing journalists based on content posted online. For example, a Russian blogger was detained and jailed for 25 days after covering the January 23 protest in Ulan-Ude, the Russian Far East District near the Mongolian border, in support of Russian opposition leader Alexei Navalny (CPJ, "Russian blogger jailed"). During the onset of the COVID-19 pandemic, officials in China arrested video journalist Zhang Zhan from Wuhan for posting a video to YouTube critical of the government's response to the virus (CPJ, "Journalist Zhang Zhan"). It is also worth noting that Russia has drastically ramped up censorship since the beginning of the war in Ukraine, with arrests, fines, and detainments of thousands of individuals for online and offline anti-war speech (Human Rights Watch, "Russia: Harsh Sentence").

These examples demonstrate that although surveillance online does not directly censor content, it allows the government to monitor individuals, who in turn know they are being surveilled and may change their behavior in response. For example, Zhang's video remains on YouTube, so the video was not necessarily censored, but she still faced consequences that led her to refrain from posting additional critical content online. In another example, one key informant interview relayed a story in which a Chinese student in Australia used Twitter to criticize the Chinese government. After her tweet, the student received a phone call from her father in China—with Chinese authorities present—asking her to remove the post. The student complied. In Russia, policies promote surveillance, such as the Investigative Committee (the country's main investigative body) requiring service providers to grant them network access and provide any requested information during search operations. Furthermore, recent laws prevent Russian citizens from using anonymized subscriber identity module (SIM) cards, which allows cooperative telecom companies to reveal critical online voices to the Kremlin (HRW, "Critics Under Attack"). This is related to a general policy that China started but Russia soon followed on reducing anonymity online. Both countries have passed legislation to do so, with the aim of registering users who can be easily found and subjected to fines or other punishments for posting content unfavorable to the government.[12]

[12] Such legislation includes Russia's Law on Information, Information Technology and Information Security that took effect in 2018 (Freedom House, "Freedom on the Net 2018: Russia") and several of

Likewise, companies with a digital presence often self-censor to avoid penalties and fines from the government. They are also often required to self-audit content. Penalties can also be applied to individuals. For example, local police in the Chinese city of Ankang fined a man 500 yuan for accessing international content illegal in China using an illegal VPN service. The story sparked a rare backlash among citizens on China's internet (Feng).

China has also acted in silencing media outlets in Hong Kong. In the case of the tabloid *Apple Daily*, not only did it suffer a social media shaming campaign from a senior political figure seen as strongly pro-China (CPJ, "One Country, One Censorship"), but the government went further in its censorship efforts and the police froze bank accounts belonging to Apple Daily's publicly listed parent company (Marlow). Since the newspaper was forced to shut down, cyber activists in Hong Kong have started to back up articles on censorship-proof block chain platforms (You).

Both China and Russia have paid and non-paid individuals that scour the internet to both tear down criticism and prop up government actions. The Kremlin hires paid commenters, or trolls, and automated "bot" accounts to post and engage with digital content. In some cases, Kremlin-linked oligarchs also support such activities. For example, Yevgeny Prigozhin—a close ally of Putin's—is the main financial backer of the Internet Research Agency, a prominent troll farm that spreads misinformation (CBS News, "Russian oligarch"). China also hires paid commenters known as the "50 Cent Party" and enlists volunteers called "ziganwu" to post pro-government remarks and promote the CCP (Freedom House, "Freedom on the Net 2021: China"). While this is not censorship per se, key informant interviews indicated that the volume of posts tends to create noise and drown out potential critics. This can frustrate citizens, to the point where they do not bother engaging in any conversation that could be critical of the government, effectively self-censoring.

In sum, the findings indicate that China appears to be a standard for digital censorship against which countries in this report's sample can be measured. Beijing is so successful at generating and maintaining this "censorship ecosystem" that, "[t]he Chinese public has been inoculated against outside information" (French). Though both China and Russia are digital censorship "innovator" countries, Russia is learning from China in significant ways. What stands out is the timeline of when these countries strongly committed to censoring the internet. China began much earlier, both before the internet was built into the daily lives of people around the world, as well as before penetration was widespread in China. Russia, on the other hand, did not begin any serious attempts to implement a similar regime until much later, when the internet and social media were already fixed into the lives of its citizens. Russia, though a censorship innovator on the world stage, is playing catch up with China in both censorship tools and in becoming more fully autocratic.

Despite the limited evidence of Russia and China deliberately working together to "export" an authoritarian censorship model, a joint statement in which they talk about "reshaping the international order" reveals a deepening relationship grounded on their shared authoritarian vision of global information control and related questions of national sovereignty such as cyber sovereignty (Bandurski). Moreover, an existing digital partnership between Russia and China has been ongoing for several months, with several Russia-Chinese state media agreements in place, but these are described as largely symbolic and formalistic (Gabuev and Kovachich).

In the following section, this report introduces five "emulator" countries that are adopting some of the same tools and techniques already widely used by China and Russia for digital censorship: Azerbaijan, Nicaragua, Serbia, Turkey, and Uganda. The section below discusses their technological and governance landscapes, before describing and comparing their digital censorship tools with those of Russia and China.

China's data privacy laws first implemented in 2012 with updates in 2017 and 2019 (Freedom House, "Freedom on the Net 2020: China").

4. Emulators

How do the tools of digital censorship in this report's sample of autocratizing countries stack up against those of Russia and China? This section compares and contrasts these two authoritarian countries to Azerbaijan, Nicaragua, Serbia, Turkey, and Uganda. These countries come from diverse geographic regions, as well as varying democratic and economic development levels. Below, the report identifies the overlapping digital censorship tools these countries have with China and/or Russia, and looks for similarities in path development toward digital censorship approaches. To emphasize the study's purpose, this analysis is purely descriptive—not causal—but remains valuable to provide a baseline assessment of which tools the five "emulator" countries utilize similarly to China and/or Russia. Before comparing and analyzing tools of digital censorship, the section below provides a descriptive overview of these emulator countries' democratic and digital censorship levels, and lays out their internet infrastructure. This discussion provides a solid basis upon which to contextualize the tools of digital censorship they possess before comparisons are made to China and Russia.

4.1. Institutional and Technological Environment

Autocratic Governance

Our five pilot countries display variation both within and between their forms of governance and digital censorship levels. Examining the period between 2010 to 2021 (the most recent available data), this report presents a secondary analysis of key governance indicators using data on democracy levels and judicial independence compiled by V-Dem and Freedom House.[13] While democracy level is a common indicator of democratic governance, the analysis also includes judicial independence to isolate this component of democracy. These figures are available in the Appendix but the key findings are described here, highlighting trends to paint a picture of the countries' style of governance and digital censorship profiles.

Azerbaijan, Nicaragua, and Uganda possess the deepest autocratic institutions among the five pilot countries, with levels approaching or even matching the authoritarian levels of Russia and China.[14] By contrast, Turkey and Serbia are less autocratic but appear to display diminishing democracy levels over time, with noticeable declines recently in key indicators.

The data also indicate low and declining levels of judicial independence over the study period in all cases except for Uganda. A judiciary that is not independent from the government is unlikely to provide genuine oversight and can serve as a rubber stamp for government actions that limit civil liberties and legitimize censorship (La Porta et al.). Among the five countries, Azerbaijan's judicial independence stands out as the lowest. The State Department reported a 2013 case where Azerbaijan's courts confirmed that libel laws—perhaps the most common criminal charge used against government critics—apply to social media posts. This case involved AccessBank and a former employee who posted on Facebook accusing the bank of corruption and greed (Aliyev and Sindelar).

In Nicaragua, courts have become an instrument of the government, used to shutter critical independent media, including traditional media outlets with a large online presence (US Department of State, "2020 Country Reports on Human Rights Practices: Nicaragua"). In September 2020, the Nicaraguan government seized the assets of Canal 12 News, a television broadcaster. According to Voice of America, the "order to seize the broadcast facilities, station vehicles and the owner's personal estate is the latest in a series of audits and asset seizures faced by news organizations that report critically on the government of President Daniel Ortega."[15] Turkey's once respectable level of judicial independence—the highest among the five case study countries at the beginning of the period—has steadily declined since the mid-2010s but especially since the attempted coup in 2016.

[13] This study uses the Varieties of Democracy (V-Dem) dataset on electoral democracy, judicial independence, and government attempts at digital censorship from 2010 to 2021 (Coppedge et al.). To provide balance to these measures, Freedom House's measure of Freedom in the World (Freedom House, "Freedom in the World") is included during the same time frame, which encompasses a broader concept of liberal democracy (including electoral democracy, judicial independence, and other components such as civil liberties and civil rights).

[14] See Figure A1 in the Appendix.

[15] For content removals, Nicaragua often utilizes the United States' Digital Millennium Copyright Act (USDMCA) to target the removal of online content. The USDMCA criminalizes the reproduction of copyrighted information.

These low and declining democracy levels reflect other illiberal outcomes, including rising levels of digital censorship. All countries except Azerbaijan have seen increases in digital censorship efforts by their governments, according to the quantitative data. Nicaragua saw the most dramatic increase over the decade and is currently the country with the worst internet censorship climate of the five—even higher than China's. Key informant interviews indicated "there was never an expectation of private data in Nicaragua because the Sandinistas always collected information on individuals from telecommunications companies, though digital censorship and internet blackouts did increase following the 2018 political protests via collaboration with telecommunications companies."

Turkey has also seen a steady increase in internet censorship. Censorship peaked in 2017, soon after the 2016 coup attempt in which parts of the military tried to overthrow Turkish President Recep Tayyip Erdogan (BBC News, "Turkey's Coup Attempt"), but has slightly receded since. Both Azerbaijan and Uganda have more moderate levels of internet censorship, and those have remained relatively stable throughout the past decade. Serbia has the lowest level of internet censorship of the five countries, experiencing a considerable increase in the early 2010s but remaining stable since then.

In sum, the contextual data indicate that, while Russia and China are often painted as firmly autocratic countries, there is variation over time, mirrored by changes in emulator countries. Levels of judicial independence in Russia decreased over time, and digital censorship efforts rose drastically between 2012 and 2015 before reaching a plateau.[16] Serbia, Turkey, and Nicaragua follow the pattern of these developments. Uganda and Azerbaijan's key indicators over this period are more like China's—these countries began the time period with autocratic institutions and generally maintained them over time. The KIIs also identified Turkey as an "innovator country"—more so than Russia or China—to Azerbaijan, given their historic ties and friendly relations. While it is certainly in a process of autocratization, Turkey is fairly sophisticated in its digital censorship applications and can also be seen as an "authoritarian innovator" to other countries.

Internet Infrastructure

All seven countries have access to the internet, though in more developing countries the access is limited, particularly in rural areas.

Uganda and Nicaragua, the two least developed countries in this report's sample,[17] display similar internet landscapes with the least internet penetration (the percentage of the population with access to the internet). Uganda's internet penetration is low but rapidly growing, rising from under 5% in 2010 to nearly 20% in 2020 (World Bank, "Uganda"). The South African company MTN is a major telecommunications company in Uganda. In recent years, Uganda has taken steps to improve its internet infrastructure and sought partners to finance its efforts. One key informant expert mentioned many partnerships with China and Chinese companies like Huawei for the building of physical internet infrastructure, while another discussed the large number of loans Uganda has received from China. Due to the human rights requirements embedded in loans from the EU and the United States, Uganda has turned to China as a provider of both financial aid and infrastructure development.[18]

Though double that of Uganda's internet penetration, Nicaragua's remains quite low at about 45% in 2020, rising from 10% in 2010. However, experts from the KIIs are skeptical of these official numbers and believe they may be inflated.[19] There are two main ISPs in Nicaragua: Claro and Tigo. Claro is owned by the Mexican telecommunications company América Móvil and dominates both the fixed and mobile broadband sectors. Tigo is owned by Luxembourg-based Millicom and has captured around 33% of the mobile market and 10% of the fixed-line market. Experts from the KIIs stated that the companies often acquiesce to the Nicaraguan government's content removal requests.

Azerbaijan, Serbia, and Turkey have similar levels of internet penetration and growth over the last decade. In Azerbaijan, internet access is expensive and of poor quality. Nevertheless, internet penetration has increased dramatically, from 46% in 2010 to almost 85% in 2020 (World Bank, "Azerbaijan"). Social media is widely used to disseminate information and organize

[16] These data do not cover the time period since the 2022 Ukraine invasion.

[17] The World Bank Classifies Uganda as a low-income country, while it classifies Nicaragua as a lower-middle income country in their latest classification (World Bank, "World Bank Country and Lending Groups").

[18] The expert explained that loans from China did not require pre-conditions or requirements to be met for disbursement. Huawei has been engaged in a number of building projects (the usual roads and bridges), including the laying of cables for the internet and building of a "fiber backbone." Huawei has also provided CCTV cameras.

[19] KIIs estimated the level of internet penetration as somewhere closer to 20% in Nicaragua. While they did not have hard data to prove this, the experts explained that there is little transparency on the government's part and no information on how the internet penetration data was collected. They stated earlier that although Nicaragua has the most expensive internet costs in Central America, cellular data is still very limited, and the political situation since 2018 has halted the implementation of much internet infrastructure.

rallies, a phenomenon largely observed since the COVID-19 pandemic. While social media websites such as Facebook, Twitter, and Instagram generally remain unblocked, connectivity issues prevent users from accessing them during rallies. Watchdog reports and KIIs indicate that the government effectively controls internet infrastructure and has intentionally restricted connectivity (see a discussion of Azerbaijan's tools of digital censorship below). The three state-owned ISPs are Aztelekom, Baktelecom (BTC), and AzDataCom. Together they control approximately 50% of the market.

Turkey saw a similar pattern of internet penetration growth, from about 40% of the population in 2010 to about 81% by 2020 (World Bank, "Turkey"). According to watchdog reports and KIIs, telecommunications are heavily concentrated in just a small number of companies, with Turkcell as the main mobile phone provider and Türk Telekom as the main ISP. State-run companies and public-private partnerships allow the Turkish state and current President Erdogan himself to maintain high levels of control over the telecommunications infrastructure.

Serbia mirrors the above countries with about 40% internet penetration in 2010, rising to about 81% in 2021 (World Bank, "Serbia"). The telecommunications sector is relatively diverse, but the state-owned provider Telekom Serbia holds the largest shares of both mobile and fixed-line broadband markets. Other large ISPs are Serbia Broadband (SBB) and Yettel. Social media is widely used in Serbian political life. During protests of state-imposed curfews in 2020, vital information related to assemblies was shared on Facebook, Twitter, and Telegram. This has also been the case in the past during anti-government protests.

In sum, most "emulator" countries in this study are in the process of democratic backsliding or deepening autocratic institutions, particularly those that were more democratic at the start. Simultaneously, internet censorship has been on the rise and internet infrastructure is concentrated in the hands of relatively few companies, apart from Serbia. This level of control of the telecommunications infrastructure is used by both China and Russia to perpetrate digital censorship, though it is only part of their arsenal. The following section analyzes the tools used by China and Russia, in comparison to those used in the five "emulator" countries. Specifically, it examines the compounding impact of these authoritarian "innovators" in the areas of institutional and technological censorship tools, as well as the means to induce self-censorship.

4.2. Compounding Influence? Comparison and Analysis

This section further examines the tools the five pilot "emulator" countries utilize in digital censorship within the following categories: institutional tools, technological tools, and traditional tools that encourage self-censorship.

4.2.1. Institutional Tools

Legislation

Much like Russia and China, the pilot countries use legislation to justify some of their more overt digital censorship tactics. In some cases, they are blatantly following the lead of Russia, with Nicaragua as the most glaring example, according to expert interviews. Though little legislation exists to regulate digital content in Nicaragua, the landmark Special Cybercrimes Law (2020) recently took effect, and experts describe it as mirroring existing Russian legislation. As one KII participant noted, "the Law of Foreign Agents, the Cybercrime Law is, as I understand, basically [a] copy-paste from Russia." The law established punishment for a broad range of offenses, including the "dissemination of false information, incitement of hatred or violence, and endangerment of national security" (Freedom House, "Freedom on the Net 2021: Nicaragua"). It also authorizes the blocking of websites and other messaging and communication services, but there is limited evidence that the Nicaraguan government has done this on any large scale, likely due to its lack of technological ability.

Much like legislation from China and Russia, the language in Nicaragua's law is generally vague but provides for harsh punishments. For example, Article 28 prescribes two to four years in prison for the use of technology "to slander a person's honor or prestige or divulging a person's secrets" (Freedom House, "Freedom on the Net 2021: Nicaragua"). Article 30 mandates two to four years in prison for the dissemination of "fake news" but fails to differentiate between deliberate false information and unintentionally wrong information. The article also does not define what makes news "fake," leaving it open to a wide range of interpretations. The penalty further increases to three to five years in prison if the information "incites hatred or violence, or puts at risk economic stability, public health, national sovereignty or law and order" (Freedom House, "Freedom on the Net 2021: Nicaragua"). Users can also face four to six years in prison for sharing

"unauthorized" information, or eight years for accessing information that endangers national security.[20]

Azerbaijan resembles China, with *ad hoc* censorship that was eventually codified into law. There is also institutional backing of government surveillance. This can be observed in the case of the Law on Information, Informatization, and Information Protection which was amended twice, in 2017 and again in 2020, to expand the definition of "prohibited information" to include false information risking human health during the COVID-19 pandemic or information "causing significant property damage, mass violation of public safety, disruption of life support facilities, financial, transport, communications, industrial, energy and social infrastructure facilities, or leading to other socially dangerous consequences" (Freedom House, "Freedom on the Net 2021: Azerbaijan"). This broadening of what constitutes "prohibited information" gives additional leeway to Azerbaijan's regulatory bodies. Furthermore, since the 2016 clashes in Nagorno-Karabakh, Azerbaijan amended the Law on the Status of the Armed Forces, providing additional grounds for censorship and restricting journalists' ability to report on matters related to the military.

Azerbaijan's Law on Operative Search Activity authorizes law enforcement agencies to conduct surveillance without a court order when it is considered necessary to prevent serious crimes against individuals or the state. Like Russia, the language of Azerbaijan's laws is often vaguely worded, allowing the government to censor whatever it wants. Also like Russia, Azerbaijan passed laws in response to the COVID-19 pandemic and conflict, usually with a stated focus to combat "fake news." Azerbaijan's government also manipulates the online information landscape; for example, blocking websites that host unfavorable news coverage.

Other pieces of legislation are aimed at digital content in selected "emulator" countries. In Serbia, there is no formal legislation allowing censorship by the government, but a package of media laws, which passed in 2014, empowered state bodies to co-finance media "to serve in the public interest" (Freedom House, "Freedom on the Net 2021: Serbia"). The government framed this as an attempt to improve the media environment. However, the laws gave the government a mechanism to support private media outlets owned by members or sympathizers of the ruling party and encouraged self-censorship. The government's declaration of a state of emergency in response to the COVID-19 pandemic and its decision to centralize pandemic information negatively affected the circulation of information. Serbia's Law on Electronic Communications mostly aligns with EU rules, although it resembles Russia's response-to-crisis form of censorship.

Similarly to Russia and China's tactics, legislation in Uganda is vaguely worded to allow for a wide reach and flexible application in censoring online content. Legislation is often used to arrest individuals for sharing content critical of the government and is deployed to deter internet use altogether. Articles 43 and 44 of the Ugandan constitution were used by the government to justify its internet shutdowns during elections. These articles give the government the ability to take power when there is a threat to national security. Moreover, Sections 24 and 25 of the Computer Misuse Act restrict "offensive communication," which is broadly defined as the use of "electronic communication to disturb or attempt to disturb the peace, quiet, or right of privacy of any person" (Freedom House, "Freedom on the Net 2021: Uganda"). Section 179 of the Penal Code Act, which deals with criminal libel, is often used to prosecute online activity due to the law's lengthy prison terms.

Uganda's Regulation of Interception of Communication (RIC) Act requires telecommunications companies to retain user metadata and disclose personal information to government authorities when an individual is considered a terrorist or a threat to national security, economic interests, or public safety. Uganda's "Social Media Tax," the Over-the-top (OTT) Services Tax, was repealed under the Excise Duty (Amendment) Act 2021 after users began avoiding the Social Media Tax with VPNs. This new law replaces the Social Media Tax with a 12% tax on internet data, placing a heavy financial burden on internet use. This new tax on internet bundles is equivalent to $2 USD (6,000 shillings) per month in a country where many citizens make only $40 USD a month. Much of this reflects China's push against anonymity that Uganda may be trying to replicate.

Turkey has limited legislation to explicitly censor digital content. The "Law on Regulation of Publications on the Internet and Suppression of Crimes Committed by means of Such Publication" or the Internet Law No. 5651 of 2007 censors specific digital content (meant to prevent access to a broad category of illegal and harmful content, including drug use, gambling, the promotion of suicide, and "crimes against Mustafa Kemal Ataturk"). Beyond that, there are no laws that specifically criminalize online activities such as posting one's opinions, downloading information, sending emails, or sending text messages. Instead, many provisions of the criminal code and other laws, such as the Anti-Terrorism Law,

[20] The Nicaraguan cybercrimes law is based on Russia's combined Fake News Law and Law on Defamation from 2019, while the Foreign Agents Law is based on the Russian law of the same name.

are applied to both online and offline activity. The constitution and laws theoretically provide broad protections for freedom of expression, but online journalists and ordinary users frequently face civil and criminal penalties for legitimate expression. The proliferation of restrictive laws has further formalized censorship.

Turkey's Social Media Regulations Law was passed in Parliament and came into effect in 2020. It further includes registration requirements for social media companies, forces platforms to remove content within 48 hours, and has troubling data localization provisions. Noncompliance with the law is punishable with steep fines or potential bandwidth throttling. Article 29/A of Law No. 6112 compels streaming services to apply for a license, which Netflix and Amazon Prime did in 2020. Additionally, Turkey often justifies content removal for the protection of "family values," in a move that a KII linked to conservative rhetoric and causes in the US. This suggests that, in some instances, "emulator" countries are learning not only from autocratic regimes, but also from the West.[21]

Regulatory Bodies

Like Russia and China, the pilot "emulator" countries also rely on regulatory bodies to implement legislation, monitor digital content, and perform censorship when necessary. This section describes some of those regulatory bodies. Russia has at least 18 regulatory bodies while China has at least 13, but Roskomnadzor appears to exhibit more control over the direction of Russia's 17 other regulatory bodies, while China's regulatory bodies have more specific or discrete roles (despite the CAC's increasing power).

In Azerbaijan, the Ministry for Transportation, Communications, and High Technologies (MTCHT) maintains a list of court-approved blocks on websites, following the Law on Information, Informatization, and Information Protection. In Nicaragua, TELCOR and the Foreign Ministry, both controlled by the president, oversee the decisions to block websites, following the Special Cybercrimes Law of 2020. Furthermore, the Nicaraguan Institute of Telecommunications and Postal Services (TELCOR) is the main regulatory body for telecommunications providers, and while it is legally supposed to operate independently from the government, in practice it acts as a government institution and follows the government's policies (Freedom House, "Freedom on the Net 2021: Nicaragua").

Turkey has a number of regulatory bodies with different roles. The Information and Communication Technologies Authority (BTK) can fine ISPs for failing to comply with blocking orders within four hours of their issuance. Failure to take measures to block all alternative means of accessing the targeted site, such as proxy sites, may also result in fines. The Radio and Television Supreme Council (RTÜK) regulates online content, including audio and video streaming services. The Ministry of Family, Work, and Social Services can request the removal of content it deems "harmful to children."

The Uganda Communications Commission (UCC) is mandated to independently coordinate, facilitate, and promote the sustainable growth and development of information and communications technology (ICT) in the country. The UCC provides information about the regulatory process and quality of service and issues licenses for ICT infrastructure and service providers. The UCC also has the power to order an internet shutdown. The Media Council of Uganda was established to, among other things, "…regulate the conduct and promote good ethical standards and discipline of journalists; arbitrate disputes between the public and the media; and the State and the media; exercise disciplinary control over journalists, editors, and publishers; and promote, generally, the flow of information" (Muhindo). The Council requires all journalists to register with it in order to cover government events. The Uganda Media Center is another government-appointed media regulatory body. It has assembled a new social media monitoring unit that scans the profiles of users to find critical posts.

Lastly, although Serbia does not have a single state body or authority tasked with overseeing or regulating internet content, the Serbian Telecommunication Agency (RATEL) can control entry to the telecommunications market. Serbia appears to be emulating Russia and China the least. As one KII participant noted, "[although] there is big, big Chinese and Russian influence in Serbia as it is, but in the digital media landscape and censorship, I don't see any models that are characteristic of those countries that are happening here…Our censorship is much more plain and simple." However, the other case study countries are all generally streamlining their efforts into the hands of one or just a few regulatory bodies.

[21] While the KII mentioned only US conservatives, we acknowledge that the Turkish government may take influence from a broad spectrum of ideological sources.

4.2.2. Technological Tools

Digital Content Censorship

When digital content censorship is examined directly, it becomes clearer that the five select "emulators" are at different stages with respect to the intensity of their censorship efforts. Turkey uses the most diverse set of tools. Beyond targeting insults as a form of censorship,[22] digital censorship also takes the form of website blocking (such as the blocking of Wikipedia), electrical blackouts (though sometimes unintentional), and the use of online trolls to spread disinformation and personal attacks. Website blocking is especially easy, given the close relationships between telecommunications companies and the Turkish government, such that companies will quickly implement these blocks as directed. Yet Turkish citizens commonly use VPNs in order to bypass some of these restrictions; for example, to obtain access to Netflix after the government banned it for "morality" issues. Anonymity is also in jeopardy. Turkish-made telecommunications products are heavily promoted to further expand the country's power to monitor and control its population, with Turkish SIM cards being widely pushed (even for use by foreigners) to track people's mobile phones.

Content removals often occur without transparency in Turkey; however, the prominence of Western social media sites highlights the strong connections that Turkey's population still has with the West and its internet, especially among internet-using young people, and allows some insight into how much content is removed. According to Twitter's Transparency report, in 2021 Turkey was responsible for 9% of global legal demands of removal (Twitter, "Turkey: Insights into Information Requests").

Azerbaijan has continuously blocked key opposition and independent news websites, including 24saat.org, Abzas.net, Azadliq, Azadliq Radio (the Azerbaijan language service for RFE/RL), Gununsesi, Kanal 13 TV, and Meydan TV. The government also deliberately throttled internet access and blocked social media websites (Facebook, WhatsApp, Instagram, YouTube, TikTok, LinkedIn, Twitter, Zoom and Skype) for 46 days during the 2020 Nagorno-Karabakh military conflict with Armenia. Investigative journalist Khadija Ismayilova has reported that the government is seeking court approval to restrict users' ability to access news websites already blocked in the country via Facebook. A ruling in favor of the government may oblige Facebook and other companies to prevent Azerbaijani users from seeing content from these websites. The authorities could also instruct ISPs to block these websites' social media profiles, which would effectively block entire social media platforms (although no steps have been taken in that direction yet).

Uganda and Nicaragua have a more limited set of tools for content censorship, likely due to a lack of technical capacity. In Uganda, the main tools are direct digital content removal and keyword flagging. However, there has been some institutional validation of censorship efforts, with a Ugandan court case deciding that government officials can block users on their own personal account, leading to the common practice of authorities blocking individuals on sites like Twitter for criticizing them. Unlike China's Great Firewall technology, the Ugandan government must resort to less sophisticated and more direct methods of digital censorship. This usually takes the form of complete internet shutdowns during contentious political periods, such as the day of an election. In the past, the government has gone directly to the telecommunications companies to have them block the internet when requested. During the 2011 Walking Movement, records showed that MTN had also been given a list of keywords they should flag by the government.

China's influence in Uganda is still concentrated on infrastructure projects, and the Chinese government does not yet play a pervasive and direct digital censorship role. However, China's infrastructure toehold in Uganda, particularly as a counterbalance to US and Western development aid, is certainly setting the stage for a more direct role in digital censorship. As one KII participant noted, "If the Americans are putting a lot of conditions on us—or the Europeans—we can go to China. We can go to Russia. We can get foreign aid there, we can get a loan there—we don't need the Europeans or the Americans… Also, when they [the Ugandan government] see what's happening in China, they say 'well, we can also do it the Chinese way.'"

In Nicaragua, though the government has the authority to block and filter websites and content, it does so very rarely. KIIs explained this was due in large part to a lack of technological capacity. One case occurred in August 2021, when the Nicaraguan government shut down electricity and the internet at the office of *La Prensa*, an independent newspaper outlet in Managua (BBC News, "Nicaragua: Police

[22] In Turkey, the key informant expert explained that anytime an individual "insults" someone else, the person could take them to court, even if the exchange occurred online or between strangers. There is no clear definition of what an "insult" is or what topics are considered to be insults, only that a person "cannot insult Turkishness." See Kaya Genç, "Turkey: Number of "insulting Turkishness" cases drops as parliament discusses changing definition of citizenship," for more detail on this law.

Raid Offices"). Notably, the government did not block or filter the newspaper's website.

In Serbia's case, the key tool used is the blocking of websites, albeit in a very limited manner.[23] The government has shown intent to remove specific applications from their internet domains, but Serbian providers at the time did not have the technical ability to do so. That was the case with the rideshare application Car:Go. Following criticism from government bodies and the taxi industry, ISPs were ordered to remove the application from their platforms, but Serbian providers were not able to do so for mobile app stores run by Google, Apple, and Huawei (Freedom House, "Freedom on the Net 2021: Serbia").

Overall, all the countries in this study engage in website blocking, one of the most basic forms of digital content censorship. Some countries also perform content removal and title or keyword blocking; yet notably, none of the five "emulator" countries close social media accounts, a censorship tool used by both China and Russia. This is likely because these countries do not have local social media websites, which would be easier to influence; when dealing with Western or US-based companies, countries are limited to requesting companies to block the entire website.

Software Censorship

With respect to software censorship, a wide range of technical capacity influences which tools are used in each of the five countries. Nicaragua only uses cyberattacks and at a limited scale. The government typically hires trolls to perpetrate cyberattacks against opponents (though it apparently does not have "in-house" technological capabilities for these attacks). The news website *Confidencial* and the newspapers *La Prensa* and *Hoy* reportedly faced DDoS attacks, though it is unclear if these were government directed. State-sponsored troll factories operate via the "Digital Project," which is run out of government buildings using employees from various public agencies (Freedom House, "Freedom on the Net 2021: Nicaragua"). Though not a law or regulation, another major example of Russia's influence was a 2021 agreement it signed with Nicaragua to prevent online threats and collaborate on preserving "information security" (Confidencial, "Convenio de 'seguridad'").

Serbia sees a wider range of types of cyberattacks, which are relatively common. These include DDoS attacks and technical attacks, with civil society and media outlets often being targeted. However, these attacks typically come from other countries or non-state actors with little evidence of such attacks being used by the government to censor (Dragojlo and Tesic, Freedom House, "Freedom on the Net 2021: Serbia").

The extent of Chinese surveillance and digital censorship technology being used by Uganda remains unclear, though a watchdog report from the Ugandan group Unwanted Witness claims the government now has the ability to monitor and remove content based on their recent technological purchases from China. The Ugandan government is now able to digitally trace videos posted online back to their source. Huawei has also provided the Ugandan government with spyware to use for "security threats and political enemies" (Parkinson et al.). In 2018, Huawei technicians directly supported a group of Ugandan intelligence officers in penetrating the WhatsApp and Skype communications of opposition leader Bobi Wine. Authorities then ruined his plans to organize street rallies and arrested the politician and some of his supporters (Parkinson et al.). In addition to Huawei's support of Uganda's surveillance efforts, the large role China plays in Uganda's infrastructure development may open space for further support from Beijing for Uganda's censorship efforts in the future.[24] Chinese tech companies such as Alibaba and Tencent are developing sophisticated content moderation systems that intentionally target political content, and they may sell these systems to anyone interested. So far, these technologies are mostly purchased by other Chinese companies and foreign customers are rare. But since 2017 a Singaporean subsidiary of a Chinese social media company has been selling a content moderation system powered by AI to the Indonesian government; the same company has also been in talks with governments in Egypt, India and the Middle East (Li). However, at present, the most common form of software censorship in Uganda is still simple blackouts and internet shutdowns around politically tumultuous times, such as elections. That stems from Uganda's currently limited technical capabilities for digital censorship.

Turkey, as mentioned previously, has a more sophisticated toolkit and is the only "emulator" to use VPN blocking through DPIs that can detect and block VPN traffic, as China and Russia both do. That greatly limits the ability of users to evade digital censorship through website blocking. Furthermore, despite the common occurrence of phone tapping, monitoring, and other forms of digital censorship, many Turkish citizens have become used to these limits on

[23] So far, only gambling websites have been blocked under Serbia's 2020 Gambling Law, but there is a lack of transparency in the process.

[24] China has committed $147 million USD in 2009 to Warid Telecom for the development of Global System for Mobile communications (GSM) network services in Uganda and $138 million USD between 2009 and 2015 to the Government of Uganda to support the development of data transmission infrastructure and e-government infrastructure.

their freedom. Moreover, even on the websites that the government struggles to censor, such as foreign social media sites, it still finds ways to influence the narrative on those sites via trolls, bots, and pro-government users.[25]

Finally, there are no reports yet of Azerbaijan limiting access to VPN use, but the Azerbaijani government has purchased and used equipment with DPI capabilities from Israel and Canada (Freedom House, "Freedom on the Net 2021: Azerbaijan").

In 2020, the "Right to be Forgotten" was recognized by Turkish authorities, allowing citizens to have content removed from search results. However, authorities have manipulated the law to remove negative press of prominent politicians from online databases. Russia has a similar law, also used in favorable ways toward the government.

4.2.3. Self-Censorship

As stated previously, self-censorship is an ideal aim for an autocratic state seeking to achieve widespread digital censorship. Under the appropriate conditions, autocratic governments can rely on self-censorship rather than trying to fully control the digital space. Traditional forms of censorship, such as threats, detainment, and physical or online harassment to oneself or others, all can induce self-censorship.

Due to a lack of technological capacity, much of Nicaragua's current digital censorship remains focused on traditional face-to-face methods of harassment, physical violence, detention, and jail sentences. Examples include two journalists from the website *100% Noticias* being detained and tortured for six months (CPJ, "Nicaraguan police raid"); the government coercing citizens to delete anti-government videos or photos that depict anti-government protests from their devices (HRW, "Critics Under Attack"); and sentencing a journalist to a nine-year prison sentence for disseminating "fake news" on social media (CPJ, "CPJ condemns").

The Nicaraguan government also uses crude surveillance techniques to intimidate and identify critics of the government. Beginning in 2019, the director of the digital news outlet *El Portavoz Ciudadano*, Emiliano Chamorro, reported police watching and videoing him outside his office (CPJ, "Nicaraguan journalist"). In May 2020, TELCOR amended a 2013 administrative agreement to include giving TELCOR greater control over the creation of regulations that can infringe user security and the protection of personal information (Freedom House, "Freedom on the Net 2021: Nicaragua"). However, there are signs that the Nicaraguan government is beginning to utilize more sophisticated technology, and it has recently purchased spyware from Israel called Pegasus that it appears to be using to some extent (Bow).

Furthermore, the Nicaraguan government also uses paid trolls and inauthentic social media activity to promote its political interests. The Digital Project is an initiative with over 100 employees from different public agencies that work from the Nicaraguan Post Office building to produce and share content across multiple social media platforms, including TikTok, Instagram, Facebook, and Twitter. The trolls spread fake news and information to depict the Ortega regime positively while also slandering critics and creating anxiety that will stimulate self-censorship, such as by claiming that the police will arrest someone. The Vice President, Ortega's wife Rosario Murillo, reportedly ordered the creation of these "troll factories" in 2018 (Freedom House, "Freedom on the Net 2021: Nicaragua").

Turkey once was the largest jailer of journalists in the world, according to the Committee to Protect Journalists (CPJ), but it has recently fallen to the sixth worst (CPJ, "Number of journalists"). Prosecutions and detentions are high: 6,743 social media users were subjected to judicial processes for propagating terrorism, attempting to manipulate public perception, or sharing provocative content online between January and August 2020 (Freedom House, "Freedom on the Net 2021: Turkey").

Digital media outlets in Turkey are inhibited by heightened self-censorship. The many prosecutions for defaming the president have had a chilling effect on social media users in recent years, and online self-censorship has been exacerbated by decrees passed under the 2016 state of emergency that expanded the government's surveillance powers.

In Azerbaijan, self-censorship is also pervasive and comes from the fear of retribution from the government as well as family members, along with the risk of social ostracization. In the social media sphere, users are aware that they may face criminal charges for their expression online. Furthermore, the government not only censors those who live in Azerbaijan, but also those who live in exile through threats to family members and friends. Azerbaijan passed a media law in 2022 which introduced a requirement that journalists register with authorities (CPJ, "New Azerbaijan media law"), which according to KII's was "inspired by Russia." Registered journalists still risk their credentials being revoked without

[25] It remains unclear (and unproven) that these trolls are paid by the government.

explanation from the government. Furthermore, China has provided Azerbaijan with surveillance tools like Pegasus, according to expert interviews.[26]

The same can be said for Uganda, where the threat of harassment, arrests, and/or torture leads many Ugandans to self-censor to protect their personal safety. Ugandans also deal with the threat of having their identity exposed online if they choose to post anonymously, and civil servants risk losing their jobs for posting about political issues on social media as well, according to expert interviews. The Facebook user and critic of Ugandan President Yoweri Museveni "TVO" is one example; the Ugandan government has arrested people who have been accused of being TVO in the past. While individuals are usually arrested under existing laws in Uganda, extrajudicial arrests and attacks still occur. For example, a key informant expert relayed an anecdote of a pastor who was arrested at a cafe and tortured for his posts on Facebook about the president's son.

Beyond self-censorship, highly costly social media and internet data taxes in Uganda further disincentivize internet and social media use. The government also maintains teams of state-sponsored social media accounts tasked with posting positively about the government and identifying users who criticize the president and his family.

Finally, Serbia has a limited institutional framework for censorship, with most of the actual censorship happening in the form of self-censorship, which permeates the media sphere both online and offline. The government mostly targets journalists and other "information brokers" through traditional censorship methods, with threats, arrests, harassment, etc. A particular characteristic of Serbian censorship is the attempt to discredit journalists by linking those few independent media sources (without links to the government) to "foreign propagandists'' if they receive any funding from the EU. One KII mentioned the Serbian government's use of China's cameras and facial recognition under the guise of "smart city technology." While some observers see this as a way to surveil the public (Kynge et al.), we have yet to see evidence that this technology is being used to target journalists.

Box 5 below presents a summary and comparison of the digital censorship tools discussed in this section to those found in China and Russia. It illustrates that every digital content censorship tool used in the case study "emulator" countries is already used by both China and Russia. Nearly all software censorship techniques and nearly all self-censorship techniques (except for taxes on social media) are used by both China and Russia. Although investigating precisely how China sought to export digital authoritarianism to other countries was beyond the scope of this research, Box 6 below provides an example of China's efforts in Uganda.

[26] AidData was able to confirm that Azerbaijan's government has used Pegasus against its journalists (Patrucic and Bloss) but was unable to confirm from a secondary source if China actually provided the technology.

Box 5: Comparison of Digital Censorship Tools, "Innovators" and "Emulators"

Digital content censorship techniques	China	Russia	Azerbaijan	Nica-ragua	Serbia	Turkey	Uganda
Blocking/closing social media accounts	x	x				x	x
Blocking websites (including social media platforms)/digital content filtering, removal	x	x	x		x	x	x
Blocking website titles or removing applications from their internet domains	x	x	x		x	x	
Internet shutdowns, restricted/disrupted online access	x	x	x	x		x	x
Keyword blocking	x					x	
Keyword flagging	x						

Software censorship techniques	China	Russia	Azer-baijan	Nica-ragua	Serbia	Turkey	Uganda
Deliberate throttling (slow load time of webpages), or bandwidth throttling of social media platforms that do not comply with administrative decisions and court orders	x	x	x			x	x
Cyberattacks (DDoS, spear-phishing, or other technical attacks)	x	x	x	x	x	x	
Deep Packet Inspection (DPI)	x	x	x			x	
DNS poisoning (returning fake pages, or replacing the requested site with content retrieved from an unrelated IP address)	x						
Regulation or restriction of circumvention tools (VPNs)	x	x				x	x

Spyware	x		x	x		x	x
Self-censorship techniques	China	Russia	Azer-baijan	Nica-ragua	Serbia	Turkey	Uganda
Requirements that reduce anonymity, such as "real name registration", fees for and registry of foreign bought mobile devices	x	x				x	
Requirements for companies to censor	x	x				x	
Traditional forms of media freedom violations[27]	x	x	x	x	x	x	x
Surveillance	x	x	x	x	x	x	
Paid/volunteer online trolls, automated "bots"	x	x	x	x		x	
Data retention on digital users	x	x		x	x	x	
Social media tax							x

[27] Including prison, threats of arrest, detainment, physical harassment or torture, online harassment, threats to family members, deportation, and/or barring entry into the country.

Box 6: China's links to Uganda telecom deepen

China's public diplomacy—or action by state actors with at least some intention of influencing the perceptions, preferences, and actions of foreign citizens in favor of its interests—has steadily increased worldwide over the last two decades (Custer et al., "Ties That Bind"; Custer et al., "Silk Road Diplomacy"). China's overtures to attract governments and their citizens into its sphere of influence include cultivating "influence by attracting foreign publics to empathize with its preferred narrative and adopt its views" (Custer et al., "Ties That Bind").

In Uganda, China has invested a total of $3.67 billion USD between 2000 and 2017 in direct official finance (AidData, "China's Global Public Diplomacy"). Examples of China's investments in the telecom sector include $147 million USD in 2009 to Warid Telecom for the development of Global System for Mobile communications (GSM) network services in Uganda and $138 million USD between 2009 and 2015 to the Government of Uganda to support the development of data transmission infrastructure and e-government infrastructure. Huawei, a Chinese multinational telecom company, remains quite active in Uganda as well. Freedom House found that 90% of Uganda's telecom contracts are held by Huawei and ZTE, another Chinese Telecom company (Shahbaz, "Freedom on the Net 2018"). For example, Huawei provided Uganda with $126 millions USD's worth of CCTV and other surveillance technology (Biryabarema). The Ugandan watchdog group Unwanted Witness noted how the Ugandan government used these technologies to monitor opposition and protests during the 2019 election, a threat to Uganda's democratic process (Privacy International, "Huawei infiltration"; Unwanted Witness, "Surveillance, censorship threaten").

Additionally, as Freedom House notes in its 2018 Freedom on the Net report, China has also sponsored and conducted several training seminars in several countries to train officials on new media and information technology management (Shahbaz, "Freedom on the Net 2018"). In Uganda, the seminars focused on a "comprehensive cyber-security solution, including technical capacity to monitor and prevent social media abuse" (Monitor, "China to help Uganda"). As Freedom House notes, "[i]ncreased activity by Chinese companies and officials in Africa similarly preceded the passage of restrictive cybercrime and media laws in Uganda…over the past year" (Shahbaz, "Freedom on the Net 2018"). Along with increased public finance and telecom investments, China does appear to be making a play for influence in Uganda and trying to appeal to its government.

5. Key Takeaways

What do the results from this study of "innovator" and "emulator" countries of digital censorship reveal about the tools used from both sets of countries and how "emulators" may learn from "innovators"? This section presents five key takeaways from the analysis.

Takeaway #1: While China is the top digital censorship "innovator," there is a diffusion of digital censorship.

Although other countries look to both China and Russia for inspiration for digital censorship strategies and tools, China stands out as the standard of digital censorship. It recognized at the internet's onset the potential of this new technology and began implementing measures to monitor and censor it very early on. Though the report classifies Russia as an "innovator," this report finds that even it learned a great deal from China. In addition, Turkey, a country the study labels as an "emulator," also exhibits the characteristics of "innovator" to some extent, illustrating censorship's diffusion among similar governments. As one KII expert noted, "…it's definitely an issue of also diffusion, obviously these countries all have similar governments and similar aspirations on the side of the dictators." The example of Turkey's regional influence suggests that while development practitioners and policy makers will look to China and Russia as potential malign influences globally, they should not overlook the influence of countries with regional dominance.

Takeaway #2: Digital censorship is generally increasing.

A wide consensus across both media watchdog reports and key informant interviews is that digital censorship is on the rise in all countries examined. As the popularity and effectiveness of digital media and platforms increase, autocratic actors and would-be autocrats are increasingly seeing this as a form of media to which attention must be paid to affect and influence the narrative. In addition, real public health concerns surrounding the COVID-19 pandemic beginning in 2020 further accelerated digital censorship. Quantitative data presented in the Appendix tracks changes in government attempts to censor the internet and also show overall increases in most countries, with Nicaragua having the greatest increase. Though Azerbaijan shows no noticeable increases in the quantitative data, our KII indicates that the government is stepping up efforts.

Takeaway #3: Timing matters when installing a digital censorship regime.

Implementing technological infrastructure as well as norms and legislation around digital censorship was easier for China than Russia. It appears that a country is more susceptible to a comprehensive, government-installed digital censorship regime when its internet penetration is lower (such as China at the time it began implementing widespread digital censorship) than when the internet permeates and is more ingrained in society (such as Russia). Russia appears to be fighting an uphill battle to wrangle its internet from the clutches of the global network, whereas China seamlessly censors using its Great Firewall that it began to implement decades ago. This may have implications for countries like Uganda and Nicaragua that both currently possess low levels of internet penetration. It may be easier for these countries to implement a "China standard" regime of digital censorship than for countries like Serbia and Turkey, where internet penetration is higher and norms and tastes around usership of Western apps and platforms are much more developed. Countries like Azerbaijan, Serbia, and Turkey would need to take Russia's route to installing a comprehensive digital censorship apparatus.

China's development assistance (through its Belt and Road Initiative, for example) may open further space for support from Beijing to countries' censorship efforts in the future. In deciding the time and urgency of resource allocation to combat governments from establishing digital censorship, development professionals and policy makers may wish to devote resources sooner to places with less internet infrastructure and lower internet penetration. The clock is ticking for the Ugandas and Nicaraguas of the world.

Takeaway #4: Albeit limited, there are potential action points to limit the spread of digital censorship.

Policy makers and development practitioners have limited reach in trying to prevent the spread of digital censorship in autocratizing countries. Nevertheless, there are still ways in which they can act to prevent the spread of negative influence without infringing on other countries' sovereignty. Coordinating between democracies around digital and internet governance, particularly standard setting, in a

multilateral setting is crucial to strengthen global internet freedom. Furthermore, the West is on the forefront of many technologies, including surveillance, that may be used with malign intent. Monitoring the spread of these technologies and potentially restricting exports may be necessary.

Takeaway #5: Digital censorship legislation is vaguely worded to allow for a wide reach and flexible application in censoring online content.

One common theme that KIIs and watchdog reports noted was the intentional vagueness of legislation, something seen in both "innovator" and "emulator" countries. This vagueness allows governments to act more aggressively to censor digital media, while still maintaining an air of the rule of law. Policy makers and development practitioners should monitor proposed legislation of digital censorship and advocate for more precise wording that curbs government digital censorship.

6. Conclusion

This report presents results from AidData's examination of the institutional and technological environment and digital censorship tools used in China and Russia, along with five other autocratic or autocratizing countries: Azerbaijan, Nicaragua, Serbia, Turkey, and Uganda. The results indicate a diverse set of censorship tools that come from varied sources, including legislation, regulatory bodies, direct content and software forms of censorship, as well as new and traditional approaches to induce self-censorship among individuals and businesses alike. The stakes remain high for "emulator" countries in this study, as governments race to censor and stifle dissent and opposition discourse in digital spaces.

The objective of this report is to provide better information for policymakers, advocates, and development partners to pinpoint how countries slipping further into autocracy might be learning digital censorship methods from China and Russia. The five "emulator" countries in this study are particularly relevant to this discussion of digital censorship, given their importance as battlegrounds for influence among China, Russia, and the West. With Russia's invasion of Ukraine in early 2022, the Kremlin is already developing new digital censorship tools domestically (Ceccanese). As the situation evolves, the Russian government may deepen or innovate new tools beyond what this study was able to find. Future iterations of this work may expand to additional countries, as well as continue to refine the tools and presentation of results. Further studies might also look to explore "innovator" countries' attempts to censor digital content abroad.

7. References

AidData. China's Global Public Diplomacy Dashboard Dataset, Version 1.3, 2022. http://china-dashboard.aiddata.org.

Alexanyan, Karina and Barash, Vladimir and Etling, Bruce and Faris, Robert and Gasser, Urs and Kelly, John and Palfrey, John G. and Palfrey, John G. and Roberts, Hal, Exploring Russian Cyberspace: Digitally-Mediated Collective Action and the Networked Public Sphere (March 2, 2012). Berkman Center Research Publication No. 2012-2, Available at SSRN: https://ssrn.com/abstract=2014998.

Aliyev, Kenan, and Daisy Sindelar. "In Azerbaijan, Bank Tied to EBRD Breaks Seal On Controversial Libel Law." Radio Free Europe / Radio Liberty, Aug. 21, 2013. https://www.rferl.org/a/azerbaijan-ebrd-libel-law/25082305.html.

Alizada, Nazifa, et al. Autocratization Turns Viral: Democracy Report 2021, University of Gothenburg, Varieties of Democracy Institute (V-Dem), 2021. https://www.v-dem.net/static/website/files/dr/dr_2021.pdf.

Anthony, Sebastian. "GitHub battles "largest DDoS" in site's history, targeted at anti-censorship tools." ARS Technica. Mar. 3, 2015. https://arstechnica.com/information-technology/2015/03/github-battles-largest-ddos-in-sites-history-targeted-at-anti-censorship-tools/ .

Bandurski, David. "China and Russia are joining forces to spread disinformation." Brookings' Tech Stream, Mar., 11, 2022. https://www.brookings.edu/techstream/china-and-russia-are-joining-forces-to-spread-disinformation/.

Biryabarema, Elias. "Uganda's cash-strapped cops spend $126 million on CCTV from Huawei." Reuters, Aug. 15, 2019. https://www.reuters.com/article/us-uganda-crime-idUSKCN1V50RF.

Boese, Vanessa A., et al. Autocratization Changing Nature? Democracy Report 2022, University of Gothenburg, Varieties of Democracy Institute (V-Dem), 2022. https://v-dem.net/media/publications/dr_2022.pdf.

Boulianne, Shelley. "Twenty Years of Digital Media Effects on Civic and Political Participation." Communication Research, vol. 47, no. 7, 2020, pp. 947-966. https://doi.org/10.1177/0093650218808186.

Bow, Juan Carlos. "Ortega Spies Using Israeli Technology." Confidencial, Oct. 29, 2018. https://www.confidencial.digital/english/ortega-spies-using-israeli-technology/.

Boxell, Levi, and Zachary Steinert-Threlkeld. "Taxing Dissent: The Impact of a Social Media Tax in Uganda." World Development, Vol. 158, Oct. 2022. https://doi.org/10.1016/j.worlddev.2022.105950.

Busch, Andreas, et al. "Internet Censorship in Liberal Democracies: Learning From Autocracies?" Managing Democracy in the Digital Age, Springer International Publishing, Sep. 2017, pp. 11-28. https://doi.org/10.1007/978-3-319-61708-4_2.

Cadell, Cate. "China's robot censors crank up as Tiananmen anniversary nears." Reuters, May 26, 2019, https://www.reuters.com/article/us-china-tiananmen-censorship/chinas-robot-censors-crank-up-as-tiananmen-anniversary-nears-idUSKCN1SW03Y.

Ceccanese, Alicia. "'Disastrous for press freedom': What Russia's goal of an isolated internet means for journalists." Committee to Protect Journalists May 23, 2022. https://cpj.org/2022/05/disastrous-for-press-freedom-what-russias-goal-of-an-isolated-internet-means-for-journalists/.

Chen, Stephen. "Chinese researchers say they've developed an AI text censor that is 91% accurate." The Star, Apr. 15, 2022, https://www.thestar.com.my/tech/tech-news/2021/04/15/chinese-researchers-say-theyve-developed-an-ai-text-censor-that-is-91-accurate.

"China to help Uganda fight Internet abuse." Monitor, Jul. 26, 2017 (updated Jan. 15, 2021).
https://www.monitor.co.ug/uganda/news/national/china-to-help-uganda-fight-internet-abuse-1712478.

Committee to Protect Journalists (CPJ). "CPJ condemns 'harsh' 9-year sentence for Nicaraguan journalist Miguel Mendoza." Feb. 17, 2022. https://cpj.org/2022/02/cpj-condemns-harsh-9-year-sentence-for-nicaraguan-journalist-miguel-mendoza/.

——. "Journalist Zhang Zhan arrested for covering COVID-19 in Wuhan." May 18, 2020.
https://cpj.org/2020/05/journalist-zhang-zhan-arrested-for-covering-covid-/.

——. "New Azerbaijan media law increases restrictions on the press." Feb. 10, 2022.
https://cpj.org/2022/02/new-azerbaijan-media-law-increases-restrictions-on-the-press/.

——. "Nicaraguan journalist Emiliano Chamorro faces police harassment and surveillance." Mar. 11, 2020.
https://cpj.org/2020/03/nicaraguan-journalist-emiliano-chamorro-faces-poli/.

——. "Nicaraguan police raid independent news station, arrest two journalists." Dec. 22, 2018.
https://cpj.org/2018/12/nicaraguan-police-raid-independent-news-station-ar/.

——. "Number of journalists behind bars reaches global high." Dec. 9, 2021.
https://cpj.org/reports/2021/12/number-of-journalists-behind-bars-reaches-global-high/.

——. "One Country, One Censorship: How China undermines media freedom in Hong Kong and Taiwan." Special Report, Dec. 16 2019, https://cpj.org/wp-content/uploads/2019/12/China_ForWeb_DONE.pdf.

——. "Russian authorities harass family of exiled journalist Roman Dobrokhotov." Oct. 1, 2021.
https://cpj.org/2021/02/russian-blogger-jailed-for-25-days-over-coverage-of-navalny-protests-hospitalized-after-hunger-strike/.

——. "Russian blogger jailed for 25 days over coverage of Navalny protests, hospitalized after hunger strike." Feb. 10, 2021.
https://cpj.org/2021/02/russian-blogger-jailed-for-25-days-over-coverage-of-navalny-protests-hospitalized-after-hunger-strike/.

——. "Russia labels Mediazona, OVD-Info, and 2 journalists as 'foreign agents.'" Sept. 30, 2021.
https://cpj.org/2021/09/russia-labels-mediazona-ovd-info-and-2-journalists-as-foreign-agents/

——. "Russia uses 'foreign agents' law to hit independent outlet with massive fine." Oct. 29, 2018.
https://cpj.org/2018/10/russia-uses-foreign-agents-law-to-hit-independent/.

——. "Russia-Ukraine Watch: How the War is Affecting Press Freedom in the Region." Jun. 16, 2022.
https://cpj.org/2022/03/russia-ukraine-war-press-freedom-watch/.

Coppedge, Michael, et al. "V-Dem Codebook v12." 2022 Varieties of Democracy (V-Dem) Project.

Coppedge, Michael et al. "VDem [Country–Year/Country–Date] Dataset v12." 2022, Varieties of Democracy (V-Dem) Project.
https://doi.org/10.23696/vdemds22 and https://www.v-dem.net/data/the-v-dem-dataset/.

"Convenio de 'seguridad de la información' con Rusia: una nueva arma del régimen ['Information security' agreement with Russia: a new weapon of the regime]." Confidencial, Aug. 27, 2021.
https://www.confidencial.digital/nacion/convenio-de-seguridad-de-la-informacion-con-rusia-una-nueva-arma-del-regimen/.

Cook, Sarah. The Long Shadow of Chinese Censorship: How the Communist Party's Media Restrictions Affect News Outlets Around the World, Center for International Media Assistance, National Endowment for Democracy, Oct. 22, 2013. https://www.cima.ned.org/wp-content/uploads/2015/02/CIMA-China_Sarah%20Cook.pdf.

Custer, Samantha, et al. Silk Road Diplomacy: Deconstructing Beijing's toolkit to influence South and Central Asia, AidData at William & Mary, 2019. https://www.aiddata.org/publications/silk-road-diplomacy.

Custer, Samantha, et al. Ties That Bind: Quantifying China's public diplomacy and its "good neighbor" effect, AidData at William & Mary, 2018. https://www.aiddata.org/publications/ties-that-bind.

Dragojlo, Sasa and Aleksa Resic. "Hackers Likely Accessed Emails of Serbia's Cadastre Staff, BIRN Reveals." Balkan Insight, Sept. 21, 2022. https://balkaninsight.com/2022/09/21/hackers-likely-accessed-emails-of-serbias-cadastre-staff-birn-reveals/.

Feng, Gao. "Fine For VPN Use Sparks Rare Backlash on Chinese Internet." Radio Free Asia (RFA), May 21, 2020. https://www.rfa.org/english/news/china/vpn-punishments-05212020103537.html.

Freedom House. Freedom on the Net 2016: China. https://freedomhouse.org/country/china/freedom-net/2016.

——. Freedom on the Net 2016: Russia. https://freedomhouse.org/country/russia/freedom-net/2016.

——. Freedom on the Net 2017: China. https://freedomhouse.org/country/china/freedom-net/2017.

——. Freedom on the Net 2018: Russia. https://freedomhouse.org/country/russia/freedom-net/2018.

——. Freedom on the Net 2020: China. https://freedomhouse.org/country/china/freedom-net/2020.

——. Freedom on the Net 2021: China. https://freedomhouse.org/country/china/freedom-net/2021.

——. Freedom on the Net 2021: Azerbaijan. https://freedomhouse.org/country/azerbaijan/freedom-net/2021.

——. Freedom on the Net 2021: Nicaragua. https://freedomhouse.org/country/nicaragua/freedom-net/2021.

——. Freedom on the Net 2021: Russia. https://freedomhouse.org/country/russia/freedom-net/2021.

——. Freedom on the Net 2021: Serbia. https://freedomhouse.org/country/serbia/freedom-net/2021.

——. Freedom on the Net 2021: Turkey. https://freedomhouse.org/country/turkey/freedom-net/2021.

——. Freedom on the Net 2021: Uganda. https://freedomhouse.org/country/uganda/freedom-net/2021.

——. Freedom in the World 2022. Dataset. (2022). https://freedomhouse.org/report/freedom-world.

French, Howard. "Ukraine Exposed the True Danger of Chinese Censorship." Foreign Policy, Apr. 11, 2022. https://foreignpolicy.com/2022/04/11/russia-ukraine-war-china-propaganda-censorship-taiwan/.

Gabuev, Alexander and Leonid Kovachich. "Comrades in Tweets? The Contours and Limits of China-Russia Cooperation on Digital Propaganda." Carnegie Endowment for International Peace, Jun. 3, 2021. https://carnegieendowment.org/2021/06/03/comrades-in-tweets-contours-and-limits-of-china-russia-cooperation-on-digital-propaganda-pub-84673.

Genç, Kaya. "Turkey: Number of "insulting Turkishness" cases drops as parliament discusses changing definition of citizenship." Index on Censorship: A Voice for the Persecuted, Feb. 8, 2013.
https://www.indexoncensorship.org/2013/02/turkey-number-of-insulting-turkishness-cases-drops-as-parliament-discusses-changing-definition-of-citizenship/.

Gritsenko, Daria, et al. The Palgrave Handbook of Digital Russia Studies, Palgrave MacMillan, 2021.
https://doi.org/10.1007/978-3-030-42855-6_33.

Hellmeier, Sebastian. "The Dictator's Digital Toolkit: Explaining Variation in Internet Filtering in Authoritarian Regimes." Politics & Policy, vol. 44, no. 6, Wiley, Dec. 2016, pp. 1158-1191. https://doi.org/10.1111/polp.12189.

Hoffman, Samantha. "Managing the State: Social Credit, Surveillance and the CCP's Plan for China." AI, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives, U.S. Department of Defense, Strategic Multilayer Assessment (SMA) Periodic Publication, edited by Nicholas D. Wright, December 2018, pp. 42-47.

Human Rights Watch (HRW). "Critics Under Attack: Harassment and Detention of Opponents, Rights Defenders and Journalists Ahead of Elections in Nicaragua." Jun. 22, 2021.
https://www.hrw.org/report/2021/06/22/critics-under-attack/harassment-and-detention-opponents-rights-defenders-and.

——. "Russia: Growing Internet Isolation, Control, Censorship." June 18, 2020.
https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship#_ftn7.

——. "Russia: Harsh Sentence for Opposition Politician." Dec. 9, 2022.
https://www.hrw.org/news/2022/12/09/russia-harsh-sentence-opposition-politician.

Karppinen, Kari. "Human Rights and the Digital." The Routledge Companion to Media and Human Rights, edited by Howard Tumber and Silvio Waisbord, Routledge, 2019, pp. 95-103. https://doi.org/10.4324/9781315619835-9.

Kawerau, Lukas, et al. "Attack or Block? Repertoires of Digital Censorship in Autocracies." Journal of Information Technology & Politics, Apr. 2022, pp. 1-14. https://doi.org/10.1080/19331681.2022.2037118.

Kravchenko, Maria. "Russian anti-extremism legislation and internet censorship." The Soviet and Post-Soviet Review, vol. 46, no. 2, Apr. 2019, pp. 158-186. https://doi.org/10.1163/18763324-04602004.

Krivokapić, Đorđe. "A Disturbing Marriage: Serbia and China Team Up on Digital Surveillance." Center for European Policy Analysis (CEPA), Jan. 27, 2022. https://cepa.org/article/a-disturbing-marriage-serbia-and-china-team-up-on-digital-surveillance/.

Krushelnycky, Askold. "Chechnya: Rebels Use Internet in Propaganda War with Russians." Radio Free Europe/Radio Liberty, May 5, 2000. https://www.rferl.org/a/1093909.html.

Kynge, James, et al. "Exporting Chinese surveillance: the security risks of 'smart cities.'" Financial Times, June 9, 2021.
https://www.ft.com/content/76fdac7c-7076-47a4-bcb0-7e75af0aadab.

La Porta, Rafael, et al. 2004. "Judicial Checks and Balances." Journal of Political Economy, vol. 112, no. 2, 2004, pp. 445-470.
https://doi.org/10.1086/381480.

Li, Shan. "Made-in-China censorship for sale." The Wall Street Journal, Mar. 6, 2020.
https://www.wsj.com/articles/made-in-china-censorship-for-sale-11583448433.

Lin, Liza. "China Fines Weibo for Spreading 'Illegal Information.'" The Wall Street Journal, Dec. 14, 2021.
https://www.wsj.com/articles/china-fines-weibo-for-spreading-illegal-information-11639482120.

Lokot, Tetyana and Mariëlle Wijermars. "The Kremlin forced U.S. tech firms to shut down an app some Russian voters hoped to use. Now what?" The Washington Post, Sep. 30, 2021.
https://www.washingtonpost.com/politics/2021/09/30/kremlin-forced-us-tech-firms-shut-down-an-app-its-opponents-were-using-now-what/.

Lupion, Miranda. "The Sino-Russian Digital Cooperation and Its Implications for Central Asia." Digital Silk Road in Central Asia: Present and Future, edited by Nargis Kassenova and Brendan Duprey, Davis Center for Russian and Eurasian Studies, Harvard University, Jun. 2021, pp. 55-75. https://daviscenter.fas.harvard.edu/digital-silk-road.

Lutscher, Philipp M. "Hot Topics: Denial-of-Service Attacks on News Websites in Autocracies." Political Science Research and Methods, Cambridge UP (CUP), Dec. 2021, pp. 1-16. https://doi.org/10.1017/psrm.2021.68.

Maranto, Lauren. "Who Benefits from China's Cybersecurity Laws?" CSIS Blog Post: New Perspectives on Asia, Jun. 25, 2020.
https://www.csis.org/blogs/new-perspectives-asia/who-benefits-chinas-cybersecurity-laws.

Marlow, Ian. "The assault on Apple daily." Bloomberg, Feb. 3 2022,
https://www.bloomberg.com/features/2022-apple-daily-china-hong-kong-crackdown/?leadSource=uverify%20wall.

Meserve, Stephen A., and Daniel Pemstein. "Google Politics: The Political Determinants of Internet Censorship in Democracies." Political Science Research and Methods, vol. 6, no. 2, Feb. 2017, pp. 245-263. https://doi.org/10.1017/psrm.2017.1.

Mueller, Milton L. "Against Sovereignty in Cyberspace." International Studies Review, vol. 22, no. 4, Oxford UP (OUP), Sep. 2019, pp. 779-801. https://doi.org/10.1093/isr/viz044.

Muhindo, Clare. "Uganda's Media Council issues directive on registration of journalists; timing questioned." African Centre for Media Excellence (ACME), Dec. 11, 2020.
https://acme-ug.org/2020/12/11/ugandas-media-council-issues-directive-on-registration-of-journalists-timing-questioned/.

"'My friend, you are a transformer' against Roskomnadzor." Mediazona, Jan. 20, 2020.
https://zona.media/online/2020/01/20/batenka-vs.

"Nicaragua: Police Raid Offices of La Prensa Newspaper." BBC News, Aug. 14, 2021.
https://www.bbc.com/news/world-latin-america-58212024.

Nicas, Jack, et al. "Censorship, Surveillance and Profits: A Hard Bargain for Apple in China." The New York Times, May 17, 2021 (updated Jun. 17, 2021). https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html?smid=url-share.

Papada, Evie, et al. "Defiance in the Face of Autocratization. Democracy Report 2023." 2023. University of Gothenburg: Varieties of Democracy Institute (V-Dem Institute). https://www.v-dem.net/documents/29/V-dem_democracyreport2023_lowres.pdf.

Parker, Emily. "Russia Is Trying to Copy China's Approach to Internet Censorship." New America Weekly, Apr. 6, 2017.
https://www.newamerica.org/weekly/russia-trying-copy-chinas-approach-internet-censorship/.

Parkinson, Joe, et al. "Huawei Technicians Helped African Governments Spy on Political Opponents." The Wall Street Journal, Aug. 15, 2019. https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017.

Patrucic, Miranda and Kelly Bloss. "Life in Azerbaijan's Digital Autocracy: 'They Want to be in Control of Everything.'" Report, Organized Crime and Corruption Reporting Project, 2021.
https://www.occrp.org/en/the-pegasus-project/life-in-azerbaijans-digital-autocracy-they-want-to-be-in-control-of-everything.

Polyakova, Alina and Chris Meserole. "Exporting Digital Authoritarianism: The Russian and Chinese Models." Democracy & Disorder Policy Brief, Brookings Institution, 2019. https://www.brookings.edu/research/exporting-digital-authoritarianism/.

"Press freedom is under attack: Journalists are struggling against the worst conditions since the cold war." The Economist. May 3, 2022. https://www.economist.com/interactive/briefing/2022/05/03/press-freedom.

"Huawei infiltration in Uganda." Privacy International, Jun. 25, 2020.
https://privacyinternational.org/case-study/3969/huawei-infiltration-uganda.

Puyosa, Iria. "Venezuela's 21st Century Authoritarianism in the Digital Sphere." Toda Peace Institute, Policy Brief No. 62, Nov. 2019. https://ssrn.com/abstract=3483913.

Qiang, Xiao. "The Road to Digital Unfreedom: President Xi's Surveillance State." Journal of Democracy, vol. 30, no. 1, Jan. 2019, pp. 53-67. https://www.journalofdemocracy.org/articles/the-road-to-digital-unfreedom-president-xis-surveillance-state/.

Reporters Without Borders (RSF). "Leading Russian search engine is removing banned sites from its results." Oct. 30, 2018. https://rsf.org/en/leading-russian-search-engine-removing-banned-sites-its-results.

RFE/RL's Russian Service Current Time. "Russian Media Watchdog Blocks Facebook After Limiting Access To Multiple Other Sites," Mar. 4, 2022. https://www.rferl.org/a/russia-rferl-bbc-facebook-google-twitter-blocked/31735597.html.

Roberts, Margaret E. Censored: Distraction and Diversion inside China's Great Firewall. Princeton University Press, 2018. https://www-jstor-org.proxy.wm.edu/stable/j.ctvc77b21.

——. "Resilience to Online Censorship." Annual Review of Political Science, vol. 23, no. 1, 2020, pp. 401-419. https://doi.org/10.1146/annurev-polisci-050718-032837.

Roskomnadzor. "Historical Background," May 20, 2014. https://eng.rkn.gov.ru/about/background_information/.

"Russian oligarch Yevgeny Prigozhin, "Putin's chef," admits interference in U.S. elections." CBS News, Nov. 7, 2022. https://www.cbsnews.com/news/russia-us-election-interference-yevgeny-prigozhin-putin-chef-oligarch/.

Savov, Vlad. "Russia's Telegram ban is a big, convoluted mess." The Verge, Apr. 17, 2019. https://www.theverge.com/2018/4/17/17246150/telegram-russia-ban.

Schearf, Daniel. "Russian Censorship Group Seeks Chinese Help to Better Control Internet." Voice of America News, Apr. 29, 2016. https://www.voanews.com/a/russian-censorship-group-seeks-chinese-help-better-control-internet/3308924.html.

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

Shahbaz, Adrian, et al. Freedom on the Net 2022: Countering an Authoritarian Overhaul of the Internet, Freedom House, 2022. https://freedomhouse.org/sites/default/files/2022-10/FOTN2022Digital.pdf.

Sherman, Justin. "What's behind Russia's decision to ditch its ban on Telegram?" New Atlanticist, The Atlantic Council, Jun. 26, 2020. https://www.atlanticcouncil.org/blogs/new-atlanticist/whats-behind-russias-decision-to-ditch-its-ban-on-telegram/.

Siu, Phila. "Media Watchdog in Legal Challenge over Censorship of Gay Content." South China Morning Post, Jan. 5, 2018, https://www.scmp.com/news/china/society/article/2127057/chinas-media-watchdog-legal-challenge-over-censorship-gay-content.

Smyth, Regina. "Studying Russia's Authoritarian Turn: New Directions in Political Research on Russia." Russian Politics, vol. 1, no. 4, Dec. 2016, pp. 337-346. https://reginasmythnet.files.wordpress.com/2021/02/studying-russias-authoritarian-turn.pdf.

Stoycheff, Elizabeth, et al. "Online Censorship and Digital Surveillance: The Relationship Between Suppression Technologies and Democratization Across Countries." Information, Communication & Society, vol. 23, no. 4, Informa UK Limited, Sept. 2018, pp. 474-490. https://doi.org/10.1080/1369118x.2018.1518472.

Telesoft. "Activists claim Russian government hacked Telegram accounts." Telecoms, May 6, 2016. https://www.telecomstechnews.com/news/2016/may/06/activists-claim-russian-government-hacked-telegram-accounts/.

Troianovski, Anton. "China Censors the Internet. So Why Doesn't Russia?" The New York Times, Feb. 21, 2021 (updated Oct. 22, 2021). https://www.nytimes.com/2021/02/21/world/europe/russia-internet-censorship.html.

Troianovski, Anton, and Valeriya Safronova. "Russia Takes Censorship to New Extremes, Stifling War Coverage." The New York Times, Mar. 4, 2022 (updated May 18, 2022). https://www.nytimes.com/2022/03/04/world/europe/russia-censorship-media-crackdown.html.

"Turkey's Coup Attempt: What You Need to Know." BBC News, Jul. 17, 2016. https://www.bbc.com/news/world-europe-36816045.

Twitter Transparency. Turkey: Insights into Information Requests and Removal Request Originating from Turkey. Accessed Dec. 2022. https://transparency.twitter.com/en/reports/countries/tr.html.

US Department of State. 2020 Country Reports on Human Rights Practices: Nicaragua, United States Department of State, Bureau of Democracy, Human Rights and Labor, March 2021. https://www.state.gov/reports/2020-country-reports-on-human-rights-practices/nicaragua/.

——. 2019: Country Reports on Human Rights Practices: Russia, United States Department of State, Bureau of Democracy, Human Rights and Labor, 2019. https://www.state.gov/reports/2019-country-reports-on-human-rights-practices/russia/.

"Surveillance, censorship threaten Internet freedom and Democracy in Uganda, says Unwanted Witness." Unwanted Witness, Jan. 18, 2020. https://www.unwantedwitness.org/surveillance-censorship-threaten-internet-freedom-and-democracy-in-uganda-says-unwanted-witness/.

World Bank. World Bank Country and Lending Groups. https://datahelpdesk.worldbank.org/knowledgebase/articles/906519-world-bank-country-and-lending-groups.

——. "Individuals using the Internet (% of population) – Azerbaijan." *World Development Indicators*, The World Bank Group, 2022, https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=AZ.

——. "Individuals using the Internet (% of population) – Serbia." *World Development Indicators*, The World Bank Group, 2022, https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=RS.

——. "Individuals using the Internet (% of population) – Turkey." *World Development Indicators*, The World Bank Group, 2022, https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=TR.

——. "Individuals using the Internet (% of population) – Uganda." *World Development Indicators*, The World Bank Group, 2022, https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=UG.

Yang, Zeyi. "Now China wants to censor online comments." MIT Technology Review, Jun. 18, 2022. https://www.technologyreview.com/2022/06/18/1054452/china-censors-social-media-comments/.

You, Park. "Hong Kong's Apple Daily to live in blockchain, free of censors." Reuters, Jun. 24, 2021. https://www.reuters.com/world/asia-pacific/hong-kongs-apple-daily-live-blockchain-free-censors-2021-06-24/.

Yuan, Li. "China's Information Dark Age Could Be Russia's Future." The New York Times, Mar. 18, 2022. https://www.nytimes.com/2022/03/18/business/chinas-russia-information.html.

8. Appendix

Key Informant Interview Overview

This section lists the number of key informant interviews and experts used for the report. Due to the sensitive nature of the subject matter, we opt for their identities to remain anonymous. Table A1 shows the number of interviews and experts by country of expertise. In some cases, the number of experts exceeded the number of interviews when more than one expert was interviewed in a single interview.

Table A1: Overview of Key Informant Interviews

Country	*Interviews*	*Experts*
China	4	4
Russia	1	1
Azerbaijan	1	1
Nicaragua	2	6
Serbia	2	3
Turkey	1	1
Uganda	2	2

Democracy and Censorship Level Indicators

Figure A1 below presents institutional governance and digital censorship data covering the years 2010 to 2021. The figure displays four variables that provide an overall snapshot of democracy and government digital censorship efforts in China, Russia, Azerbaijan, Nicaragua, Serbia, Turley, and Uganda.

We take three variables from the Varieties of Democracy (V-Dem) dataset: electoral democracy, judicial independence, and government attempts at digital censorship. *Electoral democracy* captures the level to which a country experiences (i) free and fair elections and (ii) electoral competition for national leadership, as well as other factors that contribute to this aim. The variable is continuous and runs from 0 to 1, with higher values indicating greater electoral democracy. For *Judicial independence*, we utilize V-Dem's measure of high court independence. This variable evaluates "how often [high courts] make decisions that merely reflect government wishes regardless of its sincere view of the legal record" (Coppedge et al. 171, "Codebook"). The variable is continuous and ranges from 0 to 1, with higher scores indicating great levels of independence.

In addition, we present a measure of *digital censorship* using V-Dem's government Internet censorship efforts variable that measures restrictions on political information online. Censorship attempts include Internet filtering (blocking access to certain websites or browsers), denial-of-service attacks, and partial or total Internet shutdowns. The variable is an interval, continuous, and runs from -1.846 to 4.205 with higher values indicating higher levels of Internet censorship.[28]

As a point of comparison, we include another measure of democracy – Freedom House's Freedom in the World index. This index is constructed using a more expansive measure of democracy that includes concepts of civil rights and civil liberties, which encompasses electoral democracy, judicial independence, media freedom, as well as several other criteria. The score runs from 0 to 100, with higher scores indicating great levels of independence.

[28] The non-traditional range is a result of the data generating process that utilizes an Item Response Theory model. This range comes from the global sample of all V-Dem's countries and years.

For Figure A1, we normalize all variables so that they run from 0 to 1,[29] where scores closer to 1 indicate higher instances/intensities of the concept and scores approaching 0 indicate its absence. We note that V-Dem's digital censorship variable is reversed so that high scores indicate greater levels of government attempts to censor the internet.

Figure A1: Governance and Digital Censorship Data in Seven Countries

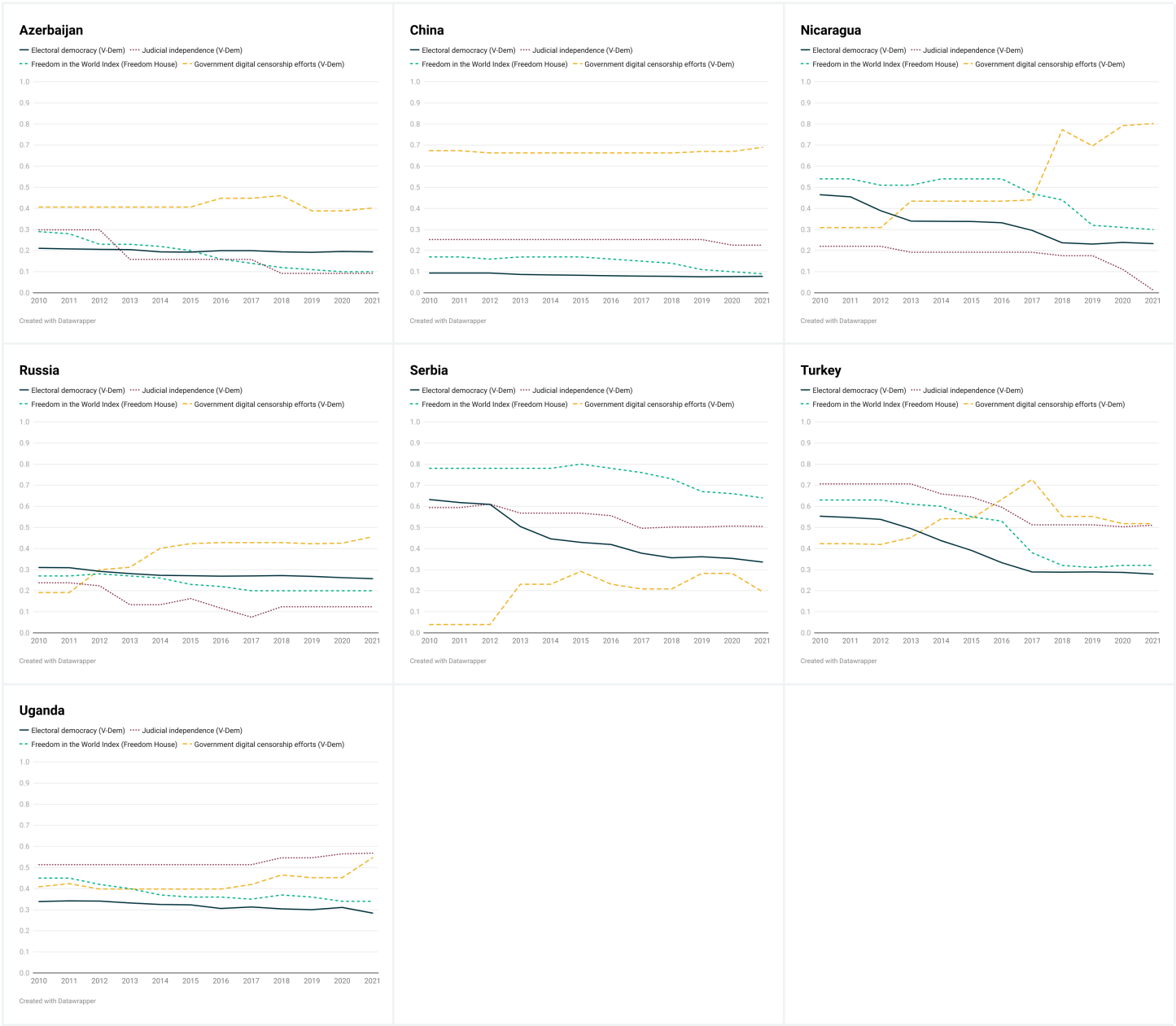


Figure Note: This figure presents four variables that provide an overall snapshot of governmental institutions and digital censorship in seven countries featured in the main report. 'Electoral Demo' (purple) shows democracy levels as measured by V-Dem's electoral democracy variable, 'Freedom House' (light green) shows Freedom House's Freedom in the World democracy index, 'Internet Censorship' (red) show V-Dem's measure of government attempts to censor the Internet, and 'Judicial Ind.' shows V-Dem's measure of a country's high court independence.

[29] We normalized the entire V-Dem and Freedom House dataset before extracting the countries and years we presented in Figure A1.