HOTSPOTS

The Internet and Collective Action in Authoritarian Settings

Bertelsmann
FOUNDATION

HOTSPOTS

The Internet and Collective Action in Authoritarian Settings

Bertelsmann
FOUNDATION

About the Author

Samuel George is the Bertelsmann Foundation's Global Market & Digital Advisor. A specialist in International Politics and Economics, he is completing a PhD at the Johns Hopkins University School of Advanced International Studies.

About the Bertelsmann Foundation

The Bertelsmann Foundation (North America), Inc., established in 2008, was created to promote and strengthen the transatlantic relationship. Through research, analysis, forums and audiovisual and multimedia content, we seek to educate and engage our audience on the most pressing economic, political and social challenges facing the United States and Europe. We are the U.S. arm of the Germany-based Bertelsmann Stiftung.

www.bfna.org

Layout and Graphic Design

Mateo Zúñiga and Ángela Ramírez
.Puntoaparte Editores

www.puntoaparte.com.co

Image cover by GDubuc (WMF)

Table of Contents

HOTSPOTS

1: Liberation Technology?

Over the last decade, a degree of cynicism has set in regarding how society views the internet's impact on democracy.[1] Americans have seen the internet cheapen policy debate, with honest dialogue scuttled in favor of dunk tweets that reduce complex topics to 280 characters. We have seen the stagnation of the U.S. Congress and Senate, bodies rendered incapable of improving the lives of the electorate, in part due to a digitally inspired and digitally enforced polarization.[2] We have seen ill-prepared, illiberal candidates rise to awesome power on the back of digital fame. We have observed the creation of online echo chambers that have Americans convinced that we are at the brink of a national divorce, even if our goals, challenges, and daily life in general remain remarkably similar across red and blue states. All told, some of the shine of digital technology has begun to dim, and this is reflected in polling: The Pew Research Center finds that 64% of Americans believe social media has had a negative impact on democracy. Across rich democracies, a median of 84% "believe access to the internet and social media have made people easier to manipulate with false information and rumors".[3]

But what about the impact of digital tools on non-democracies? After all, according to the Economist Intelligence Unit, only 8% of the globe's population lived in "full democracies" in 2022. Just a further 37% lived in "flawed democracies". Meanwhile, more than a third of the world's population lived under authoritarian rule.[4] Could it be that digital tools such as social media, private messaging, and video streaming are positioning people under authoritarianism to push for accountability from their leaders? Could these tools help repressed people fight for a more representative form of governance?

But what about the impact of digital tools on non-democracies? After all, according to the Economist Intelligence Unit, only 8% of the globe's population lived in "full democracies" in 2022. Just a further 37% lived in "flawed democracies".

This paper considers the impact of digital technology in authoritarian settings. Specifically, it questions the extent to which the internet breaks authoritarian control over information and facilitates online networking. The paper tests the hypothesis that, in countries where civil society is restricted, online networks represent a new, digital civil society ultimately capable of mobilizing offline. The subject warrants closer examination, especially as democracies around the world appear to be weakening.

To date, the literature on the collective-action impact of digital tools in authoritarian settings is mixed. Some scholars emphasize the internet's mobilization potential and how it can ultimately lead towards civil activization, liberalization and even democratization. Others counter that this potential has been oversold. They believe that, while digital tools may inspire flashes of collective action, authoritarian regimes have reacted to and strategized for this, and that the internet can be reduced to simply another tool wielded by an autocratic body to maintain dominance.

This section seeks guidance on if, when, and how the internet can act as an arena for collective action in an authoritarian context. The inverse is equally important: This section also considers if, when, and how the internet thwarts the possibility of collective action.

Liberation Technology
The Internet and Collective Action

One line of thought—particularly common during the end of the 20th century and the first decade of the 21st—is manifestly optimistic about the democratizing potential of digital tools. The literature that follows this line posits "a causal relation posited among specific forms of technology, the expansion of rights, and other forms of economic and social development".[5] The optimism stems from the internet's potential to interrupt a status quo. In an authoritarian context, mass media most often serves "government purposes as propaganda devices, and scholarly work points to the advantage that [this] constitutes for the people in power".[6] By providing citizens of an authoritarian regime access to information and ideas beyond the direct control of that regime, and the ability to share that information, internet access breaks this dynamic, challenging the state's monopoly on knowledge.[7] Given the portability of the tools and the viral, interactive nature of the platforms, this "digital scaffolding" can produce "information cascades that motivate participation in social movements and [raise] the costs of repression for image-conscious states".[8]

In 2010, leading political scientist Larry Diamond summarized these democratizing features as "liberation technology"[9] that empowers individuals to "facilitate independent communication and mobilization, strengthening an emergent civil society".[10] Diamond also discusses the potential of grass roots mobilization via online activity, and the technology's additional capacity to serve as an "accountability technology", or as tools for transparency and monitoring where previously little existed to counter the abuse of power.

Theoretically, digital tools place authoritarian regimes in a lose-lose situation, also dubbed the "dictator's dilemma".[11] A regime that permits digital penetration could eventually cause its own demise. A regime that declines to use digital technology and infrastructure cuts itself, and the country it rules, off from vital elements of the 21st-century global economy. "Since internet penetration world-wide has been deepened," wrote analyst Nivien Saleh, "the dilemma implies that dictatorships are bound to fall one by one, paving the way for democracy."

Yet determining the causal impact of the internet on democratization may be impossible due to "indeterminant micronarratives".[12] That is why some have focused on "more precise causal mechanisms … such as whether internet access increases individual propensity to take risky political action or lowers the transaction costs for organizing a political protest".[13] Collective-action research has long highlighted the importance of personal ties, especially for "high risk protest movements".[14] Could digital networks provide an arena to create those ties?

Beyond simply sharing and obtaining information, the internet can create a "participatory culture", as anyone with access can view, share and produce content.[15] The nature of social media implies that its consumers are exposed to potentially dissenting content without necessarily seeking it out in the first place.[16] The internet also provides a sphere for like-minded individuals to "meet and mobilize for collective action" in settings where such action would otherwise be far more difficult, if not impossible. Any mobilization would still require grievances and triggers, but as Dutch scholar Kris Ruijgrok suggests, "these are everywhere" and are usually not enough to provoke collective action.[17] The internet increases the likelihood that grievances and triggers will result in mobilization.

How might this happen? Ruijgrok offers four causal mechanisms that tie digital access to collective action in illiberal settings. First, he suggests digital tools reduce the costs and risks for opposition groups. Communication is cheap, rapid and viral, and planning is not "hampered by spatial or temporal barriers". Second, the internet accounts for an attitudinal change, as for a period of time (potentially years) prior to a mobilization, people will have had access to views beyond the official government narrative. Third, access decreases informational uncertainty for potential protesters. Finally, the knock-on effects of photos, videos and on-the-ground accounts impact individuals' decision-making processes via the heuristic of availability. The dramatic digital content that goes viral during mobilization is what is believed to swell protests.[18]

Scholars also theorize mechanisms that connect online activity to offline action. Digital platforms offer the infrastructure to organize and advertise such action, which allows for mobilization even where formal structures, such as trade unions, may be repressed or barred.[19] Online activism may also "cultivate the psychological preconditions to embolden individuals to embrace more burdensome offline protest".[20] One key hinderance to collective action in repressive settings is that frustrated citizens often are unaware that others share their frustrations and may be willing to act on them. Perhaps content on social media generates a collective identity that gets built up before any public protests. This online identity can subsequently have a spillover effect that leads participants to take to the streets.[21]

The literature cites numerous events that appear to highlight technology's seemingly unencumbered ability to spread these benefits. Diamond's 2010 paper offers a series of examples. He begins with Philippine President Joseph Estrada's fall in 2001 as the first time a head of state lost his position due to a "smart mob". "Since then," Diamond wrote, "liberation technology has been instrumental in virtually all of the instances where people have turned out *en masse* for democracy or political reform." Diamond subsequently cites the Ukrainian Orange Revolution of 2004, the Lebanese Cedar Revolution of 2005, 2007 Venezuelan student uprisings, a 2008 general strike in Egypt and Iran's Green Movement of 2009.

Digital tools reduce the costs and risks for opposition groups. Communication is cheap, rapid and viral, and planning is not "hampered by spatial or temporal barriers".

Repression Technology?
The Regimes Respond

The prior examples may raise eyebrows because none of the countries subsequently transitioned to democracy. In fact, some of them have become less liberal since these digitally inspired moments of collective action. The failures led to a second line of thought, one that posits that the optimism of prior scholarship was exaggerated. This more pessimistic interpretation does not challenge the ability of digital tools to generate moments of collective action. The issue is whether the ultimate impact of these moments is considerably less than initially imagined. As Ruijgrok writes, "internet use is more likely to have direct effects on mobilization than to lead directly to democratization. [In] the Arab uprisings, the turmoil in Moldova in 2009, the Green Revolution in Iran, or the Ukrainian Orange Revolution, the internet can be seen to have been an important tool for bringing people into the streets, but not for democratizing these societies."

Authoritarian governments have demonstrated the capacity and will to block potentially offending social media networks and search engines, and identify and prosecute online "offenders". This generates an online environment of self-censorship based on fear. Digital technology can also be a tool for authoritarian regimes to launch propaganda campaigns, promote disinformation, and spread fake news. President Vladimir Putin's Russia, for example, has weaponized the internet against democracy within its borders and beyond.[22]

Scholars who "emphasize 'repression technology' contend that the internet, similar to traditional media, is not free from government interference".[23] As Sarah Oates found in 2013, internet access can in fact impede collective action in "non-free states" as

> "the real asymmetry in power between repressive states and citizens lies in the ability of states to deploy the internet in a carefully choreographed manner that simultaneously promotes state interests through propaganda as well as discredits opponents via information campaigns and strategic takedowns of internet sites at critical political moments. At the same time, the state can use the internet to penetrate resistance organizations with ease, allowing them to selectively intimidate or arrest cyber-dissidents."

In simple words, citizens have had the internet, but so have authoritarian regimes. And the latter have developed techniques to stymie the internet's collective-action potential. These strategies developed over time based on trial and error. Political scientist Ronald Deibert offers three "generations" of controls.[24] First-generation controls are defensive. They are aimed at preventing access to and blocking information. These controls can be crude and error-prone, and possible work-arounds exist, but they are widely used blunt tools. Second-generation tools are used to regulate digital information "through laws, regulations, or requirements that force the private sector to do the state's bidding by policing privately owned and operated networks according to the state's demands". Most countries have such regulations, but in authoritarian settings these mechanisms are abused to limit expression and information sharing. Via third-generation controls, authoritarian regimes go on the offensive. These tools involve "surveillance, targeted espionage, and other types of covert disruptions in cyberspace". The existence or threatened use of these tools can have a critically dampening impact on the internet's potential mobilization impact. As Deibert found, "at the very least, persistent cyberespionage attacks breed self-censorship and undermine the networking advantages that civil society might otherwise reap from digital media."[25]

Moreover, digital technology may be a "little first-amendment machine",[26] but some have argued it is an opiate of the masses. By itself, a few million "thumbs-up" on a *cause de jour* social media post will not generate change and could even undermine any groundswell should individuals solely exercise armchair activism. Evgeny Morozov, a Belarusian scholar, calls this "slacktivism: a feel-good online activism that has zero political or social impact" on the ground.[27] Others suggest "slacktivism" may even play into the hands of regimes, keeping protesters off the street and in an online setting where the tenor can be easily monitored and action controlled.[28] Additional skepticism stems from the comparatively thin bonds created by online connections. Elizabeth Ann Stein, writing in *Social Science Quarterly*, notes that the word "friend" is frequently placed in quotation marks when referencing the relationship between individuals connected via social media. The quotation marks underscore the tenuous nature of the relationship and, in turn, highlight the comparatively thin ties created by digital tools.

Finally, a number of scholars have highlighted the importance that technology companies, themselves, play in this equation. As scholar and analyst Simin Kargar explains, "The so-called liberation technology's success or failure is not merely a product of the state's capacity for information control versus civil society's ability to mobilize. The outcome is also affected by external factors such as tech—and sometimes even economic policies—that target audiences in authoritarian states."[29] For example, Ankara has succeeded for years in pressuring social media companies to censor content available in Turkey.[30] Supposed free speech warrior Elon Musk was only the latest to succumb to such pressure when Twitter limited the content available on its platform in Turkey in the run-up to that country's hotly contested 2023 presidential election.[31] The equation is further muddied when Western-imposed sanctions limit the ability of technology companies to operate in authoritarian environments. Kargar sites Iran and Sudan as two countries in which the impact of digital technology has been blunted by such sanction regimes.[32]

Thus, the scholarship offers theoretical arguments for why digital media may offer the tools to overcome the collective-action dilemma and for why authoritarian regimes could stymie the impact of any such activism. Ruijgrok, for his part, warns against simplifying the debate into reductive "cyber utopian" and "cyber pessimist" camps. He suggests that more recent scholarship has devoted attention to "how various actors (including governments) and social contexts interact with the internet". In other words, additional process tracing is required to understand why the impact of digital mobilization can vary among authoritarian settings.

To further explore how context impacts outcomes, the next chapter considers three cases, those of the Arab Spring, and contemporary China and Russia.

The so-called liberation technology's success or failure is not merely a product of the state's capacity for information control versus civil society's ability to mobilize. The outcome is also affected by external factors such as tech that target audiences in authoritarian states.

HOTSPOTS

2. The Arab Spring

Dreams Deferred

The Arab Spring, a series of uprisings that arose unexpectedly in several Middle Eastern and North African (MENA) countries in late 2010 and 2011, would seem to be a logical case study to consider first. After all, the initial protests appeared to confirm the high hopes that many had for the internet's democratizing potential. Media outlets heralded the "Twitter Uprising" and the "Facebook Revolution",[33] which reflected digital tools' apparent ability to achieve their prophesized impact as "liberation technology". Yet today, more than a decade later, the results are far more complex and ambiguous than the initial narrative of digitally inspired democratization. Reconsidering the Arab Spring offers insight into such tools' potential and limitations under authoritarian regimes.

Prior to gaining access to digital tools, citizens may have tired of corruption and economic stagnation in the region, but they had little opportunity to publicly challenge oppressive regimes. They had no mechanism for overcoming the challenges of collective action. Arab Spring protesters, who first appeared in Tunisia before making their voices heard in Egypt, Libya, Yemen and other nearby countries, relied on social media to organize and share images and videos, and to raise awareness at home and abroad.

This review considers the cases of Tunisia and Egypt, two focal points of the Arab Spring where populations lived under "repressive regimes [that managed] to sustain political power in large part through censorship and limiting access to news and information via state run media".[34] In the concluding section, Syria is also discussed.

Digital Networking and The Arab Spring

The self-immolation of Tunisian merchant Mohammed Bouazizi in late 2010 sparked the uprisings. Bouazizi had been unable to navigate the bribery-laden bureaucracy required to sell vegetables on the streets of Sidi Bouzid, a regional capital, and had been harassed by public officials for his efforts. Bouazizi's dramatic action itself may not have triggered collective action in a pre-digital era. The cocktail of brutality, petty corruption and bureaucracy that Bouazizi experienced was unremarkable across the much of the region.[35] These were the potentially triggering events, daily occurrences for decades.

Given the extensive government control over traditional media in the region, the coverage of Bouazizi's death could easily have been muted in traditional outlets.[36] In fact, during the initial weeks of the Tunisian uprising, national media did not cover it, even as protesters took over urban areas.[37] However, in an era of digital connection, the images spread rapidly on social media.

Critically, the MENA region had become increasingly digitized, and mundane expressions of frustration on the internet "set the scene for the moment of confrontation".[38] Before the Arab Spring, Tunisia and Egypt had "active blogospheres" addressing government abuses.[39] In Egypt, liberals, minorities and religious groups had been using internet tools to challenge the oppressive regime of Hosni Mubarak (1981–2011) as early as 2005.[40]

In the years leading up to the Arab Spring, Egyptians increasingly turned to social media in a manner that facilitated collective action. They used "cell phones, blogs, Twitter, Facebook, and YouTube to document police excesses, organize meetings and protests, alert each other to police movements, and get legal help for those who had been arrested".[41] During this period, online activists also learned and developed tactics that would allow them to access digital tools even in the event of a government crackdown on internet access.

By 2011, "a cottage industry of bloggers and activists used the internet to evade government censorship by … building spaces online where individuals could publish information critical of the government without attaching their names to it."[42] This digital incubation period ensured that when a trigger event occurred, it would fire a potent shot.

Once the uprisings began, the central role of social media solidified. This outcome hued closely to what researchers Yiran Wang and Gloria Mark found elsewhere, that in "regulated news environments… citizens will trust online news and citizen media more than government news, and will turn to their social networks and other citizens for alternative information sources."[43] In Egypt and Tunisia, digital tools allowed citizens to solve the problem of organizing collective action against a repressive regime: 88% of surveyed Egyptian citizens reported accessing information regarding protests there via social media, as did 94% of surveyed Tunisians.[44]

Regime Efforts to Stifle Mobilization

Throughout the MENA region, regimes implemented a series of digital censorship mechanisms years before the crises emerged. Their systems had not been fully tested, however, and these governments initially proved incapable of blunting the spread of digital content during the Arab Spring. Tech-savvy Tunisians continued to find mechanisms to evade the censors. Once the protests began, the regime in Tunis tried more draconian censorship measures, such as blocking Facebook and Twitter.[45] But the government lacked the capacity to sustain these blocks. It could not control the platforms themselves, and it did not have the technological ability to prevent access.[46] Tunisian citizens were using international social media platforms, which the regime could not control, while the regime was censoring with international technology that it could not rapidly update or tailor.

"Software activists" rapidly figured out work-arounds to firewalls using VPN networks, and Tunisians found ways to access and post content as if they were outside the country, avoiding filters and blackouts. While service was interrupted at various points, it was never comprehensively blocked. When one outlet went dark, Tunisians simply moved to another. When YouTube access was cut, Tunisians shifted to sites such as Facebook and Twitter to share protest-related content.[47]

The Tunisian regime's inability to shut off the web was mirrored elsewhere in the region. In Egypt, "a small group of tech-savvy students and civil society leaders stayed connected by organizing satellite phones and dialup connections to Israel and Europe."[48] Mubarak was able to knock the country offline for several days, but those most affected were middle-class Egyptians for whom the loss of access was further incentive to take to the street. At the same time, blackouts did not impede use by the digitally adept. It was, as a group of scholars led by Philip Howard concluded, "not the information blackout Mubarak had ordered".[49]

Once digital networks were activated, and as they began to spill over into offline events, the regimes struggled to curtail the spread of digital information. They were forced to react not online but on the ground. It was still insufficient to turn the tide. Tunisian protesters were able to force a political transition and spur significant liberalization. President Zine El Abidine Ben Ali's regime collapsed weeks after the protests began, and he fled to Saudi Arabia in mid-January 2011. One of his last actions as president was to remove all restrictions on internet access, but even this was not enough to save his position.[50]

Following the regime's downfall, digital tools continued to be instrumental in facilitating transitions towards accountable democracy and increased liberalization—even if that progress has recently tempered.[51] Tunisian civil society, for example, made progress in promoting open data and transparency, exemplifying how citizens can use technology to check governmental actions.[52] Following the revolution, Amira Yahyaoui, a young Tunisian activist, launched Marsad ("Observatory"), a watchdog website. The platform monitored the activities of the National Constituent Assembly, the body that devised a new Tunisian constitution, and it now monitors the country's parliament. In pivotal moments after the regime's downfall and as the political transition got underway, Yahyaoui and her team ensured that Tunisians could track legislative processes. The team attended parliamentary sessions, photographing and videoing votes to ensure transparency in a country whose political tradition was marred by secrecy. The team later published the content on their website.[53]

Tunisia, in other words, might be a digital success story; at least in the near term. But such success was by no means uniform throughout the region. In Egypt, though the uprisings removed Mubarak from power, the result was not a transition towards participatory democracy. Instead, a series of tumultuous governments ultimately gave way to a hardline military coup led by Abdel Fattah al-Sisi, the country's current authoritarian ruler.

Having learned a lesson during the Arab Spring, the Sisi regime, to curtail online activism, has further restricted

internet use through blackouts, shutdowns, physical and psychological intimidation of users, and their imprisonment.[54] A 2017 Harvard investigation found that Egypt substantially blocks politically themed content and that this practice has increased notably since 2012.[55] The fall of the Mubarak regime created a power vacuum the was ultimately filled by another authoritarian body that regained control by rolling back liberalization.

What explains the divergent outcomes in Tunisia and Egypt? After all, in both cases, the regimes collapsed, the military did not intervene (initially), and political parties subsequently organized democratic elections. Scholars do not link success or failure to digital maturity. According to Limor Lavie, Tunisia benefited from comparative consensus on the country's political direction, in effect allowing democratic infrastructure to rapidly fill an emergent power vacuum. Egypt, by contrast, faced a far more divided populace marked by long-standing political, religious, and ethnic cleavages.[56]

Overall, scholars argue that given Tunisia's higher levels of development and education, combined with a lack of deep social cleavages, it was better positioned for post-regime cohesion compared to Egypt. These advantages positioned Tunisians to rapidly and comprehensively fill the power vacuum left by the authoritarian regime.

Syria, however, offers an example of a much different outcome of a digitally inspired uprising. The Arab Spring protests arrived later in Syria—the first protests began on January 26—some 12 days after Ben Ali abdicated. This additional time not only allowed the regime of Syrian President Bashar al-Assad to prepare, but it also underscored just what was at stake should the mobilizations continue unchecked.[57] Al-Assad made an early and decisive decision to respond to Arab Spring mobilizations with brute force. His ability to adopt this strategy stemmed from elite cohesion: In Syria, no split occurred between ruling elites, which, given its Alawite minority composition, had a strong ethnic incentive to stick together.[58] The approach did not require extensive internet censorship capacity, but it did require a willingness to kill hundreds of thousands of citizens and plunge the country into civil war. The strategy succeeded in blunting the uprising and al-Assad maintains his position to the present day.

The Syrian regime crushed the protestors in the streets, not online. Throughout the protests, tech-savvy Syrians found ways to work around state censorship. In October 2010, the "Alkasir" proxy server used by protestors fulfilled 13,826 Syrian requests to access content blocked by the regime. As the Arab Spring unfolded and Syrian censorship increased, use of Alkasir spiked; in October 2012 nearly 1 million requests were fulfilled in Syria.[59] These findings led Professor Walid Al-Saqaf to conclude that the Alkasir program was "indeed used effectively to bypass government-imposed censorship at a very delicate and important period".[60] Yet access alone could not engender a transition, and the Syrian example indicates that regimes can overcome inefficiencies of digital censorship with a willingness to resort to brute force.

A 2017 Harvard investigation found that Egypt substantially blocks politically themed content and that this practice has increased notably since 2012.

3. China

Taking a Walk, Hitting a Firewall

China stands out as an example of an authoritarian regime that has liberalized internet access without incurring widescale collective action.[61] Many authoritarian regimes would hope to duplicate this success, but China has achieved the result under particular circumstances that are difficult to replicate. China has invested significant resources and effort into minimizing online tools' collective-action potential. A closer look at the country's digital experience finds that, on the one hand, the internet can, even in China, instigate moments of collective action. On the other hand, the Chinese government's heavy-handed attempts to minimize the impact of these moments have been largely successful.

The internet was introduced in China in 1994, and by 1997 the country had roughly 620,000 internet users.[62] In the last 25 years, that number has spiked, with the current total topping 1 billion, surpassing the *combined* number of users in the U.S., Japan, Russia, Brazil, Germany and the U.K.[63]

The country is highly connected. A 2015 study found that the average Chinese internet user is online for 26 hours per week, that the country had 1.3 billion active mobile phones, and that over three quarters of those phones had active digital networking capacity.[64] Sina Weibo, the Chinese microblogging website frequently compared to Twitter, is estimated to have had more than 253 million daily users in 2022, up from 184 million in 2018.[65] The tools have been used to express dissent and to create networks outside of those sanctioned by the state, and to spread information that differs from the official narrative.[66] A "general consensus" emerged by 2010 "that some form of nascent or embryonic civil society is taking shape in China outside of the sphere of influence of the once all-powerful and all-inclusive state".[67]

Meanwhile, local protests increased in China, rising from 10,000 in 1994 to 80,000 in 2008, before again jumping to 180,000 in 2010.[68] Reflecting on the fact that the Chinese Gini coefficient, a measure of economic inequality, declined during those years (and thus, by their reading, diminishing the sense of grievance), scholars attribute this spike to digital activity and connection.[69] In fact, some of the most noteworthy examples of collective action mobilization in 21st-century China have been facilitated by online connection. For example, in 2011, when residents of Wukan protested the unauthorized sale of public land by village leaders, the Sina Weibo platform featured extensive discussion on the events, including input from Wukan residents themselves, who advocated for their cause.[70]

Chinese social media has also impacted in-person events, such as environmental protests and taxicab strikes; microblogging on the latter even led to similar strikes occurring in other regions of the country.[71] These digitally inspired offline events are known as *jiti sanbu* or "taking a collective walk", language used online to organize without attracting censorship.[72] Meanwhile, other digital movements have remained online but have had offline impact. *Wangluo shijian*, or "online events", have, for example, led to the removal of corrupt officials.[73]

While scholars are typically drawn to the larger-scale expressions of frustration, this event-based analysis fails to capture the daily digital interactions that ultimately boil over and become *jiti sanbu* or *wangluo shijian.* This approach "privileges open, visible, and public confrontation but leaves out a great deal of what is politically significant that sets the scene for the moment of confrontation".[74] Such an approach, according to Jun Liu of the University of Copenhagen,

> "first, fails to provide a big picture of structural change that has been introduced by the integration of ICTs into Chinese life and that, in turn, facilitates contentious collective action. Second, it fails to reveal possible interconnections across periods of digitally mediated political contention. Third, it fails to recognize the long-term, or 'gradual revolution' introduced by the imprints, or cumulative effects, of digitally mediated political contention on (contentious) politics in particular and Chinese society in general."

Liu highlights "everyday digital resistance" that features the use of "humor, jokes, parody satire, and homophones" collectively and repeatedly used on the Chinese internet with the aim of evading censorship. This also includes the concept of "rumor" (*yaoyan*), text messages that offer an alternative to government discourse that comes with the request that the receiver shares the message with as many people as possible before the regime censors the content. In this sense, the sharing of rumors becomes a digital engagement mechanism, and it is part of an ongoing game of cat-and-mouse between some internet users and the regime's censors.

Thus, China is not immune to the viral potential of digital content. Yet the aforementioned mobilizations have remained local in nature. How, then, has the Chinese state managed to spread digital access without incurring the wrath of netizens? The answer lies in a massive effort to specifically control the collective-action potential of digital tools.

Preventing Collective Action in China

In China, internet censorship occurs in three primary ways.[75] First, certain websites are proscribed from operating in the country, a program known as the "Great Firewall". A second mechanism is "keyword blocking", whereby users are prevented from posting or searching certain specific words or phrases. Both of these mechanisms have work-arounds: Facebook and Twitter may be inaccessible in China, but Chinese programmers have created popular domestic alternatives. Meanwhile, Chinese posters can use word games, puns and double meanings to avoid triggering automatic censorship. The Chinese government has been consequently forced to ramp up "soft" censorship methods, meaning manual review of digital content—a third form of censhorship.

Manual censorship is the most labor intensive, expensive and impactful mechanism. A legion of functionaries reviews online content and removes that which is found objectionable. By observing this process, scholars can gain insight into the online content that the Chinese government views as threatening.

In a groundbreaking study from Harvard University, scholars Gary King, Jennifer Pan and Margaret Roberts engineered a program capable of downloading more than 11 million Chinese social media posts and revisiting them to determine if they had been tampered with or removed. They found that 13% of posts overall were censored. Because the researchers had downloaded the posts before they were removed, they could categorize them and develop hypotheses about the Chinese government's strategy.

King, Pan and Roberts did not determine that the underlying goal of the censorship program is to repress state critique. Instead, they found the purpose is to "reduce the probability of collective action by clipping social ties whenever any collective movements are in evidence or expected".[76] In other words, they determined that the primary goal of Chinese internet censorship is to prevent the emergence of civil society.

The researchers found examples of uncensored, scathing criticism of, for instance, a local state functionary, China's One Child policy, and even the Tiananmen square massacre. They also found examples of censored posts that supported the state but had collective-action potential. They concluded that "censorship is primarily aimed at restricting the spread of information that may lead to collective action, regardless of whether or not the expression is in direct opposition to the state."

"censorship is primarily aimed at restricting the spread of information that may lead to collective action, regardless of whether or not the expression is in direct opposition to the state."

Does Censorship or Threat Influence User Behavior?

Of the different elements of China's censorship strategy, which mechanism most influences behavior? Jiayin Lu and Yupei Zhao offer fascinating insight into this critical question in a 2018 study. As a jumping-off point, they consider self-censorship as the main method that the government and internet providers rely on, a supposition supported by other scholars.[77] In other words, mechanisms are in place for the government to block or remove disproved content, but the most important tool is influencing citizens to adopt constraint in what they post and share.

To explain this behavior, the authors apply structural threats theory, arguing that internet censorship in China "possesses the characteristics of both intended threat and perceived threat".[78] "Intended threat" refers to legal codes and laws, and the scholars measure this quantitatively in terms of an internet user's familiarity with these regulations. "Perceived threat" refers to the degree of concern that individuals feel about the potential of being punished. The fundamental issue Lu and Zhao investigated was which threat was playing a greater role in Chinese self-censorship. The pair engaged 2,188 Chinese university students in an online survey, and they used the results to conduct statistical regressions.

The investigation found a statistically significant *positive* relationship between knowledge of censorship laws and both online and offline political activity. In other words, the more knowledge of the laws a given student had, *the more likely* they were to actively express political sentiment. However, the regressions also found a statistically significant *negative* correlation between the psychological perception of the capacity of the state and online expression. The finding led the authors to conclude that "young adults who have a perception that there is a more serious degree of internet censorship will have a lower level of online political expression and protest … while simply knowing about internet laws and regulation does not directly decrease people's interest in political protest and expression."[79]

The regressions also found a statistically significant negative correlation between the psychological perception of the capacity of the state and online expression.

A Difficult Context to Replicate

Such findings indicate that China's capacity (or perceived capacity) diminishes digital risk-taking. China, of course, maintains a capacity that few other countries possess. The state and state-owned enterprises own the internet infrastructure, and private interests must rent bandwidth from them.[80]

Thus, China's success in censoring social media is "inexorably tied to the dominance of domestic companies … in China's market for social media content."[81] This is a unique dynamic as the social media options available in most countries, authoritarian or otherwise, are rarely based in those countries themselves: They are usually from the United States. Sites such as Twitter and YouTube do not automatically remove content at the request of national governments.[82] By contrast, Chinese-based companies have no choice but to abide by government censorship requests, and they have "widely tolerated" censorship as a cost of doing business in China.

Beyond digital censorship, China combines traditional intimidation with an astounding ability to use digital tools and artificial intelligence to monitor its citizens' physical activity. All internet users in China must register for internet service, logging in with a national identity or passport number. Similarly, internet cafés record such information prior to servicing a customer. Chinese internet users are aware that the government can trace online activity back to an individual, even if it rarely does so.[83] China has also developed an extensive network of surveillance cameras that can identify citizens using face-recognition technology, particularly in the Uyghur-heavy Xinjiang region. This technology can also scan for behavioral traits, such as nervousness or agitation.[84] The process may be effective, and few countries can replicate it.

China's A4 Protests

In late November 2022, at least 10 people died in an apartment fire in Urumqi, Xinjiang's capital. The victims were apparently unable to exit the building due to draconian "zero-COVID" policies that "restricted the movement of both victims and rescuers".[85] The catastrophe occurred as millions of Chinese were already at wits' end after nearly three years of heavy-handed government restrictions on movement meant to stop the spread of COVID-19.

The casualties sparked the so-called A4 nationwide protests, named after the size of blank pieces of paper that protesters would wave. The paper alluded to their inability to share their frustrations in words due to censorship. Such a public display is rare in China and presented a challenge to the regime. The protests themselves attest to digital tools' potential as mechanisms to trigger collective action since their usage was a critical catalyst for mobilizing demonstrators. However, Beijing's swift response, online and in the streets, illustrates the authoritarian capacity to control the power of those tools.

In the days following the deadly fire, neighbors placed flowers near the burned building. If not for social media, such actions may not have spread far beyond Urumqi Road. But passersby shared images of the makeshift memorial on microblogging sites. This, in turn, spread awareness of the memorial, and within hours hundreds of people gathered at the scene. As the crowd swelled, it became rowdy, with chants directed against the regime of President Xi Jinping.[86]

Videos and images of the protest ricocheted worldwide on the internet thanks to two factors. First, Chinese netizens had become increasingly fluent in techniques to avoid the censors on domestic platforms. Strategies included puns, memes and coded language. Digital users could, for example "post screengrabs to avoid text filters, or add filters to videos before sharing to sidestep automated detection systems".[87]

However, observers noted that in many cases, especially those involving younger netizens, the language used in posts was blunter. It was not couched in ambiguous terms that analysts had seen before.[88] The Chinese censorship system appeared initially flooded. It could not keep up, and the posts spread even on Chinese-based apps such as WeChat.

Secondly, Chinese internet users demonstrated better knowledge of ways to circumvent the digital firewall and access the global internet, especially via platforms such as Twitter, Instagram and Facebook. During the protests, international providers observed a sharp uptick in downloads of VPN services, tools that allow users in China to appear to be accessing the internet from abroad, thereby gaining access to censored content.[89]

This increase occurred on top of the millions of Chinese who already accessed VPNs; a 2018 survey found that 31% of Chinese netizens used VPN technology.[90] As a result, Twitter, in theory a platform inaccessible in China, was the eighth-most downloaded app in the Apple App Store in China during the protests, the highest it had ever ranked in the country.[91]

The protests appear to have had a degree of success. Beijing discontinued the most onerous requirements of its zero-COVID policy immediately after the protests. This indicates digital tools can resolve the collective-action dilemma and influence tangible change, even in the most powerful autocracies.

Beijing did not remain flat-footed, however. The regime's response reflected an ability to ramp up digital repression and a willingness to pursue physical intimidation. Before the month was out, the Cyberspace Administration of China issued guidance to key Chinese internet platforms, instructing them to increase censorship capacity. Within days, most protest-related content on Chinese platforms disappeared.[92] Similarly, access to VPN technology quickly became far more difficult.[93] Both steps indicate that the regime could respond to acute moments of digital challenge.

Ominously, authorities also began detaining individuals found to have protested. Some were subjected to questioning prior to release. Others were arrested for "provoking trouble", "a notoriously vague charge that carries a maximum sentence of five years, and one which critics say is often used to stifle dissent".[94] Given its widespread control over digital infrastructure and the need for users to register, Beijing could access phone tower data to triangulate who was likely present at the protests.[95] Additional regulation issued after the protests appeared to make even "liking" disapproved content a crime.[96] The increasingly low level of tolerance, combined with state enforcement capacity, could have a chilling effect on future digital risk-taking.

HOTSPOTS

4. Russia Shaping the Internet

Like the MENA countries and China, Russia underwent a period of rapid digitization in the 21st century. In 2002, only 2.1 million Russians, or 2% of the adult population, accessed the internet. By 2008, 14 million Russians, or 16% of adults, had.[97] By 2018, Russia was Europe's largest internet market, with 90 million users, a penetration rate above 75%.[98]

Yet, the internet has not led to extensive civil society mobilization in Russia. As Floriana Fossato, an expert on the country, notes, "Russia is shaping the internet, rather than Russian society being shaped by the internet."[99] The state, rather than citizens online, acts as "the main mobilizing agent."[100] This leads Sarah Oates to conclude that "the Russian masses seem to reap little to no benefit from the democratizing potential of the internet, while the state successfully uses the online world to further its non-democratic agenda of citizen compliance and control."[101] In fact, the regime has "used the internet as an additional political tool for control and co-optation."[102]

This was not always the case. The Russian internet was more open than traditional media outlets in the first decade of the 21st century. This changed dramatically following the Winter of Discontent, the nickname given to a series of protests against government corruption that unexpectedly erupted in December 2011. The protests stemmed from electoral violations and corruption, and the national media's blatant manipulation of the news. Content shared widely on the internet brought the misconduct to light. These subsequent expressions of civil society, spurred by the internet, represent a watershed moment in the Kremlin's approach to digital tools.

Oates traces the beginning of the mobilization to Putin's appearance at a sporting event, when some in the audience voiced their displeasure with him. When the heavily censored Russian media shared video of the event, the booing had been edited out, in contrast to online postings. This and other, similar examples of media manipulation lent credence to the internet as a more reliable information source.

Following the Winter of Discontent, "the Kremlin grew increasingly intolerant of political and civic activism",[103] and this disposition led Moscow to adjust its attitude to the internet. In a transition that began in 2012, the Russian government increased "monitoring web traffic, blacklisting websites, and employing teams of pro-Putin online trolls", as well as jailing dissident bloggers.[104] By 2014, hundreds of Russian websites were blocked. A group of scholars led by Sergey Sanovich of Stanford University extrapolate from the Russian crackdown three broad classifications for "government response to online opposition in authoritarian … regimes."[105] The first, offline responses, entails actions taken in the physical world to control the digital one. These include regulations, legal action and physical intimidation. This mechanism leverages the government's monopoly on the use of force, legal codification and taxation. By using arbitrary and draconian use of the law, Moscow could mute troublesome domestic outlets and enforce an atmosphere of self-censorship.[106] In particular, a notorious Law on Extremism can be used to prosecute even the "liking" of certain content on social media, while a blogger law forced posters to register using offline physical identities and locations.[107]

In particular, a notorious Law on Extremism can be used to prosecute even the "liking" of certain content on social media, while a blogger law forced posters to register using offline physical identities and locations.

The second category is denial of service, or online filtering. For example, a state-owned bank purchased in 2009 the Yandex search engine, commonly referred to as the Russian Google. That gave Moscow the capacity to shut off a popular blogging service during controversial periods, such as that following the 2014 Russian incursion into Ukraine.[108] Vkontakte, "the Russian Facebook", similarly succumbed to state pressure, as did LiveJournal, another popular, Russian-owned blogging platform.[109] Like China, Russia enjoys an ability to implement social media censorship when a platform is domestically owned and operated. International platforms such as Facebook and Twitter, however, remained available through early 2022. These platforms were unwilling to follow censorship requests (at least not uniformly), and blocking their services risked provoking broad discontent as many apolitical Russians used them for non-contentious activities.[110]

Unable to impose the level of censorship it would like, Moscow began perfecting a third mechanism of restricting digital collective action—fake news, bots and trolls. Specifically, using bots, or automated social media accounts, the regime "alters the balance of opinions"[111] on social media, drowning out individual users with a flood of fake posters sharing pro-regime content. According to Sanovich's qualitative analysis on Russian Twitter, "among accounts with more than ten tweets in our dataset, around 45 percent are bots."[112]

The researchers recorded a sharp spike in bot activity during controversial moments such as the Crimea annexation.[113] Scholars refer to these as "third generation" controls of the internet in which a regime, rather than prohibiting access, "competes with potential threats through effective counterinformation campaigns that overwhelm, discredit or demoralize opponents."[114]

As Putin's grip over Russia tightened, these tactics have become further entrenched. A host of new internet regulations came into effect in late 2019 as part of Russia's new Sovereign Internet Law, which was geared towards expanding surveillance of domestic internet activity, increasing state control over digital infrastructure and increasing the state's ability to isolate the "Russian internet" from its counterpart in the free world.[115]

Meanwhile, Russia's use of digital misinformation has increased at home and abroad, leading to characterizations that Russia has "weaponized" the internet.[116] This weaponization is meant to "foment confusion, chaos and distrust", with the overarching goal to "divide the target population", and thus prevent the kind of collective action observed in late 2011.

The Russian Invasion of Ukraine

In February 2022, Russia invaded neighboring Ukraine. The rational for the war was morally and intellectually bankrupt. The military campaign has lasted over a year now, with no end in sight. Ill-prepared and ill-equipped Russian soldiers have suffered demoralizing defeats and, at times, significant casualties. It is a situation in which, conceivably, some Russians are displeased. Yet major protests have not emerged, online or offline.

The Putin regime further tightened its control over the Russian internet at the war's onset. Within the opening days of the invasion, "Putin signed legislation criminalizing the deliberate dissemination of anything the government deemed to be false information about the war."[117] Shortly thereafter, Facebook, Instagram and Twitter became inaccessible. More than 2,000 websites were blocked in the first six months of the conflict.[118]

What was left online was of dubious value. A BBC study used VPN technology to conduct searches on Yandex as if in Russia. The top results for "Bucha", the Ukrainian town where Russian troops massacred hundreds of civilians, were anonymous blogs that claimed the murders were staged. A search of "Lyman", a town where mass graves had been discovered, returned pro-Kremlin results "blaming the deaths on Ukrainian Nazis."[119]

These developments have led some analysts to posit that Russia is attempting to follow the Chinese firewall model and create a "Russian internet that can be disconnected from the rest of the world."[120] However, others find that Russia may be far from achieving this lofty goal. VPN technology remains popular in Russia, with downloads surging since the outbreak of war.[121] Twitter, *The New York Times*, *The Washington Post* and other outlets have also taken steps to make their content available in Russia, in Russian, in ways that circumvent the block.[122]

To date, digital tools have not sparked tangible collective action in Russia. That could change as the war's cost in blood and treasure continues to rise. In the meantime, digital tools *have* been used to create networks and share information from the frontlines with family members and friends back home. This information would be otherwise unavailable. As *The New York Times* reported in fall 2022, the Ukrainian government has intercepted and eavesdropped on thousands of private cellphone calls and text messages sent back to Russia from Ukrainian battlefields. These messages in no uncertain terms convey a level of carnage, chaos and futility that Russian national media outlets studiously ignore,[123] and they could prove to be the kinds of daily interactions that ultimately lead to the emergence of digital tools as a solution to the collective-action dilemma.

5. Logging Off

Five Observations

So, has the internet made it easier or harder for authoritarian regimes to maintain their grip on power? The three cases considered in this paper elucidate the complicated relationship between digital tools and the rise of collective action in authoritarian countries. Any attempt to draw a definitive conclusion would soon be rendered foolhardy. How many forecasters expected the internet to spark widespread public protests in Cuba on June 11, 2021? After that day, when thousands of young Cubans took to the street across the country, how many forecasters would have expected there to be no similar moment of collective action since? Just as the internet's impact on democracies is rapidly evolving, so too is the impact on non-democracies. Nevertheless, this section considers the existing scholarship, and lessons from the three case studies, to offer five closing observations.

1. Digital Tools Can Spark Collective Action in Authoritarian Conditions

This paper reviewed the impact of digital technology in three highly repressive contexts. In all three, at one point or another, digital tools sparked moments of collective action against a regime. While this small sample size precludes any robust conclusion, the cases offer compelling evidence that, where digital connections are available, a repressed society will use them to create networks and bonds that are difficult to forge in the physical world. Digital tools can interrupt authoritarian control of access to information, and the internet can act as an arena for public networking and dialogue—a public square, so to speak—where such activities are repressed. Specific causal mechanisms include the reduced cost of information sharing, as well as the rapid and viral nature of digital connections.

2. Connection Can be A Critical Precursor to Collective Action

In all three case studies, we observe the importance of an incubation period for a trigger. In other words, the use of digital tools matures over time. Netizens are, perhaps at first, simply happy to be online—to connect with family, to tag friends on social media and keep tabs on romantic interests. But this apparently innocent networking creates a digital civil society that can subsequently be activated. In the interim, repressed citizens create networks and establish a better understanding of their compatriots' experience with a regime. As Liu argues, these mundane interactions "set the scene for the moment of confrontation". At this moment, the latent power of billions of connected people living under repressive regimes exists worldwide.

3. Collective Action Does Not Ensure Regime Transition or Liberalization

There is no doubt about digital tools' capacity to generate acute periods of collective action. Yet few cases of digitally inspired uprisings have led to regime change, and many have, in fact, resulted in rollbacks of liberalization. Common threads of digital collective action are its spontaneity and frequent lack of leadership, whether human or organizational. Rather, individuals respond to social media triggers and cues. This is not necessarily a bad thing. In highly authoritarian settings, such spontaneous moments can be the first acts of mass public protest observed in decades. However, when the moment lacks clarity of initiative and leadership, it may be easier to suppress, and more likely to dissipate. In this sense, moments of unorganized, digitally inspired collective action may not be as threatening to the state, which can use it to allow protesters to vent without accomplishing much else. At the same time, a regime gains an opportunity to identify those willing to take to the street. In China, the state was able to rapidly quell the A4 protests and to subsequently prosecute participants. Moreover, authoritarian regimes have developed strategies to blunt the impact of digital access. These strategies have become more effective over time, with regimes transitioning from defensive tools (filtering and blocking) to offensive ones (such as surveillance and manipulation). Even when a movement is successful in toppling a regime, as was the case in Egypt, its disorganized nature can lead to a power vacuum that can be filled with an equally bad or even worse government.

4. Controlling the Internet Requires Awesome Domestic Power

China stands out as particularly effective in blunting collective action spurred by the internet. The country's capacity to finance a long-term, massive surveillance campaign facilitates the ability to implement it. Chinese

netizens' use of Chinese platforms, which are subject to Chinese censorship, also aids this. In contrast, during the Arab Spring, MENA regimes proved unable to fully censor Facebook, Twitter, YouTube, WhatsApp and other Western platforms in great demand during the protests. Other authoritarian regimes' plans for neutering the internet's impact, such as the Kremlin's strategy to create Russian alternatives to globally dominant sites, have sought to copy the control that China exercises. But that country's approach is difficult to replicate, and few others will prove able to do it.

5. Expectations of State Capacity Influence Risk-Taking

Internet laws and regulations on their own are not clear deterrents for contentious, online political action. In fact, users worldwide have executed strategies to defeat censorship. These range from word play, humor and puns, to more tech-savvy options such as VPNs. Users are more influenced by a regime's perceived capacity to execute those laws and, if they are applied, the potential punishment. All three case summaries reveal the importance of self-censorship. The extent to which it exists is influenced by regime capacity, or perceived capacity, and the expectation of regime response. In cases such as Syria and Russia, whose regimes have demonstrated a willingness to brutalize their citizens, the risk of action remains high, even if both states lack China's capacity to pursue protesters.

These observations, taken together, suggest that digital tools are likely to force authoritarian regimes to reveal the extent to which they will go to maintain power. In countries where enough people have consistent access to the internet, digital tools are likely to engender acute moments of collective action. These moments will likely be spontaneous and may lack a clear leader or objective. They are, therefore, unlikely to achieve desired results quickly. Challenged regimes, however, will be forced to react. Those willing to double down on repression and violence have already established successful survival strategies.

There is no guarantee that digital technology will ultimately prove vital for populations to overcome authoritarian governance. The first quarter of the 21st century indicates that technology's liberation potential is not as clear-cut or immediate as initially hypothesized.

Endnotes

1. For example, see Janna Anderson and Lee Rainie, "Concerns about democracy in the digital age", Pew Research Center, February 21, 2020. https://www.pewresearch.org/internet/2020/02/21/concerns-about-democracy-in-the-digital-age/
2. Jonathan Haidt, "Yes, Social Media Really is Undermining Democracy", *The Atlantic*, July 28, 2022. https://www.theatlantic.com/ideas/archive/2022/07/social-media-harm-facebook-meta-response/670975/
3. Richard Wike, Laura Silver, Janell Fetterolf, Christine Huang, Sarah Austin, Laura Clancy and Sneha Gubbala, "Social Media Seen as Mostly Good for Democracy Across Many Nations, But U.S. is a Major Outlier", Pew Research Center, December 6, 2022. https://www.pewresearch.org/global/2022/12/06/social-media-seen-as-mostly-good-for-democracy-across-many-nations-but-u-s-is-a-major-outlier/
4. Economist Intelligence Unit, "Democracy Index 2022: Frontline democracy and the battle for Ukraine", Economist Intelligence Unit, 2023.
5. Christian Christensen, "Discourses of Technology and Liberation: State Aid to Net Activists in an Era of 'Twitter Revolutions'", *The Communication Review*, Vol. 14, Issue 3, 2011. https://www.tandfonline.com/doi/abs/10.1080/10714421.2011.597263
6. Espen Geelmuyden Rød and Nils Weidnmann, "Empowering activists or autocrats? The Internet in authoritarian regimes", *Journal of Peace Research*, Vol 52, No 3. https://www-jstor.org.proxy1.library.jhu.edu/stable/pdf/24557404.pdf
7. Susan Khazaeli and Daniel Stockemer, "The Internet: A New route to good governance.," *International Political Science Review*, Vol 34, No 5, 2013. https://www-jstor org.proxy1.library.jhu.edu/stable/i24573385
8. Dana Moss, "The ties that bind: Internet communication technologies, networked authoritarianism, and 'voice' in the Syrian diaspora", *Globalization*, Vol. 15, Issue 2, 2018. https://www.tandfonline.com/doi/full/10.1080/14747731.2016.1263079
9. Diamond defines "liberation technology" as "any form of information and communication technology that can expand political, social and economic freedoms". See Larry Diamond, "Liberation Technology", *Journal of Democracy*, Vol. 21, No. 3, July 2010.
10. Diamond, 2010.
11. Nivien Saleh "Egypt's digital activism and the Dictator's Dilemma: An evaluation", *Telecommunications Policy*, Vol 36, 2012.
12. Sean Aday, Henry Farrell, Marc Lynch, John Sides, Deen Freelon, John Kelly and Ethan Zuckerman, "Blogs and Bullets: New Media in Contentious Politics", United States Institute of Peace, 2010.
13. Ibid.
14. For example, see Diani, Mario, *Green Networks*, Edinburgh University Press, 1995).
15. Henry Jenkins, *Confronting the Challenges of Participatory Culture*, The MacArthur Foundation, 2009.
16. Ethan Zuckerman, "Cute Cats to the Rescue? Participatory Media and Political Expression", Massachusetts Institute of Technology, 2013.
17. Kris Ruijgrok, "From the web to the streets: internet and protests under authoritarian regimes", *Democratization*, Vol. 24, No. 3, 2017. https://www.tandfonline.com/doi/full/10.1080/13510347.2016.1223630
18. Ibid.
19. Hedy Greijdanus, Carlos Ade Matos Fernandes, Felicity Turner-Zwinkels, Ali Honari, Carla Roos, Hannes Rosenbusch and Tom Postmes, "The Psychology of Online Activism and Social Movements: Relations between Online and Offline Collective Action", *Current Opinion in Psychology*, 2020. https://www.sciencedirect.com/science/article/pii/S2352250X20300324
20. Ibid.
21. Henry Jenkins. *Convergence Culture*, New York University Press, 2006.
22. Arkady Ostrovsky, *The Invention of Russia: The Rise of Putin and the Age of Fake News*, Penguin Books, 2017.
23. Rød and Weidmann.
24. Ronald Deibert. "Cyberspace Under Siege: Authoritarianism Goes Global", *Journal of Democracy*, Vol. 26, No. 3, 2015. https://muse.jhu.edu/article/586479/pdf
25. Ibid.
26. Jay Rosen, "The People Formerly Known as the Audience", PressThink, December 2, 2006.
27. Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom*, Penguin Press, 2011.
28. Athina Karatzogianni, Galina Miazhevich and Denisova Anastasia, "A comparative Cyberconflict Analysis of Digital Activism Across Post-Soviet Countries", *Comparative Sociology* #16, 2007.
29. Simin Kargar, from written notes gives on a draft of this paper.
30. Robby Soave. "Don't Blame Elon Musk for Turkey's Authoritarian Twitter Censorship." *Reason*, May 17, 2023. Available online at https://reason.com/2023/05/17/elon-musk-turkey-twitter-censorship-free-speech/
31. Nitish Pahwa. "Elon Musk Didn't Just Do Turkey's Bidding. Censoring for Strongmen Is Now a Pattern." *Slate*, May 15, 2023. Available online at https://slate.com/technology/2023/05/elon-musk-turkey-twitter-erdogan-india-modi-free-speech.html
32. For further reading on this topic, see Pinky Mehta. "Sanctioning Freedoms: U.S. Sanctions Against Iran Affecting Information and Communications Technology Companies." *University of Pennsylvania Journal of International Law*, Vol. 37:2, 2015. Available online at https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1915&context=jil
33. See Maeve Shearlaw, "Egypt five years on: was it ever a 'social media revolution'?", *The Guardian*, January 25, 2016. https://www.theguardian.com/world/2016/jan/25/egypt-5-years-on-was-it-ever-a-social-media-revolution
34. Carty, 2014.
35. Christie Chonghyun Byun and Ethan Hollander, "Explaining the Intensity of the Arab Spring", *Digest of Middle East Studies*, Vol. 24, No, 1, 2015.
36. Simon Cottle. "Media and the Arab uprisings of 2011: Research notes", *Journalism*, Vol 12, No 5, 2011. https://journals-sagepub com.proxy1.library.jhu.edu/doi/pdf/10.1177/1464884911410017
37. Andrea Kavanaugh, Steven Sheetz, and Hamida Skandrani, John Tedesco, Yue Sun, Yue and Edward Fox, "The Use and Impact of Social Media during the 2011 Tunisian Revolution", Proceedings of the 17th International Digital Government Research Conference on Digital Government Research, June 2016. https://dl.acm.org/doi/10.1145/2912160.2912175

38. Jun Liu. "From 'moments of madness' to 'the politics of mundanity' - researching digital media and contentious collective actions in China", *Journal of Social, Cultural and Political Protest*, 2016. http://dx.doi.org/10.1080/14742837.2016.1192027
39. Philip Howard, Aiden Duffy, Deen Freelon, Muzammil Hussain, Will Mari, and Marwa Mazaid, "Opening Closed Regimes: What was the Role of Social Media During the Arab Spring", *Project on Information Technology & Political Islam*, 2011.
40. Zeynep Tufeksci and Christopher Wilson, "Social media and the decision to participate in political protest: Observations from Tahrir Square", *Journal of Communication*, Vol. 62, Issue 2, 2012.
41. Sahar Khamis and Katherine Vaughn, "Cyberactivism in the Egyptian Revolution: How Civic Engagement and Citizen Journalism Tilted the Balance", *Arab Media & Society*, 2011. https://www.arabmediasociety.com/cyberactivism-in-the-egyptian-revolution-how-civic-engagement-and-citizen-journalism-tilted-the-balance/
42. Howard *et al*, 2011.
43. Wang, Y. and Mark, G. "Trust in online news: Comparing social media and official media use by Chinese citizens." *Proceedings of the 2013 Conference on Computer Supported Cooperative Work*, 2013.
44. Carol Huang, "Facebook and Twitter key to Arab Spring uprisings: report", *The National*, June 6, 2011. https://www.thenational.ae/uae/facebook-and-twitter-key-to-arab-spring-uprisings-report-1.428773
45. Howard, *et al*., 2011.
46. Ben Wagner, "Push-button-autocracy in Tunisia: Analyzing the role of Internet infrastructure, institutions and international markets in creating a Tunisian censorship regime", *Telecommunication Policy*, Vol. 36, 2012.
47. Victoria Carty, "Arab Spring in Tunisia and Egypt: The Impact of New Media on Contemporary Social Movements and Challenges for Social Movement Theory", *International Journal of Contemporary Sociology* 51(1), 2014. https://digitalcommons.chapman.edu/cgi/viewcontent.cgi?article=1011&context=sociology_articls
48. Howard *et al*., 2011.
49. Ibid.
50. Wagner, 2012.
51. See Chuchu Zhang and Yahia Zoubir. "Tunisia: A Failed Democratic Experiment?" *Georgeotwn Journal of Internatioanl Affairs*. November 12, 2021. Available online at https://gjia.georgetown.edu/2021/11/12/tunisia-a-failed-democratic-experiment/
52. OECD, 2016.
53. See Rebecca Chao, "The People's 'Marsad' for the Tunisian Parliament", *Personal Democracy Media,* April 18, 2014. http://techpresident.com/news/wegov/24936/people%27s-marsad-tunisian-parliament. Marsad also compiled photos and biographies of elected officials, as well as their voting records and political tendencies. The site publicized attendance information, raising awareness of absent deputies and promoting accountability. It also provided a portal for citizens to submit questions to officials and published the responses (Chao, 2014).
54. Meera Selva, "Reaching for the off switch: Internet shutdowns are growing as nations seek to control public access to information", *Index on Censorship*, Vol. 48, Issue 3, September 2019. https://journals-sagepub-com.proxy1.library.jhu.edu/toc/ioca/48/3
55. Justin Clark, Robert Faris, Ryan Morrison-Westphal, Helmi Noman, Casey Tilton and Jonathan Zittrain, "The Shifting Landscape of Global Internet Censorship", Berkman Klein Center for Internet & Society Research Publication, Harvard University, 2017. https://dash.harvard.edu/bitstream/handle/1/33084425/Internet_Monitor_2017_Filtering_Report_draft_for_SSRN_and_DASH_process.pdf?sequence=2 Specifically, the investigation found that "starting in late 2015, Egypt has selectively blocked political websites that contain content critical of the government. In May 2017, the Egyptian authorities began to substantially filter political content, and as of June 2017, the lists of blocked URLs had grown to more than 60 and continues to grow.
56. Limor Lavie, "Consensus vs. dissensus over the 'civil state' model: a key to understanding the diverse outcomes of the Arab Spring in Egypt and Tunisia", *British Journal of Middle Eastern Studies*, 2019.
57. Steven Heydemann and Reinoud Leenders, "Authoritarian Learning and Counterrevolution", in Marc Lunch, ed., *The Arab Uprisings Explained: New Contentious Politics in the Middle East*, Columbia University Press, 2014.
58. Ibid.
59. Al-Saqaf, Walid. "Internet Cencroship Circumvention Tools: Escaping the Control of the Syrian Regime." *Media and Communications*, Vol 4, Iss. 1, 2016.
60. Ibid.
61. Jennifer Pan, "How Market Dynamics of Domestic and Foreign Social Media Firms Shape Strategies of Internet Censorship", *Problems of Post Communism*, Vol. 64, Nos. 3-4, 2017.
62. Jun Liu, "From 'moments of madness' to 'the politics of mundanity' - researching digital media and contentious collective actions in China", *Journal of Social, Cultural and Political Protest*, 2016. http://dx.doi.org/10.1080/14742837.2016.1192027
63. China Internet Network Information Center and Internet World Stats.
64. China Internet Network Information Center, "The 35th statistics report on internet development in China", 2015. https://www.cnnic.cn/hlwfzyj/hlwxzbg/201502/P020150203551802054676.pdf
65. Statista
66. David Kurt Herold, "Noise, spectacle, politics: carnival in Chinese Cyberspace", in Kurt Herold and Peter Marolt, eds., *Online Society in China: Creating, Celebrating and Internalizing the Online Carnival,* Routledge, 2011.
67. Peter Marolt, "Grassroots agency in a civil sphere: Rethinking Internet control in China", in Kurt Herold and Peter Marolt, eds., *Online Society in China: Creating, Celebrating and Internalizing the Online Carnival,* Routledge, 2011.
68. Haifeng Huang, Serra Boranbayakan and Ling Huang, "Media, protest diffusion, and authoritarian resilience", *Political Science Research and Methods,* Vol. 7, No. 1, 2019.
69. Ibid.
70. Ibid.
71. Ibid.
72. Liu, 2016.
73. Huang, et al., 2019.
74. Liu, 2016.
75. Gary King, Jennifer Pan and Margaret Roberts, "How Censorship in China Allows Government Criticism but Silences Collective Expression", *American Political Science Review*, Vol. 107. No. 2, May 2013.
76. Ibid.

77. For examples, see Maria Repnikova, "Media openings and political transitions: Glasnost versus Yulun Jiandu", *Problems of Post-Communism*, Vol. 64, No. 3-4, 2017. https://www.tandfonline.com/doi/abs/10.1080/10758216.2017.1307118; see King et al., 2013, and S. Y. Lee, "Surviving online censorship in China: Three satirical tactics and their impact", *China Quarterly*, Vol. 228, 2016.
78. Jiayin Lu and Yupei Zhao, "Implicit and Explicit Control: Modeling the Effect of Internet Censorship on Political Protest in China", *International Journal of Communication,* Vol. 12, 2018.
79. Ibid.
80. Herold, 2011.
81. Pan, 2017.
82. Ibid. According to Pan, "overall, from 2012 to 2014, Twitter complied with 10 percent of removal requests, taking actions that include removal as well as withholding content form specific countries." (Pan, 2017)
83. Herold, 2011.
84. Robin Barnwell. *China Undercover* (documentary film), "Frontline", April 2020.
85. Kian Vesteinsson and Angeli Datt, "Chinese Protestors and the Global Internet Need One Another", *The Diplomat*, January 13, 2023. https://thediplomat.com/2023/01/chinese-protesters-and-the-global-internet-need-one-another/
86. Emily Feng, "China's authorities are quietly rounding up people who protested against COVID rules", National Public Radio, January 11, 2023. https://www.npr.org/2023/01/11/1148251868/china-covid-lockdown-protests-arrests
87. Jennifer Conrad, "How Chinese Netizens Swamped China's Internet Controls", *Wired*, December 2, 2022. https://www.wired.com/story/how-chinese-protests-netizens-swamped-chinas-internet-controls/
88. Ibid.
89. Liza Lin, "China Clamps Down on Internet as It Seeks to Stamp Out Covid Protests", *The Wall Street Journal*, December 1, 2022. https://www.wsj.com/articles/china-clamps-down-on-internet-as-it-seeks-to-stamp-out-covid-protests-11669905228
90. Rob Marvin, "Breaking Down VPN Usage Around the World", *PC Magazine*, September 21, 2018.
91. https://www.pcmag.com/news/breaking-down-vpn-usage-around-the-world
92. Lin, 2022.
93. Lin, 2022.
94. Conrad, 2022.
95. Tessa Wong and Grace Tsoi, "The protesters who've gone missing as China deepens crackdown.", BBC, February 18, 2023. https://www.bbc.com/news/world-asia-china-64592333Feng, 2023.
96. Laura He, "China to punish internet users for 'liking' posts in crackdown after zero-Covid protests", CNN, November 30, 2022. https://www.cnn.com/2022/11/30/media/china-new-internet-rule-punish-liking-posts-intl-hnk/index.html
97. Sergey Sanovich, "Computational Propaganda in Russia: The Origins of Digital Misinformation", New York University, Working Paper No. 2017.3.
98. GfK, Проникновение Интернета в России: итоги, 2018. https://www.gfk.com/fileadmin/user_upload/dyna_content/RU/Documents/Press_Releases/2019/GfK_Rus_Internet_Audience_in_Russia_2018.pdf
99. Fossato, et al., 2009.
100. Oates, 2015.
101. Ibid.
102. Ibid.
103. Maria Lipman, "How Putin Silences Dissent: Inside the Kremlin's Crackdown", *Foreign Affairs*, Vol. 95, No. 3, 2016.
104. Ibid.
105. Sergey Sanovich, Denis Stukal and Joshua Tucker, "Turning the Virtual Tables: Government Strategies for Addressing Online Opposition with an Application to Russia", *Comparative Politics,* Vol. 50, No. 3, 2018.
106. Sanovich, 2017.
107. Anastasia Denisova, "Democracy, protest and public sphere in Russia after the 2011–2012 anti-
108. government protests: digital media at stake", *Media, Culture & Society*, Vol. 39, No 7, 2016.
109. A Smirnova, "Yandex Blogs to partially shut down", Look at Me, 2014. www.lookatme.ru/mag/live/experience-news/203183-rip-yandex-blogs
110. Sanovich, 2017?
111. Ibid.
112. Sanovich, 2017?
113. Ibid.
114. Denis Stukal, Segey Sanovich, Ricahrd Bonneau and Joshua Tucker, "Detecting Bots on Russian Political Twitter", *Big Data*, Vol. 5, No. 4, 2017. https://www-liebertpubcom.proxy1.library.jhu.edu/doi/pdf/10.1089/big.2017.0038.114 Ronald Deibert, John G. Palfrey, Rafal Rohozinski and Jonathan Zittrain, *Access Denied: The Practice and Policy of Global Internet Filtering*, The MIT Press, 2009.
115. Alena Epifanova, "'Deciphering Russia's "Sovereign Internet Law': Tightening Control and Accelerating the Splinternet", German Council on Foreign Relations Analysis, 2020. https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law
116. Sherri Gordon, *Weaponized Social Media,* Enslow Publishing, LLC, 2018. https://ebookcentral.proquest.com/lib/jhu/detail.action?docID=5851598
117. Daniil Belovodyev and Bayev Anton, "Inside The Obscure Russian Agency That Censors The Internet: An RFE/RL Investigation", Radio Free Europe, February 9, 2023. https://www.rferl.org/a/russia-agency-internet-censorship/32262102.html
118. Matt Burgess, "Russia is Quietly Ramping Up Its Internet Censorship Machine", *Wired*, July, 25, 2022. https://www.wired.com/story/russia-internet-censorship-splinternet/
119. Adam Robinson, Olga Robinson and Kayleen Devlin, "Ukraine war: Russians kept in the dark by internet search", BBC, November 11, 2022. https://www.bbc.com/news/world-europe-63246153
120. Burgess, 2022.
121. Arjun Kharpal,"Russia may aspire to a China-style internet, but it's a long way off", CNBC, March 16, 2022. https://www.cnbc.com/2022/03/17/russia-ukraine-war-internet-censorship-china-great-firewall.html
122. Robert McMahon, "Russia is Censoring News on the War in Ukraine. Foreign Media Are Trying to Get Around That", Council on Foreign Relations, March 18, 2022. https://www.cfr.org/in-brief/russia-censoring-news-war-ukraine-foreign-media-are-trying-get-around
123. Yousur Al-Hlou, Masha Froliak and Evan Hill, "Putin Is a Fool': Intercepted Calls Reveal Russian Army in Disarray", *The New York Times*, September 28, 2022. https://www.nytimes.com/interactive/2022/09/28/world/europe/russian-soldiers-phone-calls-ukraine.html

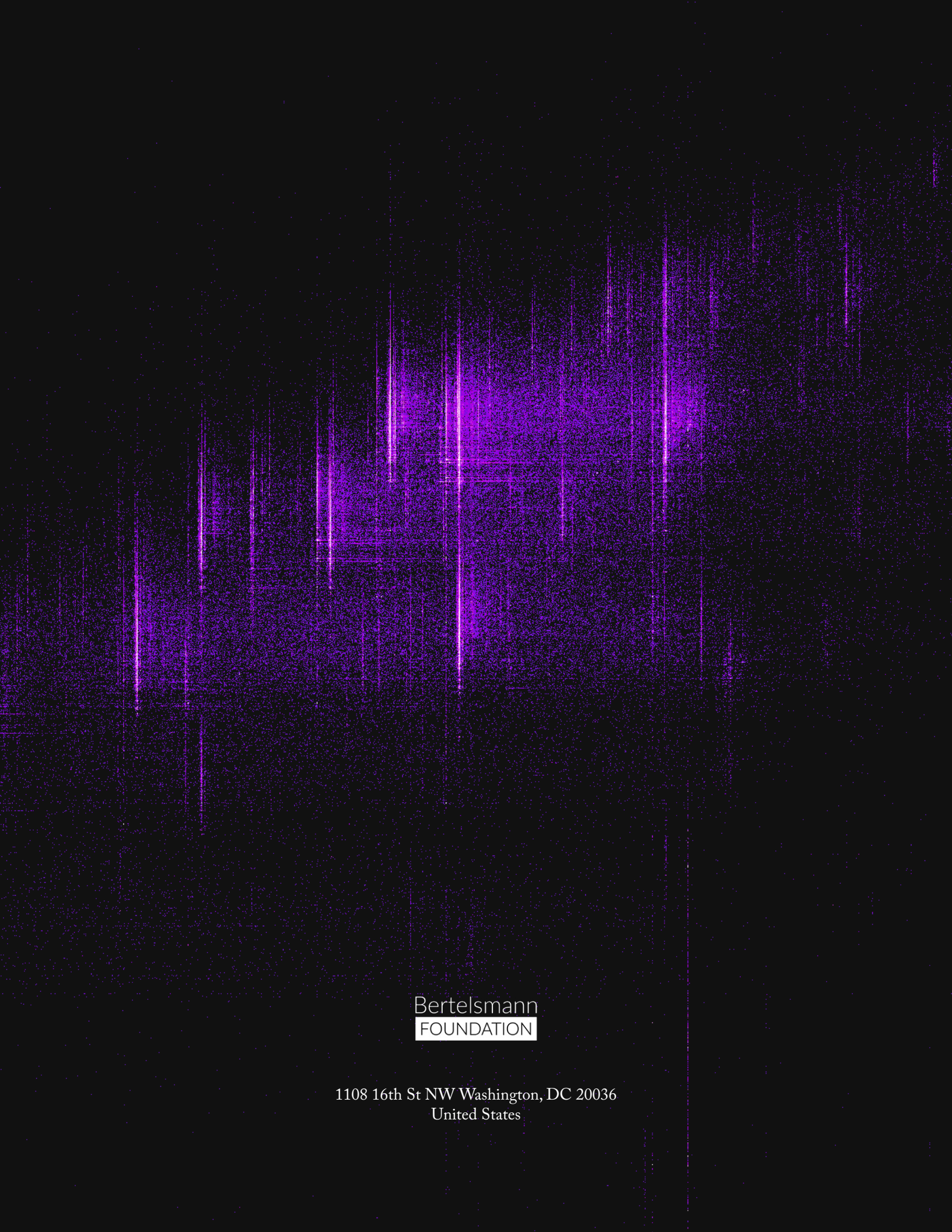
Acknowledgments

The Bertelsmann Foundation wishes to acknowledge the contributions of those who helped make this publication possible.

We would like to thank graphic designer Mateo Zúñiga, editor Andrew Cohen, and peer review expert, Simin Kargar.

A special thank you to the author of the publication, Samuel George, and the Bertelsmann Foundation staff.

Irene Braam
Executive Director
Bertelsmann Foundation



Bertelsmann
FOUNDATION

1108 16th St NW Washington, DC 20036
United States