1

Introduction

Scott J. Shackelford, Frédérick Douzet, and Christopher Ankersen

Rising to speak in the House of Commons in November 1947, Winston Churchill – by then no longer prime minister but still member of parliament, his party having been defeated in the general election of May 1945 – remarked that "No one pretends that democracy is perfect … Indeed, it has been said that democracy is the worst form of Government except for all those other forms that have been tried." Churchill felt especially convinced that it was superior to those varieties of governance that relied upon "a group of super men and super-planners … 'playing angel' … and making the masses of the people do what they think is good for them, without any check or correction."[1] The following year, the Universal Declaration of Human Rights was signed. While the term democracy is not mentioned, its essence is enshrined in the document, signed by democracies and autocracies alike: "The will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures."[2]

Despite its fundamental recognition, democracy has never been guaranteed. Benjamin Franklin once famously quipped after being asked what sort of government the Founders had gifted the new nation of the United States of America: "a republic, if you can keep it" (Beeman, n.d.). Since that time, many threats to democracies have emerged, stemming from internal divisions fed by inequality, injustice, and racism and from foreign nations wishing to distract and destabilize democratic governments, most recently through cyber-enabled means (Zeitz, 2016).

Portions of this chapter have been previously published under Scott J. Shackelford, Angie Raymond, Abbey Stemler, & Cyanne Loyle, Defending democracy: Taking stock of the global fight against digital repression, disinformation, and election insecurity, *Washington and Lee Law Review*, 77, 1747 (2021).

[1] Winston Churchill, HC Deb, 11 November 1947, vol. 444 cc203–321, https://api.parliament.uk/historic-hansard/commons/1947/nov/11/parliament-bill.

[2] Universal Declaration of Human Rights (1948) Article 21, para. 3.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 09:21:22, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.001

Recently, Russia has been particularly active, by one estimate interfering in twenty-seven elections since 1991, beginning with the nations of Eastern Europe that had been former members of the Cold War-era Warsaw Pact (Way & Casey, 2018). Such efforts have been extended since 2014 to Western Europe and the United States, reaching a culmination in their interference with the 2016 Brexit vote and US presidential election, made easier by the rise of internet platforms generally and social networking in particular (Way & Casey, 2018). Such efforts continued into the 2018 US midterm elections, when U.S. Cyber Command shut down a Russian troll farm on Election Day (Thomsen, 2019), and have expanded to target elections across Africa and Asia (Alba & Frenkel, 2019; Tennis, 2020), as other nations have similarly both followed and improved upon Russia's playbook.

Furthermore, today's threats to democratic institutions are both acute and expansive, extending from the protection of voting machines and media sites to related issues of critical infrastructure, 5G, and even Internet of Things (IoT) vulnerabilities (Shackelford et al., 2017). The weaponization of artificial intelligence (AI) and spread of immersive environments such as the Metaverse that make targets more receptive to emotional manipulation are reinforcing these threats (Rosenberg, 2022). Defending democracy for the next century, then, requires a range of policy responses from reigning in the rampant spread of disinformation on leading internet platforms to securing the voting process itself. Luckily, there are a number of success stories from around the world that policymakers can and should learn from what has worked elsewhere in our common quest to make democracy "harder to hack" (Shackelford et al., 2017). Consider Australia, which has long been grappling with repeated Chinese attempts to interfere with its political systems through cyber-enabled means including disinformation (Borys, 2018). Yet Australia has taken a distinct approach in how it has sought to protect its democratic institutions, including reclassifying its political parties as "critical infrastructure," a step that the US government has yet to take despite repeated breaches at both the Democratic and Republican National Committees (CNN Editorial Research, 2023).

In this edited volume, we have – for the first time – assembled a diverse cadre of scholars and practitioners to address both vulnerabilities in election infrastructure as well as the overriding problem of managing disinformation. A common thread throughout this edited volume is that democracies can and should work closely together to share both cyber threat information and best practices to build democratic resilience the world over, and that a multifaceted approach is needed that combines both targeted reforms to secure election infrastructure – such as requiring paper ballots and risk-limiting audits – with deeper structural interventions to limit the spread and impacts of disinformation that are being made that much more challenging by the rapid evolution of cyberattacks and AI technologies. We assert that it is vital to take this wider view of defending democracy against foreign nation-state-sponsored cyber-enabled threats that includes not only a focus on protecting election infrastructure but also digital repression – both are means to an end, that is,

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 09:21:22, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.001

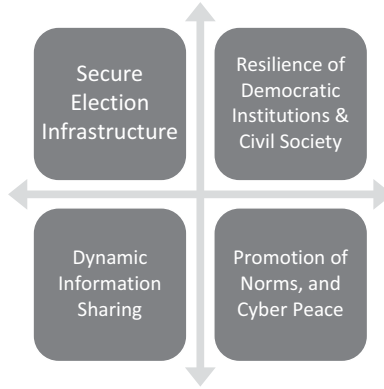


FIGURE 1.1 Defending democracy matrix.

undermining trust, and confidence, in democratic institutions. As such, defending democracy requires implementing multilevel policy responses that tackle this full range of cyber-enabled threats, which include such pressing issues as insecure voting machines and processes but also relate to the promotion and operationalization of cyber norms. This may be envisioned as the matrix illustrated in Figure 1.1.

This edited volume investigates attacks on both voting processes and on the broader informational environment within which voting takes place around the world. It highlights interconnections among such attacks across sectors and countries and identifies ways of preventing, defending against, and mitigating the effects of such attacks on both the technical and informational aspects of cybersecurity. As a case in point, the 2020 US election was among the "most secure in American history" according to the U.S. Department of Homeland Security (CISA, 2020), and yet also, in many ways, it was among the most divisive, leading to record levels of distrust that fueled the toxic political environment leading to the insurrection on the U.S. Capitol on January 6, 2021 (Pew Research Center, 2022). As such, this edited volume is both a call to action and the first draft of a game plan to operationalize needed next steps. Democracy's enemies are determined and innovative; its defenders must be likewise.

WHAT ARE DEMOCRACIES?

The word "democracy" is derived from the Greek words "demos," (people), and "kratos" (power) (Annan, n.d.). Although the ancient Greeks are often credited with establishing the first nascent democracy in the fifth century BC, earlier examples abounded; the Athenian model is noteworthy for the facts that it was direct (i.e., not representative), and who counted as the "people" was much more narrow than today given that it excluded women, along with immigrants and slaves (Annan, n.d.). The franchise has expanded throughout much of the Western world since the era of self-determination following World War II and accelerating after the end of the Cold

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 09:21:22, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.001

War. However, it is the case that still in 2023, the Economist Intelligence Unit reported that less than 8 percent of the world's population reside in a liberal democracy, whereas "nearly 40% live under authoritarian rule – a share that has been creeping up in recent years" (European Intelligence Unit, 2023). The trend toward global democratic backsliding has been noted by Freedom House, which has tracked aggregate declines every year since 2006, though 2022 did mark a dramatic improvement from previous years (Freedom House, 2023). This global retreat from democratic rule then predates the rise of social media-fueled disinformation and polarization, though these phenomena hold the promise of exacerbating the trend if left unchecked as is explored throughout the volume. Still, definitions abound, though for purposes of this work we will rely on Philippe Schmitter and Terry Karl's definition, that is: "a system of governance in which rulers are held accountable for their actions in the public realm by citizens acting indirectly through the competition and cooperation of their elected representatives" (Lynn-Jones, 1998).

WHY ARE DEMOCRACIES WORTH DEFENDING?

The year 2024 is "a remarkable milestone in human history." From Bangladesh to Venezuela, "over four billion people – more than half of the world's population across more than 40 countries" are eligible to vote (Reece, 2024). Included in this group are new, emerging, and established democracies. Where once the latter category may have appeared immune from election anxiety, this is no longer the case. US President Joe Biden has said, "Make no mistake: Democracy is on the ballot" (Milligan, 2022). Such sentiments paint a stark contrast to the remarks of former President Donald Trump, who as of this writing is facing dozens of criminal counts, including for his role in inciting the January 6 insurrection at the U.S. Capitol. Even more worryingly, Trump has claimed that if elected, he will act as a dictator on day one of his new term in office (Colvin & Barrow, 2023). Yet what can get lost in the partisan noise is the big picture of *why* democracy is so important, and worth the cost of defending both at home and abroad. The reasons are manifold, many of which are beyond the scope of this edited volume but include democratic peace theory (the notion that democracies do not attack one another), prosperity, empowerment of civil society, promotion of international peace and security, and less corruption than autocracies (Lynn-Jones, 1998). That is not to say that democracy in and of itself is a panacea for all the ills of humanity – what is after all – but it is a proven system that allows people to "choose how to live together, realizing our freedom in rational and consensual constraint . . . without being ruled" (Salter, 2022). We believe that is worth defending.

THEMES

This edited volume is not designed to diagnose and offer treatments for all the myriad ails afflicting democracies around the world, from disenfranchisement and

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 09:21:22, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.001

gerrymandering to the impacts of structural racism and socioeconomic divides in the electorate. Rather, it is focused on exploring how cyber-enabled themes are making these problems that much tougher to solve, particularly efforts to interfere with voting itself by targeting election infrastructure or by shaping opinions through disinformation and foreign influence operations.

Foreign electoral interference is nothing new. One study found that from 1945 to 2000, the United States and Russia combined tried to influence foreign elections 117 times, using both overt and covert methods (Levin, 2016). It is not even a novelty to use cyberattacks to influence the outcome of an election. As far back as 1994, Nelson Mandela's presidential victory in South Africa was initially diluted due to an illicit computer program.[3] Russia, in particular, has been developing its disinformation capabilities for decades, long before the first packet of information was sent on a fiber-optic cable. Pre-Soviet Union, the Tsarist secret police (the Komitet Gosudarstvennoy Bezopasnosti [KGB], now Federalnaya Sluzhba Bezopasnosti [FSB], which is the predecessor of the Federal Security Service) used disinformation (Popken, 2018). Joseph Stalin created an independent agency for *dezinformatsiya* designed to undermine political opponents and mislead Soviet citizens and foreigners alike as to the USSR's intentions (Popken, 2018). During the Cold War, for example, Russian agents helped plant "hundreds of bogus headlines around the world" such as the claim that the US government created the autoimmune disease AIDS, a false claim that was first mentioned in an Indian newspaper in the 1980s after being planted by a KGB agent (Popken, 2018). That story eventually circled the world, and was even mentioned by a famous American newsperson, Dan Rather, on the *CBS Evening News* in 1987 (Popken, 2018).

Effective foreign disinformation campaigns typically have three components: (1) a state-sponsored news outlet to originate the fabrication; (2) alternative media sources willing to spread it without adequately checking the underlying facts; and (3) witting or unwitting "agents of influence" (e.g., accomplices or unknowing agents) to advance the story in other outlets (Popken, 2018). Not all covert operations follow this formulation; many, for example, do not involve news outlets at all, and others may be better considered as exercises of public diplomacy using disinformation. But the advent of cyberspace has put the disinformation process into overdrive, both speeding the viral spread of stories across national boundaries and platforms with ease, using at times deceptive practices, and causing a proliferation in the types of traditional and social media willing to run with fake stories (Alba & Satariano, 2019). One tragic example is a false story about adopted children being butchered for their organs and sold to wealthy US citizens that first appeared in Honduras in 1986, which was quickly debunked with the official who was quoted denying the episode and issuing a correction, but that did not stop Soviet newspapers from spreading it

[3] Unfortunately, the hacker who installed this program was never identified (Laing, 2010). For more on this topic, see Shackelford et al. (2017, p. 629).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 09:21:22, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.001

around the world (Popken, 2018). But this is just one tool among many. Nations such as China and Russia also inundate internet discussion forums with so-called flooding attacks that enable distraction and disinformation. As Henry Farrell and Bruce Schneier write: "Libertarians often argue that the best antidote to bad speech is more speech. What Vladimir Putin discovered was that the best antidote to more speech was bad speech" (Schneier & Farrell, 2018).

Such actions are not confined to the physical or digital borders of illiberal regimes. Russia has been linked with "confidence attacks" aimed at destabilizing democracies (especially those in bordering countries, such as Ukraine) and undermining trust in elections (Schneier & Farrell, 2018), a practice that, as we have seen, dates back centuries but now makes use of modern technologies along with the implicit trust and openness in democratic societies. Russia, of course, is not alone in such efforts. As will be discussed further, China is increasingly emulating Russian disinformation efforts, particularly in Taiwan and Australia, as is Iran, North Korea, and an array of non-state actors including criminal organizations, terrorist groups, and hacktivists (Mak, 2018). These groups are employing a range of tactics to undermine trust in electoral processes ranging from directly or indirectly intimidating voters to compromising candidates by releasing damaging (and potentially fabricated) information (listing thirty-five ways in which the integrity of an election could be compromised by foreign actors; Janda, 2017). This points to the multifaceted phenomenon of disinformation, which needs to be thought of as a spectrum from licit to illicit actions, including more transparent and covert techniques using both true and false information and organic as well as fabricated virality. One way to analyze this nuance is in reference to the ABC Disinformation Framework offered by Camille François in which: "A is for Actors (manipulative Actors) who knowingly engage in online deception campaigns while obfuscating their identity and intentions; B is for Behaviour (deceptive Behaviour), encompassing a variety of techniques and vectors (platforms, websites, blogs) used to amplify the reach, virality and impact of the campaigns on line; C is for Content (harmful Content), the most subjective and complex criterion to define" (Francois, 2019). Understanding this continuum is key to managing these threats and then, in turn, gauging policy responses that avoid the pitfalls of potentially playing into manipulators' hands.

It is impossible to say with certainty what the long-term impacts have been of Russian, Chinese, and other state-sponsored efforts to undermine trust in democratic elections. John Sides, Michael Tesler, and Lynn Vavreck, for example, did not find a lasting measurable impact of Russia's efforts in the United States following the 2016 election (Sides, Tesler, & Vavreck, 2018, as cited in Francois, 2019), while Yochai Benker, Robert Farris, and Hal Roberts have argued "that Fox News was far more influential in the spread of false news stories than any Russian effort" (Benkler, Farris, & Roberts, 2018, as cited in Francois, 2019) Still, the fact that such efforts are spreading and that, to date, the efforts of the US government, allied nations, and internet platforms have proven insufficient to stem the flood raises questions about

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 09:21:22, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.001

how best to inoculate both advanced and emerging democracies against these threats, some of which stem from authoritarian regimes as is discussed throughout this volume. It should be noted, though, that domestic political actors and groups can also use the same tools to undermine democracies from within, sometimes acting in concert with external actors that may be manipulating the ideology of existing factions.

DIGITAL REPRESSION

As Farrell and Schneier have argued, "Cybersecurity today is not only about computer systems. It's also about the ways attackers can use computer systems to manipulate and undermine public expectations about democracy" (Schneier & Farrell, 2018). This process has only accelerated after the end of the Cold War, with the vast majority of nations enjoying some degree of internet access and more than thirty nations developing offensive cyberattack capabilities (Ranger, 2017; Schneier & Farrell, 2018). Rather than being the final nail in the coffin of authoritarianism, as was hoped by early cyber libertarians such as John Perry Barlow's maxim in his *Declaration of the Independence of Cyberspace*: "Governments of the Industrial World, you weary giants of flesh and steel … [,] [y]ou have no sovereignty where we gather" (Shea, 2006), illiberal regimes from Damascus to Beijing have coopted the internet to entrench their power and control their populations (Morozov, 2011). The autocratic threat to democracy is therefore not confined to election interference or disinformation campaigns. There are a myriad other ways in which illiberal regimes are using digital technologies to undermine democratic values at home and abroad.

Generally conceived, digital repression is the coercive use of information and communication technologies by the state to exert control over potential and existing challenges and challengers. Digital repression includes a range of tactics through which states are able to use digital technologies to monitor and restrict the actions of their citizens that include, but are not limited to, digital surveillance, advanced biometric monitoring, disinformation campaigns, and state-based hacking (Feldstein, 2019). While digital repression does not specifically entail the use of physical sanctions against an individual or organization, it often carries with it the implicit assumption that information gathered could be used for more violent means. This often has the outcome of inflicting a chilling effect on dissent against the state without sustained violence (Feldstein, 2019, p. 42). Furthermore, as discussed earlier, these repressive activities can be directed to individuals outside the state's national borders, in some cases compelling them to organize domestic dissident groups or even compromise the election process itself (Shane, 2018).

States have always repressed (Davenport, 2007; Goldstein, 2001). Even democracies, particularly those democracies under threat (Rummel, 1995), have used surveillance and sometimes physical repression against their own citizens (Conrad,

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 09:21:22, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.001

Hill, & Moore, 2018; Davenport, 2007). Repressive tactics include the violation of physical integrity rights, such as harassment, detainment, torture (Rejali, 2007), and extrajudicial killings (Krain, 1997; Midlarsky, 2005; Valentino, 2004), as well as covert repression through monitoring and surveilling which can include wiretapping, organizational infiltration, and the use of informants and agents provocateurs (Davenport, 2005). Repression in all forms is costly for the state, and its citizens. Repression carries the physical costs of maintaining a coercive apparatus and, in more open regimes, it carries the potential audience costs of having these actions exposed to the public. States choose to incur these costs when they are under (real or perceived) threat, which may be created or reinforced through disinformation (Davenport, 2007a, p. 2).

While the repressive power and potential of the state is not a new phenomenon, digital technologies are offering a fresh platform through which governments can exercise their powers of control and self-preservation domestically. Rather than offering the liberating potential originally associated with these technologies (Diamond, 2010), many are now arguing that "social media [is] driving the spread of authoritarian practices" (Deibert, 2019). Examples of this phenomenon include the Arab Spring, as well as more recent conflicts across the Middle East, and beyond (Caywood, 2018).

Digital technologies are changing the nature of state repression in two primary ways. First, the speed and scope with which information can be collected and processed is far greater than any monitoring or surveillance techniques of the past. As Ron Deibert and Rafal Rohozinski write, "Digital information can be easily tracked and traced, and then tied to specific individuals who themselves can be mapped in space and time with a degree of sophistication that would make the greatest tyrants of days past envious" (Deibert & Rohozinski, 2010). This can be done on a much wider swath of the population than was ever previously possible. For example, states threatened by mass mobilization are able to closely monitor, in real time, crowd formations with the potential to become mass rallies allowing police to be put on standby to immediately break up a protest before it grows (Feldstein, 2019, p. 43). They can use facial recognition to identify their leaders.

Second, the nature of repressive technologies has shifted the capacity required for repression, which in turn has shifted the costs. As outlined earlier, repression is costly. It carries the physical costs associated with maintaining a repressive apparatus (e.g., training and paying soldiers and police, maintaining detention facilities, etc.). In the past, mass surveillance required an extensive network of informers. In Poland in 1981, for example, at the height of the Sluzba Bezpieczenstwa's (Security Service) work to undermine the Solidarity movement, there were an estimated 84,000 informers (Day, 2011). New technologies produce the same level of surveillance or greater from far fewer people. Such digital technologies can be expensive. The Xinjian authorities, for example, reportedly budgeted more than $1 billion in the first quarter of 2017 for the monitoring and detention of the Uyghur population there

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 09:21:22, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.001

(Chin & Bürge, 2017). Yet this is likely a low figure when compared with the amount the Chinese state would have spent to construct a comparable system without using digital technologies (Feldstein, 2019, pp. 45–46).

Steven Feldstein attributes these impacts of digital repression to the increased availability of big data from both public and private sources, enhanced machine learning and algorithmic approaches to the processing of that data, and the corresponding advances in computer processing power (Feldstein, 2019, p. 41). As Feldstein writes, "From facial-recognition technologies that cross-check real-time images against massive databases to algorithms that crawl social media for signs of opposition activity, these innovations are a game-changer for authoritarian efforts to shape discourse and crush opposition voices" (Feldstein, 2019, p. 41). In many ways, digital technologies have ushered us into a new era, what Larry Diamond calls "postmodern totalitarianism," in which we appear to be free to go about our daily lives, but governments are controlling and censoring all information flows.

Furthermore, digital technologies serve a very specific function for autocratic states. While leader removal by coups and civil war defeats are declining, it is increasingly common for leaders to be removed on the basis of internal pressure and mass public uprisings (Hollyer, Rosendorff, & Vreeland, 2015). In this way, "the gravest threats to authoritarian survival today may be coming not from insider-led rebellions, but from discontented publics on the streets or at the ballot box" (Feldstein, 2019, p. 43). Such observations might explain Vladimir Putin's response to the December 2011 protests in Russia, along with the color revolutions and Arab Spring (Crowley, 2016). These new trends in leadership removal increase the incentives for leaders to pursue repressive tactics capable of monitoring public opinion and mobilization potential.

As is discussed further in Parts II and III, the target of digital repression need not solely be a country's own citizens. Surveillance, state-sponsored hacks, election interference, and disinformation campaigns have all been documented strategies of autocratic governments' attempts at destabilizing rivals and undermining democracy globally. In several cases, those interfering governments target, or at least attempt to instrumentalize, members of their own diaspora groups (Onishi, 2023). In addition to challenging the functioning of democratic governments, there have been attempts to change the behavior of non-state actors in pursuit of a global liberal agenda, such as human rights nongovernmental organizations (NGOs).[4] Moreover, while the focus of this volume is mainly on digital influence from major powers, the nature of digital technologies is impacting which states can monitor and repress. As the financial and material costs of digital repression decrease, the capacity to influence is no longer confined to global powers. Finally, much like repression itself, digital repression is not and will not be confined to autocratic regimes.

[4] See many of the reports written on this topic by Citizen Lab, for example, (Marczak et al., 2019; Scott-Railton et al., 2019).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 09:21:22, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.001

Democracies monitor, surveille, and repress their own citizens, particularly in times of threat. We should, therefore, not only look for digital repression and interference from our autocratic rivals but acknowledge its potential even within the most stalwart democracies, including the United States. Democracies must be alert to the temptation to silence legitimate dissent, including protest activity that asserts a difference of opinion, in the name of rooting out disinformation (Nardi, 2024). All democracies have a great deal to learn from one another in partnership with the private sector, and similarly can help buttress their common defenses against common cyber-enabled threats, which is a key theme that is explored throughout this collection.

STRUCTURE

The book is structured as follows. It is broken into three main parts, each with several chapters. Part I is entitled "Challenges to Democratic Institutions" and consists of four chapters. In Chapter 2, "Hacking Elections: Contemporary Developments in Historical Perspective," Andrew Grotto and Ashray Narayan from Stanford University advance the argument that the twenty-first century challenge of safeguarding elections from cyberattacks should be understood through the lens of the U.S. Constitution's silence on an affirmative right to vote. In Chapter 3, Professor Rachel Brooks of the University of Bradford builds from this foundation in her piece, "From Free Speech to False Speech: Analyzing Foreign Online Disinformation Campaigns Targeting Democracies," in which she globalizes the issue by comparing and contrasting the roles and goals of Russia and China in undermining trust in democratic institutions. Next, in Chapter 4, Professor Renée Marlin-Bennett from Johns Hopkins University analyzes antidemocratic efforts using cyber-enabled technologies as malign soft power in her contribution entitled, "Cyber Challenges to Democracy and Soft Power's Dark Side." In Chapter 5, entitled "Cyber Disinformation Risk Perception and Control: Integration of the Extended Theory of Planned Behavior and a Structural Equation Model," Professors Małgorzata Pańkowska and Ioana Vasiu of Babeş-Bolyai University take on the global challenges presented by these technologies, arguing that individual users' behavior plays a key role in the control of the phenomenon, and aim to identify factors that impact on users' behavioral intentions and cyber hygiene behavior.

Part II builds from the global challenges to both election infrastructure and more broadly democratic integrity that were introduced in Part I by exploring a series of regional case studies. These were curated from leading academics and practitioners from around the world and focus on three primary regions that are at the frontline of geopolitical fissures pitting authoritarian and democratic regimes against one another. These include the Middle East, Eastern Europe, and Ukraine, along with Asia, in particular India, China, and Taiwan. Chapter 6, "Innovative Frontrunner or

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 09:21:22, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.001

Delayed by Political Gridlock? Israel's Attempts at Countering Disinformation," authored by Inga Kristina Trauthig and Gabrielle Dora Beacken from the University of Texas-Austin's Center for Media Engagement, kicks off the case studies by examining Israel's efforts to counter disinformation through both policy and its private industry related in particular to its controversial push to reform the judicial review powers of the Israeli Supreme Court. The next contribution, Chapter 7, similarly focuses on Israel and the broader Middle East, with a submission authored by David Amsellem entitled "Israeli Information Strategies and Maneuvers," which focuses on the extent to which Israel has been able to achieve many of its strategic objectives despite global public opinion turning against it.

Chapter 8 pivots our case study analysis away from the Middle East and toward Eastern Europe beginning with "Ukraine's Support Coalition and the Long (Info) War: Mitigating the Disinformation Threat to Democratic Collaboration" by Jaclyn A. Kerr, which examines the role of cyber-enabled information and influence in relation to transatlantic support for Ukraine as a case study of the challenge of addressing transnational coordinated strategic disinformation campaigns. Chapter 9 then follows on this broad theme and features a contribution from Professors Jean Camp, Julia R. Fox, Inna Kouper, Sandra Kübler, and Maria Shardakova entitled "Weapons of Mass Derision: Humor, War, and Democracy." In this chapter, they explore the role of humor in building resilience to authoritarianism and disinformation, especially among the younger generation of Russians. The focus then remains on Russia but shifts to Central Asia in Chapter 10, entitled "Election Cyber Threats in Central Asia: A Multistakeholder Approach to Tackling Election Interference and Increasing Resilience," by Pavlina Pavlova of the Cyber Peace Institute. This chapter analyzes regional trends in influencing elections and impacting electoral integrity by cyber means in two key areas, the informational and the technical domain, and proposes action-oriented recommendations for cross-sectoral cooperation toward securing elections and the wider digital ecosystem across Central Asia. In Chapter 11, Ravi Nayyar, a PhD candidate at the University of Sydney, brings our focus to South Asia with "Stacking Up for Resilience: Digital Public Infrastructure – The India Way." This contribution links together democratic integrity with broader issues surrounding critical infrastructure protection, focusing on India's efforts aimed at securing Digital Public Infrastructure (DPI). Finally, Chapters 12 and 13 focus on China and Taiwan respectively. Professor Jun Liu of the University of Copenhagen examines the narrative of cybersecurity in China's mass media, with a focus on the domestication of cybersecurity and its subsequent challenge to democracy in her chapter entitled, "The Domestication of Cybersecurity in Authoritarian Regime: China's Media Narrative on Cybersecurity and Its Challenge to Democracy." Simon Sun, an SJD candidate at Indiana University, next analyzes Taiwan's approach to internet governance relative to China's embrace of cyber sovereignty in his chapter entitled, "Defending Taiwan's Democracy in the Internet Commons."

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 09:21:22, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.001

Part III, "Policy Responses," applies lessons from these case studies as they relate to managing disinformation by relying on theoretical insights gleaned from the literature and frameworks associated with the Ostrom Workshop. In Chapter 14, entitled "Some Truths about Lies: Misinformation and Inequality in Policymaking and Politics," Professors Lindsay Flynn of the University of Luxembourg and Barbara Allen of Carleton College use insights gleaned from the Institutional Analysis and Development (IAD) Framework to explore how the dual trends of increased disinformation in politics and increased socioeconomic inequality contribute to an erosion of trust and confidence in democratic institutions. Finally, the volume concludes in Chapter 15 with Professors Deike Schulz, Joyce Kerstens, and Dustin Sajoe of NHL Stenden University and their contribution, "Getting a Grip on Disinformation: From Distrust to Trust within Learning Communities," which highlights an experiment with methodology to empower communities to recognize and fight disinformation.

Together, these chapters can barely scratch the surface of the myriad efforts underway around the world both in and between democracies to secure election infrastructure and build trust in democratic institutions such as by battling disinformation and deep fakes. Yet they do illustrate the common challenges that are faced by both advanced and emerging democracies, along with the important roles played by technological, regulatory, and geopolitical trends in shaping the landscape of defending democracy in the digital age. Our hope is that this is among the first, but certainly not the last, such effort, particularly given the series of consequential elections taking place around the world in 2024.

REFERENCES

Alba, D., & Frenkel, S. (2019, October 30). Russia tests new disinformation tactics in Africa to expand influence. *The New York Times*. https://thehill.com/policy/cybersecurity/431614-us-cyber-operation-blocked-internet-for-russian-troll-farm-on-election/

Alba, D., & Satariano, A. (2019, September 26). At least 70 countries have had disinformation campaigns. *The New York Times*. https://nytimes.com/2019/09/26/technology/government-disinformation-cyber-troops.html

Annan, K. (n.d.). *Compass: Manual for human rights education with young people. Democracy*. Council of Europe Portal. https://coe.int/en/web/compass/democracy

Beeman, R. R. (n.d.). *Perspectives on the Constitution: A republic, if you can keep it*. National Constitution Center. https://constitutioncenter.org/learn/educational-resources/historical-documents/perspectives-on-the-constitution-a-republic-if-you-can-keep-it

Borys, S. (2018, May 28). *China's "brazen" and "aggressive" political interference outlined in top-secret report*. ABC News Australia. https://abc.net.au/news/2018-05-29/chinas-been-interfering-in-australian-politics-for-past-decade/9810236

Caywood, C. (2018, November 21). *This is how social media is being used in the Middle East*. The National Interest. https://nationalinterest.org/blog/middle-east-watch/how-social-media-being-used-middle-east-36857

Chin, J., & Burge, C. (2017, December 19). Twelve days in Xinjiang: How China's surveillance state overwhelms daily life. *The Wall Street Journal*. https://wsj.com/articles/twelve-days-in-xinjiang-how-chinas-surveillance-state-overwhelms-daily-life-1513700355

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 09:21:22, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.001

CISA. (2020, November 12). *Joint Statement from Elections Infrastructure Government Coordinating Council & the Election Infrastructure Sector Coordinating Executive Committees*. CISA. https://cisa.gov/news-events/news/joint-statement-elections-infrastructure-government-coordinating-council-election

CNN Editorial Research. (2023, October 23). *2016 presidential campaign hacking fast facts*. CNN. https://cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html#:~:text=According%20to%20the%20report%2C%20hackers,Podesta%2C%20according%20to%20the%20report

Colvin, J., & Barrow, B. (2023, December 7). *Trump's vow to only be a dictator on "day one" follows growing worry over his authoritarian rhetoric*. AP News. https://apnews.com/article/trump-hannity-dictator-authoritarian-presidential-election-f27e7e9d7c13fabbe3ae7dd7f1235c72

Conrad, C. R., Hill, D. W., Jr., & Moore, W. H. (2018). Torture and the limits of democratic institutions. *Journal of Peace Research*, *55*(1), 3–17.

Crowley, M., & Ioffe, J. (2016, July 25). Why Putin hates Hillary. *Politico*. https://politico.com/story/2016/07/clinton-putin-226153

Davenport, C. (2005). Understanding covert repressive action: The case of the U.S. government against the Republic of New Africa. *The Journal of Conflict Resolution*, *49*(1), 120–140.

(2007a). *State repression and the domestic democratic peace*. Cambridge University Press. https://doi.org/10.1017/CBO9780511510021

(2007b). State repression and political order. *Annual Review of Political Science*, *10*, 1–23. https://doi.org/10.1146/annurev.polisci.10.1140.143216

Day, M. (2011, October 18). Polish secret police: How and why the Poles spied on their own people. *The Telegraph*. https://telegraph.co.uk/news/worldnews/europe/poland/8831691/Polish-secret-police-how-and-why-the-Poles-spied-on-their-own-people.html

Deibert, R. J. (2019). The road to digital unfreedom: Three painful truths about social media. *Journal of Democracy*, *30*(1), 25–39.

Deibert, R. J., & Rohozinski, R. (2010). Liberation vs. control: The future of cyberspace. *Journal of Democracy*, *21*(4), 43–57.

Diamond, L. (2010). Liberation technology. *Journal of Democracy*, *21*(3), 69–83.

European Intelligence Unit (EIU). (2023). *EIU report: Democracy index 2023*. EIU. https://eiu.com/n/campaigns/democracy-index-2023/

Feldstein, S. (2019). How artificial intelligence is reshaping repression. *Journal of Democracy*, *30*(1), 40–52.

Janda, J. (2017, November 5). *A framework guide to tools for countering hostile foreign electoral inference*. European Values. https://europeanvalues.net/wp-content/uploads/2017/05/35-measures-in-15-steps-for-enhancing-the-resilience-of-the-democratic-electoral-process-1-1.pdf

Francois, C. (2019, September 20). *Actors, behaviors, content: A disinformation ABC*. Transatlantic Working Group. https://ivir.nl/publicaties/download/ABC_Framework_2019_Sept_2019.pdf

Freedom House. (2023, March). *Freedom in the world 2023*. Freedom House. https://freedomhouse.org/sites/default/files/2023-03/FIW_World_2023_DigtalPDF.pdf

Goldstein, R. J. (1978). *Political repression in modern America: From 1870 to the present*. G. K. Hall.

Hollyer, J. R., Rosendorf, P. B., & Vreeland, J. R. (2015). Transparency, protest, and autocratic instability. *The American Political Science Review*, *41*(3), 764–784.

Krain, M. (1997). State-sponsored mass murder: The onset and severity of genocides and politicides. *The Journal of Conflict Resolution*, *41*(3), 331–360.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 09:21:22, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.001

Laing, A. (2010, October 24). Election won by Mandele "rigged by opposition". *The Telegraph*. https://telegraph.co.uk/news/worldnews/africaandindianocean/southafrica/8084053/Election-won-by-Mandela-rigged-by-opposition.html

Levin, D. H. (2016, February 13). When the great power gets a vote: The effects of great power electoral interventions on election results. *International Studies Quarterly*, *60*(2), 189–202. https://doi.org/10.1093/isq/sqv016

Lynn-Jones, S. M. (1998, March). *Why the United States should spread democracy*. Harvard Kennedy School, Belfer Center. https://belfercenter.org/publication/why-united-states-should-spread-democracy

Mak, T. (2018, June 20). *Former U.S. diplomat warns China is emulating Russian political interference*. NPR. https://npr.org/2018/06/20/621963286/former-u-s-diplomat-warns-china-is-emulating-russian-political-interference

Marczak, B., Hulcoop, A., Maynier, E., Razzak, B. A., Crete-Nishihata, M., Scott-Railton, J., & Deibert, R. (2019, September 24). *Missing link: Tibetan groups targeted with 1-click mobile exploits*. The Citizen Lab. https://citizenlab.ca/2019/09/poison-carp-tibetan-groups-targeted-with-1-click-mobile-exploits/

Midlarsky, M. I. (2005). *The killing trap: Genocide in the twentieth century*. Cambridge University Press. https://doi.org/10.1017/CBO9780511491023

Milligan, S. (2022, November 2). *Biden: "Make no mistake: Democracy is on the ballot"*. U.S. News & World Report. https://usnews.com/news/elections/articles/2022-11-02/biden-make-no-mistake-democracy-is-on-the-ballot

Morozov, E. (2011). *The net delusion: The dark side of internet freedom*. PublicAffairs.

Nardi, C. (2024, January 24). Trudeau's use of the Emergencies Act was ruled unconstitutional. What happens now? *National Post*. https://nationalpost.com/news/politics/a-judge-ruled-trudeaus-use-of-the-emergencies-act-unconstitutional-so-what-happens-next#:~:text=OTTAWA%20%E2%80%93%20In%20a%20landmark%20ruling,Convoy%20blockades%20in%20early%202022

Onishi, N. (2023, December 14). He won election to Canada's Parliament. Did China help? *The New York Times*. https://nytimes.com/2023/12/02/world/americas/canada-elections-china.html#:~:text=Lawmakers%20are%20separately%20examining%20whether,Dong%20%E2%80%94%20has%20been%20named

Pew Research Center. (2022, January 5). *Trust in America: Do Americans trust their elections?* Pew Research Center. https://pewresearch.org/2022/01/05/trust-in-america-do-americans-trust-their-elections

Popken, B. (2018, November 5). *Factory of lies: Russia's disinformation playbook exposed*. NBC News. https://nbcnews.com/business/consumer/factory-lies-russia-s-disinformation-playbook-exposed-n910316

Ranger, S. (2017, January 5). *US intelligence: 30 countries building cyber attack capabilities*. ZDNet. https://zdnet.com/article/us-intelligence-30-countries-building-cyber-attack-capabilities/

Reece, N. (2024, January 14). *More than 4 billion people are eligible to vote in an election in 2024. Is this democracy's biggest test?* The Conversation. https://theconversation.com/more-than-4-billion-people-are-eligible-to-vote-in-an-election-in-2024-is-this-democracys-biggest-test-220837

Rejali, D. (2009). *Torture and democracy*. Princeton University Press.

Rosenberg, L. (2022, December 27). *Mind control in the Metaverse*. Medium. https://medium.com/predict/mind-control-in-the-metaverse-48dfbd88c2ae

Rummel, R. J. (1995). Democracy, power, genocide, and mass murder. *The Journal of Conflict Resolution*, *39*(1), 3–26.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 09:21:22, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.001

Salter, A. (2022, August 22). *Why American democracy is worth defending*. Imaginative Conservative. https://theimaginativeconservative.org/2022/08/american-democracy-alexander-salter.html

Schneier, B., & Farrell, H. (2018, November 19). *The most damaging election disinformation campaign came from Donald Trump, not Russia*. Vice. https://vice.com/en/article/mbyg3x/the-most-damaging-election-disinformation-campaign-came-from-donald-trump-not-russia

Scott-Railton, J., Marczak, B., Anstis, S., Razzak, B. A., Crete-Nishihata, M., & Deibert, R. (2019, March 20). *Reckless VII: Wife of journalist slain in cartel-linked killing targeted with NSO group's spyware*. The Citizen Lab. https://citizenlab.ca/2019/03/nso-spyware-slain-journalists-wife/#:~:text=Key%20Findings,Andr%C3%A9s%20Villarreal%20and%20Ismael%20Boj%C3%B3rquez

Shackelford, S., Schneier, B., Sulmeyer, M., Boustead, A., & Buchanan, B. (2017). Making democracy harder to hack. *University of Michigan Journal of Law Reform*, 50(3), 629–668. https://doi.org/10.36646/mjlr.50.3.making

Shane, S. (2018, February 18). How unwitting Americans encountered Russian operatives online. *The New York Times*. https://nytimes.com/2018/02/18/us/politics/russian-operatives-facebook-twitter.html

Shea, C. (2006, January 15). Sovereignty in cyberspace. *Boston Globe*. http://worldtradelaw.typepad.com/ielpblog/2006/01/sovereigntyjuri.html

Tennis, M. (2020, July 20). *Russia ramps up global elections interference: Lessons for the United States*. Center for Strategic & International Studies. https://csis.org/blogs/technology-policy-blog/russia-ramps-global-elections-interference-lessons-united-states

Thomsen, J. (2019, February 26). US cyber operation blocked internet for Russian troll farm on Election Day 2018: Report. *The Hill*. https://thehill.com/policy/cybersecurity/431614-us-cyber-operation-blocked-internet-for-russian-troll-farm-on-election/

Valentino, B. A. (2004). *Final solutions: Mass killing and genocide in the 20th century*. Cornell University Press.

Way, L. A., & Casey, A. (2018, January 8). Russia has been meddling in foreign elections for decades. Has it made a difference? *Washington Post*. https://washingtonpost.com/news/monkey-cage/wp/2018/01/05/russia-has-been-meddling-in-foreign-elections-for-decades-has-it-made-a-difference/

Zeitz, J. (2016, July 27). Foreign governments have been tampering with U.S. elections for decades. *Politico*. https://politico.com/magazine/story/2016/07/russia-dnc-hack-donald-trump-foreign-governments-hacking-vietnam-richard-nixon-214111

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 09:21:22, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.001

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 09:21:22, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.001