Washington and Lee Law Review

Volume 77 | Issue 4 Article 7

Fall 2020

Defending Democracy: Taking Stock of the Global Fight Against Digital Repression, Disinformation, and Election Insecurity

Scott J. Shackelford
Indiana University, Kelley School of Business, sjshacke@indiana.edu

Angie Raymond
Indiana University, Kelley School of Business, angraymo@indiana.edu

Abbey Stemler
Indiana University, Kelley School of Business, astemler@indiana.edu

Cyanne Loyle
Penn State University, cloyle@psu.edu

Defending Democracy: Taking Stock of the Global Fight Against Digital Repression, Disinformation, and Election Insecurity

Scott J. Shackelford JD, Ph.D.*
Angie Raymond, JD**
Abbey Stemler, JD, MBA***
Cyanne Loyle, Ph.D.****

Abstract

Amidst the regular drumbeat of reports about Russian attempts to undermine U.S. democratic institutions from Twitter bots to cyber-attacks on Congressional candidates, it is easy to forget that the problem of election security is not isolated to the United States and extends far beyond safeguarding insecure voting machines. Consider Australia, which has long been grappling with repeated Chinese attempts to interfere with its

* Chair, IU-Bloomington Cybersecurity Program; Executive Director, Ostrom Workshop; Associate Professor of Business Law and Ethics, Indiana University Kelley School of Business.

** Data Governance Program Director, Ostrom Workshop; Associate Professor of Business Law and Ethics, Indiana University Kelley School of Business.

*** Assistant Professor of Business Law and Ethics, Indiana University Kelley School of Business; Faculty Associate, Berkman Klein Center for Internet & Society at Harvard University.

**** Associate Professor of Political Science, Penn State University; Global Fellow, Peace Research Institute Oslo.

political system. 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 U.S. government has yet to take despite repeated breaches at both the Democratic and Republican National Committees.

This Article analyzes the Australian approach to protecting its democratic institutions from Chinese influence operations and compares it to the U.S. response to Russian efforts. It then moves on to discuss how other cyber powers, including the European Union, have taken on the fight against digital repression and disinformation, and then compares these practices to the particular vulnerabilities of Small Pacific Island Nations. Such a comparative study is vital to help build resilience, and trust, in democratic systems on both sides of the Pacific. We argue that a multifaceted approach is needed to build more resilient and sustainable democratic systems. This should encompass both targeted reforms focusing on election infrastructure security—such as requiring paper ballots and risk-limiting audits—with deeper structural interventions to limit the spread of misinformation and combat digital repression.

Table of Contents

I. Introduction

> Democracy has never been and never can be so durable as Aristocracy or Monarchy. But while it lasts it is more bloody than either . . . Remember, democracy never lasts long. It soon wastes exhausts and murders itself. There never was a Democracy Yet, that did not commit suicide.
>
> U.S. President John Adams[1]

Since the U.S. was founded, detractors and critics have heralded its ultimate downfall.[2] Benjamin Franklin once famously quipped after being asked what sort of government the Founders had gifted the new nation: "A republic, if you can keep it."[3] For the more than 230 years since that time, many of the threats to American democracy, as with other emerging and advanced democracies around the world, have stemmed from

1. Letter from John Adams to John Taylor (Dec. 17, 1814), http://perma.cc/724R-ESVB.

2. *See, e.g.*, Richard R. Beeman, *Perspectives on the Constitution: A Republic, If You Can Keep It*, NAT'L. CONST. CTR., https://perma.cc/J36F-2EAP (presenting the initial, objectionable reactions of the Founding Fathers when they were presented with the United States Constitution).

3. *Id.*

internal divisions fed by inequality, injustice, and racism; fissures that have from time to time purposefully been widened and deepened by foreign nations wishing to distract and destabilize the U.S. government.[4]

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.[5] 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 U.S. Presidential election, made easier by the rise of internet platforms generally and social networking in particular.[6] Such efforts continued into the 2018 U.S. midterm elections, when U.S. Cyber Command shut down a Russian troll farm on Election Day.[7]

Furthermore, today's threats to democratic institutions in the United States and abroad are acute, extending from the protection of voting machines and media sites to related issues of critical infrastructure, 5G, and even Internet of Things (IoT) vulnerabilities.[8] Keeping the Republic for the next century, then, requires a range of policy responses from reigning in the worst excesses of internet platforms to securing the voting process itself to safeguarding democratic institutions from being

4. *See, e.g.*, Josh Zeitz, *Foreign Governments Have Been Tampering with U.S. Elections for Decades*, POLITICO (July 27, 2016), https://perma.cc/CAQ8-UW5A (noting multiple occasions of foreign interference with American presidential elections).

5. *See* Luncan Ahmad Way & Adam Casey, *Russia Has Been Meddling in Foreign Elections for Decades. Has it Made a Difference?*, WASH. POST (Jan. 8, 2018, 6:00 AM), https://perma.cc/2BC8-J9MK (examining the two waves of Russian interference with United States presidential elections since the early 1990s).

6. *See id.* (noting that since 2014, Russia has used the internet to spread disinformation campaigns, create fake Facebook profiles, leak emails and fake documents to WikiLeaks, and engage in cyberattacks and phishing attacks).

7. *See* Jacqueline Thomsen, *US Cyber Operation Blocked Internet for Russian Troll Farm on Election Day 2018: Report*, HILL (Feb. 26, 2019, 12:32 PM), https://perma.cc/MB9T-SWX6 (discussing the ability of the United States Cyber Command to block Russian interference in the 2018 midterm elections).

8. *See* Scott J. Shackelford et al., *Making Democracy Harder to Hack*, 50 MICH. J.L. REFORM 629, 630–33 (2017) (highlighting cybersecurity vulnerabilities in the United States' national and state electoral systems).

undermined by both foreign and domestic efforts, offline and online.[9] Luckily, much as U.S. states are often seen as laboratories for democracy, this debate does not exist in a vacuum.[10] U.S. policymakers can and should learn from what has worked elsewhere in our common quest to make democracy "harder to hack."[11]

Indeed, amidst the regular drumbeat of reports about Russian attempts to undermine U.S. democratic institutions from Twitter bots to cyber-attacks on congressional candidates, it is easy to forget that the problem of election security is not isolated to the United States and extends far beyond safeguarding insecure voting machines.[12] Consider Australia, which has long been grappling with repeated Chinese attempts to interfere with its political system. One 2018 report found that the Chinese have infiltrated "every layer of Australian Government, right down to local councils."[13] 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 U.S. government has yet to take despite repeated breaches at both the Democratic and Republican National Committees.[14]

This Article details the Australian approach to protecting its democratic institutions from Chinese influence operations and compares it to the U.S. response to Russian meddling efforts. Such a comparative study is vital to help build resilience, and trust, in democratic systems on both sides of the

9. *See id.* (evaluating the policy debate surrounding the designation of the United States electoral system as a critical infrastructure).

10. *See id.* (detailing instances of election tampering, both internationally and in the United States).

11. *See generally id.*

12. *See* Michael Wines & Julian E. Barnes, *How the U.S. Is Fighting Russian Election Interference*, N.Y. TIMES (Aug. 2, 2018), https://perma.cc/B7LH-D57T (stating that the most pervasive Russian threats are those concerning social media).

13. Stephanie Borys, *China's 'Brazen' and 'Aggressive' Political Interference Outlined in Top-Secret Report*, ABC NEWS (May 29, 2018, 5:28 PM), https://perma.cc/D27J-JGDQ.

14. *See 2016 Presidential Campaign Hacking Fast Facts*, CNN (Oct. 31, 2019, 1:10 PM), https://perma.cc/VUR3-ZJAD (offering a timeline for the investigations and conclusions about the 2016 election hacking efforts).

Pacific. But we do not stop there. For the first time in the literature that we could identify, we also analyze the efforts of other leading cyber powers—including the European Union—comparing them against not only the United States and Australia, but also Small Pacific Island Nations, to better understand how to deter misinformation and disinformation campaigns in 2020 and beyond.[15]

In all, we argue that democracies can and should work together to share both cyber threat information and best practices to build resilience in democratic institutions the world over, and that a multi-faceted 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 of misinformation and combat "digital repression."[16] We assert that it is vital to take this wider view of defending democracy that includes not only a focus on protecting election infrastructure, but also digital repression—both are means to an end, undermining trust, and confidence, in democratic institutions. As such, defending democracy in 2020 and beyond requires implementing policy responses that tackle this full range of cyber-enabled threats, which are not limited to insecure voting machines and processes.[17]

The Article is structured as follows. Part II offers a short history of the cyber threat facing democracies, focusing on the

---

15. *See Australia Increases Investment in South Pacific Islands in an Apparent Response to China's Growing Economic Influence in the Region*, RWR ADVISORY GRP. (July 13, 2018, 11:52 AM), https://perma.cc/AR8W-5Q7G (recounting the Australian government's MoU with the Solomon Islands and Papua New Guinea to address China's growing economic activity in the areas).

16. *See* Brandon Valeriano, *Welcome to the Age of Digital Repression*, QUARTZ (Jan. 14, 2016), https://perma.cc/W9A9-HRTN (deeming cyber repression as one of the digital age's most important challenges and revealing that Donald Trump and Hillary Clinton previously called for shutting down the internet).

17. Further, it is important to note that prevalent cyber insecurity can feed digital repression; indeed, oftentimes new regulations from autocratic nations that are designed to address cybersecurity issues often wind up further entrenching repression. *See* Adrian Shahbaz, *Fake News, Data Collection, and the Challenge to Democracy*, FREEDOM HOUSE, https://perma.cc/Z3UB-386H (referencing the growing censorship of the internet leading to the disruption of democracies).

role of authoritarian regimes in furthering digital repression. Part III summarizes U.S. efforts to protect election infrastructure post-2016. Part IV features a comparative case study summarizing EU efforts to similarly safeguard their democratic societies as compared to efforts from Australia and Oceania. Finally, Part V crystallizes implications and suggests policy responses to better manage both threats to election infrastructure and digital repression.

II. Unpacking the Cyber Threat to Democracies

Threats to democracy, both foreign and domestic, take a variety of forms, which is part of the challenge in coming up with coherent policy responses.[18] For example, depending on the scale and preferred lens, it is possible to view post-2016 efforts to secure democracies as an exercise in regulating social media firms to guard against both misinformation and disinformation,[19] protecting vulnerable critical infrastructure,[20] or even as one facet of a larger needed debate on governing the Internet of Things,[21] to name a few. This Part helps to frame out this broader discussion by providing a short history of cyber-enabled election interference and how authoritarian

18. *See* THE WHITE HOUSE, NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 26–28 (2017), https://perma.cc/SGG4-9TLH (PDF) (explaining that, due to the patient and strategic combination of political, economic, military, and informational strategies employed against the United States, responding to threats such as those related to cyber security, are more challenging).

19. Disinformation is commonly understood as false information that is spread deliberately with the goal of deceiving a targeted population, while misinformation may or may not be intentional, but is inaccurate. *See Propaganda vs. Misinformation*, JOHNS HOPKINS UNIV. SHERIDAN LIBRS., https://perma.cc/E2QW-G74W (last updated June 20, 2020, 4:28 PM) (comparing propaganda, information, misinformation, and disinformation).

20. *See* Scott J. Shackelford, Opinion, *How to Make Democracy Harder to Hack,* CHRISTIAN SCI. MONITOR (July 29, 2016), https://perma.cc/S6M6-EDFU (listing the items that are considered critical infrastructure).

21. *See* Scott J. Shackelford, *When Toasters Attack: Enhancing the 'Security of Things' Through Polycentric Governance*, 2017 U. ILL. L. REV. 415, 418 (considering the protection measures needed for cybersecurity resulting from the Internet of Things).

regimes use digital repression both at home and abroad to help shape political debates.

A. Understanding Election Insecurity

In general, election security is discussed in two interconnected yet separate areas of research.[22] The first involves election infrastructure security and is focused on the security of the system itself, such as voting machines and tabulation systems.[23] The second is the fight against digital repression, including misinformation disseminated by social media.[24] Both areas are essential to the overall goal of defending democracy, and one cannot be successful without the other.[25]

Hacking into voting machines remains far too easy.[26] The vulnerabilities are not just theoretical.[27] They have been exploited around the world, such as in South Africa, Ukraine, Bulgaria and the Philippines.[28] In 2014, for example,

22. *See* THE NAT'L. ACADS. OF SCIS., ENG'G., & MED., SECURING THE VOTE: PROTECTING AMERICAN DEMOCRACY, xi–xiii (2018) (ebook) [hereinafter SECURING THE VOTE] (explaining that while the authors thought that their attentions would be devoted to the threats posed by long polling lines and outdated election systems, they also had to focus on the threats emerging from social media and other digital media).

23. *See* LAWRENCE NORDEN & CHRISTOPHER FAMIGHETTI, BRENNAN CTR. FOR JUST., AMERICA'S VOTING MACHINES AT RISK 8–15 (2015), https://perma.cc/5ZP7-JDV2 (PDF) (discussing the need to replace and upgrade aging voting systems and address insecure tabulation systems to protect election security).

24. *See* Shahbaz, *supra* note 17 (discussing the connection between digital censorship and repression).

25. *See* SECURING THE VOTE, *supra* note 22, at 4 (articulating the threats of both election infrastructure and digital media on election security).

26. *See* Shackelford, *supra* note 20 (detailing the ability of researchers from the University of Michigan to hack into government webpages in 2012 to have the University's fight song play after votes were casted).

27. *See id.* (providing concrete examples of hacking incidents on voting machines and databases in South Africa and the United States).

28. *See* John Leyden, *Hacker Almost Derailed Mandela Election in South Africa*, REGISTER (Oct. 27, 2010), https://perma.cc/LW3L-MJKX (detailing the ability of an unidentified hacker to almost successfully derail the democratic elections in South Africa); Daniel Funke & Daniela Flamini, *A Guide to Anti-Misinformation Actions Around the World*, POYNTER (Sept. 8, 2020),

Russian-backed hackers targeted Ukraine by attempting to fake vote totals for its presidential election.[29] They were caught just in time, but the sophistication of the attacks should have been seen as "a warning shot for future elections in the US and abroad."[30] Unfortunately, the U.S. government did not take the warning as seriously as it should have, as is discussed in Part III. But it should be noted that successful attacks do not need the resources and expertise of national governments—even kids have managed to orchestrate them.[31]

Election security suffers from common threats, as are summarized in Table 1, that range from outdated voting machines to insecure tabulation systems, each of which requires a different policy response as is discussed in Part V. This non-comprehensive list underscores the extent to which cyber insecurity enables digital repression, and vice versa, such as when hackers target vulnerabilities in government IT systems to spread misinformation about an upcoming election purportedly through official channels.[32]

---

https://perma.cc/2MPG-DWP9 (last updated Aug. 13, 2020) (referencing reports conducted by the EU to address the growing concern about misinformation and summarizing the responses of different countries to the spread of online misinformation).

29. *See* Mark Clayton, *Ukraine Election Narrowly Avoided 'Wanton Destruction' from Hackers*, CHRISTIAN SCI. MONITOR (June 17, 2014), https://perma.cc/23H9-AGZ6 (discussing the three-pronged cyber-attack on Ukraine's presidential election).

30. *Id*.

31. *See* Alex Hern, *Kids at Hacking Conference Show How Easily US Elections Could be Sabotaged*, GUARDIAN (Aug. 22, 2018), https://perma.cc/TBM2-VD87 (highlighting a child's ability to hack into websites, including those used for voter registration and campaigning efforts and the significant potential that creates for undermining election security).

32. *See, e.g.*, *Seven Ways Misinformation Spread During the 2016 Election*, KNIGHT FOUND. (Oct. 4, 2018), https://perma.cc/ZBR5-633R (providing a list of the many ways that misinformation was conveyed during the 2016 election).

Table 1: Non-Comprehensive List of Election Security Threats[33]

Phase(s)	Assets	Examples of Threats
Setup	Party/ candidate registration	• Tampering with registrations • Denial-of-service (DoS) attacks or overload of party/campaign registration causing them to miss the deadline • Fabricated signatures from sponsor
Setup	Electoral rolls	• Identity fraud during voter registration • Deleting or tampering with voter data • DoS or overload of voter registration system suppressing voters
Campaign	Campaign IT	• Hacking candidate laptops or email accounts • Hacking campaign websites (defacement, DoS) • Misconfiguration of a website • Leak of confidential information
All phases	Government IT	• Hacking/misconfiguration of government servers

33. NIS COOP. GRP., COMPENDIUM ON CYBER SECURITY OF ELECTION TECHNOLOGY 16 (2018), [hereinafter COMPENDIUM] https://perma.cc/BMG4-C8WS (PDF).

		• Communication networks, or endpoints • Hacking government websites, spreading misinformation on the election process, registered parties/candidates, or results • DoS or overload of government websites
Voting	Election technology	• Tampering or DoS of voting and/or vote confidentiality during or after the elections • Software bug altering election results • Tampering with logs/journals • Breach of voter privacy during the casting of votes • Tampering, DoS, or overload of the systems used for counting or aggregating results • Tampering or DoS of communication links used to transfer (interim) results • Tampering with supply chain involved in the movement or transfer of data

Campaign, public communication	Media/ press	• Hacking of internal systems used by media or press • Tampering, DoS, or overload of media communication links • Defacement, DoS, or overload of websites or other systems used for publication of the results

Table 1 serves as a framework for exploring the complex issue of democracy insecurity; however, no single issue should be focused on in isolation as each forms a complex backbone of the overall needs of the democratic system.[34] This Article focuses specifically upon the dual, related issues of securing election infrastructure and digital repression.[35] Yet, as is clear, these threats only constitute a small fraction of the larger conversation about maintaining the integrity of democratic systems.[36] As such, this Article attempts to break down these areas into discrete conversations, without losing sight of the larger context in which the system is placed.

B. A Brief History of Cyber-Enabled Election Interference

Foreign electoral interference is nothing new.[37] One study found that from 1945 to 2000, the United States and Russia combined tried to influence foreign elections 117 times, using

34. *See* SECURING THE VOTE, *supra* note 22, at 4 (discussing the impacts of election infrastructure and digital media).

35. *See id.* (exploring the relationship between election infrastructure and digital repression).

36. *See* COMPENDIUM, *supra* note 33, at 16 (providing a list of election security threats).

37. *See* Don H. Levin, *When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results*, 60 INT'L. STUD. Q. 189, 189 (2016) (discussing electoral interventions).

both overt and covert methods.[38] It is not even a novelty to use cyber-attacks 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.[39] 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.[40] Pre-Soviet Union, the Tsarist secret police (the Komitet Gosudarstvennoy Bezopasnosti (KGB), now Federalnaya Sluzhba Bezopasnosti (FSB), which is the predecessor Federal Security Service) used disinformation.[41] 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.[42] During the Cold War, for example, Russian agents helped plant "hundreds of bogus headlines around the world" such as the claim that the U.S. 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.[43] That story eventually circled the world, and was even mentioned by a famous American newsperson, Dan Rather, on the *CBS Evening News* in 1987.[44]

Effective 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

38. *Id.*

39. *See* Aislinn Laing, *Election Won by Mandela 'Rigged by Opposition*,' TELEGRAPH (Oct. 24, 2010, 6:47 PM), https://perma.cc/C63L-VW5K (stating that a hacker rigged the election). Unfortunately, the hacker who installed this program was never identified. *Id.* For more on this topic, see Shackelford et al., *supra* note 8, at 629.

40. *See* Ben Popken, *Factory of Lies: Russia's Disinformation Playbook Exposed*, NBC NEWS (Nov. 5, 2018, 8:02 PM), https://perma.cc/H974-GPDY (noting Russia's early efforts to spread disinformation during the Cold War through inaccurate newspaper headlines).

41. *See id.* (dating Russia's use of disinformation back to the 1880s when it was utilized by the Tsarist secret police).

42. *See id*.

43. *See id* (describing the worldwide spread).

44. *Id*.

unknowing agents) to advance the story in other outlets.[45] 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, and causing a proliferation in the types of traditional and social media willing to run with fake stories.[46] One tragic example is a false story about adopted children being butchered for their organs and sold to wealthy U.S. citizens that first appeared in Honduras in 1986, which was quickly debunked with the official whom was quoted denying the episode and issuing a correction, but that did not stop Soviet newspapers from spreading it around the world.[47] But this is just one tool among many.[48] Nations such as China and Russia also inundate internet discussion forums with so-called "flooding attacks" that enable distraction and disinformation.[49] 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."[50]

Such actions are not confined to the physical or digital borders of illiberal regimes.[51] Russia has been linked with "confidence attacks" aimed at destabilizing democracies (especially those in bordering countries, such as Ukraine) and

45. *See id*. (detailing a successful disinformation campaign).

46. *See, e.g.*, Davey Alba & Adam Satariano, *At Least 70 Countries Have Had Disinformation Campaigns, Study Finds*, N.Y. TIMES (Sept. 26, 2019), https://perma.cc/TGZ4-93FS (demonstrating that at least seventy countries have suffered from political disinformation campaigns despite overwhelming efforts by programs designed to stop them).

47. *See* Popken, *supra* note 40 (explaining the promulgation of false headlines by Russian and Soviet agents during the Cold War).

48. *See* Henry Farrell & Bruce Schneier, *The Most Damaging Election Disinformation Campaign Came from Donald Trump, Not Russia*, VICE (Nov. 19, 2018, 10:26 AM), https://perma.cc/5GYL-KE4S (articulating the many methods of undermining election security, including the spread of false information, flooding attacks, confidence attacks, and Donald Trump's own comments about fraudulent election results).

49. *See id.* (discussing flooding attacks and their effect on democracy).

50. *Id.*

51. *See id*. (stating that the United States felt like the internet could positively spread liberal, American values).

undermining trust in elections,[52] 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.[53] 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.[54] 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.[55]

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.[56] 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,[57] while Yochai Benker, Robert Farris, and Hal Roberts have argued "that Fox News was far more influential in the spread of false

52. *See id*. (describing the "Russian social media trolls" that spread rumors to create confusion during the 2016 election).

53. *See* Tim Mak, *Former U.S. Diplomat Warns China Is Emulating Russian Political Interference*, NAT. PUB. RADIO (June 20, 2018, 4:19 PM), https://perma.cc/W2N6-NMRC (discussing a former U.S. official's warning that nations, including China, Iran, and North Korea, are beginning to interfere with elections).

54. *See id.* (discussing the National Security Council's observation that China, Iran, and North Korea are discovering that cyberspace is a good outlet for their political agendas).

55. *See, e.g.*, JAKUB JANDA, EUR. VALUES: KREMLIN WATCH REP., A FRAMEWORK GUIDE TO TOOLS FOR COUNTERING HOSTILE FOREIGN ELECTORAL INTERFERENCE, 13–15 (2017), https://perma.cc/B22B-7HB9 (PDF) (listing thirty-five ways the integrity of an election can be compromised by foreign actors).

56. *See* Farrell & Schneier, *supra* note 48 (citing JOHN SIDES ET AL., IDENTITY CRISIS: THE 2016 PRESIDENTIAL CAMPAIGN AND THE BATTLE FOR THE MEANING OF AMERICA (2018)).

57. *Id.* (citing JOHN SIDES ET AL., IDENTITY CRISIS: THE 2016 PRESIDENTIAL CAMPAIGN AND THE BATTLE FOR THE MEANING OF AMERICA (2018)).

news stories than any Russian effort."[58] Still, the fact that such efforts are spreading and that, to date, the efforts of the U.S. government, allied nations, and internet platforms have proven insufficient to stem the flood raises questions about how best to inoculate both advanced and emerging democracies against these threats, some of which stem from authoritarian regimes as is discussed next.

C. Digital Repression

As Farrell and Schneier have argued, "[c]ybersecurity 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."[59] 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 cyber-attack capabilities.[60] 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."[61] Instead, illiberal regimes from Damascus to Beijing have coopted the internet to entrench their power and control their populations.[62] The autocratic threat to democracy is therefore not confined to election interference or

58. *Id.* (quoting YOCHAI BENKLER ET AL., NETWORK PROPAGANDA: MANIPULATION, DISINFORMATION, AND RADICALIZATION IN AMERICAN POLITICS (2018)).

59. *Id.*

60. *See id.* (contrasting the Cold War era to today); Steve Ranger, *US Intelligence: 30 Countries Building Cyber Attack Capabilities*, ZDNET (Jan. 5, 2017), https://perma.cc/QMP3-UYAR (claiming that more than thirty nations have started to develop offensive cyber-attack strategies in response to increased cybersecurity threats).

61. Christopher Shea, *Sovereignty in Cyberspace*, INT'L. ECON. L. & POL'Y BLOG (Jan. 15, 2006), https://perma.cc/CZ5D-8HKG.

62. *See* EVGENY MOROZOV, THE NET DELUSION: THE DARK SIDE OF INTERNET FREEDOM 100–03 (2011) (arguing that the internet presents many avenues through which governments can censor information, including outsourcing).

misinformation campaigns.[63] There are myriad other ways in which illiberal regimes are using digital technologies to undermine democratic values at home and abroad.[64]

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.[65] Digital repression includes a ranges of tactics through which states are able to use digital technologies to monitor and restrict the actions of their citizens, which include, but are not limited to, digital surveillance, advanced biometric monitoring, misinformation campaigns, and state-based hacking.[66] 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.[67] This often has the outcome of inflicting a chilling effect on dissent against the state without sustained violence.[68] Furthermore, as discussed above, 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.[69]

---

63. *See id.* at 13 (outlining political implications that an email in the United States had on foreign relationships with Iran, China, and the Soviet Union).

64. *See id.* at 99–101 (outlining ways that authoritarian governments can censor internet information, including using hyperlinks and aggregation).

65. *See* Erica Frantz et. al., *Digital Repression in Autocracies* 1–5 (Varieties of Democracy Inst., Working Paper No. 27, 2020), https://perma.cc/6U5D-G58F (PDF) (defining digital repression and identifying the tools employed by governments engaging in it).

66. *See* Steven Feldstein, *The Road to Digital Unfreedom: How Artificial Intelligence Is Reshaping Repression*, 30 J. DEMOCRACY 40, 41 (2019) (arguing that AI technology and computer systems have provided autocracies with substantially more political control over constituents).

67. *See id.* at 42 ("Because of this omnipresence, [AI systems] can induce changes in behavior and create a significant 'chilling effect' even in the absence of sustained physical violence.").

68. *See id.* (asserting that AI systems motivate the public to conform and avoid sending dissentious messages against the government).

69. *See, e.g.*, Scott Shane, *How Unwitting Americans Encountered Russian Operatives Online*, N.Y. TIMES (Feb. 18, 2018), https://perma.cc/6L7C-

States have always repressed.[70] Even democracies, particularly those democracies under threat,[71] have used surveillance and sometimes physical repression against their own citizens.[72] Repressive tactics include the violation of physical integrity rights, such as harassment, detainment, torture,[73] and extrajudicial killings,[74] as well as covert repression through monitoring and surveilling which can include wiretapping, organizational infiltration, and the use of informants and agents provocateur.[75] Repression in all forms is

KAKZ (recounting the Russian operators who created phony Heart of Texas and Blacktivist groups and announced rallies to interfere with the 2016 election).

70. *See* Christian Davenport, *State Repression and Political Order*, 10 ANN. REV. POL. SCI. 1, 1 (Margaret Levi et al. eds., 2007) (proposing that repression is as old as "the founding of the nation-state"); *see also* ROBERT JUSTIN GOLDSTEIN, POLITICAL REPRESSION IN MODERN AMERICA FROM 1870 TO THE PRESENT 547 (1978) ("Political repression has been an important and neglected factor in shaping major aspects of American political development since 1870.").

71. *See* Rudolph Rummel, *Democracy, Power, Genocide, and Mass Murder*, 39 J. CONFLICT RES. 3, 3 (1995) (articulating that governments, themselves, commit democide and repress their citizens).

72. *See generally* CHRISTIAN DAVENPORT, STATE REPRESSION AND THE DOMESTIC DEMOCRATIC PEACE (2007) (discussing the repressive practices of the then Hutu-led government); *see also* Courtenay Conrad et al., *Torture and the Limits of Democratic Institutions*, 55 J. PEACE RSCH. 3, 4 (2018) (highlighting the approval of executives in democratic nations that engage in torture and repression).

73. *See* DARIUS REJALI, TORTURE AND DEMOCRACY 1–3 (2007) (arguing that there are physical forms of torture but also silent torture tactics that generally go unnoticed).

74. *See* Matthew Krain, *State-Sponsored Mass Murder: The Onset and Severity of Genocides and Politicides*, 41 J. CONFLICT RESOL. 331, 332 (1997) (asserting that the internal and external characteristics of a state influence the degree of genocide and politicide therein); *see generally* MANUS I. MIDLARSKY, THE KILLING TRAP: GENOCIDE IN THE TWENTIETH CENTURY (2005) (offering a comparative analysis of genocides, politicides, and ethnic cleansings); BENJAMIN A. VALENTINO, FINAL SOLUTIONS: MASS KILLING AND GENOCIDE IN THE 20TH CENTURY (Robert J. Art et al. eds., 2004) (discussing mass killings).

75. *See* Christian Davenport, *Understanding Covert Repressive Action: The Case of the U.S. Government Against the Republic of New Africa*, 49 J. CONFLICT RESOL. 120, 122 (2005) (describing the numerous covert techniques that nations can use to learn about its constituents, the information spread therein, and the social movements taking hold).

costly for the state, and its citizens.[76] 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.[77] States choose to incur these costs when they are under (real or perceived) threat, which may be created or reinforced through disinformation.[78]

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.[79] Rather than offering the liberating potential originally associated with these technologies,[80] many are now arguing that "social media [is] driving the spread of authoritarian practices."[81] Examples of this phenomenon include the Arab Spring, as well as more recent conflicts across the Middle East, and beyond.[82]

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.[83] As Ron Deibert and Rafal Rohozinski write, "[d]igital information

76. *See* Davenport, *supra* note 70, at 4 (exploring the costs associated with repression and the cost-benefit analysis employed by repressive leaders).

77. *See id.* at 10 (noting that democratic nations have increased costs associated with repressive action because officials are held accountable through the electoral process).

78. *See* DAVENPORT, *supra* note 72, at 2 (discussing the Hutu- and Tutsi-led governments' repressive tactics).

79. *See* Ronald J. Deibert, *Three Painful Truths About Social Media*, 30 J. DEMOCRACY 25, 31 (2019) (arguing that social media enables authoritarianism).

80. *See* Larry Diamond, *Liberation Technology*, 21 J. DEMOCRACY 69, 70 (2010) (examining social media as a tool for activists to organize against authoritarianism).

81. Deibert, *supra* note 79, at 31.

82. *See, e.g.*, Caroline Caywood, *This Is How Social Media Is Being Used in the Middle East*, NAT'L INT. (Nov. 21, 2018), https://perma.cc/96LF-8258 ("Governments are using social media to rally domestic and foreign support for their policies.").

83. *See* Ronald Deibert & Rafal Rohozinski, *Liberation vs. Control: The Future of Cyberspace*, 21 J. DEMOCRACY 43, 43 (2010) (noting that no technology other than digital technology has "grown with such speed and spread so far geographically in such a short period of time").

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."[84] 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.[85]

Second, the nature of repressive technologies has shifted the capacity required for repression which in turn has shifted the costs. As outlined above, repression is costly.[86] It carries the physical costs associated with maintaining a repressive apparatus (e.g., training and paying soldiers and police, maintaining detention facilities, etc.).[87] In the past, mass surveillance required an extensive network of informers.[88] 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.[89] New technologies produce the same level of surveillance or greater from far fewer people.[90] Such digital

84. *Id*. at 44.

85. *See* Feldstein, *supra* note 66, at 44 (noting that governments can use AI to control protests).

86. *See supra* notes 76–78 and accompanying text.

87. *See* Feldstein, *supra* note 66, at 43 ("[Autocrats] relying on security forces to repress their citizenry . . . entails . . . resource costs and political risk.").

88. *See, e.g.*, Andreas Lichter et al., *The Long-Term Costs of Government Surveillance: Insights from Stasi Spying in East Germany* 2 (SOEPpapers, Working Paper No. 865, 2016), https://perma.cc/3DDH-2BRX (PDF) (stating that the number of informants relied on by East Germany's *Stasi* secret police "accounted for more than one percent of the East German population in the 1980s").

89. *See* Matthew Day, *Polish Secret Police: How and Why the Poles Spied on Their Own People*, TELEGRAPH (Oct. 18, 2011, 7:00 AM), https://perma.cc/C88T-MKS6 (describing how the *Sluzba Bezpieczenstwa* "was at the forefront of the Polish authoritarian state's long war against opposition to communist rule").

90. *See* Feldstein, *supra* note 66, at 42 ("[T]he most advanced surveillance operations rely on relatively few human agents: Many functions are instead automated through AI.").

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.[91] 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.[92]

Steven Feldstein attributes the 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.[93] As Feldstein writes, "[f]rom 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."[94] 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.[95]

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 based on internal pressure and mass

91. *See* Josh Chin & Clément Bürge, *Twelve Days in Xinjiang: How China's Surveillance State Overwhelms Daily Life*, WALL ST. J. (Dec. 19, 2017, 10:58 PM), https://perma.cc/SM8E-QG8B ("China's efforts to snuff out a violent separatist movement . . . have turned the autonomous region of Xinjiang . . . into a laboratory for high-tech social controls that civil-liberties activists say the government wants to roll out across the country.").

92. *See* Feldstein, *supra* note 66, at 45–46 (discussing the budget for "security-related investment projects").

93. *Id.* at 41.

94. *Id.*

95. *See* Larry Diamond, *The Threat of Postmodern Totalitarianism*, 20 J. DEMOCRACY 20, 23 (2019) (comparing this reality to "a nightmarish modern-day version of *Nineteen Eighty-Four*").

public uprisings.[96] 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."[97] Such observations might explain Vladimir Putin's response to the December 2011 protests in Russia,[98] along with the color revolutions,[99] and Arab Spring.[100] These new trends in leadership removal increase the incentives for leaders to pursue repressive tactics capable of monitoring public opinion and mobilization potential.[101]

As is discussed further in Parts III and IV, the target of digital repression need not solely be a country's own citizens. Surveillance, state-sponsored hacks, election interference, and misinformation campaigns have all been documented strategies of autocratic governments' attempts at destabilizing rivals and undermining democracy globally.[102] In addition to challenging the functioning of democratic governments, there have also been attempts to change the behavior of non-state actors in pursuit

96. *See* Feldstein, *supra* note 66, at 43 (stating that popular revolt and electoral defeat "have overtaken coups" as "the most common causes of departure for dictators").

97. *Id*.

98. *See* Michael Crowley, *Why Putin Hates Hillary*, POLITICO (July 25, 2016, 6:20 PM), https://perma.cc/2WVT-KW98 (stating Putin blamed Hillary Clinton for rigging Russian elections and causing the protests).

99. *See* Yulia Nikitina, *The "Color Revolutions" and "Arab Spring" in Russian Official Discourse*, 14 CONNECTIONS 87, 88 (2014) (stating the "main concern" with the color revolution is that problems are not being resolved through the constitution or existing laws, but instead through "revolutions" and "street democracy.").

100. *See id*. at 92–93 (discussing Putin's negative reaction to Western intervention of parties involved in the Arab Spring).

101. *See* Feldstein, *supra* note 66, at 43 ("[A]utocratic leaders are embracing digital tactics for monitoring, surveilling, and harassing civil society movements and for distorting elections.").

102. *See* Charles Marsh, *How Autocratic Regimes Try to Undermine Democracy at Home and Abroad*, DEMOCRACY WITHOUT BORDERS (Dec. 17, 2017), https://perma.cc/U9SJ-HBHP (summarizing recent research on autocrats' attempts to weaken democracy using, among other tactics, "internet censorship and controlled narratives").

of a global liberal agenda, such as human rights NGOs.[103] Moreover, while the focus of this Article is mainly on digital influence from Russia and China, the nature of digital technologies is impacting which states have the ability to monitor and repress.[104] As the financial and material costs of digital repression decrease, the capacity to influence is no longer confined to global powers.[105] Finally, much like repression itself, digital repression is not and will not be confined to autocratic regimes. Democracies monitor, surveille, and repress their own citizens, particularly in times of threat.[106] 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, which we turn to next.

III. U.S. Efforts to Protect Democratic Institutions

When adversaries interfere with elections, they threaten more than the integrity of electoral process, they threaten collective faith in democracy. Indeed, a core focus of the Russian strategy to undermine confidence in the 2016 U.S. presidential election was not necessarily to target voting machines directly,

---

103. *See, e.g.*, Bill Marczak et al., *Missing Link: Tibetan Groups Targeted with 1-Click Mobile Exploits* (Citizen Lab 2019), https://perma.cc/R8XL-CQCS ("[S]enior members of Tibetan groups received malicious links in individually tailored WhatsApp text exchanges with operators posing as NGO workers, journalists, and other fake personas."); JOHN SCOTT-RAILTON ET AL., RECKLESS VII: WIFE OF JOURNALIST SLAIN IN CARTEL-LINKED KILLING TARGETED WITH NSO GROUP'S SPYWARE 8–9 (2019), https://perma.cc/X8B6-9SPJ (PDF) (describing NSO Group's attempts to target various non-state actors, including journalists, lawyers, and anti-corruption activists).

104. *See* Adrian Shahbaz, *The Rise of Digital Authoritarianism*, *in* FREEDOM HOUSE, FREEDOM ON THE NET 2018, 1 (2018), https://perma.cc/53HC-C7EK (PDF) ("[A] cohort of countries is moving toward digital authoritarianism by embracing the Chinese model of extensive censorship and automated surveillance systems.").

105. *See id.* at 9 (listing countries, such as Rwanda, Bahrain, and Kazakhstan, that use telecommunications infrastructure, AI surveillance, and trainings in a similar way as China).

106. *See* GOLDSTEIN, *supra* note 70, at 559 ("[I]ncreased strain and tension in society and increased dissent (which frequently, but not always, occur together) have been the most important causes of political authorities increasing political repression.").

but instead to use low-cost techniques through social media and otherwise to "undermine and distract the Clinton campaign," which would, to Russia's delight, result in a benefit to Donald Trump's campaign.[107] This is why so many state and private actors have taken action in response to Russia's "sweeping and systematic" interference in both U.S. and European elections, and why it is so surprising that the U.S. federal government did not take more comprehensive and decisive action to counter this ongoing threat ahead of the 2020 election cycle.[108] This section summarizes attempts within the U.S.'s public and private sectors to improve election security. It concludes by identifying particular weaknesses in the overall U.S. response to date, while Part V offers a series of steps for how to fill these governance gaps.

A. U.S. Efforts to Safeguard its Election Infrastructure

This section begins by discussing federal and state protections for voting infrastructure. We next move on to analyze companion efforts from civil society and the private sector. After that, we explore U.S. efforts to combat digital repression and then offer several critiques of U.S. efforts to make democracy harder to hack.

1. Federal & State Approaches to Election Security

In the United States, elections are primarily administered by the states.[109] Unlike other countries with federal governments, such as Australia explored in Part IV, the U.S. federal government has historically played a minimal role in

107. Eric Geller, *Collusion Aside, Mueller Found Abundant Evidence of Russian Election Plot*, POLITICO (Apr. 18, 2019, 12:35 PM), https://perma.cc/L3S3-9CJZ.

108. *See* U.S. DEP'T OF JUST., OFF. OF SPECIAL COUNS., REPORT ON THE INVESTIGATION INTO RUSSIAN INTERFERENCE IN THE 2016 PRESIDENTIAL ELECTION 1 (2019) [hereinafter MUELLER REPORT], https://perma.cc/QBB3-QGF4 (PDF) ("The Russian government interfered in the 2016 presidential election in sweeping and systematic fashion.").

109. *See Elections & Voting*, WHITE HOUSE, https://perma.cc/T7TU-24MA (stating that the federal government "grant[s] the states wide latitude in how they administer elections").

election oversight.[110] Yet, as the Congressional Research Service has noted, "the federal government . . . has steadily increased its presence in campaigns and elections in the past fifty years. Altogether, dozens of congressional committees and federal agencies could be involved in federal elections under current law."[111] As a result, there is a patchwork of voting systems throughout the country, with many states—including core swing states like Pennsylvania—using outdated voting machines and, as of August 2019, more than ten using paperless ballots, which leave no paper trail preventing an effective post-election audit in the aftermath of a cyber-attack.[112] While the federal government can regulate aspects of federal voting and appropriate funds for state voting systems[113] along with, of course, providing for the common defense,[114] the political response at the federal level can, as of this writing, at best be described as apathetic to election security concerns.[115]

---

110. *See* R. SAM GARRETT, CONG. RSCH. SERV., R45302, FEDERAL ROLE IN U.S. CAMPAIGNS AND ELECTIONS: AN OVERVIEW i (2018) https://perma.cc/3LYE-2SBT (PDF) ("Conventional wisdom holds that the federal government plays [a] relatively little role in U.S. campaigns and elections.").

111. *Id.*

112. *See* Tim Lau, *U.S. Elections Are Still Vulnerable to Foreign Hacking*, BRENNAN CTR. FOR JUST. (July 18, 2019), https://perma.cc/DGY8-WSVC ("Many states have outdated election security infrastructure . . . ."); CHRISTOPHER R. DELUZIO ET AL., DEFENDING ELECTIONS: FEDERAL FUNDING NEEDS FOR STATE ELECTION SECURITY 4 (2019), https://perma.cc/33FK-UF34 (PDF) ("Aging voting systems often use outdated hardware . . . .").

113. *See* Dylan Lynch & Wendy Underhill, *Election Security Cybersecurity: What Legislators (and Others) Need to Know*, NAT'L CONF. OF STATE LEGIS. (Feb. 4, 2019), https://perma.cc/HLJ4-F5MY (stating that the federal government acts "in an advisory role" to states focused on election security).

114. *See* U.S. CONST. art. I, § 8 ("The Congress shall have Power To . . . provide for the common Defence and general Welfare of the United States.").

115. *See* Li Zhou, *Republicans Are Still Blocking Election Security Bills After Mueller's Testimony*, VOX (July 25, 2019, 11:47 AM), https://perma.cc/42S7-UBHC (explaining that Republicans were blocking "Democratic efforts to put stronger election security restrictions in place"); Josh Dawsey et al., *As Security Officials Prepare for Russian Attack on 2020 Presidential Race, Trump and Aides Play Down Threat*, WASH. POST (Apr. 30, 2019, 8:21 AM), https://perma.cc/Q3CA-G45H ("During discussions in the Oval Office, Trump has regularly conflated the threat of foreign interference with attacks on the legitimacy of his election . . . .").

Congress did appropriate $380 million for state election security efforts after the 2016 election,[116] along with another $425 million in December 2019.[117] These are steps in the right direction, and are in line broadly with how much it would cost to replace paperless voting machines across the nation, and will allow more states to upgrade their voting equipment and conduct post-election audits.[118] Yet these appropriations did not stem from any authority created in the aftermath of the 2016 election.[119] Instead, these were part of a 2002 bill, the Help America Vote Act,[120] passed as a consequence of the contested presidential election between George W. Bush and Al Gore in 2000.[121] Multiple bills, some bipartisan, were subsequently proposed and passed by one of the two chambers of Congress, but thus far all have stalled.[122] In particular, the most widely reported on bill, the Election Security Act, would have pushed states to implement back-up paper ballots and would have provided $1 billion in election security grants for

116. *See* Press Release, U.S. Election Assistance Comm'n, U.S. Election Assistance Commission to Administer $380 Million in 2018 HAVA Election Security Funds (Mar. 29, 2018), https://perma.cc/2JSH-ZBA2; *see also* Blake Paterson & Ally J. Levine, *Fund Meant to Protect Elections May Be Too Little, Too Late*, PROPUBLICA (Aug. 21, 2018, 9:00 AM), https://perma.cc/YG9X-GAUP ("[Q]uestions remain about how much [the $380 million set aside for election infrastructure] will help secure the 2018 election.").

117. *See* Miles Parks, *Congress Allocates $425 Million for Election Security in New Legislation*, NAT'L PUB. RADIO (Dec. 16, 2019, 5:02 PM), https://perma.cc/28PC-GYBT.

118. *See* BRENNAN CTR. FOR JUST., ESTIMATE FOR THE COST OF REPLACING PAPERLESS, COMPUTERIZED VOTING MACHINES 1, https://perma.cc/5PHX-RABA (PDF) (estimating the cost would "range [from] $130 million to $400 million").

119. *See* GARRETT, *supra* note 110, at 8 (describing the Help America Vote Act of 2002).

120. Help America Vote Act of 2002, Pub. L. No. 252, 116 Stat. 1666.

121. *See* GARRETT, *supra* note 110, at 8 ("Congress enacted the Help America Vote Act (HAVA) in 2002, after the disputed 2000 presidential election raised concerns about election administration, ballot design, and voting equipment around the country.").

122. *See, e.g.*, Katherine Tully-McManus, *House Passes Election Security Measure Requiring Cybersecurity Safeguards, Paper Ballots*, ROLL CALL (Jun. 27, 2019, 4:49 PM), https://perma.cc/4HN6-63DX (noting that "an election security measure" passed by the House "faces stiff opposition from Republicans" in the Senate).

modernization.[123] However, Senate Majority Leader, Mitch McConnell, argued that such a bill would federalize the election process and take control away from states.[124]

The Senate Intelligence Committee released a report in 2019 on the 2016 election and provided recommendations for securing elections.[125] These recommendations—including the need for paper ballots—have yet to be implemented in any concerted way.[126] In addition, a widely disseminated report from the National Academies of Sciences, Engineering, and Medicine, entitled *Securing the Vote*, put together a series of recommendations, which included: election administrators "routinely assess[ing] the integrity of voter registration databases," ensuring backups for pollbooks should disruptions occur, conducting regular penetration testing, requiring paper ballots along with post-election audits and the removal of "[v]oting machines that do not provide the capacity for independent auditing," and empowering the National Institute for Standards and Technology (NIST) to "develop security standards and verification and validation protocols for electronic pollbooks in addition to the standards and verification and validation protocols they have developed for voting systems."[127] However, most of these recommendations have similarly not been acted upon as of this writing.[128]

---

123. *See* Maggie Miller, *2020 Democrats Accelerate Push for Action to Secure Elections*, HILL (June 30, 2019, 7:00 AM), https://perma.cc/79KU-S5JZ (describing the bill as a way to "strengthen cybersecurity information sharing and require all jurisdictions to perform post-election audits").

124. *See id.* (reporting McConnell's argument); *see also* Alex Padill, *What Do States Need to Secure Upcoming Elections?*, PBS NEWS HOUR (Aug. 2, 2018, 6:30 PM), https://perma.cc/2RXM-RGKR (asserting that election security should be viewed as a matter of national defense, to which $700 billion is dedicated each year).

125. S. REP. NO. 116-XX, at 54 (2019), https://perma.cc/5Q3Y-N78L (PDF).

126. *See* Dana Farrington, *READ: Senate Intelligence Report on Russian Interference in the 2016 Election*, NAT. PUB. RADIO (July 25, 2019, 3:08 PM), https://perma.cc/NY7Y-FK8M (stating "Congress has been slow to take action" on the report's recommendations).

127. SECURING THE VOTE, *supra* note 22, at 5–7.

128. *C.f.* Miller, *supra* note 123 (noting that as of June 2019, the year following the Securing the Vote report, a technology entrepreneur was still concerned about "foreign interference in elections").

As a matter of national defense, election security has received more attention at the federal level through agencies such as the Central Intelligence Agency, Department of Defense, Department of Homeland Security (DHS), National Security Agency, and Federal Bureau of Investigation.[129] Most notably, DHS designated the election infrastructure[130] as critical infrastructure.[131] This means that DHS can offer states resources and intelligence insights to ensure election security.[132] It does not mean, however, the same degree of regulatory oversight as is common in other jurisdictions, such as the European Union discussed in Part IV. Despite a multitude of efforts, the pains taken by various U.S. agencies and departments have been relatively ad hoc and siloed.[133] This is likely why the Director of National Intelligence established the position of Intelligence Community Election Threats Executive

129. *See* R. SAM GARRETT, CONG. RSCH. SERV., IF11265, CAMPAIGN AND ELECTION SECURITY POLICY: BRIEF INTRODUCTION 1–2 (2019) https://perma.cc/5QZ7-N2P4 (PDF) (discussing agency roles in election security).

130. "Election infrastructure" includes "storage facilities, polling places, and centralized vote tabulations locations used to support the election process, and information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and report and display results on behalf of state and local governments." Press Release, Jeh Johnson, Sec'y, Dep't of Homeland Sec., Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector (Jan. 6, 2017), https://perma.cc/LGD8-D5BJ; *see* Danielle Root et al., *Election Security in All 50 States: Defending America's Elections*, CTR. FOR AM. PROGRESS (Feb. 12, 2018, 12:01 AM), https://perma.cc/T9LE-DWDS (describing election infrastructure across the country).

131. *See* Johnson, *supra* note 130 ("Given the vital role elections play in this country, it has been determined that certain systems and assets of election infrastructure meet the definition of critical infrastructure.").

132. *See* Kaveh Waddell, *Why Elections Are Now Classified as 'Critical Infrastructure,'* ATLANTIC (Jan. 13, 2017), https://perma.cc/6GXU-GP6D ("[The classification] makes it easier for DHS to offer [state and local organizations] resources and intelligence information.").

133. *See* Julian E. Barnes, *Intelligence Chief Names New Election Security Oversight Official*, N.Y. TIMES (July 19, 2019), https://perma.cc/83TU-5CNU (noting that analysts viewed the intelligence community's increased focus on election security before the 2018 midterm races as rather impromptu).

(ETE) in July of 2019.[134] The goal of that position is to coordinate election security activities across the federal government.[135] Another useful step in this same vein has been the creation of Election Infrastructure Information Sharing and Analysis Center (EI-ISAC) to help share information about cyber threats and best practices with election agencies and other interested stakeholders.[136] But it is still unclear whether such coordination will ultimately address the problems associated with election insecurity in the United States, to say nothing of other vulnerable democracies.

At the state level, many state and local governments have organized and funded their own initiatives to improve election security in the absence of effective federal leadership.[137] For example, California created the Office of Elections Cybersecurity.[138] Virginia switched from paperless electronic voting to a statewide paper ballot system.[139] Colorado instituted a risk-limiting audit that is being emulated by other states.[140] Indiana passed a plan to phase out paperless voting machines

134. Press Release, Daniel R. Coats, Dir. of Nat'l Intelligence, Director of National Intelligence Daniel R. Coats Establishes Intelligence Community Election Threats Executive (July 19, 2019), https://perma.cc/V77W-AGS7.

135. *See id.* ("[T]he . . . Election Threats Executive (ETE) . . . will coordinate and integrate all election security activities, initiatives, and programs across the [Intelligence Community] and synchronize intelligence efforts in support of the broader U.S. government.").

136. *See Elections Infrastructure ISAC*, CTR. FOR INTERNET SEC., https://perma.cc/93ZZ-QUT7.

137. *See* Root et al., *supra* note 130 (describing New York's new election security initiative, among others).

138. *See* Sara Friedman, *California Creates Elections Security Office*, GCN (Aug. 31, 2018), https://perma.cc/6635-PH67 (reporting on the new organization).

139. *See* Root et al., *supra* note 130 (describing Virginia's switch to a paper ballot system).

140. *See* Jesse Paul, *Colorado's First-of-its-Kind Election Audit Is Complete, with All Participating Counties Passing*, DENVER POST (Nov. 22, 2017, 1:59 PM), https://perma.cc/D6RK-P5DF (stating the process involves the "manual recount of a sample of ballots from the more than 50 counties that had elections this year and compar[ing] them with how they were interpreted by tabulating machines").

fully by 2029.[141] In total, as of this writing at least thirty-six states have made efforts to improve and are working with DHS or the National Guard to assess and identify voting systems.[142] However, wait times for help, especially with DHS, are reportedly very long (up to nine months), and with state and local elections happening multiple times per year, it is likely that vulnerabilities will go unaddressed for several more election cycles.[143]

2. Private Sector & Civil Society Efforts

In the United States (and unlike Australia, as we will see), election security has very deep ties with the private sector and is a topic watched closely, but largely passively, by civil society organizations and academia.[144] The private sector plays such a strong role because voting machines are manufactured without direct government involvement and are only subject to *ex post* testing.[145] Thus, among the first lines of defense of election infrastructure security lies primarily in the hands of private voting machine manufacturers, who despite the various stress tests required by many states, produce equipment that may still

141. *See* Tom Davies, *Indiana Election Upgrade Leaves Widespread Paperless Voting*, ASSOCIATED PRESS (Sept. 27, 2019), https://perma.cc/79GS-JBNK (noting that paperless voting machines are not prohibited until 2029).

142. *See* Root et al., *supra* note 130 (explaining that those states are working with federal entities in "assessing and identifying potential threats to voter registration systems").

143. *See* Tim Starks, *The Latest 2018 Election-Hacking Threat: 9-Month Wait for Government Help*, POLITICO (Dec. 29, 2017, 5:05 AM), https://perma.cc/RRY9-UGJD ("[S]ome states might not get the service until weeks before the November midterms and may remain unaware of flaws that could allow homegrown cyber vandals or foreign intelligence agencies to target voter registration databases and election offices' computer networks . . . .").

144. *See* Joseph Marks, *The Cybersecurity 202: Even a Voting Machine Company Is Pushing for Election Security Legislation*, WASH. POST (June 10, 2019, 7:13 AM), https://perma.cc/PU7B-V2PJ (noting that because one company's "commitment to third-party testing is entirely voluntary, it also gets to say who those third-party testers are").

145. *See id.* (reporting that the company urged Congress to pass legislation that would "mandate security testing of voting equipment by outside researchers"); Tim Starks, *Voting Machine Vendors Under Pressure*, POLITICO (July 12, 2018, 10:00 AM), https://perma.cc/LE5U-KQWG (stating that voting machine vendors sell electronic voting machines without paper backups).

contain vulnerabilities that can go undetected.[146] While manufacturers have taken steps to boost election infrastructure security, such as by refusing to sell paperless machines to those jurisdictions that do not have paper voting machines as their primary machines, machines continue to be in operation without any serious recall regime in place and there are no legal obligations to notify election officials when vulnerabilities and breaches are detected.[147] "I know America's voting machines are vulnerable," said J. Alex Halderman during Congressional testimony, "because my colleagues and I have hacked them—repeatedly—as part of a decade of research studying the technology that operates elections and learning how to make it stronger."[148] He has gone on to argue: "Our highly computerized election infrastructure is vulnerable to sabotage and even to cyberattacks that could change votes."[149]

Halderman demonstrated, for example, how a mock contest between George Washington and Benedict Arnold could be won by the latter, simply by infecting a voting machine's memory with malware.[150] The vulnerabilities that Halderman and his group have exploited include not only outdated voting machines, but also election-management systems that design ballots, which election officials often access via memory cards that may

146. For a list of standards and tests required of voting machines, see *Voting System Standards, Testing and Certification*, NAT'L CONF. OF STATE LEGIS. (Aug. 6, 2018), https://perma.cc/4JHL-V3VG.

147. *See* Lily Hay Newman, *Election Security Is Still Hurting at Every Level*, WIRED (June 6, 2019, 12:01 AM), [hereinafter Newman I] https://perma.cc/H8XC-QHHR (quoting the president of Verified Voting, as saying that "I don't think the for-profit commercial model works particularly well for voting systems, because there's not enough profit in them to do really good R&D").

148. Steve Freiss, *Hacking the Vote: It's Easier Than You Think*, MICH. ALUMNI ASS'N, https://perma.cc/J9QA-D6SX.

149. Alexander Freund, *Democracy in Danger: Elections are Easy to Manipulate*, DEUTSCHE WELLE (Oct. 16, 2018), https://perma.cc/7Q63-LXBG.

150. *See* Jen Schwartz, *The Vulnerabilities of Our Voting Machines*, SCI. AM. (Nov. 1, 2018), https://perma.cc/GP64-2MHX ("[W]ithout a paper trail of each vote, neither the voters nor a human auditor could check for discrepancies. In real elections, too, about 20 percent of voters nationally still cast electronic ballots only.").

be corrupted.[151] Other cybersecurity researchers have corroborated these findings, including those affiliated with the Defcon hacker conference, and found numerous vulnerabilities in many voting machines still in use across more than twenty-six states in 2019.[152]

Within civil society and academia, numerous comprehensive reports on election security have been written exploring what to do about these problems.[153] The most notable of these publications include the National Academies of Sciences' *Securing the Vote* mentioned above; the Brennan Center for Justice at New York University School of Law's *Defending Elections*; and the Center for American Progress's *Election Security in All 50 States*.[154] However, once again, because of political stagnation, there has been very little implementation of their policy proposals.[155] As for active participation in election security, some universities play a role in certifying and testing voting machines, but this role is limited.[156]

B. U.S. Attempts to Combat Digital Repression

Unlike the tentative steps that have been taken to protect U.S. election infrastructure, the U.S. government's response to misinformation remains nascent, which is in part due to demanding requirements of the First Amendment and deep

151. *See id.* (discussing how malicious code can be introduced to the election-management systems).

152. *See* Lily Hay Newman, *Some Voting Machines Still Have Decade-Old Vulnerabilities*, WIRED (Sept. 26, 2019, 2:41 PM), https://perma.cc/S6E7-L38X [hereinafter Newman II] (highlighting "detailed vulnerability findings related to six models of voting machines" including one model "used in 28 states in 2018" and another model "used in 26 states that same year").

153. *See, e.g.*, SECURING THE VOTE, *supra* note 22, at xii (outlining numerous recommendations "designed to harden our election infrastructure and safeguard its integrity and credibility").

154. *See generally id.*; DELUZIO, *supra* note 112; Root, *supra* note 130.

155. *See supra* notes 115–143 and accompanying text.

156. *See, e.g.*, CONN. GEN. STAT. ANN. § 9-241(b) (West 2020) (allowing Connecticut's Secretary of State to enter into agreements with universities to assist with ensuring the integrity of voting equipment); *see also* IND. CODE. ANN. § 3-11-16-4 (West 2020) (allowing Indiana election officials to work with universities to perform audits and assist with certifications).

divisions about the proper role of the federal government in policing content.[157] There are, however, a patchwork of state laws aimed at combatting the effects of misinformation.[158] One example is a California law that requires the state's Department of Education to provide a list of education materials on its websites to teach students how to distinguish misinformation from real news and advertisements.[159] The impetus behind the law was a Stanford University study,[160] which found that 82 percent of middle school students could not distinguish between advertisements and news stories.[161] Other states have followed suit, by including more programming related to misinformation and disinformation in their educational programming.[162]

Congress has unsuccessfully tried to pass the Honest Ads Act,[163] a bill that requires platform political ads to follow the same rules as the Federal Election Campaign Act of 1971, such

157. *See* Sara Prendergast, *It Must be True, I Read It on the Internet: Regulating Fake News in the Digital Age*, MICH. TECH. L. REV. (Mar. 4, 2019), https://perma.cc/8UYS-ULF2 (discussing the hesitancy of the United States to combat misinformation); John Samples, *Why the Government Should Not Regulate Content Moderation of Social Media*, CATO INST. (Apr. 9, 2019), https://perma.cc/E5DP-RK8T (noting that a California bill aimed at reducing the spread of misinformation on social media through the creation of an advisory board was vetoed by former Governor Jerry Brown, citing First Amendment concerns).

158. *See* Funke & Flamini, *supra* note 28 (listing state actions).

159. *See* CAL. EDUC. CODE § 51206.4 (West 2020) (ordering California's Department of Education to provide a list of resources on media literacy); *see also* Funke & Flamini, *supra* note 28 (noting that California is one of a few states to enact legislation promoting media literacy); Susan Minichiello, *California Now Has a Law to Bolster Media Literacy in Schools*, PRESS DEMOCRAT (Sept. 18, 2018), https://perma.cc/7VBR-RSKW (reporting that Gov. Jerry Brown signed the bill to encourage media literacy).

160. *See* Minichiello, *supra* note 159 (discussing the bill's origins).

161. *See* SAM WINEBURG ET AL., EVALUATING INFORMATION: THE CORNERSTONE OF CIVIC ONLINE REASONING 10 (2016), https://perma.cc/FC3T-9VQ6 (PDF) ("More than 80% of students believed that the [fake] advertisement . . . was a real news story.").

162. *See* Funke & Flamini, *supra* note 28 (stating that at least twenty-four states are attempting to improve media literacy).

163. S. 1989, 115th Cong. (2017).

as identifying the organization or person sponsoring the ad.[164] In addition, the Act would require platforms to engage in "reasonable efforts" to ensure that ads are not purchased "directly or indirectly" by foreign governments.[165] Major tech companies have strongly opposed such a bill, arguing instead for self-regulation.[166] Some, such as Twitter, have come out with new limits—and even bans—on political ads on their platforms due, in part, to concerns over enabling the spread of misinformation,[167] but as of this writing Facebook has not followed suit.[168]

C. Critiques of U.S. Response

While there are many efforts afoot within the public and private sectors to improve the security of U.S. election infrastructure and combat digital repression, as the foregoing analysis made clear there remains a great deal to be done. Consider the work done at Defcon since 2017 that was referenced above.[169] Defcon is the world's largest "white hat"

---

164. *See id.* (requiring advertisement sponsors to provide their name, address, phone number, etc.); *see also* Tim Lau, *The Honest Ads Act Explained*, BRENNAN CTR. FOR JUST. (Jan. 17, 2020) https://perma.cc/G56T-HJH8 (noting that the Honest Ads Act is still a proposed law before the United States Senate).

165. Honest Ads Act, S. 1989, 115th Cong.; *see* Natasha Bertrand, *Senators Have a New Plan to Fix a Major Loophole that Let Russia Take Advantage of Facebook and Tech Giants*, BUS. INSIDER (Oct. 19, 2017), https://perma.cc/VF2B-7H3A (stating that the Act's requirements are a departure from the Federal Election Campaign Act of 1971).

166. *See* Ben Brody & Bill Allison, *Lobbying Group for Facebook and Google to Pitch Self-Regulation of Ads*, BLOOMBERG (Oct. 23, 2017, 8:49 PM), https://perma.cc/3VRB-VCFR ("[G]oogle, Facebook, and Twitter . . . pitch self-regulation instead of a proposed federal law requiring more disclosure for political advertising on their online platforms . . . .").

167. *See* Kate Conger, *Twitter Will Ban All Political Ads, C.E.O. Jack Dorsey Says*, N.Y. TIMES (Oct. 30, 2019), https://perma.cc/Q2L3-T6XG ("Twitter announce[d] that it would eliminate political ads, starting Nov. 22, [2019].").

168. *See* Danielle Abril, *Google and Twitter Changed Their Rules on Political Ads. Why Won't Facebook?*, FORTUNE (Nov. 22, 2019), ("Despite a recent political ad ban from Twitter and new limitations from Google, Facebook has yet to back down from its 'anything goes' policy.").

169. *See supra* note 152 and accompanying text.

hacker conference, and it reports out the numerous ways its participants have been able to hack into U.S. voting machines annually.[170] In its 2018 report, conference participants found, among other vulnerabilities, that: (1) a tabulator used by twenty-three states could be hacked via a network attack; (2) a machine used in eighteen states was able to be hacked within two minutes, which is remarkable considering that it takes the average voter six minutes to vote; and (3) hackers had the ability to wirelessly reprogram an electronic card used by many Americans to activate the voting terminal.[171] The latter issue would allow a single voter to cast multiple ballots in a given voting session.[172] As Senator Ron Wyden said at Defcon in 2019, "Election officials across the country as we speak are buying election systems that will be out of date the moment they open the box."[173] He added: "[This is] the election security equivalent of putting our military out there to go up against superpowers with a peashooter."[174]

The vulnerabilities exposed at Defcon stem from the lack of comprehensive federal and state oversight discussed above. Leaving voting machine hardware and software to the private

170. *See* Taylor Telford, *Hackers Were Told to Break into U.S. Voting Machines. They Didn't Have Much Trouble.*, WASH. POST (Aug. 12, 2019), https://perma.cc/T85A-YCKJ (reporting on a conference that involves skilled hackers attempting to break into U.S. voting machines)*; see generally* MATT BLAZE ET AL., DEF CON 26 VOTING VILLAGE: REPORT ON CYBER VULNERABILITIES IN U.S. ELECTION EQUIPMENT, DATABASES, AND INFRASTRUCTURE (2018), https://perma.cc/H7F8-LCV4 (PDF) [hereinafter DEFCON 2018] (reporting the findings of the Voting Village in 2018); MATT BLAZE ET AL., DEF CON 25 VOTING MACHINE HACKING VILLAGE: REPORT ON CYBER VULNERABILITIES IN U.S. ELECTION EQUIPMENT, DATABASES, AND INFRASTRUCTURE (2017), https://perma.cc/5Y83-ZLWV (PDF) [hereinafter DEFCON 2017] (discussing the findings from the 2017 Voting Village).

171. *See* DEFCON 2018, *supra* note 170, at 5 (noting various vulnerabilities in the U.S. voting process); *see also* Lily Hay Newman, *Voting Machines Are Still Absurdly Vulnerable to Attacks*, WIRED (Sept. 28, 2018, 11:04 AM), https://perma.cc/K3HW-CA82 [hereinafter Newman III] ("Many of the weaknesses Voting Village participants found were frustratingly basic, underscoring the need for a reckoning with manufacturers.").

172. *See* DEFCON 2018, *supra* note 170, at 21 (explaining the vulnerabilities).

173. Telford, *supra* note 170.

174. *Id*.

sector without adequate regulatory oversight is insufficient to protect election security.[175] Moreover, the failure of effective federal oversight has meant a greater burden on state and local officials, who often do not have the expertise necessary to compare and assess the quality of voting systems when making purchasing decisions.[176] Some with the means and will, such as Los Angeles, with its $300 million Voting Solutions for All People program, have taken it upon themselves to make major investments in new technology and practices, but these are outliers.[177] Furthermore, many state and local governments remain insufficiently trained to respond to cybersecurity threats[178] and still more jurisdictions are using voter databases that are over a decade old—a lifetime in tech terms.[179] The continued weakness of the U.S. response leaves election security a "significant counterintelligence threat,"[180] which adversaries may continue to exploit, along with abusing social media firms with lax policies to combat digital repression.[181]

The United States is not alone in facing these vulnerabilities, though. Both advanced and emerging democracies around the world are similarly grappling with how

175. *See* Newman III, *supra* note 171 (detailing the "nation's vulnerable election infrastructure").

176. *See* Newman II, *supra* note 152 ("[W]e're still using antiquated equipment that should be replaced, both for security and reliability reasons . . . [which] is one reason why Congress and the states need to step up on election security spending." (quoting the deputy director of Brennan Center's Democracy Program)).

177. *See* Matt Stiles, *Sweeping Change Is Coming for L.A. County Voters. If Things Go Wrong, He'll Get the Blame*, L.A. TIMES (Aug. 19, 2019), https://perma.cc/27GC-NK42 (PDF) (stating that major investments into better election technology is rare).

178. *See* Elizabeth Warren, *My Plan to Strengthen Our Democracy*, MEDIUM (June 25, 2019), https://perma.cc/WK9T-PDQ7 (noting that a number of states do not train election officials to deal with cyber security threats).

179. *See id.* ("Forty-two states use voter registration databases that are more than a decade old.").

180. Julian E. Barnes & Adam Goldman, *F.B.I. Warns of Russian Interference in 2020 Race and Boosts Counterintelligence Operations*, N.Y. TIMES (Apr. 26, 2019), https://perma.cc/AXD3-TRDN (quoting FBI Director Christopher Wray).

181. *See id.* (citing weak social media policies as a contributor to mass misinformation).

best to enhance the security and integrity of their own elections and democratic societies. Part IV focuses on some of these efforts, notably from the European Union, Asia, Australia, and Oceania. Implications for policymakers stemming from this analysis are explored in Part V.

IV. Lessons from Other Democracies

Aside from the United States, other advanced and emerging democracies around the world are working to manage threats to their own election security, as well as creating strategies to manage digital repression and disinformation. These efforts form only one component of a larger debate happening around enhancing cybersecurity, which in turn suffers from a lack of clear definition. According to former General Michael Hayden, for example, "rarely has something been so important and so talked about with less clarity and less apparent understanding [than cybersecurity]."[182] This Part surveys some of these efforts to help provide a framework for discussion in Part V, which in turn considers a range of potential reforms to help make democracy harder to hack.

A. European Union

This section begins by discussing EU protections for voting infrastructure. We next move on to analyze companion efforts from civil society, and the private sector.

182. Michael V. Hayden, *The Future of Things Cyber*, 5 STRATEGIC STUD. Q. 3, 3 (2011); *see* Karen O'Donoghue, *Some Perspectives on Cybersecurity*, INTERNET SOC'Y (Nov. 12, 2012), https://perma.cc/49V2-L5SW (noting that the Internet Society maintains that "as a catchword, cybersecurity is frighteningly inexact and can stand for an almost endless list of different security concerns, technical challenges, and 'solutions' ranging from the technical to the legislative").

1. EU Efforts to Safeguard its Election Infrastructure

Europeans went to the polls in 2019 for the first time in five years for widely anticipated elections.[183] Cybersecurity was a key concern going into the summer after a series of high-profile breaches and disinformation campaigns.[184] For example, electoral websites in the Netherlands were targeted by denial-of-service (DoS) attacks in 2017,[185] as was the elections oversight body in Bulgaria and the Czech Republic.[186] Evidence is mounting as well of manipulation of the 2016 Brexit debate through the use of Facebook data.[187] As revealed by whistleblower Christopher Wylie at a hearing in the European Parliament, it is "almost certain that systematic fraud and voter deception took place . . . [and that] Facebook's system allowed it to happen."[188] Other recent examples include the release of thousands of internal documents of then French presidential candidate Emmanuel Macron prior to his 2017 election victory.[189] However, unlike the DNC hack of 2016, this breach did not have a major impact on the French elections given that: (1) French media were prohibited from reporting on the breach within forty-four hours of the election; (2) the lack of a "thriving tabloid culture" in France as in the UK, or the equivalent of a Fox News Network; and (3) the actions of the Macron campaign

183. *See* John Borland, *As Europe Went to the Polls, Cyber Election Efforts Paid Off*, SYMANTEC (June 5, 2019), https://perma.cc/96WB-8NME (stating that the election hacks of 2016 contributed to the anticipation of the election cycle).

184. *See id.* (noting that Europe had a prodigious focus on cybersecurity during the election cycle).

185. *See id.*

186. *See id.*

187. *See, e.g.*, Jane Mayer, *New Evidence Emerges of Steve Bannon and Cambridge Analytica's Role in Brexit*, NEW YORKER (Nov. 17, 2018), https://perma.cc/NM8N-Y6RA (citing evidence of Facebook data being used to interfere with Brexit debate).

188. Freund, *supra* note 149.

189. *See* Andy Greenberg, *Hackers Hit Macron with Huge Email Leak Ahead of French Election*, WIRED (May 5, 2017), https://perma.cc/9UGY-97K7 (describing the "data dump" that occurred less than forty hours before France's election).

in releasing faked documents to mislead the attackers.[190] There have also been spear phishing campaigns aimed at "German Chancellor Angela Merkel's Christian Democratic Union" party,[191] along with successful cyber-attacks on the German parliament (Bundestag),[192] and its federal data network.[193] In those attacks, the hackers had worked their way so deep into the system that the entire Bundestag IT architecture had to be rebuilt.[194] The breadth of these attacks remind us that a multifaceted approach is essential to the issues associated with influence, repression, and manipulation.

To its credit, the European Union has taken a more proactive approach to managing the full range of cyber-enabled threats facing the integrity of its democratic systems including both election security and disinformation than the United States has managed to date. First, most EU nations have minimized the use of technology in elections, with the Netherlands rejecting the use of electronic voting machines (EVMs) entirely,[195] France backing away from the use of online voting after 2016,[196] and Germany stopping the use of EVMs due to a court order in 2005,[197] just to name a few national actions. Among the more important of these is the Network Information Security (NIS) Directive, which was adopted by the European

190. *See* Rachel Donadio, *Why the Macron Hacking Attack Landed with a Thud in France*, N.Y. TIMES (May 8, 2017), https://perma.cc/425H-VQXE (explaining the "bereft coverage" of the hack).

191. Borland, *supra* note 183.

192. *See Hack on German Government Network 'Ongoing*,' DEUTSCHE WELLE (Jan. 3, 2018), https://perma.cc/AD9S-PNPK (discussing the hack on the German Parliament and the controversy surrounding the German government's response).

193. *See id.* (reporting the cyber-attack on Germany's main network).

194. *See id.* ("[S]ecurity officials were taken aback by the sophistication of the attack, which had exceeded levels of complexity previously seen.").

195. *See* Borland, *supra* note 183 ("The Netherlands rejected the use of electronic voting machines in the 2000s, after studies showed they were susceptible to fraud.").

196. *See id.*

197. *See The Constitutionality of Electronic Voting in Germany*, NDI, https://perma.cc/X5W3-7CG2 ("The German Constitutional Court upheld the first argument . . . that the use of [electronic] voting machines was unconstitutional.").

Parliament in 2016 and was the first comprehensive piece of EU wide cybersecurity legislation.[198]

The NIS Directive requires that EU Member States work in cooperation[199] to improve cybersecurity risk management.[200] Unlike other attempts to combat cyber related issues, the NIS Directive expects nations to exchange information through Cooperation Groups, which may be considered a form of international ISAC.[201] Of particular note to the readers, the 2018 *Compendium on Cyber Security of Election Technology* summarized a wide array of election security best practices, including: "[A]nti-DoS protections, access control and authentication procedures for election IT systems, digital signatures and duplicate data-entry practices to ensure data integrity, network flow analysis and logging procedures, and network segmentation."[202]

Despite the progress, it is important to note the *Compendium* takes a balanced, realistic approach to embracing cybersecurity. As pointed out by the report, despite the

198. *See* Council Directive 2016/1148, 2016 O.J. (L 194) 1.

199. *See id*. at 1–2 ("A Cooperation Group, composed of representatives of Member States, the Commission, and the European Union Agency for Network and Information Security ('ENISA'), should be established to support and facilitate strategic cooperation between the Member States regarding the security of network and information systems.").

200. *See A Cyber Security Framework for Europe*, CORDIS, https://perma.cc/3UZY-WNJ5 (last updated Aug. 5, 2014) (discussing the EU's plan to enhance cybersecurity).

201. *See* Council Directive 2016/1148, *supra* note 198, at 11 (creating Cooperation Groups to facilitate cooperation and the exchange of information).

202. Borland, *supra* note 183. The EU's groundbreaking General Data Protection Regulation (GDPR) is also a relevant and useful regime to better protect personal data, including with regards to political preferences. This is an expansive regulatory regime with a wide array of requirements on covered firms ranging from ensuring data portability and consent to mandating that firms disclose a data breach within seventy-two hours of becoming aware of the incident and then conducting a postmortem to ensure that a similar scenario will not recur. *See Top 10 Operational Responses to the GDPR*, INT'L ASS'N PRIV. PRO., https://perma.cc/Y3MM-LMH7 (providing access to different commentary related to the GDPR). However, some nations have been criticized by the likes of Privacy International for creating exceptions to GDPR safeguards for political parties. *See* Ailidh Callander, *GDPR Loopholes Facilitate Data Exploitation by Political Parties*, GDPR TODAY (Mar. 25, 2019), https://perma.cc/ECG4-SAMV.

widespread use of analogue practices and paper ballots, cyber threats are not eliminated given that these same jurisdictions may still "rely on electronic solutions for voter and candidate registration, vote counting or the communication of the results" that could be susceptible to cyber-attacks, along with the myriad other risks shown in Table 1.[203] As such, the EU also embraces the use of risk-limiting audits that both monitor and ensure robust election security; however, these remain to be widely implemented across the EU.[204]

2. EU Efforts to Combat Digital Repression

As highlighted in Part II, faith in the democratic process also demands a firm commitment to combatting digital repression, including the need to manage disinformation. For example, in 2018, then President of the European Commission Jean-Claude Juncker said: "We must protect our free and fair elections."[205] As such, the EU Commission proposed new rules building from the work of the Compendium to "better protect our democratic processes from manipulation by third countries or private interests."[206] In particular, in 2018 the European Commission pushed Facebook, Google, and Twitter to sign the "Code of Practice on Disinformation,"[207] committing them to boost "transparency around political and issue-based advertising."[208]

This initiative was groundbreaking since the technology industry agreed "to self-regulatory standards to fight

203. COMPENDIUM*, supra* note 33, at 9.

204. *See id*. at 25 ("Testing and auditing are the cornerstones of network and information system security, as they are the only methods of gaining a practical assurance of functionality and security. Therefore, testing and auditing need to take a comprehensive and multifaceted approach.").

205. European Commission Press Release IP/18/5681, State of the Union 2018: European Commission Proposes Measures for Securing Free and Fair European Elections (Sept. 12, 2018), https://perma.cc/4RF2-7P7P.

206. *Id*.

207. European Union, Code of Practice on Disinformation (2018) https://perma.cc/9C26-HL67 (PDF) [hereinafter Code on Disinformation].

208. *Id.*; *see* Borland, *supra* note 183 (noting that Microsoft has also expressed its desire to join the Code).

disinformation."[209] Among other provisions, the Code requires signatories to cull fake accounts, create safeguards against misrepresentation, and the misuse of automated bots, along with empowering consumers and the broader research community.[210] In response, these firms have set up "searchable political-ad databases" and have begun to take down "disruptive, misleading or false" information from their platforms, and to reject ads that are inconsistent with election integrity policies.[211] In 2019, Twitter rolled out a reporting feature in which individuals can report a tweet with misleading information by clicking on a drop down menu, select "It's misleading about voting," choose an option that explains how the tweet is misleading, and submit the report to Twitter.[212] Unfortunately, this did not seem to have the impact desired, as several organizations reported EU election hashtags, such as #EUElections2019, still "received a high level of suspiciously inorganic engagement."[213] Similarly, an activist group called Avaaz found that, despite these efforts, that there were more than "500 far-right and anti-EU Facebook pages and groups" being followed by some thirty-two million people.[214]

In a similar regulatory vein, the Commission underscored the need for greater transparency in online political advertisements and targeting.[215] It also sought further regulation of online advertising campaigns such as by "disclosing which party or political support group is behind online political advertisements as well as by publishing information on targeting criteria used to disseminate information to citizens,"[216] and even called for national

209. Code on Disinformation, *supra* note 207.

210. *See id.* (listing requirements to protect against disinformation).

211. *Id*.

212. *See* Foo Yun Chee, *Twitter Unveils New Tool Against EU Elections Meddlers*, REUTERS (Apr. 24, 2019), https://perma.cc/L3WS-4MJX (explaining the new reporting feature).

213. Kevin Townsend, *Research Shows Twitter Manipulation in Weeks Before EU Elections*, SEC. WEEK (May 28, 2019), https://perma.cc/Q37M-CR8B.

214. Borland, *supra* note 183.

215. *See* Townsend, *supra* note 213 (discussing the "large scale political social engineering through social media").

216. European Commission Press Release IP/18/5681, *supra* note 205.

sanctions for the failure to comply with the new disclosure requirements.[217] And, to address potential difficulties arising from cyberinfrastructure issues in elections, the Commissions called for the creation of a Network of Cybersecurity Competence Centers, in cooperation amongst the EU Member States, to better target and coordinate available funding for cybersecurity cooperation, research and innovation.[218]

In a more widespread regulatory initiative, in June of 2019, the European Commission produced a report on the implementation of the Action Plan Against Disinformation ("Report").[219] The Action Plan proposes a set of actions that should further enable a joint and coordinated EU approach to addressing disinformation. The Action Plan focuses on four pillars:

> (1) Improving the capabilities of the Union's institutions to detect, analyze, and expose disinformation;
> (2) Strengthening coordinated and joint responses by EU institutions and Member States to disinformation;
> (3) Mobilizing the private sector to tackle disinformation; and
> (4) Raising awareness about disinformation and improving societal resilience.[220]

Within these pillars are previously unexplored areas of enhancements, which are not often considered within the

---

217. *See id.* (noting that the sanctions would be imposed for the illegal use of personal data to influence the outcome of European elections).

218. *See Commission Proposal for a European Cybersecurity Competence Network and Centre*, COM (2018) 630 final (Sept. 19, 2018), https://perma.cc/T2YS-CYKR (PDF) ("[T]he initiative will help to create an inter-connected, Europe-wide cybersecurity industrial and research ecosystem.").

219. *See generally Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Concerning the Tackling of Online Disinformation*, COM (2018) 236 final (Apr. 26, 2018), https://perma.cc/C847-EPFX (PDF) [hereinafter *Tackling Disinformation*].

220. *See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Action Plan against Disinformation,* at 5, COM (2018) 36 final (May 12, 2018), https://perma.cc/R8TE-L5CP (PDF) (stating the four pillars).

context of cybersecurity. For example, in the area of communications, the European Commission declared the importance of supporting quality journalism as an essential element of a democratic society and "[c]ountering internal and external disinformation threats through strategic communication" while safeguarding the diversity and sustainability of the European news media ecosystem.[221]

The Action Plan encourages a "more transparent, trustworthy and accountable online ecosystem" while "fostering education and media literacy" to secure resilient election processes.[222] Key to this plan is the improvement of societal resilience in Europe and beyond to foster critical thinking and media-literate citizens.[223] This requires focus to be placed on improving the detection, analysis, and exposure of disinformation by investing in digital tools, data analysis skills, and specialized staff as well as strengthening efforts to assess the reach and impact of disinformation.[224] To accomplish such a lofty goal across the European Union, the Members will necessarily need to strengthen their cooperation and joint responses to disinformation as described above.[225]

One such attempt at coordination exists in the EU's Rapid Alert System.[226] The system is designed to provide warnings on

221. *See Tackling Disinformation*, *supra* note 219, at 15. Building a more knowledgeable, media-savvy user, though, is no simple matter. Trust in media outlets takes time to build. We attach a given level of trust to an outlet based on our view of the institution, the organization, and our prior experience with the individual reporter. Yet, in the digital world, journalists proliferate, and no system of verifiable trustworthiness yet exists.

222. *Id.* at 12.

223. *See id.* ("The life-long development of critical and digital competences, in particular for young people, is crucial to reinforce the resilience of our societies to disinformation.").

224. *See id.* at 9 (noting that "[a]n effective response [to disinformation] requires a solid body of facts and evidence on the spread of disinformation and its impact" and advocating for "[a]dditional data gathering and analysis by fact-checkers and academic researchers").

225. *See supra* notes 183–204 and accompanying text.

226. *See* European Commission Memo/18/6648, Questions and Answers—The EU Steps Up Action Against Disinformation (Dec. 5, 2018), https://perma.cc/596S-YW36 (PDF) (rationalizing the planned system by noting that "[a] strong European response requires Member States and EU

disinformation campaigns in real-time and national contact points for disinformation in the Member States.[227] It is designed to share real-time warnings, react and ensure coordination between EU capitals and Brussels, and has been active since March 2019.[228] A joint EU sanctions regime goes along with the early-warning system to better deter adversarial nations such as Russia from interfering with European Parliament elections,[229] though the effectiveness of this approach has been called into question.[230] In short, criticism has arisen that "[i]t's not rapid. There are no alerts. And there's no system."[231] Core issues—such as the level at which an alarm should be sounded and how to incentivize robust, real-time information sharing—remain to be resolved.[232]

---

institutions to work together much more closely, and to help each other understand and confront the threat").

227. *See id.* (outlining the system's goals and defining disinformation as "verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public—distorts public debate, undermines citizens' trust in institutions and media, and even destabilises democratic processes such as elections").

228. *See Report on the Implementation of the Action Plan Against Disinformation*, at 2–3, JOIN (2019) 12 final (June 14, 2019), https://perma.cc/7UYU-PRS8 (PDF).

229. *See id.* at 8 (describing the recent adoption of legal measures providing for sanctions to deter and respond to cyber-attacks).

230. *See* Matt Apuzzo, *Europe Built a System to Fight Russian Meddling. It's Struggling.*, N.Y. TIMES (July 6, 2019), https://perma.cc/G5UR-TDVA (highlighting disagreement over the success of the Rapid Alert System and noting critiques that the system is hampered by internal politics and incomplete, disorganized data collection).

231. *Id.*

232. *See id.* (noting that disagreement over when to sound an alarm has led to no alerts being issued and that only one-third of European nations contributed information to the system before the 2019 European Parliament elections). Further, and ahead of the European Parliament elections, in April 2019 ENISA hosted a "war game" that was focused on identifying governance gaps and deepening ties to aid in regional election security efforts. Such efforts can help train election officials across the EU, though much more remains to be done help get local staffers up to speed, which is a similar issue facing many campaigns and election boards in the United States. That is why the Harvard Kennedy School's Belfer Center on Science and International Affairs, for example, has focused on training these officials on the basics of cyber hygiene and election security best practices. For further discussion of the Belfer

At its most basic, the Report fails to "cover the issue of domestic or non-state actors in any substantive way or provide any real solutions."[233] Yet it is overly simplistic to believe all misinformation is produced from foreign actors, as was discussed in Part II. The Report's failure to appreciate the nature and varied sources of potential actors is a significant limitation.[234] Moreover, there has been little to suggest that the reporting to date has been as robust or useful as originally hoped.[235] Nonetheless, the report and various initiatives are noteworthy first steps to improve the EU's election cybersecurity, steps that other nations are watching closely.

B. Illustrative Examples: Australia, Oceania, and Asia

This section builds from the comparative transatlantic case study outlined above with illustrative examples from how other advanced and emerging democracies are both protecting their election infrastructure and working to fend off digital repression. We begin by examining Australia, before moving on to several examples from Oceania and Asia before summarizing our key findings and moving on to policy implications.

Center's work in this area, see BELFER CTR. FOR SCI. & INT'L AFFS., HARVARD KENNEDY SCH., THE STATE AND LOCAL ELECTION CYBERSECURITY PLAYBOOK (2018), https://perma.cc/7SK2-SYLP (PDF).

233. Jakub Kalenský, *Evaluation of the EU Elections: Many Gaps Still Remain*, DISINFO PORTAL (June 24, 2019), https://perma.cc/3TGJ-2LFC (last updated Sept. 3, 2019).

234. *See id.* ("If we do not know how many channels hostile actors control, how many messages they spread, and how many people they manage to persuade, how can we talk about proportional defense?").

235. *See id.* (stating that in private conversations EU Member State representatives report that "many countries apparently still lack their own monitoring systems for the disinformation ecosystem, and . . . the RAS is barely used"); James Pamment, *The EU's Role in Fighting Disinformation: Taking Back the Initiative*, CARNEGIE ENDOWMENT FOR INT'L PEACE (July 15, 2020), https://perma.cc/EFF6-UXM8 (arguing that the EU's current disinformation policy is "characterized by . . . a weak evidence base" and that "a lack of trust between member states has led to low levels of information sharing and engagement").

1. Australia

Australia, like EU Member States, the U.S., and other democracies throughout Oceania, is no stranger to disinformation campaigns and other attempts to subvert its democratic institutions.[236] The threats to Australian democracy do differ in several notable ways, though, from the nation's other Western peers.[237] For example, voting is mandatory in Australia,[238] and the major parties in Australia must agree on boundary lines.[239] This thereby reduces some of the common issues that can arise in the context of broader U.S. democracy preservation conversations.[240] The process of voting is also distinct from its American and even some European counterparts.[241] For example, all Australians vote on paper, their votes are tallied by hand, and a robust Electoral Commission oversees the process to check for irregularities.[242]

---

236. *See* Stephanie Borys, *China's 'Brazen' and 'Aggressive' Political Interference Outlined in Top-Secret Report*, ABC NEWS (May 29, 2018), https://perma.cc/7URJ-E6MU (last updated May 29, 2018) (describing the release of an intelligence report from the Australian government concluding that the Chinese government had attempted to infiltrate all levels of the Australian government for years).

237. *See* Scott J. Shackelford & Matthew Sussex, *How Australia Can Help the US Make Democracy Harder to Hack*, CONVERSATION (Sept. 27, 2018, 6:35 AM), https://perma.cc/E289-3B5X (observing that threats to Australia's voting system may largely relate to the government's centralization of the system, while threats to voting in the U.S. are tied to the privatization and decentralization of voting).

238. *See id.* (discussing Australia's voting system).

239. *See id.* (stating that the major parties agree on electoral boundaries to prevent gerrymandering); Rodney Smith, *Chapter 8: Drawing Electoral Boundaries*, ST. LIBR. N.S.W., https://perma.cc/S65W-WLCR (last updated Apr. 2019) (explaining how Australia draws its electoral boundaries).

240. *See* Shackelford & Sussex, *supra* note 237 (arguing that Australia's mandatory voting law means that "there aren't thorny political battles over who is allowed to vote," and that party agreement on electoral boundaries prevents gerrymandering); Smith, *supra* note 239 (observing that the involvement of state legislatures in drawing electoral boundaries in the U.S. "means that American redistribution processes are much more involved with party politics than they are in Australia").

241. *See* Shackelford & Sussex, *supra* note 237.

242. *See id.*; *Counting the Votes*, AUSTRALIAN ELECTORAL COMM'N, https://perma.cc/8HBG-AMNB (last updated Dec. 3, 2019) (outlining the Australian ballot tabulation process).

Australia has also taken the affirmative step of designating its political parties as critical infrastructure, similar to the U.K.'s approach,[243] along with investing in efforts to guard Australians against information warfare using micro-targeting.[244] The U.S., on the other hand, continues to rely on outdated technologies and systems despite years of warnings, as was discussed in Part III. Yet even these safeguards cannot inoculate Australia, the U.S., or any nation against the full range of attacks designed to influence public opinion, interfere with politicians, and the media.[245] For example, in February 2019, despite these efforts, the Australian Parliament was breached by a state-sponsored cyber-attack allegedly from China.[246]

Australia has no rapid-alert system or code of conduct of the kind being tried in the EU to better manage the spread of disinformation.[247] It did, however, sign both the Paris and Christchurch Calls, which are discussed further below, further

243. *See* Press Release, Scott Morrison, Prime Minister of Austl., Statement to the House of Representatives on Cyber Security (Feb. 18, 2019), https://perma.cc/5LE8-CPAB (declaring that "Australia's democratic process is . . . our most critical piece of national infrastructure" and announcing that the Australian Cyber Security Centre was ready to provide immediate support to any political party).

244. *See* Shackelford & Sussex, *supra* note 237 ("Australia has decided to invest early to guard against future information warfare, such as micro-targeting audiences with tailor-made messaging and machine learning-enhanced deepfake videos.").

245. *See, e.g.*, Aaron Patrick, *Sam Dastyari is a Chinese 'Agent of Influence': Ex-Intelligence Chief*, FIN. REV. (Dec. 3, 2017, 11:00 PM), https://perma.cc/ETE6-5WCV (last updated Dec. 4, 2017) ("A top former intelligence official believes there is evidence that Labor senator Sam Dastyari was deliberately targeted by the China government to advance its interests in Australia.").

246. *See China Rejects Australian Parliament Cyber Attack Claims as 'Baseless' and 'Irresponsible*,*'* ASSOCIATED PRESS (Feb. 18, 2019, 3:39 PM), https://perma.cc/ML5T-PC95 (reporting that Australian cyber experts were investigating a sophisticated cyber-attack on the "Liberal, Labor and National party platforms . . . [that occurred] during a breach of the Australian Parliament House network").

247. *See* Daniel Funke & Daniela Flamini, *A Guide to Anti-Misinformation Actions Around the World*, POYNTER INST., https://perma.cc/2MPG-DWP9 (last updated Aug. 13, 2020) (describing the Australian government's work to stop misinformation, including the establishment of a government task force and implementation of a media literacy campaign).

isolating the United States as the only member of the Five Eyes intelligence sharing partners to stay out of these agreements.[248]

2. Oceania

Examining the regional context surrounding Australia is a useful exercise to better understand the unique approaches being taken by developing nations in response to the cyber threats they face.[249] Given the lack of attention in the area relative to other more often studied cyber powers, such a study is vital to help build resilience, and trust, in democratic systems of strategic significance in the South Pacific.[250]

As for election infrastructure, Pacific island nations' election infrastructure and security efforts across Oceania range from quite sophisticated to relatively immature. New Zealand, for example, has a fairly robust, formal election infrastructure,[251] while in others—such as the Federated State

248. *See World Leaders and Tech Giants Sign Ardern's 'Christchurch Call' to Curb Online Extremism*, SBS NEWS (May 16, 2019), https://perma.cc/G433-QEUS (describing the Christchurch Call's goal of engaging major tech companies in the effort to "stamp[] out violent extremist content on the internet" and highlighting that the U.S. was not among the eighteen government signatories); *The Supporters*, PARIS CALL, https://perma.cc/R6NJ-HYCU (listing signatories to the Paris Call for Trust and Security in Cyberspace); *Our Values: Collaboration*, OFF. OF THE DIR. OF NAT'L INTEL., https://perma.cc/JF8T-ET53 (explaining that the "Five Eyes" group is a "long-lasting intelligence collaboration" between the U.S., United Kingdom, Canada, Australia, and New Zealand that developed after World War II).

249. *See, e.g.*, David Shullman, *Protect the Party: China's Growing Influence in the Developing World*, BROOKINGS INST. (Jan. 22, 2019), https://perma.cc/W7KN-QDYU (noting that China continues to grow its influence among Indo-Pacific countries, partly by manipulating the information space in the region).

250. This case study stems from the work of talented graduate students who worked together under the supervision of Professor Shackelford on a capstone team investigating election security in Spring 2019. These students include: Coryn Blacketer, Will Bobe, Bill Boger, Colin Darnell, Caellaigh Klemz, Janaki Reddy Gaddam, Kayla Hill, Tony Kelly, Jonathan Schubauer, and Aaron West. Jonathan Schubauer took the lead in summarizing their work for this Article.

251. *See* ONLINE VOTING WORKING PARTY, ONLINE VOTING IN NEW ZEALAND: FEASIBILITY AND OPTIONS FOR LOCAL ELECTIONS 12–16 (2014), https://perma.cc/925F-Z5F7 (PDF) (providing an overview of New Zealand's

of Micronesia, Kiribati, Tuvalu, and Vanuatu—there is little election infrastructure to monitor.[252] Yet many of the nations comprising Oceania do rely on paper ballot voting systems similar to the EU, are geographically isolated, and with the exception of New Zealand, have relatively small populations with historical connections to well-established democracies—namely the British Commonwealth, and the United States.[253]

The Russian hacking efforts during the 2016 U.S. presidential campaign were direct and intensive.[254] In contrast, Chinese efforts in Australia and throughout Oceania have been more indirect.[255] Although China denies this, it is asserting itself militarily and economically throughout Oceania in an attempt to challenge the global reach and power of the United States, particularly in the Pacific.[256] In fact, there is little evidence of extensive hacking, instead China has sought to influence policy through economic assistance and political contributions to candidates and parties,[257] a strategy which these nations have yet to effectively defend against in an

---

voting systems and infrastructure); *see also* Dylan Matthews, *3 Reasons Why New Zealand Has the Best-Designed Government in the World*, VOX, https://perma.cc/6J5W-GC5E (last updated Jan. 16, 2015) (explaining New Zealand's mixed-member proportional representation electoral system and unicameral legislative structure).

252. *See* IND. UNIV. & AUSTL. NAT'L UNIV., MAKING DEMOCRACY HARDER TO HACK 76 (2019), https://perma.cc/E3WH-MMYM (PDF) (summarizing findings from case studies of election security efforts and election infrastructure in Pacific Island nations).

253. *See* Stewart Firth, *Instability in the Pacific: A Status Report*, LOWY INST. (June 4, 2018), https://perma.cc/E2TH-MH5S (outlining trends in demographics, urbanization, and democracy in the Pacific Islands).

254. *See supra* notes 107–108 and accompanying text.

255. *See, e.g.*, Shullman, *supra* note 249 (discussing China's efforts to increase its global influence by funding infrastructure projects and "manipulating the information space to [its] advantage" in low-income countries).

256. *See* NADÈGE ROLLAND, CHINA'S EURASIAN CENTURY? 93–120 (2017) (theorizing that China is using its Belt and Road Initiative to "increase its own regional influence" and thereby prevent the United States from increasing American influence in the region).

257. *See* Shullman, *supra* note 249 (arguing that China's approach to developing nations is largely driven by a need to protect the integrity and reputation of the Chinese Communist Party).

integrated manner similar to the EU Code for Disinformation discussed above.[258]

Despite the lack of a regional strategy, there are already several efforts underway in the South Pacific to buttress cyber-threat information sharing. For example, as part of Australia's "International Cyber Engagement Strategy," the Pacific Cyber Security Operational Network (PaCSON) was established in April 2018.[259] PaCSON is intended to foster cooperation among South Pacific island nations by providing a mechanism to share cybersecurity threat information and defensive tools, techniques and ideas.[260] At its core, PaCSON consists of a network of government-appointed cybersecurity incident response experts from Australia, the Cook Islands, Fiji, Kiribati, the Marshall Islands, New Zealand, Niue, Palau, Papua New Guinea, Samoa, the Solomon Islands, Tokelau, Tonga, Tuvalu, and Vanuatu.[261] However, there is no existing or planned formal or informal regional structure in the South Pacific dealing with the security of election infrastructure.[262]

3. Asia

As with Oceania, democracies across Asia are also dealing with election insecurity and disinformation.[263] While this Article does not seek to fully address the myriad of threats to election infrastructure across Asia, it is worth briefly noting three trends in managing the twin threats of election integrity

258. *See supra* notes 207–208 and accompanying text.

259. *Pacific Cyber Security Operational Network (PaCSON)*, AUSTL. GOV'T DEP'T OF FOREIGN AFFS. & TRADE, https://perma.cc/RNC2-PNDS.

260. *See id.* ("PaCSON enables cooperation and collaboration by empowering members to share cyber security threat information, tools, techniques and ideas between nations.").

261. *See id.* (listing its members).

262. *See* IND. UNIV. & AUSTL. NAT'L UNIV., *supra* note 252, at 101 (explaining existing regional efforts dealing with cyber security and recommending the adoption of a "cohesive Pacific regional cybersecurity group").

263. *See, e.g.*, Allie Funk, *Asia's Elections Are Plagued by Online Disinformation*, FREEDOM HOUSE (May 2, 2019), https://perma.cc/GYD3-GHGZ ("Parties and candidates across the region have turned to content manipulation as a preferred campaign tactic.").

and disinformation. First, unlike efforts in the U.S., EU, or Australia, Asian democracies have been willing to criminalize the spreading of misinformation. Malaysia, for example, has criminalized the sharing of misinformation.[264] Myanmar and Thailand have leaned on law enforcement actions to reign in misinformation, which have been abused in some cases to silence critics of public corruption.[265]

Second, there has been focused attention on this issue from the highest levels of national leadership. In Indonesia, for example, President Joko Widodo spearheaded the creation of the new National Cyber and Encryption Agency to combat disinformation in their elections.[266] One example was in June 2019, when a member of the Muslim Cyber Army was arrested in Java for posting misinformation to the effect that the Indonesian government was being controlled by China.[267]

Third, it is apparent that more nations are using increasingly heavy-handed tactics to clamp down on internet freedoms in the name of fighting disinformation. The problem of disinformation in India, for example, is so severe that it has been likened to a public health crisis.[268] One Microsoft study, for

264. *See* Funke & Flamini, *supra* note 28 ("The law makes publishing or sharing fake news punishable by up to six years in jail and a fine of 500,000 ringgit ($128,000). It also makes online service providers more responsible for third-party content [and] affects foreign news outlets reporting on Malaysia . . . .").

265. *See id.* (reporting that in 2018 Myanmar authorities jailed three journalists for publishing a story about the regional government and that since 2018 Thai officials have increasingly targeted people who allegedly spread false information on social media); *Tactics to Fight Disinformation in Thailand, Indonesia, Japan, the Philippines and India*, GLOB. GROUND MEDIA (Apr. 23, 2019), https://perma.cc/BG89-JPZ8 (noting fears that Thailand's military junta would use combating misinformation on social media as a screen for increased censorship of political dissent).

266. *See* Funke & Flamini, *supra* note 28 (reporting that "the agency was hiring hundreds of people to 'provide protection' to institutions online," although the specific parameters of its authority were "still unclear").

267. *See id.* (noting that man was "charged with spreading fake news and hate speech").

268. *See* Samir Patil, *India Has a Public Health Crisis. It's Called Fake News.*, N.Y. TIMES (Apr. 29, 2019), https://perma.cc/CV4B-64FZ (arguing that India should implement citizen education campaigns modeled on successful public health campaigns in order to combat widespread disinformation).

example, found that 64 percent of Indians encountered disinformation online in 2019, which was the highest proportion among twenty-two surveyed countries.[269] Not only have these incidents affected elections such as by spreading false information about candidates on WhatsApp,[270] but they have led to real-world harms including at least thirty-three deaths and sixty-nine instances of mob violence.[271] In response, the Indian government has shut down the internet more than one hundred times over the past year,[272] and has proposed laws that would give it largely unchecked surveillance powers, mirroring Chinese-style internet censorship.[273]

C. Summary

As is apparent from these case studies and illustrative examples, there is divergent state practice with regards to both the protection of election infrastructure and the use of digital repression. The area of greatest convergence seems to be the recognition that paper ballots, or at the least EVMs using paper trails, are vital to building confidence in the outcome of an election.[274] Fewer jurisdictions that we could identify have

269. *Microsoft Releases Digital Civility Index on Safer Internet Day*, MICROSOFT (Feb. 5, 2019), https://perma.cc/QRD8-UJTS.

270. *See* Patil, *supra* note 268 (reporting that police linked a fake video that was shared on WhatsApp to the deaths of 62 people in sectarian violence and the displacement of 50,000 more six months before India's general elections in 2014).

271. *See Child-Lifting Rumours Caused 69 Mob Attacks, 33 Deaths in Last 18 Months*, BUS. STANDARD, https://perma.cc/89LK-TZ7P (last updated July 9, 2018) (reporting that between January 2017 and July 2018 rumors of "child-lifting" spread on Indian social media led to dozens of mob attacks on suspected abductors and thirty-three deaths).

272. *See* Funke & Flamini, *supra* note 28.

273. *See* Vindu Goel, *India Proposes Chinese-Style Internet Censorship*, N.Y. TIMES (Feb. 14, 2019), https://perma.cc/L48R-MPA8 (explaining that the proposed rules would allow officials to demand that social media sites remove particular categories of content, build automated screening tools to block "unlawful information," and provide authorities with greater access to individual user accounts on messaging platforms).

274. *See, e.g.*, Schwartz, *supra* note 150 ("The key insight behind auditing as a cyber defense is that if you have a paper record that the voter got to inspect, then that can't later be changed by a cyber-attack.").

taken the next step of requiring risk-limiting audits or have reclassified their election infrastructure or political parties as "critical."[275] These findings are summarized in Table 2 and are unpacked further in Part V.

Table 2: Summary of Surveyed Nation-State Efforts to Protect Election Integrity

	United States	**European Union**	**Australia**	**Asian Democracies**	**Oceania**
Paper Ballots	Fourteen U.S. states use voting machines without a paper trail as of 2019	Major EU Member States including Germany and the Netherlands use paper ballots	Paper ballots in national elections	India (EVMs with paper trail), Japan	New Zealand, Micronesia, Fiji, Kiribati, Palau, Marshall Islands, Papa New Guinea, Samoa, Solomon Islands, Tonga, Tuvalu
Risk-Limiting Audits	Four U.S. states (Colorado, Rhode Island, Nevada, and	Suggested, but not required under 2018 *EU Compendium*	No	Unclear	No

275. *See infra* Table 2.

	Virginia) [276]				
International Cooperation	Intelligence sharing through Five Eyes	Required under NIS Directive for EU Member States	Intelligence sharing through Five Eyes	ASEAN	PaCSON
Digital Repression	No integrated strategy	EU Code of Practice on Disinformation; EU Rapid Alert System	Electoral Integrity Assurance Task Force	Thailand and Myanmar criminalize the sharing of misinformation	No integrated strategy
Election Infrastructure Classified as "Critical"	Yes	Estonia	No	Unclear	No
Political Parties Classified as "Critical"	No	United Kingdom	Yes	Unclear	No

V. Implications for Policymakers

Cyberspace has long bedeviled policymakers, practitioners, and even novelists alike. As the science fiction author William Gibson admitted when he used the word 'cyberspace' in his book *Neuromancer*: "All I knew about the word 'cyberspace' when I

276. *See Post-Election Audits*, NAT'L CONF. OF ST. LEGISLATURES, (Oct. 25, 2019), https://perma.cc/N38D-C63L (listing the only four states with a statutory requirement for risk-limiting audits).

coined it, was that it seemed like an effective buzzword. It seemed evocative and essentially meaningless. It was suggestive of something, but had no real semantic meaning, even for me, as I saw it emerge on the page."[277] As with cyberspace generally, and has been shown through this Article the number of threats facing democratic institutions—including with regards to election security and digital repression—is long, and seemingly only growing longer.[278] Indeed, the likes of Henry Farrell and Bruce Schneier have argued that: "the open forms of input and exchange that it [democracy] relies on can be weaponized to inject falsehood and misinformation that erode democratic debate."[279] Opinions vary as to whether to consider democracy itself as a cyber threat vector, and how to mitigate the risks, such as by doubling down on democratic institutions or relying on other actors—including the private sector—to better manage these issues such as the spread of disinformation through the EU-organized Code discussed in Part IV. This Part proceeds by summarizing the policy suggestions made throughout using an analytical framework pioneered by Peter Swire, among others.[280]

In 1948, George Kennan, an American diplomat and a historian, defined national security as "the continued ability of the country to pursue the development of its internal life without serious interference, or threat of interference, from foreign powers."[281] Yet such a conception of national security is not so clear cut when the goal is protecting democracy itself, as seen in cases of Russian operatives organizing U.S. citizens to

277. JARICE HANSON, THE SOCIAL MEDIA REVOLUTION 113 (2016).

278. *See supra* Part II.

279. Henry Farrell & Bruce Schneier, *Democracy's Dilemma*, BOS. REV. (May 15, 2019), https://perma.cc/RF2K-XHLU.

280. *See* Peter Swire, *A Pedagogic Cybersecurity Framework*, 61 COMMC'NS ACM 23, 23–24 (2018) (proposing a multidisciplinary framework for teaching cybersecurity that "organizes the subjects that have not been included in traditional cybersecurity courses, but instead address cybersecurity management, policy, law, and international affairs").

281. Gayle Smith, *In Search of Sustainable Security*, CTR. FOR AM. PROGRESS (June 19, 2008, 9:00 AM), https://perma.cc/7XEY-U2KW.

engage in activism during the 2016 election cycle.[282] Neither is an analytical framework to ascertain all the necessary steps that must be taken to harden democratic institutions against these attacks. What follows is a suggested path forward. Before turning to the work of Swire, though, it is first necessary to provide some context.

Numerous regulatory theorists and governance scholars have considered cyberspace, including the best ways to engender change in this dynamic, interconnected environment. Yochai Benkler, for example, has offered a three-layer structure to consider interventions, including: (1) the "physical infrastructure," including the fiber-optic cables and routers making up the physical aspect of cyberspace; (2) the "logical infrastructure," comprising necessary "software such as the TCP/IP protocol;" and (3) the "content layer," which includes data and, indirectly, users.[283] This conceptualization, while helpful, only takes us so far in better understanding the various cyber threats facing democratic institutions and what to do about them. It largely ignores, for example, the role played by state and non-state actors in shaping the content layer.[284] Lawrence Lessig built from this model,[285] advocating for "decentralized innovation" making use of various modalities including interventions supporting layers.[286] However, Andrew

282. *See, e.g.*, Shaun Walker, *Russian Troll Factory Paid US Activists to Help Fund Protests During Election*, GUARDIAN (Oct. 17, 2017, 12:13 PM), https://perma.cc/C8D4-N3EJ (reporting that Russian "trolls" offered $80,000 to U.S. activists in order to support the organization of protests and events about divisive social issues).

283. Yochai Benkler, *From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access*, 52 FED. COMMC'NS L.J. 561, 562 (2000).

284. *See, e.g.*, Swire, *supra* note 280, at 24 (explaining that private organizations and national governments influence cybersecurity risks and responses by taking action to mitigate attacks, enacting and enforce laws, and engaging in dialogue or signing treaties with other nations).

285. *See* LAWRENCE LESSIG, FREE CULTURE: HOW BIG MEDIA USES TECHNOLOGY AND THE LAW TO LOCK DOWN CULTURE AND CONTROL CREATIVITY 160 (2004) (describing "the interaction between architecture and law" in the context of copyright regulation).

286. *See* LAWRENCE LESSIG, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD 85–86 (2001) (arguing that "commons" at

Murray has concluded that this is "idealistic" and that, "the harnessing of one regulatory modality through the application of another is more likely to lead to further regulatory competition, due to the complexity of the network environment."[287] Instead of solely relying on code, then, laws, norms, and markets also have important roles to play in shaping a polycentric response to addressing vulnerabilities in democratic election systems.[288]

One way to think through such a polycentric approach is to make use of Swire's stack analogy,[289] offered in adapted form as Table 3. Under this formulation, the foregoing analysis was concerned with levels seven through ten, but the chart highlights the extent to which it is vital to secure the underlying system architecture including voting machines.

Table 3: Applying Swire's Expanded OSI Stack to Election Security[290]

Layer	Vulnerability	Policy Response(s)
1. Physical	Supply chain attack; wiretap; stress equipment	Employ third-party penetration testing and audits; require

the code, content, and physical layers "create the opportunity for individuals to draw upon resources without connections, permission, or access granted by others").

287. ANDREW D. MURRAY, THE REGULATION OF CYBERSPACE: CONTROL IN THE ONLINE ENVIRONMENT 46 (2007) ("It is highly unlikely that content producers, media corporations and other copyright holders will allow for a neutral system designed to protect cultural property and creativity at the cost of loss of control over their products.").

288. *See id.* at 46–47, 124 ("[T]he effectiveness of code-based control mechanisms depends entirely upon their recognition and acceptance within these first-order regulatory environments [competition, society, and hierarchy].").

289. *See* Swire, *supra* note 280, at 24 (explaining that Swire's model adds three "layers" of cybersecurity vulnerabilities to the seven traditional layers of the Open Systems Interconnection model that computer scientists use to conceptualize computer systems).

290. *Id*. For a description of these cyber-attacks, see Chapter 3 in SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS (2014).

		NIST CSF compliance; consider smart contracts
2. Data Link	Cause delays or noise	End-to-end encryption
3. Network	Domain Name System (DNS) and Border Gateway Protocol (BGP) attacks	Utilize BGP security features as well as DNSSEC
4. Transport	Man-in-the-middle attacks	Defense in depth & security by design techniques
5. Session	Session splicing	Enhanced cyber hygiene
6. Presentation	Attacks on encryption	Stronger encryption (even quantum)
7. Application	Malware	Proactive cybersecurity measures; cyber hygiene
8. Organization	Insider attacks; lack of adequate information sharing (between election officials or with allies)	More robust information sharing; require state-of-the-art technical standards and paper ballots along with risk-limiting audits
9. Government	Weak laws for protecting critical infrastructure, IoT, voting machines, and media outlets	Reform efforts such as the Secure Elections Act; push firms to adopt Disinformation Codes of Conduct;

		train election officials
10. International	Nation-state cyber-attacks; lack of international agreements to limit the use of cyber-attacks on election infrastructure; inadequate dispute resolution	Agree on new election security international norms (such as through Paris Call or UN GGE process); ratify a treaty designed to safeguard civilian critical infrastructure; create new cyber threat information sharing forums and joint sanctions regimes for rule breakers

As Table 3 shows, there is a great deal that both the public and private sectors can do, locally and globally, to make democracy harder to hack. Particularly on levels eight through ten of Swire's Open Systems Interconnection (OSI) stack analogy, which is popular among programmers in illustrating the various levels of systems, there is a great deal more that the U.S. and other democracies can and should be doing to secure vulnerable election infrastructure and combat digital repression.

In the United States, despite post-2016 funding, still more than two-thirds of U.S. counties report insufficient funding to replace outdated, vulnerable paperless voting machines, further help is needed.[291] Aside from appropriating sufficient funds to replace outdated voting machines and tabulation systems, Congress also should encourage states to follow Colorado's

291. *See* Lawrence Norden & Andrea Córdova McCadney, *Voting Machines at Risk: Where We Stand Today*, BRENNAN CTR. FOR JUST. (Mar. 5, 2019), https://perma.cc/99U9-PVKD.

example[292] (and the best practices listed in the EU Compendium)[293] by refusing to fund voting machines that use paperless ballots, and requiring risk-limiting audits, which use statistical samples of paper ballots to check if official election results are correct, to increase confidence in election outcomes. Congress should also require NIST to update their voting machine standards, which state and county election officials rely on in deciding which machines to purchase as in the case of Australia.[294] Further, a National Cybersecurity Safety Board could also be created to investigate cyber-attacks on U.S. election infrastructure and issue reports after elections to help ensure that vulnerabilities do not go unaddressed.[295] A crash course is also needed for local and county election officials across the nation.[296] There is an opportunity for both civil society and higher education to aid in this effort, as Indiana University is doing to help the Secretary of State's Office prepare for a wide array of scenarios, conduct tabletop exercises, and create a cybersecurity guidebook for use by newly elected and appointed

---

292. *See* Nathaniel Minor, *Colorado Is a Pretty Darn Safe Place to Cast a Ballot. This Is How We Got Here*, COLO. PUB. RADIO (Oct. 25, 2018), https://perma.cc/4X9P-4HDC (describing Colorado's ballot-counting and risk-limiting audit systems and observing that the *Washington Post* called Colorado "the 'safest' place to cast a ballot" in the United States).

293. *See generally* COMPENDIUM, *supra* note 33 (listing the cyber security best practices).

294. *See* Eric Geller, *New Federal Guidelines Could Ban Internet in Voting Machines*, POLITICO (Oct. 30, 2019, 4:03 PM), https://perma.cc/U4K6-469Z ("[The Voluntary Voting System Guidelines]—produced by the Election Assistance Commission and the technical standards agency NIST—is not a set of mandatory federal rules. However, most states require voting equipment to pass VVSG-based testing before they buy it.").

295. *See* Scott J. Shackelford & Austin E. Brady, *Is It Time for a National Cybersecurity Safety Board? Examining the Policy Implications and Political Pushback*, 28 ALB. L.J. SCI. & TECH. 56, 68 (2018) ("Such a model would be an improvement on the existing reliance on Cyber Emergency Response Teams . . . and aide in effective policymaking at both the state and federal level given the lack of hard, verifiable data on the scope and scale of cyber-attacks.").

296. *See, e.g.*, *Indiana University to Help Secure Indiana's 2020 Elections*, IND. UNIV. (Oct. 25, 2019), https://perma.cc/SV86-G6VP (noting that Indiana University will host "regional 'boot camps' with [Indiana] county clerk offices to train election officials about how to respond to different forms of cyberattacks, such as phishing, phone scams and impersonation calls").

election officials.[297] Other states could engage in similar partnerships, along with pooling resources to create repositories of best practices.

Learning lessons from the case studies in Part IV, the U.S. government could build out the capability of DHS to ward off disinformation campaigns similar to Indonesia's approach, as California is doing through its Secretary of State's Office.[298] Ahead of the 2020 election cycle, the United States could also work with allies around the world to build from the Paris Call for Trust and Security in Cyberspace and the Christchurch Call with these specific actions, perhaps encapsulated in a Call to Safeguard Democracy.[299] The UN Group of Government Experts and standing working group should be leveraged in this effort, and new regional cybersecurity hubs created to speed the transfer of information between jurisdictions as has already been accomplished through the EU's Cooperation Groups.[300] One possibility is a regional approach, such as a "South Pacific Elections—Information and Analysis Center (SPE-ISAC)," a potential solution to the lack of a cohesive Pacific regional cybersecurity group.[301]

Finally, with regards to disinformation in particular, the U.S. government could work with the EU to globalize the self-regulatory Code of Practice on Disinformation for social

297. *See id.* ("[S]tate legislators have awarded Indiana University $301,958 to partner with the Indiana Secretary of State's Office to review and improve the state's election cybersecurity incident response plan.").

298. *See* Ben Adler, *California Launches New Effort to Fight Election Disinformation*, CAPRADIO (Sept. 19, 2018), https://perma.cc/6YSA-FY2L ("Under a recently-passed law, the office will 'monitor and counteract false or misleading information' that could 'suppress voter participation or cause confusion and disruption of the orderly and secure administration of elections.'" (internal citations omitted)).

299. *See World Leaders and Tech Giants Sign Ardern's 'Christchurch Call' to Curb Online Extremism*, SBS NEWS (May 16, 2019), https://perma.cc/G433-QEUS (explaining that the Christchurch Call is a pledge to eradicate "violent extremist content on the internet" signed by national governments and major technology companies).

300. *See supra* notes 199–202 and accompanying text.

301. *See* IND. UNIV. & AUSTL. NAT'L UNIV., *supra* note 252, at 101–05 (proposing specific features of a potential SPE-ISAC, considering potential benefits of such an approach, and recommending next steps for its implementation).

media firms (thus avoiding thorny First Amendment concerns).[302] It could also work to create new forums for international information sharing and more effective rapid alert and joint sanctions regimes.[303] The international community has the tools to act and hold accountable those actors that would threaten democratic institutions. Failing the political will to act, pressure from consumer groups and civil society will continue to mount on tech firms, in particular Facebook, which may be sufficient for them to voluntarily expand their efforts in the EU globally, the same way that more firms are beginning to comply with GDPR globally as opposed to designing new information systems for each jurisdiction.[304]

VI. Conclusion

No nation, however powerful, or tech firm, regardless of its ambitions, is able to safeguard democracies against the full range of threats they face in 2020 and beyond. Only a multifaceted, polycentric approach that makes necessary changes up and down the stack will be up to the task. By working together, we might even be able to prove John Adams wrong by showing that—despite the challenges—democratic sustainability is indeed possible even in a hyper-connected future.[305]

302. *See supra* notes 207–211 and accompanying text.

303. *See supra* notes 226–232 and accompanying text.

304. DIGITALEUROPE, ALMOST TWO YEARS OF GDPR: CELEBRATING AND IMPROVING THE APPLICATION OF EUROPE'S DATA PROTECTION FRAMEWORK 3 (2020), https://perma.cc/72PY-TM5X (PDF) ("[T]he fact that the GDPR has inspired other data protection regimes around the world, at least regarding its principles, has led many organisations to address data protection not only for their EU operations but also globally . . . .").

305. *See* Letter from John Adams to John Taylor, *supra* note 1 ("Remember Democracy never lasts long. It soon wastes[,] exhausts and murders itself. There never was a Democracy Yet, that did not commit suicide.").