__ Michigan Journal of Law Reform __ (forthcoming 2017)

MAKING DEMOCRACY HARDER TO HACK: SHOULD ELECTIONS BE CLASSIFIED AS 'CRITICAL INFRASTRUCTURE?'

Scott J. Shackelford JD, PhD*, Bruce Schneier **, Michael Sulmeyer JD, PhD***, Anne Boustead, JD, PhD****, Ben Buchanan, PhD*****, Amanda N. C. Deckard, JD******, Trey Herr, PhD*******, Jessica Malekos Smith, JD********

Abstract

With the Russian government hack of the Democratic National Convention email servers, and further leaks expected over the coming months that could influence an election, the drama of the 2016 U.S. presidential race highlights an important point: Nefarious hackers do not just pose a risk to vulnerable companies, cyber attacks can potentially impact the trajectory of democracies. Yet, to date, a consensus has not been reached as to the desirability and feasibility of reclassifying elections, in particular voting machines, as critical infrastructure due in part to the long history of local and state control of voting procedures. This Article takes on the debate in the U.S. using the 2016 elections as a case study but puts the issue in a global context with in-depth case studies from South Africa, Estonia, Brazil, Germany, and India. Governance best practices are analyzed by reviewing these differing approaches to securing elections, including the extent to which trend lines are converging or diverging. This investigation will, in turn, help inform ongoing minilateral efforts at cybersecurity norm building in the critical infrastructure context, which are considered here for the first time in the literature through the lens of polycentric governance.

Table of Contents

INTRODUCTION

In the wake of the alleged Russian government hack of the Democratic National Convention email servers, a debate is brewing about how to mitigate the risk of hackers who are now not only targeting individuals, firms, and governmental secrets, but who are also now going after the election machinery upon which U.S. democratic society is built.[1] Indeed, cybersecurity, which was first mentioned in the State of the Union by President Obama in 2013, has become so central to U.S. national security that the topic was featured in the first Clinton-Trump presidential debate of 2016.[2] Beyond political parties, vulnerabilities are replete across the myriad locally managed systems that together comprise the U.S. election infrastructure, including voting machines that in some cases—such as in the case of many Pennsylvania counties—have "zero paper trails" and are often running "severely outdated operating systems like Windows XP," which has not been patched since 2014.[3] This begs the question; should voting machines be

The authors wish to thank the Hewlett Foundation and the Belfer Family for their generosity in making this research possible.

*Associate Professor, Indiana University; Director, Ostrom Workshop Program on Cybersecurity and Internet Governance; Research Fellow, Harvard Kennedy School Belfer Center for Science and International Affairs; Senior Fellow, Center for Applied Cybersecurity Research; Affiliate Scholar, Stanford Center for Internet and Society.

** Research Fellow, Harvard Kennedy School Belfer Center for Science and International Affairs; Fellow Berkman Center for Internet and Society at Harvard University.

*** Director, Cybersecurity Project, Harvard Kennedy School Belfer Center for Science and International Affairs.

**** Postdoctoral Fellow, Harvard Kennedy School Belfer Center for Science and International Affairs.

***** Postdoctoral Fellow, Harvard Kennedy School Belfer Center for Science and International Affairs.

****** Senior Cybersecurity Strategist, Microsoft Corporation.

******* Postdoctoral Fellow, Harvard Kennedy School Belfer Center for Science and International Affairs.

******** Fellow, Harvard Kennedy School Belfer Center for Science and International Affairs.

[1] *See* David E. Sanger & Nicole Perlroth, *As Democrats Gather, a Russian Subplot Raises Intrigue*, N.Y. TIMES (July 24, 2016), http://www.nytimes.com/2016/07/25/us/politics/donald-trump-russia-emails.html?smprod=nytcore-iphone&smid=nytcore-iphone-share&_r=1.

[2] *See* Shanika Gunaratna, *Cybersecurity Expert: One Battleground State Most Vulnerable to Voting Hacks*, CBS NEWS (Sept. 29, 2016), http://www.cbsnews.com/news/ex-nsa-expert-if-i-were-an-election-day-hacker-id-hit-pennsylvania/?google_editors_picks=true.

[3] *See id.*; Bruce Schneier, *By November, Russian Hackers could Target Voting Machines*, WASH. POST (July 27, 2016), https://www.washingtonpost.com/posteverything/wp/2016/07/27/by-november-russian-hackers-could-target-voting-machines/?utm_term=.7711a7f60b27. *See*

treated as "critical infrastructure," e.g., one of the currently sixteen sectors of the U.S. economy that the Department of Homeland Security (DHS) has prioritized for their importance, ranging from finance to healthcare?[4] The distinction matters because when something is designated as "critical," regulation is more likely to follow. Answering that question is far from straight forward, with the long history of local and state control over elections butting up against twenty-first century global security challenges. Still, though, it is a matter that deserves scholarly analysis, and is the overriding concept with which this Article is concerned.[5]

To date, U.S. election infrastructure has not received the same level of scrutiny as other critical infrastructure sectors such as our power lines and wastewater plants. That is despite a long, international history of attacks on voting machines and databases going back as far as 1994 in South Africa (when Nelson Mandela's victory was initially diluted because of fraud, as is discussed further in Part II).[6] Even in the United States, as recently as 2012 during a pilot program in Washington, D.C. to test online voting, researchers from the University of Michigan were able to hack the government website so that the University's fight song would play

also Tim Starks, *Paperless Voting Could Fuel 'Rigged' Election Claims*, POLITICO (Sept. 7, 2016), http://www.politico.com/story/2016/09/paperless-voting-could-fuel-rigged-election-claims-227806 (arguing that four competitive states use voting machines that leave no paper ballots).

[4] *What is Critical Infrastructure*, DHS, http://www.dhs.gov/what-critical-infrastructure (last visited Jan. 16, 2014); *What is the ICS-CERT Mission?*, http://ics-cert.us-cert.gov/Frequently-Asked-Questions (last visited Jan. 17, 2014) (The U.S. Cyber Emergency Response Team, which is part of DHS, identifies sixteen critical infrastructure sectors consistent with Homeland Security Presidential Directive 7, including: agriculture, banking and finance, chemical, commercial facilities, dams, defense industrial base, drinking water and water treatment systems, emergency systems, energy, government facilities, information technology, nuclear systems, public health and healthcare, telecommunications, and transportation systems).

[5] *See* Written testimony of Andrew W. Appel House Subcommittee on Information Technology hearing on "Cybersecurity: Ensuring the Integrity of the Ballot Box" (Sept. 28, 2016), https://oversight.house.gov/wp-content/uploads/2016/09/2016-09-28-Appel-Princeton-Testimony.pdf ("I strongly recommend that, at a minimum, the Congress seek to ensure the elimination of "touchscreen" voting machines, immediately after this November's election; and that it require that all elections be subject to sensible auditing after every election to ensure that systems are functioning properly and to prove to the American people that their votes are counted as cast."); *Ten Things Election Officials Can Do to Help Secure and Inspire Confidence in This Fall's Elections*, ELECTION VERIFICATION (Sept. 5, 2016), https://electionverification.org/wp-content/uploads/2016/09/evntop109516.pdf.

[6] *See* Eric Geller, *Online Voting is a Cybersecurity Nightmare*, DAILY DOT (June 10, 2016), http://www.dailydot.com/layer8/online-voting-cybersecurity-election-fraud-hacking/.

after a vote was cast.[7] More recently, evidence has emerged that hackers have probed the voter registration systems in more than 20 U.S. states.[8] Voting is, in many ways, just as important to our long-term prosperity as functioning telecom networks and financial systems. A first step in recognizing this reality could be for the DHS to explicitly include voting booths and affiliated networks as democratic critical infrastructure, potentially as part of the already recognized "government facilities" sector,[9] the benefits and drawbacks of which are explored in Part I. This move could help pave the way for National Institute for Standards and Technology (NIST), in collaboration with industry, to craft cybersecurity best practices to help jurisdictions across the nation navigate the often confusing choices between voting technology providers.[10] In fact, the choice is so muddled that some cities—including Los Angeles—have developed their own systems incorporating various combinations of touch screens and paper ballots.[11]

Yet securing election infrastructure is not just a problem for the United States. Developing nations, emerging markets, and advanced Western democracies around the world are grappling with the best ways to manage cyber risk and build trust in diverse voting systems. These efforts range from Estonia—where more than twenty-five percent of votes were cast online in the last parliamentary elections[12]—to Mexico, where more than 90 million voter records have been breached with allegations that "one of the main political parties . . . may have played a part in its release."[13] At the global level, international cybersecurity norm building in the critical infrastructure context is also proceeding with new pronouncements from the G2, G7, G20, and the United Nations that are unpacked in Part III as part of a polycentric path forward

[7] *See* Timothy B. Lee, *The Michigan Fight Song and Four Other Reasons to Avoid Internet Voting*, ARS TECHNICA (Oct. 24, 2012), http://arstechnica.com/tech-policy/2012/10/the-michigan-fight-song-and-four-other-reasons-to-avoid-internet-voting/.

[8] *See* Geller, *supra* note 6.

[9] *See* Lawrence Norden & Christopher Famighetti, *America's Voting Technology Crisis*, ATLANTIC (Sept. 15, 2015), http://www.theatlantic.com/politics/archive/2015/09/americas-voting-technology-crisis/405262/.

[10] *See* NIST and the Help America Vote Act (HAVA), https://www.nist.gov/itl/voting (last visited Oct. 2, 2016).

[11] Krista Daly, *Los Angeles County Unveils New Voting System Prototype*, SIGNALSCV (June 30, 2016), http://www.signalscv.com/archives/153961/.

[12] *See* Independent Report on E-Voting in Estonia, https://estoniaevoting.org/ (last visited Oct. 2, 2016).

[13] Jason Murdock, *Mexico Election Hack: Political Party Behind Leak of 93.4 Million Voter Records?*, INT'L BUS. TIMES (Apr. 25, 2016), http://www.ibtimes.co.uk/mexico-election-hack-political-party-behind-leak-93-4-million-voter-records-1556608.

for enhancing the security of elections worldwide.[14] Thus, the decisions made by U.S. policymakers about the best path forward to enhance election security have the potential to reverberate in democracies the world over.

The Article is structured as follows. Part I defines critical infrastructure, identifies possible vulnerabilities in the electoral process, and examines the case for and against including elections under this designation relying foremost on a risk management perspective. Part II undertakes a comparative analysis of national case studies including South Africa, Estonia, Brazil, Germany, and India in an effort to identify governance best practices to better inform the U.S. debate. Finally, Part III delves into the global dimension by analyzing the potential for international cybersecurity norm building from existing minilateral and multilateral forums through the lens of polycentric governance. We conclude by investigating implications for policymakers in the U.S. and abroad.

I. DEFINING "CRITICAL INFRASTRUCTURE" IN THE VOTING CONTEXT

What constitutes "critical infrastructure" (CI) is often in the eye of the beholder; compared to the sixteen CI sectors in the U.S., for example, the European Union recognizes eleven.[15] Even within the United States, it cannot actually be said that the federal government has a single definition of what constitutes CI in all cases, to say nothing of how it should be secured.[16] This Part introduces the existing critical infrastructure sectors before moving on to analyze vulnerabilities in the election process and review the arguments for and against classifying it as CI.

[14] *See infra* Part III(A).

[15] *See Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* 4–5, 17–19 (Feb. 7, 2013) [hereinafter *EU Cybersecurity Strategy*] (the proposal includes five strategic priorities: (1) to "achiev[e] cyber resilience"; (2) to "[d]rastically reduc[e] cybercrime; (3) to "develop[] [a new] cyberdefense policy"; (4) to "[d]evelop the industrial and technological resources for cybersecurity"; and (5) to "[e]stablish a coherent international cyberspace policy for the European Union and promote core EU values.").

[16] *See Cybersecurity Update: Key US and EU Regulatory Developments*, SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP (June 25, 2013), https://www.skadden.com/insights/cybersecurity-update; *see also* JÖRN BRÖMMELHÖRSTER, SANDRA FABRY, & NICO WIRTZ, CRITICAL INFRASTRUCTURE PROTECTION: SURVEY OF WORLDWIDE ACTIVITIES 3 (2002) (noting the lack of an "all embracing" U.S. CI strategy, but noting significant progress in securing CI).

A. Managing Risk to 'Critical Infrastructure'

"Critical infrastructure" can elicit images of sudden and dramatic threats to national security. Contaminated water sanitation systems may injure thousands before any issue is detected; vulnerable electrical grids may blackout cities; and disrupted financial systems may destabilize economies.[17] Advanced malware (malicious software) can even cause nuclear enrichment centrifuges to spin out of control, risking collateral damage.[18] Around the world, many countries are issuing new laws and policies to secure their critical infrastructure even as they struggle to define what should be considered "critical."[19] As we will see, this line is difficult to draw, particularly in the voting context.

The threat to CI is not new. Ancient Rome struggled to protect its aqueducts from invading Germanic tribes,[20] and the Ottoman Empire went to great lengths to protect its extensive road network.[21] More recently, governments have focused on protecting a wider range of modern facilities and public services, including those that not only supply us with water and transportation but also energy, emergency services,

[17] *See* RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 70, 234 (2010). The 2007 blockbuster *Die Hard 4.0* dramatized the prospect of a large-scale cyber assault: in it, a frustrated former Pentagon insider and a team of hackers interrupted U.S. air traffic control, power, telecommunications, and financial services. According to Richard Clarke, such a scenario is feasible under certain circumstances. Michiko Takutani, *The Attack Coming from Bytes, Not Bombs*, N.Y. TIMES, Apr. 26, 2010, at C1.

[18] *See* Steven Cherry, *How Stuxnet is Rewriting the Cyberterrorism Playbook*, IEEE SPECTRUM (Oct. 13, 2010), http://spectrum.ieee.org/podcast/telecom/security/how-stuxnet-is-rewriting-the-cyberterrorism-playbook; Grant Gross, *Experts: Stuxnet Changed the Cybersecurity Landscape*, PC WORLD (Nov. 17, 2010), http://www.pcworld.com/article/210971/article.html; *Stuxnet: Computer Worm Opens New Era of Warfare*, CBS NEWS 60 MINUTES (Mar. 4, 2012), http://www.cbsnews.com/video/watch/?id=7400904n&tag=contentBody;storyMediaBox.

[19] For more on this topic, see Scott J. Shackelford et al., *Toward a Global Standard of Cybersecurity Care?: Exploring the Implications of the 2014 Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L.J. 287, 287 (2015)

[20] Michael J. Assante, *Infrastructure Protection in the Ancient World*, PROC. OF THE 42ND HAW. INT'L CONF. ON SYS. SCI. at 1-2 (2009), http://www.hicss.hawaii.edu/HICSS_42/BestPapers42/ElectricalPower/ReliabilityAndCyberSecurity.pdf.

[21] *See* ENCYCLOPEDIA OF THE OTTOMAN EMPIRE 119 (Gábor Ágoston & Bruce A. Masters eds., 2009).

communication, and access to financial resources.[22] Many of these facilities and services now rely on information technology (IT) networks.[23] The U.S. government, for example, defines a wide variety of national industries part of CI, including the defense industrial base, emergency services, healthcare, and information technology.[24] While government facilities are considered part of U.S. CI, this sector is primarily concerned with the physical buildings that are occupied by federal, state and local government, as well as the people and systems that keep these buildings safe and operational.[25] Election systems are not explicitly considered part of the U.S. CI. But should it? What role should government play in protecting these vital resources, particularly in this case as applied to securing democratic elections?[26] The next section introduces vulnerabilities to the electoral process before moving on to analyze the benefits and drawbacks of classifying these machines as CI.

B. Identifying Vulnerabilities in the Electoral Process

At least five areas of the electoral process are possibly vulnerable to hacking. These are: (1) the information received by voters in the lead-up to the election, (2) the rolls used to check voters in on Election Day, (3) the machines on which voters cast their ballots, (4) the tabulation mechanisms for determining the winners, and (5) the dissemination

[22] *See, e.g.*, *National Infrastructure Protection Plan*, DEP'T HOMELAND SEC., https://www.dhs.gov/national-infrastructure-protection-plan (last visited July 23, 2013).

[23] *See, e.g.*, PAUL CORNISH ET AL., CYBER SECURITY AND THE UK'S CRITICAL NATIONAL INFRASTRUCTURE 1-4 (2011), *available at* http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r0911cyber.pdf.

[24] Presidential Policy Directive 21 (Feb. 12, 2013), https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[25] Department of Homeland Security, *National Infrastructure Protection Plan: Government Facilities Sector*, https://www.dhs.gov/xlibrary/assets/nipp_governmt.pdf (describing the government facilities sector as comprising government buildings, "cyber elements that contribute to the protection of sector assets (e.g., access control systems and closed-circuit television systems) as well as the protection of individuals who possess tactical, operational, or strategic knowledge or perform essential functions.").

[26] *Id.* at viii (arguing that "government cannot provide all the answers and cannot guarantee national cyber security in all respects for all stakeholders.").

systems used to spread news of the results.[27] Each of these areas is discussed in turn. While a full discussion of all possible weaknesses in these areas is beyond the scope of this article, this section highlights examples to illustrate the range of potential threats in an effort to inform the CI decision.

First, shaping the information received by voters prior to an election. As was mentioned in the introduction, foreign electoral interference is nothing new; one study found that from 1945 to 2000, the United States and Russia combined tried to influence foreign elections 117 times, using overt and covert methods.[28] But events in the summer of 2016 showed that the old tactic could be adapted to the digital age. A hacker or hackers, under the pseudonym "Guccifer 2.0" posted documents obtained through network intrusions into a variety of Democratic entities in an effort to influence the election. While these operations attracted enormous media attention, they do not fall within the scope of this Article.

A second area of potential vulnerability are the poll books and systems used to verify voters' eligibility and to process registrations. In some states, these systems are primarily or entirely electronic.[29] A hacker might try to delete a limited number of entries from the poll book just prior to the election, making it difficult for voters to check in on Election Day, contributing to delay and undermining trust.[30] It has been reported that the voting rolls or registration

[27] *See also* Andrew Appel, *Security Against Election Hacking*, FREEDOM TO TINKER (Aug. 17, 2016), https://freedom-to-tinker.com/2016/08/17/security-against-election-hacking-part-1-software-independence/ (discussing three vulnerabilities to elections: the registration process, voting machines, and post-election tabulation).

[28] *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).

[29] Karen Farkas, *Electronic Poll Books Will Be at Voting Locations across the State by November 2016*, CLEVELAND PLAIN DEALER (Aug. 28, 2015), http://www.cleveland.com/metro/index.ssf/2015/08/electronic_poll_books_will_be.html; Katy Owens Hubler, *Electronic Poll Books*, NAT'L CONF. OF ST. LEGISLATURES (May 21, 2016), http://www.ncsl.org/research/elections-and-campaigns/electronic-pollbooks.aspx.

[30] Testimony of Dr. Dan S. Wallach: Protecting the 2016 Elections from Cyber and Voting Machine Attacks', House Committee on Space Science & Technology: 2016, https://science.house.gov/sites/republicans.science.house.gov/files/documents/HHRG-114-SY-WState-DWallach-20160913.pdf.

systems in more than twenty states have been targeted by hackers in 2016 alone.[31]

A third area of vulnerability constitute the voting machines themselves. Once a voter has checked in, they often cast their vote on a voting machine. These systems can also be targeted by hackers. There are two principle types of voting machines in the United States: those that generate a paper trail of some kind, and those that do not. Machines in the former category either instruct the voter to mark a paper ballot that the machine optically scans, or takes the voter's input and marks a paper ballot that is presented to the voter for verification. Machines in the latter category instruct voters to mark a digital ballot, usually on a touchscreen; the machine then aggregates all the digital ballots to produce a result.[32] Security audits of voting machines have revealed a wide range and large number of weaknesses. Some machines have wireless internet connectivity with weak encryption and insecure (or even non-existent) passwords. Others are vulnerable to physical tampering that would permit attackers to install malicious code, such as through thumb drives. Still others run out of date operating systems with unpatched critical vulnerabilities that hackers could exploit, such as the voting machines running Windows XP mentioned in the introduction.[33] Across the many jurisdictions that hold elections, there is no uniformly applied standard or machine. Nonetheless, security researchers have independently demonstrated a range of possible attacks on varying machines.[34]

[31] *See* Tami Abdollah, *US Official: Hackers Targeted Election Systems of 20 States*, ASSOC. PRESS (Sept. 30, 2016), https://www.apnews.com/c6f67fb36d844f28bd18a522811bdd18/US-official:-Hackers-targeted-election-systems-of-20-states. *See also* Dave Bangert, *An Experiment in Voter Fraud*, JCONLINE (Oct. 10, 2016), http://www.jconline.com/story/opinion/columnists/dave-bangert/2016/10/10/bangert-experiment-voter-fraud/91837292/ (demonstrating the steps required to fraudulently update voter registration).

[32] For more on this topic, see *Voting Equipment in the United States*, Verified Voting, https://www.verifiedvoting.org/resources/voting-equipment/ (last visited Oct. 12, 2016).

[33] *See* Schneier, *supra* note 3.

[34] *See ,e.g.*, *Security Assessment of Winvote Voting Equipment for Department of Elections*, COMMONWEALTH SECURITY AND RISK MANAGEMENT: VIRGINIA INFORMATION TECHNOLOGY AGENCY (Apr. 14, 2015), https://www.wired.com/wp-content/uploads/2015/08/WINVote-final.pdf; Srinivas Inguva et al., *Source Code Review of the Hart Intercivic Voting System*, CAL. SEC'Y OF ST. (2007), https://cseweb.ucsd.edu/~hovav/papers/ttbr-hart.html.

Fourth, the tabulation systems that aggregate the results of an election are also vulnerable. At the precinct level, some of the attacks that target voting machines can also manipulate tabulation. More centrally, attackers might be able to affect tabulation between precincts. A hack of the Ukrainian voting system in 2014 removed important files from the tabulation infrastructure just prior to the election, prompting officials to rely on backups.[35]

Fifth, the Ukraine hack also hints at the final area of vulnerability to election hacking; the dissemination of results to the media, and ultimately to citizens. Less than an hour before results were due to be reported in the Ukrainian election referenced above, it was discovered that hackers had managed to break into the systems that reported the results to news networks. A Ukrainian official later said that, "Offenders were trying by means of previously installed software to fake election results in the given region and in such a way to discredit general results of elections of the President of Ukraine."[36] The authorities were able to counteract the hackers effort, leaving pro-Russian TV stations alone in reporting the fake hacked results. This type of hack has the potential to create election-day chaos that, depending on the time zone involved, could impact voting behavior similar to what occurred in the 2000 election.[37]

In summary, there are an array of attack vectors that impact election security. And regardless of the success of hackers making use of these vulnerabilities, depending on the motivation of those involved, trust in the results may be undermined. Simply put, the attacker might not care who wins; the losing side believing that the election was stolen from them may be equally, if not more, valuable.

C. *Arguments For and Against Classifying Elections as Critical Infrastructure*

[35] Mark Clayton, *Ukraine Election Narrowly Avoided 'Wanton Destruction' from Hackers*, CHRISTIAN SCI. MONITOR, (June 17, 2014), http://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers-video.

[36] *Id.*

[37] *See, e.g.*, John R. Lott, Jr., *The Impact of Early Media Election Calls on Republican Voting Rates in Florida's Western Panhandle Counties in 2000*, 123 PUBLIC CHOICE 349, 350 (2005).

During testimony before the House Homeland Security Committee, Francis Taylor, the Department of Homeland Security's undersecretary of intelligence and analysis, said that cyber threats to state election offices were "a continuing concern" for DHS Secretary Jeh Johnson.[38] Elaborating, Undersecretary Taylor remarked "There is concern about reports of hacking into the electoral systems, voter systems and those sorts of things in a couple of states so far . . . We don't believe the results of the election are in jeopardy, but this is an area that we have to make sure that our [local election] jurisdictions across this country . . . have all the tools that they need to make sure those systems remain secure."[39] Unsaid in this comment was whether or not, given the vulnerabilities in election security discussed above, DHS should reclassify voting machines and potentially other elements of the election process as CI.

To date, most suggestions of treating elections as CI focuses on the vote and tabulation machines, arguing that their importance in elections demands protection from outside interference or manipulation.[40] But this presents a limited perspective on elections and the democratic process, where the inputs to this voting system matter as much, or potentially more, than the integrity of the ballot machinery itself. Why should the election machinery receive heightened focus or protection over other parts of the democratic process? Among the challenges in classifying areas of economic or social activity as "critical infrastructure" is the intensely political nature of the process and the absence of real resource constraints. Adding or reclassifying a sector deemed critical by DHS is largely a political process and so is not limited by scarce dollars, time, or talent, other than that of the legislature. This means that while risk management may play an important role in securing each of the individual sectors, it does apply well to their selection.

The benefits of reclassifying voting machines as critical infrastructure are that this would grant DHS a larger role in securing especially outdated machines. Standards bodies such as NIST could also more effectively target their resources to creating governance frameworks to help promote election integrity. Further, best practices could more easily be shared from existing

[38] Eric Geller, *Hackers Hit State Democratic Parties*, POLITICO (Sept. 15, 2016), http://www.politico.com/tipsheets/morning-cybersecurity/2016/09/hackers-hit-state-democratic-parties-senior-officials-urge-calm-on-encryption-remember-the-power-grid-216338.

[39] *Id*.

[40] Kate O'Keefe & Byron Tau, *U.S. Considers Classifying Election System as 'Critical Infrastructure*,' WALL ST. J. (Aug. 3, 2016), http://www.wsj.com/articles/u-s-considers-classifying-election-system-as-critical-infrastructure-1470264895.

Information Sharing and Analysis Centers (ISACs) organized around other CI sectors. There is the possibility of creating a voting ISAC, or Information Sharing and Analysis Organization (ISAO), to help more effectively share cyber threat information and best practices; discussed further in Part III(C). And local, state, and federal policymakers may be more willing to allocate resources to securing existing machines, or buying new ones, with a CI designation.

However, there are also substantial costs to such a reclassification. Some of these costs are political with states such as Georgia already coming out against federal involvement in state election procedures.[41] There are perceived federalism concerns discussed further in Part III(C) centered on the perception of federal oversight of state elections, as well as the implications to national and international security. For example, if voting machines are CI and foreign powers tamper with them, the U.S. government would have to make clear what steps it is willing to take to respond. This calculus could change with a CI designation. Timing is also important; it may be a mistake, for example, to designate election infrastructure as CI close to an election. However, it should be noted that even if consensus does arise as to designating elections as CI, then, as is discussed further in Part III, that should be the beginning and not the end of the conversation given the limited change that would bring to the unsustainable status quo. Weighing these benefits and drawbacks is no easy feat. To help provide context to inform the discussion, Part II summarizes the experience of various nations and how they have—to varying degrees of success—secured their own election infrastructure.

II. COMPARATIVE APPROACHES TO ENHANCING VOTING SECURITY

This Part features in-depth case studies from the United States, South Africa, Estonia, Brazil, Germany, and India, focusing on how threats to these nations' voting practices have been made manifest and what they have done to mitigate the risk. Following the case studies, a brief summary compares these national approaches to inform the norm building discussion in Part III.

A. United States

[41] *See* Eric Geller, *Elections Security: Federal Help or Power Grab?*, POLITICO (Aug. 28, 2016), http://www.politico.com/story/2016/08/election-cyber-security-georgia-227475.

In the United States, state governments have long exerted significant control over election processes and infrastructure. Under the U.S. Constitution, state legislatures are responsible for regulating the "Times, Places and Manner of holding Elections for Senators and Representatives," although Congress may "make or alter such Regulations."[42] Because states play a primary role in the administration of elections, election processes can be adopted to the special needs and circumstances of each state. However, state control over elections processes has also lead to significant variation in how states register voters and administer elections – and consequently significant variation in the challenges of securing these processes.[43]

For example, while voters in both New Jersey and Nevada both use Direct-Recording Electronic (DRE) voting machines, the voting machines used in New Jersey do not generate a paper trail.[44] However, the voting machines used in Nevada produce a paper record, which the user must approve before casting their vote.[45] Without a paper trail, it is impossible to verify the votes cast independently of the machinery used to cast them. This may make it impossible to audit the voting machines to confirm that the results are congruent with a count of paper records,[46] or produce an accurate vote count in the event that the electronic voting machines have been compromised.[47] A significant number of states—including Michigan, New York, and New Mexico—use paper ballots, which are completed by hand and then optically scanned into a voting machine.[48] Security experts have identified optical-scan paper ballots as less vulnerable to computer hacking because the paper ballot is "the ballot of record, and it can be recounted by hand, in a way we can trust,"[49] which is particularly helpful when auditing such records is required under state law.

[42] U.S. Const. art. I, § 4.

[43] For a description of variation in state adoption of voting technology, see Verified Voting, The Verifier, https://www.verifiedvoting.org/verifier/ (last visited Oct. 12, 2016). It should be noted that the variation in voting technology across states may also serve a protective function. Voting processes may be a less appealing target, as an attacker can only breach a limited number of election systems at a time.

[44] *Id.*

[45] *Id.* The Clark County Election Department offers a detailed description of how to vote in Nevada, including how voters view and confirm the paper audit trail. *See Election Department: Voting Machines and Instructions*, http://www.clarkcountynv.gov/election/Pages/VoteMachs.aspx (last visited Oct. 12, 2016).

[46] *See* Appel, *supra* note 5.

[47] *Id.*

[48] Verified voting, *supra* note 43.

[49] Appel, *supra* note 5.

While the administration of elections is an inherently local activity, there have been federal efforts to ensure the security and reliability of elections. After the extensive difficulties caused by use of punch-card ballots in Florida during the 2000 presidential election,[50] Congress passed the Help America Vote Act of 2002 (HAVA),[51] which required states to adopt voting systems that allow the voter to verify which candidate they have selected and correct an erroneous selection, as well as create an auditable record.[52] HAVA also provided funding for the purchase of new voting machines, leading some states to update their election infrastructure by adopting electronic voting machines.[53] At the time, little attention was paid to potential security risks, and some of these electronic voting machines had significant vulnerabilities.[54] In particular, the WinVote machines used by Virginia could have allowed "'anyone within a half mile . . . to modif[y] every vote, undetected' without 'any prior technical expertise.'"[55] However, to date there is no evidence that any voting machines have been hacked during a U.S. election.[56]

While voting machines have not yet been the subject of malicious activity, several state election systems have recently come under attack. Voter registration databases in Arizona and Illinois were accessed by Russian actors,[57] although these attacks cannot yet be definitively attributed to the Russian government.[58] While over 200,000 voter registration records were exposed in these breaches, there are no indications that the information in these records was altered.[59] However, there are still concerns that

[50] *Bush v. Gore*, 531. U.S. 98 (2000).

[51] Pub L. 107-252 (2002).

[52] *Id.* at § 301.

[53] Brian Barrett, *America's Electronic Voting Machines are Scarily Easy Targets*, WIRED (Aug. 2, 2016), https://www.wired.com/2016/08/americas-voting-machines-arent-ready-election/.

[54] *Id.*

[55] *Id.*

[56] Barrett, *supra* note 53.

[57] Elias Groll, *Did Russia Really Hack U.S. Election Systems?*, FOREIGN POL'Y (Aug. 30, 2016), http://foreignpolicy.com/2016/08/30/did-russia-really-hack-u-s-election-systems/.

[58] Joint Statement from the Department of Homeland Security and Office of the Director of National Security, Press Release (Oct. 7, 2016), https://www.dni.gov/index.php/newsroom/press-releases/215-press-releases-2016/1423-joint-dhs-odni-election-security-statement.

[59] Douglas Ernst, *Election Systems Hacked in Illinois, Arizona: 'The FBI is Very Much Worried*, WASH. TIMES (Aug. 29, 2016), http://www.washingtontimes.com/news/2016/aug/29/election-systems-hacked-in-illinois-arizona-the-fb/.

these attacks undermine public trust in the election process, as it is impossible to "patch this psychological vulnerability."[60]

The U.S. federal government has become increasingly concerned about the security of the 2016 election, particularly as there is evidence that the Russian government has already attempted to influence the election. Consequently, there are several federal agencies currently attempting to assist state governments in securing their electoral process. The Electoral Assistance Commission (EAC), established by HAVA, has a long established program that "certifies, decertifies and recertifies voting system hardware and software and accredits test laboratories."[61] While this program is voluntary under federal law, as of 2009 thirty states had passed legislation requiring federal certification of voting machines, testing of voting machines to federal standards, or testing of voting machines by a federally accredited laboratory.[62]

After the breach of voter registration systems in Illinois and Arizona, the DHS offered assistance to state and local election officials.[63] This assistance is "strictly voluntary and does not entail regulation, binding directives, and is not offered to supersede state and local control over the process."[64] DHS has offered to perform scans on internet-connected equipment to identify vulnerabilities, complete in-depth vulnerability assessments of election-related systems, assist in responding to cybersecurity threats and attacks through the National Cybersecurity and Communications Integration System, and facilitate the sharing of information regarding potential threats to election systems between different states.[65] DHS Secretary Johnson also raised the possibility that electoral systems might be designated part of the CI in the future.[66]

[60] Andy Greenberg, *Hack Brief: As FBI Warns Election Sites Got Hacked, All Eyes are on Russia*, WIRED (Aug. 29, 2016) (quoting Thomas Rid).

[61] Election Assistance Commission, *Testing and Certification Program*, https://www.eac.gov/testing_and_certification/default.aspx.

[62] Election Assistance Commission, *State Requirements and the Federal Voting System Testing and Certification Program*, https://www.eac.gov/assets/1/Page/State%20Requirements%20and%20the%20Federal%20Voting%20System%20Testing%20and%20Certification%20Program.pdf.

[63] Statement by Secretary Johnson Concerning the Cybersecurity of the Nation's Election System, https://www.dhs.gov/news/2016/09/16/statement-secretary-johnson-concerning-cybersecurity-nation%E2%80%99s-election-systems

[64] *Id.*

[65] *Id.*

[66] Readout of Secretary Johnson's Call with State Election Officials on Cybersecurity (Aug. 15, 2016), https://www.dhs.gov/news/2016/08/15/readout-secretary-johnsons-call-state-election-officials-cybersecurity.

However, federal attempts to promote a secure election process have met with significant bipartisan resistance from state officials, as was mentioned above. State policymakers are particularly concerned that federal efforts to secure the election process may invite further federal involvement in election activities that have traditionally been regulated on the state level. Vermont Secretary of State Jim Condos described DHS efforts to test and secure state election infrastructure as a "nose under the tent" that could create precedent for expanded federal control of election processes; Georgia Secretary of State Brian Kemp expressed concern over "whether the federal government will subvert the Constitution to achieve the goal of federalizing elections under the guise of security."[67] Similarly, the Ohio Secretary of State, Jon Husted, for example, has written Congress to block DHS from designating state election systems as CI.[68] Speaker Paul Ryan and Majority Leader Mitch McConnell have also gone on record as opposing such a classification.[69] Yet other political leaders – including Senators Tom Carper and John McCain – have expressed their support for enhanced federal protection of the decentralized U.S. election system.[70] This controversy has resulted in only limited uptake of federal tools designed to protect the election process. For example, as of September 2016, only nine states had accepted DHS assistance in identifying and repairing weaknesses in their election infrastructure.[71] It is unclear whether reclassifying election

[67] Geller, *supra* note 41.

[68] *See* Jon Husted, Letter to Mitch McConnell & Paul Ryan, http://files.constantcontact.com/b01249ec501/ca0fce53-25b4-41cd-b0f3-a8cafec27171.pdf (Sept. 29, 2016).

[69] Letter to Todd Valentine, http://www.politico.com/f/?id=00000157-7606-d0b2-a35f-7e1f2aac0001.

[70] *See, e.g.*, Senator John McCain Urges FBI to Address Cyberattacks on Arizona Election System, Press Release (Sept. 14, 2016), http://www.mccain.senate.gov/public/index.cfm/press-releases?ID=D66D63D5-23FE-4545-9E01-E8F7989F30BE; David Jones, *Feds Warn States to Batten Down Hatches Following Election System Attacks*, TECH. NEWS WORLD (Sept. 2, 2016), http://www.technewsworld.com/story/83866.html?google_editors_picks=true ("The attacks, dating back to June, led to the illegal download of information on more than 200,000 Illinois voters, leading to a 10-day shutdown of the state's voter registration system. Hackers also penetrated systems in Arizona but apparently failed to download specific voter information.").

[71] Aliya Sternstein, *9 States Accept DHS' Election Security Support*, NEXTGOV (Sept. 21, 2016), http://www.nextgov.com/cybersecurity/2016/09/9-states-accept-dhss-election-security-support/131741/. However, federal assistance may be more welcome in during other election-related activities. For example, "47 of 50 states rely on the Election Assistance Commission's (EAC) federal certification process when purchasing voting machines." Brennan Ctr. for Justice, *Voting System Security and Reliability Risks*,

systems as part of CI may exacerbate or alleviate such state resistance.

B. South Africa

Unlike the United States, South African election procedures are a product of the country's transition out of apartheid in the early 1990s.[72] As the enfranchisement of black South Africans was a critical part of the establishment of democracy in South Africa, the Independent Electoral Commission (IEC) was first established in 1993 to administer the election process and promote free elections.[73] The IEC's role in ensuring free and fair elections was enshrined in the 1996 post-apartheid Constitution, which mandates that the IEC "manage elections of national, provincial and municipal legislative bodies in accordance with national legislation."[74] These elections are held every five years,[75] and are based on a proportional representation voting system: individuals vote for political parties, and each party is allotted a number of seats based on their share of the vote.[76]

South Africa held its first post-apartheid elections in 1994. These elections were logistically challenging: the number of citizens eligible to vote had increased from three million people to eighteen million people, many of whom did not have governmental identification documents, and the newly formed IEC did not use the voting infrastructure utilized by the apartheid government.[77] As these elections were an important turning point in South African democracy, they were closely watched by both internal

https://www.brennancenter.org/sites/default/files/analysis/Fact_Sheet_Voting_System_Security.pdf.

[72] Apartheid encompasses a set of official policies of racial segregation established by the South African Government. *See South Africa: Overcoming Apartheid, Building Democracy* http://overcomingapartheid.msu.edu/index.php, Katie Nodjimbadem, *A Look Back at South Africa Under Apartheid, Twenty-Five Years After Its Repeal*, Smithsonian.com (Oct. 15, 2015), http://www.smithsonianmag.com/history/what-did-apartheid-south-africa-look-180956945/?no-ist.

[73] Independent Electoral Comm'n Act 150 of 1993 (S. Afr.).

[74] *Chapter 9 Institutions - the Electoral Commission*, LEAD SA (Mar. 17, 2014), http://www.leadsa.co.za/articles/6711/chapter-9-institutions-the-electoral-commission.

[75] Electoral Comm'n of S. Africa, *Election Types*, http://www.elections.org.za/content/Elections/Election-types/ (last visited Oct. 12, 2016).

[76] Constanze Bauer, *The 1994 and 1999 Electoral Process/Systems: Promoting Democracy in South Africa*, 6 AF. J. POL. SCI. 105, 109 (2001).

[77] Amy Mawson, *Organizing the First Post0Apartheid Election: South Africa, 1994,* http://successfulsocieties.princeton.edu/sites/successfulsocieties/files/Policy_Note_ID114.pdf (last visited Oct. 11, 2016).

and external observers.[78] Despite this scrutiny, significant problems arose during the 1994 elections, including apparent ballot stuffing,[79] submission of ballot boxes from non-existent polling stations, and voting by underage persons.[80]

The problems of the 1994 elections extended to the computing infrastructure used to count the votes. The IEC had created a Manual Verification Unit, tasked with manually duplicating the computer-created tallies.[81] This unit quickly discovered a discrepancy between the manual and computer-created counts: for "'every vote that was counted for the ANC [African National Congress][82] two other parties were getting either a 10% or 20% vote as well."[83] This miscounting was caused by a program illicitly installed on the IEC's main computer,[84] and benefited parties opposed to the ANC.[85] After the tampering was discovered, the IEC created a "new counting system with new computers" and hired clerks from external audit firms to observe data entry.[86] The hacker who installed this program was never identified.[87]

After the difficulties of the 1994 elections, the IEC undertook extensive reforms to ensure the security and reliability of the 1999 elections. These reforms included "the creation of a

[78] *See* United Nations Observer Mission in South Africa (UNOMSA), https://search.archives.un.org/united-nations-observer-mission-in-south-africa-unomsa (last visited Oct. 11, 2016).

[79] Bob Drogin, *Ballot Fraud casts Shadow on S. Africa Vote*, L.A. TIMES (May 6, 2009), http://articles.latimes.com/1994-05-06/news/mn-54514_1_ballot-fraud ("'There were sealed ballot boxes in which there were 3,000-odd votes, and all the ballots were neatly stacked up inside,' explained John Willis, a lawyer and election observer in Empangeni. 'It's physically impossible if people are voting one by one.'").

[80] *Id.*

[81] Mawson, *supra* note 77, at 14.

[82] The ANC, a South African political party that advocated against discrimination and was banned under apartheid, was the eventual winner of the election. Nelson Mandela served as ANC president. African National Congress, *A Brief History of the African National Congress*, http://www.anc.org.za/content/brief-history-anc (last visited Oct. 12, 2016).

[83] Mawson, *surpa* note 77, at 14.

[84] Paul Taylor, *Sabotage Claims Stall S. African Vote Count*, WASH. POST (May 5, 1994), https://www.washingtonpost.com/archive/politics/1994/05/05/sabotage-claims-stall-s-african-vote-count/65696691-5930-4864-912d-09e500653f53/.

[85] Aislinn Laing, *Election Won by Mandela 'Rigged by Opposition'*, TELEGRAPH (Oct. 24, 2010), http://www.telegraph.co.uk/news/worldnews/africaandindianocean/southafrica/8084053/Election-won-by-Mandela-rigged-by-opposition.html. The National Party, Freedom Front Party, and Inkatha Freedom Party benefited from the computer tampering.

[86] Mawson, *surpa* note 77, at 14.

[87] Laing, *supra* note 85.

nationwide satellite-based wide-area network and infrastructure; a bar-code system used to register 18.4 million voters in just nine days; a geographic information system used to create voting districts; a national common voters' role; a sophisticated election results center for managing the process; and the training of 300,000 people."[88] The IEC was awarded a *Computerworld* Smithsonian Award in 2000 for their actions to create a secure and fair election.[89]

As a result of these reforms, the South African election process includes many procedures aimed at ensuring a secure and fair election. Potential voters in South Africa must register in person at an IEC office, and present appropriate government identification.[90] After a voter has applied for registration, they receive a bar-coded sticker, which is scanned when they arrive at the polling place.[91] The registration sticker is stamped and the voter's thumb is marked with ink to prevent repeat voting.[92] The voter is then issued paper ballots, which they then complete in a private compartment and placed in a sealed ballot box.[93]

Votes are tabulated in a counting station, which is protected by security officers tasked with ensuring that no one interferes with the counting process.[94] Votes are first sorted based on the political party indicated on the ballot; both impartial observers and representatives from political parties observe each ballot to ensure that "a single party is identifiable on the ballot paper, and that the ballot paper has been properly issued and bears the official voting

[88] Richard Heeks, *e-Government in Africa: Promise and Practice* (2002), https://pdfs.semanticscholar.org/473d/b0a40b98d8365d0b3c6191d9351ddc7ac0bb.pdf.

[89] Linda Rosencrance, *Technology Innovators Presented with Smithsonian Awards* (2000), http://www.computerworld.com/article/2595901/it-management/technology-innovators-presented-with-smithsonian-awards.html.

[90] Potential voters must register with a bar-coded ID book, smartcard ID, or Temporary Identity Certificate. Driver's licenses and passports are not on the list of approved forms of identification. Electoral Commission of South Africa, *How do I Register?*, http://www.elections.org.za/content/For-Voters/How-do-I-register-/ (last visited Oct. 12, 2016).

[91] Electoral Comm'n of S. Africa, *Voting: How it Works*, http://www.elections.org.za/content/Elections/Voting/ (last visited Oct. 12, 2016).

[92] *Id.*

[93] *Id.*

[94] Independent Electoral Commission, *Handbook for Counting Officers and Enumerators*, http://aceproject.org/ero-en/topics/vote-counting/Manual-South%20Africa.pdf/view. *See also* Independent Electoral Commission, *The Counting Process*, http://www.elections.org.za/content/uploadedImages/counting-process.jpg?n=7097.

station stamp on the back."[95] The ballots for each political party are placed on separate tables where they are counted by an IEC official. The counting officials then switch places, and a different official recounts the ballots at each table. This process is repeated until two identical, consecutive counts are achieved.[96] Political party representatives observe the counting process; they must either challenge the vote count or sign the completed tally of votes.[97] These results are then transmitted to the municipal electoral office.[98] Together, these reforms have contributed to significant improvements in South African election security from the 1994 election issues, making it a model of African voting best practices.

C. Estonia

Much like South Africa, Estonia's approach to protecting CI and to using IT in elections is rooted in its particular history and demographics. The modern Republic of Estonia—which declared independence in 1918, was forcibly annexed by the Soviet Union in 1940, and expelled the last occupying Russian troops in 1994—has experienced phenomenal economic growth over the last two decades, powered in large part by its market and telecom policy choices.[99] With a land area that's slightly smaller than Vermont and New Hampshire combined[100] and a population of about 1.3 million people (roughly the size of San Diego), Estonia benefited from a "fast and comprehensive break from the Soviet-type economic system" in the mid-90s.[101] In addition, in the late 90s, Estonia began investing heavily in computing and network

[95] *Id.*

[96] *Id.*

[97] *Id.*

[98] *Id.*

[99] In 1995, Estonia's Gross Domestic Product (GDP) was $4.374 billion; in 2005, it was $14.006 billion; and in 2015, it was $22.691 billion. Estonia, WORLD BANK, http://data.worldbank.org/country/estonia; Tarmo Kalvet, *The Estonian ICT Manufacturing and Software Industry*, EUR. COMM'N JOINT RESEARCH CTR. (Apr. 2004), ftp://jrc.es/pub/EURdoc/EURdoc/eur21193en.pdf; About the country of Estonia, https://e-estonia.com/the-story/the-story-about-estonia/.

[100] ESTONIA, THE WORLD FACTBOOK, https://www.cia.gov/library/publications/the-world-factbook/geos/print/country/countrypdf_en.pdf.

[101] Runno Lumiste, Robert Pefferly, & Alari Purju, *Estonia's Economic Development: Trends, Practices, and Sources—A Case Study*, COMM'N ON GROWTH & DEV. (Working Paper No. 25), at 3, http://siteresources.worldbank.org/EXTPREMNET/Resources/489960-1338997241035/Growth_Commission_Working_Paper_25_Estonia_Economic_Development_Trends_Practices_Sources_Case_Study.pdf.

infrastructure, brought Internet access and computers to all Estonian schools, and passed national electronic ID card and other legislation that proved foundational for establishing its digital society.[102] As a result, Estonia has been called "the most advanced digital society in the world," and it was the world's first country to use an Internet voting system—for local elections in 2005, and for national elections in 2007.[103]

The Estonian government explicitly recognizes that its highly advanced e-government services result in a "dependency on the proper functioning of IT solutions."[104] As such, the Estonian Information System Authority (RIA), a subdivision of the Ministry of Economic Affairs and Communications, is charged with supervising "information systems used to provide vital services" and implementing "security measures of the information assets related to them."[105] More specifically, the "Section of Critical Information Infrastructure Protection" within RIA is responsible for protecting public and private sector information systems that ensure the functioning of "vital services" in Estonia.[106]

As defined in the Emergency Act, Estonia recognizes 43 "vital services" including the functioning of the data communication network and the functioning of the mobile telephone network.[107] Both networks are vital to Estonia's system of "Internet voting" or "I-voting," which has been possible via Internet-connected computer and government-issued national electronic ID card[108] since 2005 and via mobile phone and SIM

[102] Lumiste et al, *supra* note 101, at 33-34; HOW WE GOT THERE: ESTONIA'S ROAD TO A DIGITAL SOCIETY, https://e-estonia.com/the-story/how-we-got-there/; Electronic ID Card, https://e-estonia.com/component/electronic-id-card/ (last visited Oct. 12, 2016); Tim Mansel, *How Estonia became E-stonia*, BBC NEWS (16 May 2013), http://www.bbc.com/news/business-22317297.

[103] Ben Hammersley, *Why You Should be an e-resident of Estonia*, WIRED (4 Feb. 2015), www.wired.co.uk/article/estonia-e-resident; Estonian Internet voting system, http://estonia.eu/about-estonia/economy-a-it/e-voting.html; Facts, https://e-estonia.com/facts/; e-Estonia, http://estonia.eu/about-estonia/economy-a-it/e-estonia.html (last visited Oct. 12, 2016).

[104] Critical Information Infrastructure Protection, REP. OF ESTONIA INFORMATION SYSTEM AUTHORITY, https://www.ria.ee/en/ciip.html (last visited Oct. 12, 2016).

[105] Information System Authority, REP. OF ESTONIA INFORMATION SYSTEM AUTHORITY, https://www.ria.ee/en/about-estonian-information-system-authority.html (last visited Oct. 12, 2016).

[106] Critical Information Infrastructure Protection, *supra* note 104.

[107] Emergency Act, RIIGI TEATAJA, https://www.riigiteataja.ee/en/eli/ee/529012016001/consolide/current, § 34 (last visited Oct. 12, 2016).

[108] Ninety-four percent of Estonians have a national electronic ID card, which is used for many e-government services. Electronic ID Card, estonia.eu/about-estonia/economy-a-it/e-voting.html (last visited Oct. 12, 2016).

card since 2011.[109] I-voting has been utilized in eight local, parliamentary, and European Parliament elections, with the percentage of Estonian citizens opting for I-voting increasingly nearly every election—from 1.9 percent in 2005 to 30.5 percent in 2015.[110] In 2012, Estonia established an "Electronic Voting Committee" to "prepare and organise electronic voting, to resolve any cases hindering electronic voting pursuant to law and to verify the results of electronic voting."[111] Ahead of the 2014 European Parliament election, Tarvi Martens, Head of the Committee, presented on I-voting, asserting that "Internet voting is here to stay," and that "I-voting is as natural as Internet-banking but even more secure," and that trust is at the center of "what it takes" for I-voting to be successful.[112]

However, on May 12, 2014, just ahead of the European Parliament election, an "international team of independent experts" identified "major risks in the security of Estonia's Internet voting system."[113] The team, which included representatives from the UK's Open Rights Team and the University of Michigan as well as an independent security researcher, observed operations at an Estonian election center during the 2013 local elections and described numerous operational security lapses and risks.[114] But on May 14, Anto Veldre of CERT-EE (a subset of Estonia's RIA),[115] rebutted the team's assertions, citing: a need for more evidence (i.e. technical descriptions of the attacks, which could be shared discreetly with the government); a disconnect in U.S. understanding of Estonia's *Internet* (rather than "electronic") voting via ID card, which relies on Estonia's nationally supported Public Key Infrastructure system; and a cultural disconnect—namely that, in Estonia's experience, falsifying paper votes is more

[109] Estonian Internet voting system, http://estonia.eu/about-estonia/economy-a-it/e-voting.html; i-Voting, https://e-estonia.com/?component=i-voting.

[110] *See* Internet voting in Estonia, http://www.vvk.ee/voting-methods-in-estonia/ (last visited Oct. 12, 2016). Percentage of votes cast using I-voting: 2005 (local): 1.9%; 2007 (parliamentary): 5.5%; 2009 (European Parliament): 14.7%; 2009 (local): 15.8%; 2011 (parliamentary): 24.3%; 2014 (European Parliament): 31.3%; 2015 (parliamentary): 30.5%, https://e-estonia.com/?component=i-voting (last visited Oct. 12, 2016).

[111] Electronic Voting Committee, http://www.vvk.ee/general-info/electronic-voting-committee/ (last visited Oct. 12, 2016).

[112] Tarvi Martens, *Internet Voting in Estonia*, LATA, http://lata.org.lv/wp-content/conf/Drosiba/LATA_EST_iVelesanas_TarviMartens.pdf (last visited Oct. 12, 2016).

[113] Press Release, Independent Report on E-voting in Estonia (May 12, 2014), https://estoniaevoting.org/press-release/.

[114] *Id.*

[115] About CERT Estonia, https://www.ria.ee/en/cert-estonia.html (last visited Oct. 12, 2016).

of a threat than digital votes.[116] Estonia's ongoing investments in its "e-society" are critical to its approach and adherence to I-voting, and its apparent trust in digital over paper records is apparent elsewhere in government. For instance, the authoritative version of Estonia's laws, including the above-mentioned Emergency Act and the law that established the Electronic Voting Committee, are maintained online, in the "Elektrooniline Riigi Teataja," which is modeled after the paper-based Riigi Teataja.

The Estonian government is also implementing measures to increase I-voting security. In 2013, for example, it began implementing individual vote verification, giving smart device-holding and QR code-familiar voters the ability to check if their vote was cast and counted as intended.[117] According to research by Mihkel Solvak and Kristjan Vassil of the University of Tartu in cooperation with the Estonian National Electoral Committee, only 3.7, 4.7, and 4.7 percent of I-voting Estonians used the verification technology in 2013, 2014, and 2015.[118] However, as Solvak and Vassil note, in 2015, 8,439 Estonians used the technology—nearly the number of Estonians that used the Internet to vote in 2005—and adoption of new technology takes time.[119] In addition, in July 2016, the Estonian government hired Cybernetica to overhaul and regularly maintain its electronic voting system software, which was created in 2004.[120] According to Tarvi Martens, "the new system will be more universal, allowing more possible applications, in addition to using it for Estonian nation-wide elections and referendums – such as internal elections of large corporations, local government polls and also abroad."[121]

With no publicly reported cyber incidents related to its I-voting system, Estonia is powering ahead, and its election system technology may even be marketed beyond the Estonian

[116] Anto Veldre, *E-voting is (Too) Secure*, INFO. SYS. AUTHORITY (May 14, 2014), https://www.ria.ee/en/e-voting-is-too-secure.html.

[117] *What is Verification of I-votes?*, http://www.vvk.ee/public/Verification_of_I-Votes.pdf (last visited Oct. 12, 2016).

[118] Mihkel Solvak & Kristjan Vassil, *E-voting in Estonia: Technological Diffusion and Other Developments Over Ten Years (2005-2015)*, JOHAN SKYTTE INST. OF POLITICAL STUD. (2016), at 132, http://skytte.ut.ee/sites/default/files/skytte/e_voting_in_estonia_vassil_solvak_a5_web.pdf. The authors cite low penetration of smart devices and limited familiarity with QR code in older generations as possible issues.

[119] *Id.*

[120] *Cybernetica Selected to Renew Estonian Internet Voting Software*, CYBERNETICA NEWS (July 27, 2016), https://cyber.ee/en/news/cybernetica-selected-to-renew-estonian-internet-voting-software/.

[121] Estonian Internet Voting System to be Rewritten from Scratch, https://cybersec.ee/2016/08/02/estonian-internet-voting-system-to-be-rewritten-from-scratch/ (last visited Oct. 12, 2016).

government. But as Martens admits, trust will likely continue to be central to the success of I-voting. Solvak's and Vassil's research captured how, in 2013-15, trust in Internet voting was polarized but overall relatively high (i.e., higher than in other Estonian government institutions).[122] Moreover, distrust of Internet voting is lowest among Estonians who are not yet aware of the individual vote verification technology, which only began to be available in 2013.[123] In addition, Estonian public opinion may not be easily swayed; despite a very significant distributed denial of service (DDoS) attack on Estonian government websites in 2007,[124] I-voting has become increasingly popular. However, as with CI more broadly, greater dependency may lead to additional consequence, and a serious attack on Estonia's I-voting may not only impact future elections but also Estonia's broader digital society.

D. Germany

Germany has a parliamentary system that elects a large legislative body, the Bundestag, composed of representatives from across the sixteen states and that in turn appoints a head of government.[125] A smaller legislative body, the Bundesrat, contains members directly appointed by these state governments. The Federal President is the head of state, a largely ceremonial role, appointed by a convention composed of all Bundestag members and delegates from the sixteen states. The Bundestag is the primary avenue for German voter's influence on the composition of their government.[126] There are 598 seats of which half are directly elected and half are proportionally allocated according to party lists.[127] Voters have two votes, the first is used to select a representative, affiliated with a party, from among a range of candidates for their district seat. The second vote is used to select a party, whose allocation of total seats in the Bundestag is then determined by the proportion of these second votes received. In some cases, the number of seats awarded according to this first

[122] Solvak & Vassil, *supra* note 118, at 133-4.

[123] *Id*. at 132-39.

[124] Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, WIRED (Aug. 21, 2007), https://www.wired.com/2007/08/ff-estonia/.

[125] *How Does Germany's Electoral System Work?*, ECONOMIST (Sept. 11, 2013), http://www.economist.com/blogs/economist-explains/2013/09/economist-explains-3.

[126] *Id*.

[127] Leon Mangasarian, *How Germany's Election System Works: What to Watch for Today*, BLOOMBERG (Sept. 21, 2013), http://www.bloomberg.com/news/articles/2013-09-21/how-germany-s-election-system-works-what-to-watch-for-today.

vote (direct method) and second vote (proportional method) are out of sync. Seats can never be taken away from a party but so-called 'overhang' seats can be awarded to a party if they receive more second vote seats than first.[128] This means that the size of the Bundestag varies from session to session and that accuracy in ballot tabulation is critically important, highlighting the importance of mitigating that vulnerability in the election system.

In 2009, the German Federal Constitutional Court heard a case contesting the use of electronic voting machines during the 2005 Bundestag elections. The equipment in question were Direct Record Electronic (DRE) machines, used to record votes on election day and store them in memory for later tabulation.[129] These particular Electronic Voting Machines (EVMs), manufactured by a Dutch technology company called Nedap, required votes to be tabulated using a separate device and printed a paper record to verify the electronic memory's contents.[130] These Nedap EVMs had been used for elections in the Netherlands until 2006, when a group of researchers demonstrated their vulnerability to manipulation in under five minutes.[131] The Dutch government had subsequently banned the devices.[132]

In Germany, which used EVMs very similar to those from the Dutch elections, researchers contested that the devices violated a portion of the German Basic Law, which requires that "all essential steps of an election are subject to the possibility of public scrutiny unless other constitutional interests justify an exception."[133] The suit claimed that because the votes were stored in memory and then tabulated using a separate device, the voter was unable to verify the integrity of their vote as required by law, and thus the system was unconstitutional.[134] The German Constitutional Court agreed, ruling against use of the machines in the 2005 elections, though declining to overturn the results without more evidence of fraud, arguing that the average voter should be able to interpret and reliably scrutinize the ballot without special

[128] *Germany's Voting System Explained*, SPIEGEL (Sept. 19, 2013), http://www.spiegel.de/international/germany/german-election-system-explained-a-923243.html.

[129] Electronic Voting Machines (EVMs), https://www.ifes.org/sites/default/files/electronic_voting_machines.pdf (last visited Oct. 12, 2016).

[130] Wahlcomputer, https://berlin.ccc.de/wiki/Wahlmaschinen (last visited Oct. 12, 2016).

[131] ROP GONGGRIJP, NEDAP/GROENENDAAL ES3B VOTING COMPUTER: A SECURITY ANALYSIS, http://wijvertrouwenstemcomputersniet.nl/images/9/91/Es3b-en.pdf.

[132] *Id*.

[133] Art. 38 in conjunction with Article 20.1 and 20.2 of the Basic Law (Grundgesetz – GG).

[134] *Id*.

training, "or detailed knowledge of computer technology."[135] The Court ruled that the basic law did not prohibit EVMs outright but that its requirements could not be satisfied by the provision of extensive security measures or official sampling and testing of a limited number of machines for accuracy.[136] The EVMs in use did not satisfy the requirements of public scrutiny since "votes were exclusively recorded electronically on a vote recording module, neither voters nor electoral boards nor citizens who were present at the polling station were able to verify the unadulterated recording of the votes cast . . . [and] the essential steps of the ascertainment of the result could not be retraced by the public."[137] Since the Court's ruling in 2009 Germany has not employed EVMs. This follows the 2006 ban in the Netherlands and a period of controversy in Ireland over their use between 2004 and 2009, ultimately resulting in a return to paper ballots.[138]

Germany's categorization of CI makes likely includes voting machines and tabulation equipment. The definition of CI includes, "organizational and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences."[139] This has led to the classification of a number of technical and services infrastructure sectors as CI including drinking water supply and emergency services, as well as several broader categories including media, "cultural objects" and public administration.[140] Elections infrastructure could be considered as part of "public administration."[141] Similar categorization could be made under the European Union's criteria

[135] Use of Voting Computers in 2005 Bundestag Election Unconstitutional, Press Release No. 19/2009 (Mar. 3, 2009), https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2009/bvg09-019.html.

[136] *No E-Voting in Germany*, DIGITAL CIVIL RIGHTS IN EUR. (Mar. 11, 2009), http://history.edri.org/edri-gram/number7.5/no-evoting-germany.

[137] Press Release No. 19/2009, *supra* note 133.

[138] *E-Voting Machines to be Scrapped*, IRISH TIMES (June 29 2012), http://www.irishtimes.com/news/e-voting-machines-to-be-scrapped-1.722896.

[139] NATIONAL STRATEGY FOR CRITICAL INFRASTRUCTURE PROTECTION (CIP STRATEGY), FED. REP. OF GERMANY (June 17, 2009), http://www.kritis.bund.de/SharedDocs/Downloads/BBK/EN/CIP-Strategy.pdf?__blob=publicationFile.

[140] Ch. 10: Emergency Management in the Federal Republic of Germany: Preserving its Critical Infrastructures from Hazardous Natural Events and Terrorist Acts, https://training.fema.gov/hiedu/aemrc/booksdownload/compemmgmtbookproject/.

[141] *Id.*

for the identification of CI, one branch of which considers "public effects" including negative impacts on public confidence.[142]

E. Brazil

As the largest democracy in Latin America, the Federative Republic of Brazil utilizes DRE voting machines to account for approximately 120 million voters.[143] Brazil's DRE machines – *urnas* – feature two terminals: (1) "an election officer terminal used to authenticate electors by their registration number or fingerprint," and (2) a voter terminal where votes are cast."[144] In terms of mitigating the risk of system malfunctions (*e.g.* a power failure), the *urnas* are equipped with a battery as a secondary power source.[145]

Electronic voting first began in Brazil in 1996 for the purposes of "ensur[ing] secrecy and accuracy of the election process, as well as speed" and became commonplace across all voting precincts by 2000.[146] Historically, the state's efforts in developing and implementing electronic voting devices has been described as pioneering,[147] and the *urnas* garnered acclaim for both their mobility and affordability.[148] In the past, Brazil's electoral commission has provided technical guidance on voting systems to countries such as Argentina, Mexico, the Dominican Republic, India, and Ukraine.[149] In contrast, U.S. computer scientists have criticized Brazil's voting machines, as maintained by Diebold Election Systems, for being "vulnerable to tampering," given the diminished transparency from not maintaining an auditable paper trail.[150]

Interestingly, while the *urnas* once utilized printers to maintain an auditable paper trail, in fall 2004, the Brazilian

[142] Council Dir. 2008/114/EC (Dec. 8, 2008), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008L0114.

[143] *See How Brazil Has Put an "e" in Vote*, Sao Paulo Special, BBC, (Oct. 1, 2008), http://news.bbc.co.uk/2/hi/7644751.stm (last visited Oct. 7, 2016); Leslie Mira, *For Brazil Voters, Machines Rule*, WIRED, (Jan. 24, 2004), http://www.wired.com/2004/01/for-brazil-voters-machines-rule/ (last visited Oct. 7, 2016).

[144] *See* Diego F. Aranha, *et al., Software Vulnerabilities in the Brazilian Voting Machine*, https://www.researchgate.net/publication/260870433_Software_vulnerabilities_IN_the_Brazilian_voting_machineb (last visited Oct. 7, 2016).

[145] *See* Mira, *supra* note 144.

[146] *See id.*

[147] *See* BBC, *supra* note 143.

[148] *See* Mira, *supra* note 144.

[149] *See id.*

[150] *See id.*

legislature voted to abandon printing e-voting receipts.[151] This decision to modify the *urnas* drew the ire of technologists like University of Campinas Brazil professor Diego Aranha, reasoned "there is a constant danger of large-scale software fraud, as well as other non-technical tampering that could be perpetrated by former or current electoral justice staff and go totally undetected[.]"[152] Similarly, in an interview with *Wired*, Professor Michael Stanton of Universidade Federal Fluminense, decried the government's decision to abandon a paper trail, in order to reduce costs: "Obviously there's a cost (for paper receipts), but on some things you just don't skimp."[153]

A surprising to Brazil's e-voting development arose in December 2015. As a result of the recession and "substantial cuts in public spending," the state announced a return to paper-based voting and manual ballot processing in the 2016 election.[154] Given the legislature's decision in 2004 to abandon printing to save roughly $100 million,[155] it is striking that the state returned to paper ballots in 2016 due to financial considerations. In sum, Brazil's history of e-voting and cost-management approach here offers a cautionary tale to other countries that are evaluating the short-term gains from abandoning a voter-verified paper trail audit.

F. India

Is it no secret that Indian officials regard their electronic voting machines with a sense of national pride, describing them as "tamperproof."[156] As the world's largest democracy, India deploys approximately 1.4 million electronic voting machines for general elections,[157] and utilizes a polling place based Internet voting system.[158] According Alok Shukla, India's former Deputy Election Commissioner, in a 2010 *BBC* interview: "It is not just

[151] *See id.*

[152] *See* Angelica Mari, *Fraud Possible in Brazil's e-Voting System*, BRAZIL TECH, (Oct. 3, 2014), http://www.zdnet.com/article/fraud-possible-in-brazils-e-voting-system/ (last visited Oct. 7, 2016).

[153] *See* Mira, *supra* note 144.

[154] *See Brazil: Due to Recession Brazil Cans e-Voting,* VERIFIED VOTING FOUND., (Dec. 2, 2015), http://thevotingnews.com/international/south-america/brazil/ (last visited Oct. 7, 2016).

[155] *See* Mira, *supra* note 144.

[156] *See* Julian Siddle, *US Scientists 'Hack' India Electronic Voting Machines*, BBC (May 18, 2010), http://www.bbc.com/news/10123478 (last visited Oct. 7, 2016).

[157] *See id.*

[158] *See A Comparative Assessment of Electronic Voting Machines,* ELECTIONS CANADA (June 3, 2014), http://elections.ca/content.aspx?section=res&dir=rec/tech/ivote/comp&document=benefit&lang=e (last visited Oct. 8, 2016).

the machine, but the overall administrative safeguards which we use that make it absolutely impossible for anybody to open the machine."[159] In terms of the machine's design, voting record data and candidate information are captured onto "purpose-built computer chips."[160] Thus, absent any software to exploit, the computer chip raises the bar for manipulating votes on at scale, because one would first need physical access, as well as the resources, to install compromised microchips for each individual machine.[161] Another administrative safeguard, as Shukla described, is that "[b]efore the elections take place, the machine is set in the presence of the candidates and their representatives. These people are allowed to put their seal [paper and wax] on the machine, and nobody can open the machine without breaking the seals."[162] As a result, if the paper and wax seals are broken, this physical evidence can alert Indian election commission officials.[163]

The main benefits of India's polling place based Internet voting system, as described by Elections Canada, a non-partisan research entity, is that the system is primed to void mismarked, or invalid ballots, results can be quickly tabulated, and foreign language and font size fields can be easily changed to accommodate the special needs of voters.[164] In contrast, the risks associated with this system range from voters inadvertently exiting voting screens before their ballot can be properly cast, as well as the cost of maintaining the equipment, and the lack of a voter-verified paper trail audit.[165]

In summary, while India's e-voting system is impressively designed, no device is tamperproof. Indeed, in 2010 a team of computer scientists at the University of Michigan, led by Professor J. Alex Halderman, discovered a significant vulnerability that allowed them to manipulate Indian voter data by using a home-made electronic device.[166] According to Professor Halderman, by concealing a microprocessor and Bluetooth radio in the machine, their "lookalike display board intercepts the vote totals that the machine is trying to display and replaces them with dishonest totals – basically whatever the bad guy wants to show up at the end

[159] Siddle, *supra* note 156.

[160] *Id*.

[161] *See id.* (explaining that "to have any impact [manipulating votes] they would need to install their microchips on many voting machines, no easy task when 1,368,430 were used in the last general election in 2009.").

[162] *See id.*

[163] *Id*.

[164] *See A Comparative Assessment of Electronic Voting Machines, supra* note 158.

[165] *See id.*

[166] *See* Siddle, *supra* note 15. (Professor Halderman explains "We made an imitation display board [of the Indian voting machine] that looks almost exactly like the real display in the machines[.]").

of the election."[167] The researchers also posted a *YouTube* video on how the AVC voting machine could be compromised by using return oriented programing.[168] Using this "invisible vote-stealing" technique, the video reveals how three votes cast for George Washington could be easily shifted to Benedict Arnold, absent any auditable paper trail to verify votes.[169] Thus, like Brazil, the India case study serves as a sobering reminder that no voting machine, however sophisticated, is impervious to manipulation.[170]

G. Summary

This Part has summarized the experiences of the United States, South Africa, Estonia, Brazil, Germany, and India in securing their elections. As was apparent, both approaches and success rates run the gambit. Of the countries studies, two have returned to paper ballots after experimenting with voting machines (Germany and Brazil). In contrast, Estonia has gone the furthest in embracing electronic voting, though its relatively small population and robust program of national identity cards backed up by public key encryption makes its system difficult to replicate in large, diverse democracies. That being said, India boasts a nationwide system of electronic voting machines that, while not being tamperproof, boast significant security features that could be copied by other jurisdictions. While the United States has, to date, undertaken a largely voluntary effort with the DHS and the EAC working with state and local elections officials to test and certify voting machines. The next Part builds from this comparative data on state practice to inform a discussion of norm building in this space.

III. THE GLOBAL DIMENSION

As Part II illustrated, the problem of voting security is increasingly a common concern shared by societies—both advanced democracies and emerging markets alike—around the world. While solutions to this problem range widely from a federated system of experimentation in the U.S. context to Germany and Brazil's decisions to ban voting machines outright

[167] *See id.*

[168] Stephen Checkoway, *et. al., Attacking the AVC Advantage: Computer Scientists Take Over Electronic Voting Machine with New Programming,* https://www.youtube.com/watch?v=lsfG3KPrD1I (last visited Oct. 8, 2016).

[169] *See id.*

[170] *See Samson, Biblical Figure,* ENCYCLOPEDIA BRITANNICA, https://www.britannica.com/biography/Samson (last visited Oct. 8, 2016).

due to security and financial concerns respectively, this common issue provides fruitful ground for international cybersecurity norm building. This Part briefly summarizes recent developments in the field, particularly in the CI context, before couching these findings within the lens of polycentric governance. We conclude with a summary and discussion of implications for policymakers.

A. Minilateral Cyber Norm Building

According to Professors Ron Diebert and Masachi Crete-Nishihata, "states learn from and imitate" one another, and "[t]he most intense forms of imitation and learning occur around national security issues because of the high stakes and urgency involved."[171] In part because of many states' perception that cyber risk is "escalating out of control," there exists an opportunity to engage in constructive international dialogue on norm building,[172] particularly given the international political difficulties involved with new treaty formation in this dynamic space.[173] Potential cyber norms could include a duty to cooperate with victim nations if an attack occurred through information systems in a state's territory, and a duty of care to secure systems and warn potential victims.[174] The Obama Administration has also encouraged the development of norms for respecting intellectual property, mitigating cybercrime, valuing privacy, and working toward global interoperability, reliable access, multi-stakeholder governance, and cybersecurity due diligence.[175] Yet despite the "general agreement

[171] Ronald J. Deibert & Masachi Crete-Nishihata, *Global Governance and the Spread of Cyberspace Controls*, 18 GLOBAL GOVERNANCE 339, 350 (2012).

[172] James A. Lewis, *Confidence-Building and International Agreement in Cybersecurity*, DISARMAMENT FORUM: CONFRONTING CYBERCONFLICT 51, 52 (2011). Though norms do not bind states like a treaty, Lewis notes that "[n]on-proliferation provides many examples of non-binding norms that exercise a powerful influence on state behavior." *Id.* at 53. This position has also been supported by other scholars. *See, e.g.*, Roger Hurwitz, *An Augmented Summary of The Harvard, MIT and U. of Toronto Cyber Norms Workshop* 5 (2012), http://citizenlab.org/cybernorms/augmented-summary.pdf (noting "[a]t the very least, acceptance of a norm by a state puts the state's reputation at risk. If it fails to follow the norm, other states which accept that norm, will typically demand an explanation or account, rather than ignoring the violation or dismissing it as self-interested behavior.").

[173] For more on this topic, see Chapter 7 in SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS: IN SEARCH OF CYBER PEACE (2014).

[174] Eneken Tikk*, Ten Rules of Behavior for Cyber Security,* NATO CCDCOE at 5–6, 8–9 (2011).

[175] INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD, WHITE HOUSE 10 (May 2011).

on a norms-based approach" to enhancing cybersecurity,[176] "even simple norms face serious opposition. Conflicting political agendas, covert military actions, espionage[,] and competition for global influence" have created a difficult context for cyber norm development and diffusion.[177] Consequently, to be successful norms must be "clear, useful, and do-able,"[178] such as beginning with areas of common concern like protecting critical infrastructure.[179]

Positive progress has been made in 2015-16 in relation to the distillation and propagation of cybersecurity norms that may be applied to enhancing election security. The G2 Cybersecurity Code of Conduct between the US and China, for example, calls for mutual restraint in economic cyberespionage, particularly the theft of trade secrets. It could be expanded to include mutual respect for one another's political parties and election infrastructure; a topic held dearly by the Chinese leadership.[180]

Similarly, the G7 continued its work on cybersecurity in 2016, publishing its view that "no country should conduct or knowingly support [information and communication technology-enabled] theft of intellectual property" and that all G7 nations should work to "preserve the global nature of the Internet" including the free flow of information in a nod to the notion of cyberspace as a "global networked commons."[181] Such information could explicitly include data on candidates and norms against outside interference with domestic elections.

Finally, the U.S. proposed three peacetime norms that were accepted for inclusion in the 2015 UN Group of Governmental

[176] Lewis, *supra* note 172, at 55.

[177] *Id*. at 58.

[178] Martha Finnemore, *Cultivating International Cyber Norms*, *in* AMERICA'S CYBER FUTURE: SECURITY AND PROSPERITY IN THE INFORMATION AGE 90, 90 (Kristin M. Lord & Travis Sharp eds., CNAS, 2011).

[179] *See* Richard A. Clarke, *A Global Cyber-Crisis in Waiting*, WASH. POST (Feb. 7, 2013), http://www.washingtonpost.com/opinions/a-global-cyber-crisis-in-waiting/2013/02/07/812e024c-6fd6-11e2-ac36-3d8d9dcaa2e2_story.html?tid=wp_ipad; Hurwitz, *supra* note 172, at 8. Over time, a hierarchy of cyber norms may also be established and married with escalating sanctions as is common across a range of international legal instruments. *Cf.* Jure Vidmar, *Norm Conflicts and Hierarchy in International Law: Towards a Vertical International Legal System?*, *in* HIERARCHY IN INTERNATIONAL LAW: THE PLACE OF HUMAN RIGHTS 13, 14 (Erika De Wet & Jure Vidmar eds., 2012) (questioning "whether the jus cogens-based substantive norm hierarchy is more than theoretical.").

[180] *See* Teri Robinson, *U.S., China Agree to Cybersecurity Code of Conduct*, SC MAG. (June 26, 2015), http://www.scmagazine.com/us-china-summit-talks-turn-to-cybersecurity/article/423175/.

[181] *G7 Leaders Approve Historic Cybersecurity Agreement*, BOSTON GLOBAL FORUM, http://bostonglobalforum.org/2016/06/g7-leaders-produce-historic-cybersecurity-agreement/ (last visited Oct. 4, 2016).

Experts consensus report, which included language on protecting critical infrastructure, safeguarding computer security incident response teams, and collaborating on cybercrime investigations.[182] This CI norm — to which many of the cyber powers, including Russia, have already agreed — could be leveraged to explicitly include elections.[183]

In summary, there is an opportunity for states to become norm entrepreneurs identifying and hastening the uptake of cybersecurity best practices such as those pioneered in Estonia and India.[184] Such a bottoms-up approach to international cybersecurity policymaking is part and parcel of the literature on polycentric governance, introduced next.

B. Applicability of Polycentric Governance

The field of polycentric (muli-centered) governance, also known as the Bloomington School of Political Economy, is a multi-level, multi-purpose, multi-functional, and multi-sectoral model,[185] which has been championed by scholars including Nobel Laureate Elinor Ostrom and Professor Vincent Ostrom. It challenges orthodoxy by demonstrating the benefits of self-organization, networking regulations "at multiple scales,"[186] and examining the extent to which national and private control can in some cases coexist with communal management.[187] The field also posits that, due to the existence of free riders in a multipolar world, "a single governmental unit" is often incapable of managing

[182] *See* Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN General Assembly, A/70/174 (July 22, 2015).

[183] An earlier version of this research appeared as Scott Shackelford, *Opinion: How to Make Democracy Harder to Hack*, CHRISTIAN SCI. MONITOR (July 29, 2016), http://www.csmonitor.com/World/Passcode/Passcode-Voices/2016/0729/Opinion-How-to-make-democracy-harder-to-hack.

[184] *See* TIM MAURER, CYBER NORM EMERGENCE AT THE UNITED NATIONS: AN ANALYSIS OF THE ACTIVITIES AT THE UN REGARDING CYBER-SECURITY 47 (2011).

[185] Michael D. McGinnis, *An Introduction to IAD and the Language of the Ostrom Workshop: A Simple Guide to a Complex Framework*, 39(1) POL'Y STUD. J. 163, 171–72 (Feb. 2011), *available at* http://php.indiana.edu/~mcginnis/iad_guide.pdf.

[186] Elinor Ostrom, *Polycentric Systems as One Approach for Solving Collective-Action Problems* 1 (Ind. Univ. Workshop in Political Theory and Policy Analysis, Working Paper Series No. 08–6, 2008), http://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/4417/W08-6_Ostrom_DLC.pdf?sequence=1.

[187] For a detailed discussion of early Internet history, see KATIE HAFNER & MATTHEW LYON, WHERE WIZARDS STAY UP LATE: THE ORIGINS OF THE INTERNET (1996); *Brief History of the Internet*, INTERNET SOC'Y, www.isoc.org/internet/history/brief.shtml.

"global collective action problems"[188] such as cyber attacks. Instead, a polycentric approach recognizes that diverse organizations working at multiple levels can create different types of policies that can increase levels of cooperation and compliance, enhancing "flexibility across issues and adaptability over time."[189] Such an approach, in other words, recognizes both the common but differentiated responsibilities of public- and private-sector stakeholders as well as the potential for best practices to be identified and spread organically, generating positive network effects that could, in time, result in the emergence of a cascade toward CI protection generally, and voting security particularly.[190] Indeed, popular attention is engaged in the problem of voting cybersecurity in a way that has not happened before with a supermajority of sixty-six percent of respondents to one 2016 survey saying that cyber criminals are influencing the outcomes of the 2016 election,[191] potentially laying the groundwork for action by policymakers.

C. Implications for Policymakers

Previous research, including some cited in Part I, has identified areas in which election infrastructure must improve. There are practical steps states can take in order to make these improvements, though it should be noted at the outset that, due to the huge range of jurisdictions in play, there are limitations on what the federal government can or should do with regards to designating election infrastructure as CI. As such, some of these steps will necessarily be carried out by the local election administrators; these may be aided indirectly by additional funding and attention made possible via a CI designation. Other steps are of a more cross-cutting nature and could benefit more directly from a federal role.

The first key decision in electoral preparation is which technology to deploy. After the hanging chad incidents of 2000,

[188] Elinor Ostrom, *A Polycentric Approach for Coping with Climate Change* 35 (World Bank, Policy Research Working Paper No. 5095, 2009), http://www.iadb.org/intal/intalcdi/pe/2009/04268.pdf.

[189] Robert O. Keohane & David G. Victor, *The Regime Complex for Climate Change* 9 PERSP. ON POL. 7, 9 (2011); *cf.* Julia Black, *Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes*, 2 REG. & GOVERNANCE 137, 157 (2008) (discussing the legitimacy of polycentric regimes, and arguing that "[a]ll regulatory regimes are polycentric to varying degrees").

[190] *See* Martha Finnemore & Kathryn Sikkink, *International Norm Dynamics and Political Change*, 52 INT'L ORG. 887, 895–98 (1998).

[191] *See* Research, Tripwire, http://www.tripwire.com/company/research/ (last visited Oct. 3, 2016).

Congress passed HAVA as was discussed in Part I, which outlawed punch card machines and provided funding for new digital machines. Many of these machines are still in use. The lesson of 2016, and of previous cycles, should be that these systems are not always secure against modern threats. State governments, perhaps aided by federal funding and attention accompanying a CI designation, should ensure that their machines are hardened against the risk of hacking. In many jurisdictions, this will likely mean buying new machines.

Going forward, it is vital that every voting system generate a voter-verified paper audit trail as a bulwark against hacking and to build trust (something that was missing in both the German and later Brazilian approaches). This paper trail can be a ballot manually marked by the voter and scanned by computer with the ballot retained for later audits and recounts, as optical scan voting machines do. Or it can be a paper ballot marked by machine, responding to the inputs of the voter on a touch screen. If it is the latter design, the paper ballot must be visible to the voter at some point during the process for verification purposes.

In conjunction with the purchase of new machines where appropriate, security audits and vulnerability scans of all machines and registration systems are essential. These procedures can identify potential vectors of attack ahead of time, and remediate them before hackers can take advantage. As noted above, there is a long history of states that employ such audits finding and fixing weaknesses, such as misconfigured systems, Internet-connected devices, poor encryption, and weak passwords. These fixes directly improve election security. It is an essential part of a credible cybersecurity posture to expand the scope of this pre-election preparation.

Information sharing is another important aspect to mitigating the risk to voting machines. There is an argument for creating a voting ISAC or broader ISAO.[192] The creation of such an ISAC has become part of the standard response toolkit across a range of industries following a breach—such as the Retail ISAC after Target's 2014 cyber attack, or the more recent automobile ISAC post-car hacking stories.[193] These sharing centers provide a mechanism for stakeholders to share data on vulnerabilities and threats with one another to more quickly and more effectively guard against emerging threats.

[192] Dep't Homeland Sec., Information Sharing and Analysis Organizations (ISAOs), http://www.dhs.gov/isao (last visited Dec. 17, 2015).

[193] *See Retail-ISAC Launches Cyber Sharing Portal Supported by FS-ISAC*, PR Newswire (Mar. 24, 2015), http://www.prnewswire.com/news-releases/retail-isac-launches-cyber-sharing-portal-supported-by-fs-isac-300055086.html.

During an election, electoral commissions should prepare for irregularities and interference. As the previously-discussed Ukraine case shows, astute observation can spot malicious activity before it achieves its objective. Authorities should create verified, secured, and redundant lines of communication with media organizations to credibly share information in a timely manner. Media should take care to be skeptical of hacking reports, so as to not sow doubt where none need exist, but should hold election authorities to account.

After an election, all jurisdictions should carry out what is known as a risk-limited audit. Such an audit samples an appropriate percentage of paper ballots to confirm that no significant impropriety has occurred; the percentage of ballots sampled can be determined by statistical means and varies with the closeness of an election. Such a mathematically-rigorous sampling method is efficient and, while it cannot guard against all electoral manipulation, it can provide a very high degree of certainty that any manipulation that did occur did not change the winner of the election. Additionally, credible and standardized post-election audit procedures could increase voter and candidate confidence in the outcome.[194] There is currently enormous range in the quality and rigor of post-election procedures.

The Obama Administration has reportedly considered a full range of tools in response to cyber attacks on U.S. election systems, including "public shaming, sanctions and indictments."[195] As with preventing attacks on election infrastructure, it is equally vital to have a clear understanding of the ramifications for designating democratic processes as part of CI. As was discussed in Part I, there are myriad benefits and drawbacks to such a delineation, and ultimately there must be a balance that takes into account the constitutional protections of federalism in U.S. elections. This could take the form of the federal government acting predominantly as a resource for jurisdictions, though various incentives could also be used to entice states to update their election laws and boost security such as 'Race to the Top' funding reminiscent of the education sector.

One more obvious role for the federal government is to consider how best to deter foreign rivals from attempting to undermine the integrity of U.S. elections, especially through cyber-enabled means. Just how well deterrence is operating in any given

[194] Mark Lindeman et al., *Principles and Best Practices in Post Election Audits, Election Audits* (2008), http://electionaudits.org/files/best practices final_0.pdf.

[195] Lisa O. Monaco, Keynote Address, Ctr. Strategic & Int'l Stud., https://www.csis.org/transcripts-national-security-division-10 (last visited Oct. 4, 2016).

situation is notoriously different to prove (is the target not acting because she is deterred, or because she is simply unable?), but attempts should be made regardless.

The principal method of deterrence is known as deterrence by cost imposition. By threatening to impose unacceptable cost on a rival if the rival engages in a certain action, the hope is that the rival correctly understands that those costs outweigh expected gains. The challenge for the United States as it considers how to deter meddling in its election systems is to make a threat that is credible but not excessively escalatory.

One method of cost imposition the United States has previously employed against foreign hackers is to expose them. While a "naming and shaming" approach may at first blush seem unsatisfying as a response action, exposure not just of the names of the hackers but of methods of hacking can force remaining hackers to abandon the now-compromised infrastructure and allows defenders to block the now-compromised techniques of intrusion. To be effective, however, the United States would need to remain vigilant to guard against the potential of the exposed hackers continuing follow-on attacks using different infrastructure. As of this writing, the United States has attributed to Russia the hacking of the DNC, but it has officially said little more.[196]

Another method to impose cost, which can be undertaken in addition to exposure, is to indict the offending hackers. The United States pursued indictments to impose cost on five Chinese hackers from the People's Liberation Army and on several hackers with various affiliations to Iran. While these foreign hackers are behind the immediate reach of U.S. law enforcement, indicting them adds a heightened level of probably unwanted exposure to these hackers. It also hinders geographic freedom of movement, as they would not want to arrange future travel in ways that would make them susceptible to coming within grasp of the long arm of our laws.

An additional method of cost imposition is for the United States to threaten to impose sanctions on offending entities, organizations, or individuals. There are two avenues of authority under which such sanctions might be ordered. First, President Obama's April 1, 2015 executive order enables the blocking of property of those the United States determines are committing certain significant malicious cyber activities.[197] This "direct"

[196] *See, e.g.*, Katie Bo Willaims, *Obama Administration Publicly Blames Russia for DNC Hack*, HILL (Oct. 7, 2016), http://thehill.com/policy/cybersecurity/299874-obama-administration-publicly-blames-russia-for-dnc-hack.

[197] Executive Order, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities" (Apr. 1, 2015),

sanction authority is tailored to those who, among other things, harm a computer that is part, or compromise the privison of services within, a critical infrastructure sector. To sanction those who would attempt to compromise the U.S. election system under this authority, it would seem that designating the electoral system as CI is a necessary first step. As of this writing, the federal government has not sanctioned any entities under this authority.

A second avenue through which the United States could impose sanctions as a method of cost imposition is by other, "indirect" authority. Here, the federal government could sanction entities not directly for their hacking activities, but on account of their government affiliations or other non-cyber related offenses. For example, in the aftermath of North Korea's cyber attack against Sony Pictures, President Obama signed an Executive Order that authorized sanctions against almost any North Korean government official, regardless of the hand they may have had in the cyber attack against Sony.[198] The value of these indirect sanctions as a method of cost imposition is compelling because now the political masters of perpetrators of cyber attacks – not just the hackers themselves – are more at risk of having their assets frozen or their travel banned.

Another method through which the United States could threaten to impose cost to deter cyber attacks is to threaten to counter-attack. At one extreme, a Defense Science Board report encouraged policymakers to consider the threat of employing nuclear weapons as an option to deter large-scale, catastrophic cyber attacks.[199] Non-nuclear kinetic strikes are also an available method to impose cost, though the cyber attack that triggers such a response would likely need to cause significant physical damage and disruption this kind of kinetic response. The United States could also employ a non-kinetic military response option, like a proportional offensive cyber operation.

Using military force in any of these scenarios is a significant step and should never be undertaken lightly. But as cyber attacks threaten different aspects of U.S. democracitc society

https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m.

[198] *See* Executive Order, Imposing Additional Sanctions with Respect to North Korea (Jan. 2, 2015), https://www.whitehouse.gov/the-press-office/2015/01/02/executive-order-imposing-additional-sanctions-respect-north-korea.

[199] *See* DEP'T OF DEF., DEF. SCI. BOARD, RESILIENT MILITARY SYSTEMS AND THE ADVANCED CYBER THREAT 1 (2013), http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf.

and security, it becomes more plausible to consider such options to deter would-be attackers.[200]

CONCLUSION

When we flip a switch, we expect the lights to come on. When we pull a lever, or touch a screen, we expect our vote to accurately be recorded. And when we debate about the next U.S. president, we expect that dialogue to be free of foreign entanglements. A first step in realizing these goals—and ensuring that the 2016 DNC hack, or worse, is not repeated in 2020, and 2024—is by recognizing our democratic machinery as being at least as important as our industrial machinery. We recommend that the U.S. voting system be classified as CI, but that that be the beginning of the process to secure U.S. elections, not the end.

[200] It may also be desirable to begin a conversation about prioritizing risks to U.S. CI such that movie theatres are no longer on bar with the electric grid in terms of DHS policymaking. Other nations, including China, already have such a policy in place. *See* Scott J. Shackelford & Amanda N. Craig, *Beyond the New 'Digital Divide': Analyzing the Evolving Role of Governments in Internet Governance and Enhancing Cybersecurity*, 50 STAN. J. OF INT'L L. 119, 158-63 (2014).