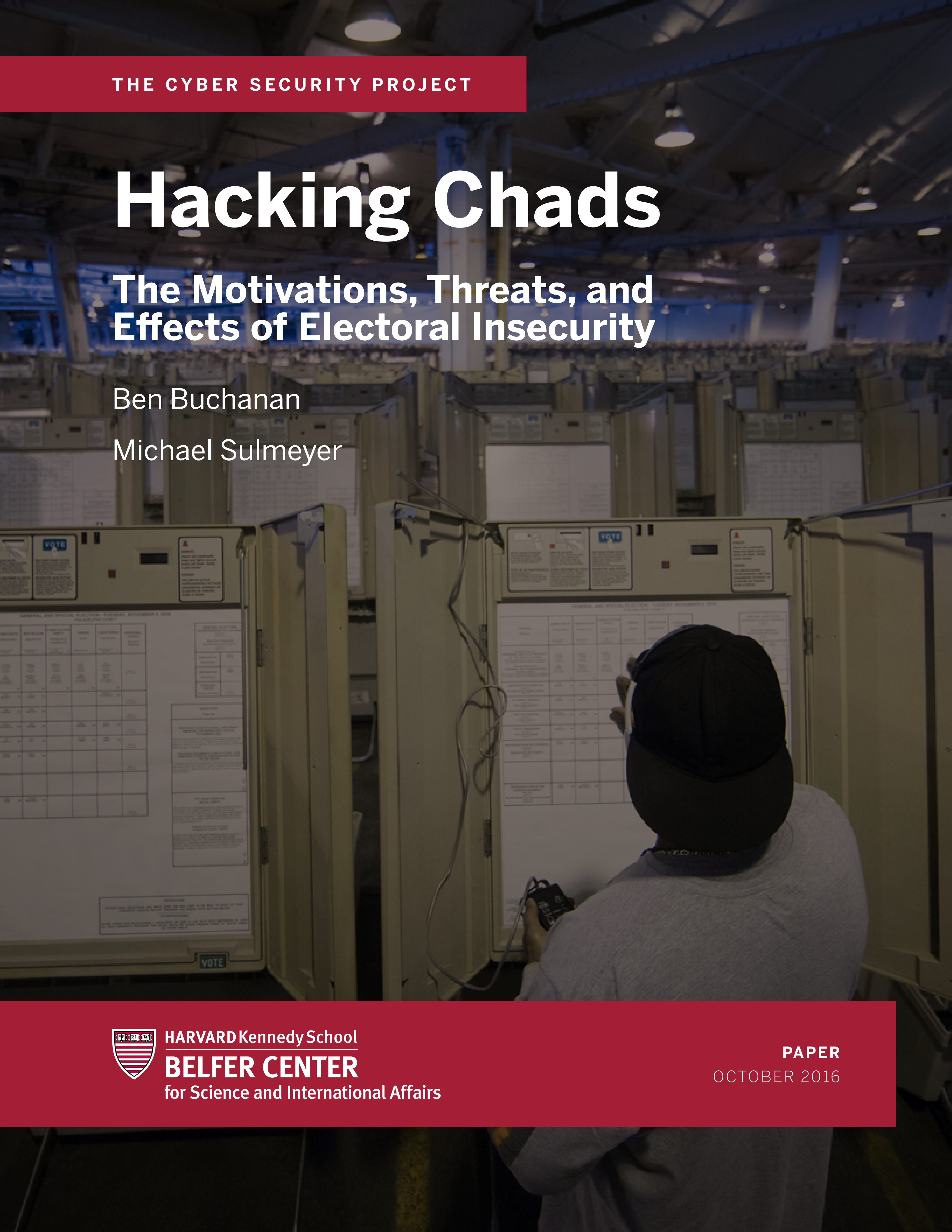


THE CYBER SECURITY PROJECT

Hacking Chads

The Motivations, Threats, and Effects of Electoral Insecurity

Ben Buchanan

Michael Sulmeyer

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
OCTOBER 2016

The Cyber Security Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138
www.belfercenter.org/cyber

Design & Layout by Andrew Facini

Cover photo: A technician works to prepare voting machines to be used in the upcoming presidential election, in Philadelphia, Friday, Oct. 14, 2016. (AP Photo/Matt Rourke)

Statements and views expressed in this discussion paper are solely those of the authors and do not imply endorsement by Harvard University, Harvard Kennedy School, or the Belfer Center for Science and International Affairs.

THE CYBER SECURITY PROJECT

Hacking Chads

The Motivations, Threats, and Effects of Electoral Insecurity

Ben Buchanan

Michael Sulmeyer

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
OCTOBER 2016

About the Authors

Ben Buchanan is a Postdoctoral Fellow at the Belfer Center Cybersecurity Project, where he conducts research on the intersection of cybersecurity and statecraft. He received his PhD in War Studies from King's College London, where he was a Marshall Scholar, and earned masters and undergraduate degrees from Georgetown University. His first book, The Cybersecurity Dilemma, will be published by Oxford University Press and Hurst this year. Previously, he has written on attributing cyber attacks, deterrence in cyber operations, cryptography, and the spread of malicious code between nations and non-state actors.

Michael Sulmeyer is the Belfer Center's Cyber Security Project director at the Harvard Kennedy School. He recently concluded several years in the Office of the Secretary of Defense, serving most recently as the Director for Plans and Operations for Cyber Policy. He was also Senior Policy Advisor to the Deputy Assistant Secretary of Defense for Cyber Policy. In these jobs, he worked closely with the Joint Staff and Cyber Command on a variety of efforts to counter malicious cyber activity against U.S. and DoD interests. Previously, he worked on arms control and the maintenance of strategic stability between the United States, Russia, and China. As a Marshall Scholar, Sulmeyer received his doctorate in Politics from Oxford University, and his dissertation, "Money for Nothing: Understanding the Termination of U.S. Major Defense Acquisition Programs," won the Sir Walter Bagehot Prize for best dissertation in government and public administration. He received his B.A. and J.D. from Stanford University and his M.A. in War Studies from King's College London. In the mid-1990s, he was the System Operator (SysOp) of The Summit BBS in Santa Barbara, California. *The views expressed in this publication are his own and do not necessarily reflect the official policy or position of the Department of Defense or the U.S. Government.*

Executive Summary

This paper addresses a growing concern to one of the most fundamental components of our democracy: how cybersecurity risks can influence the integrity of our elections. This past summer's hacks and attempted network intrusions into a variety of Democratic Party networks and into election infrastructure highlight the urgency of the issue. The mounting evidence of Russian involvement, confirmed in an unprecedented statement by the Obama Administration in October, underscores the stakes. While there previously have been occasional – and mostly unfounded – concerns about localized voter fraud in U.S. elections, this is the first time a foreign nation attempt to influence a U.S. election by taking advantage of weaknesses in our cybersecurity.

Two vital questions emerge. First, how concerned should we be about election cybersecurity? Second, how vulnerable is the United States to a foreign power or other actor trying to undermine the public's confidence in our elections? In examining these issues, we consider the motivations of hackers for targeting elections, the plausible threats to election security, and the effects of real and perceived manipulation.

We argue that foreign intelligence agencies, most prominently Russia's, have plausible motivations and capabilities for some kinds of electoral interference. In addition, there are other actors, such as terrorist groups, partisan activists, and groups with narrow parochial interests, which might

seek to manipulate an election. There is a range of possible mechanisms for carrying out these threats, including targeting voters, voting rolls, voting machines, tabulation, and the dissemination of results. We draw on security audits and demonstrated cases of previous Russian operations in analyzing these risks. We argue that it is not just the reality of fraud that is concerning, but the perception of it. The effects of perceived illegitimacy can be deeply damaging and perhaps harder to counteract. In particular, persistent questions about electoral integrity may by itself advance foreign interests.

We put forth five recommendations for improving the cybersecurity of elections, showing their integrity, and guarding against threats. First, the federal government should designate election systems as critical infrastructure, catalyzing additional federal and state attention to improving cybersecurity. Second, backed by federal funding, states should purchase and deploy voting machines that generate a voter-verifiable paper audit trail. Third, states should expand their use of pre-election security audits to identify and remediate vulnerabilities. Fourth, states should establish or improve their post-election audit procedures, applying statistically rigorous methods to increase confidence in the reported results. Lastly, the United States should outline a clear policy on the seriousness of electoral interference as a means of deterring foreign adversaries.

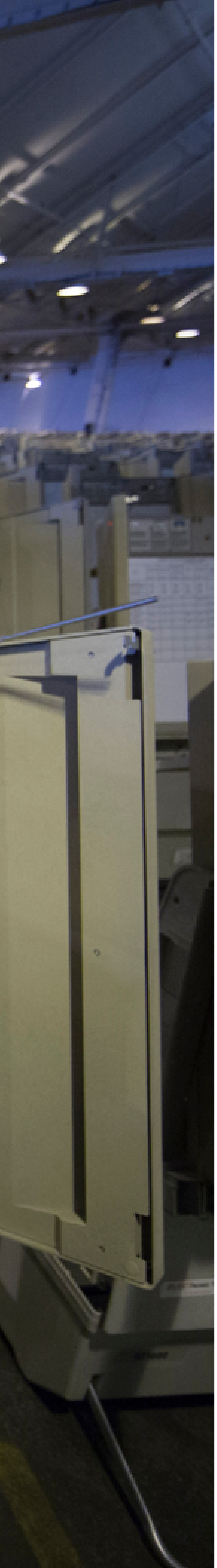
Acknowledgments

The authors would like to thank the Belfer Family and the Hewlett Foundation for supporting this research. They would also like to thank **Jessica Malekos Smith** for her excellent research assistance on this paper. In addition, the authors thank **Pamela Smith**, **Joe Nye**, and **Bruce Schneier** for providing feedback on earlier drafts

Table of Contents

A technician works to prepare voting machines to be used in the upcoming presidential election, in Philadelphia, Friday, Oct. 14, 2016.

AP Photo/Matt Rourke



Introduction

In the summer and fall of 1984, the small locale of Wasco County, Oregon, readied itself for the coming election. Candidates campaigned, citizens registered, and officials prepared. A large group of followers of Bhagwan Shree Rajneesh, an Indian spiritual teacher, lived in a commune in the county. They, too, organized for Election Day. Worried that their candidates would not win the county election, they devised a multi-step plan. First, they would bring in thousands of individuals from around the country and attempt to register them locally. Second, they would use salmonella to poison the non-Rajneeshee people of Wasco County, thereby forcing these voters to stay home. In September and October 1984, the group spread the bacteria on salad bars in ten restaurants. The germs sickened 751 people in The Dalles, population 12,000, Wasco County's largest town.

The plan failed. The county clerk ruled that those brought in from out of town were not eligible to vote. The poisonings, though significant, killed no one and were not recognized as an attack until later. As November arrived, the Rajneeshees predicted defeat and chose to boycott the election. By the next year, the group had begun to unravel. With mounting internal strife and facing federal investigation, its leaders planned—this time using guns—to assassinate the United States Attorney. That was also unsuccessful, and various Rajneeshee leaders served time in prison for the crimes.[1]

We bring up this old case because it highlights several themes of renewed modern relevance. First, it shows the range of motivation behind election fraud and manipulation; election tampering can derive from geopolitical aims, but also from purely parochial interests. Second, the incident illustrates the unusual methods groups considering such manipulation pursue, and the countermeasures election officials must take to protect the system's integrity against a wide range of threats. Third, it reveals the difficulty in achieving some kinds of electoral manipulation, especially on a large scale. The very small

[1] For more on the incident, see Judith Miller, Stephen Engelberg, and William Broad, Germs: Biological Weapons and America's Secret War, (New York: Simon & Schuster, 2002).

number of even small-scale election fraud cases is further testament to this fact.[2] Nonetheless, the perception of manipulation can be deeply detrimental to the democratic process.

The intrusions into key networks of the Democratic Party and into parts of the American voting infrastructure are foreboding. They highlight the possibility of electoral interference via cyber means. The Obama Administration's statement in October of 2016 that Russia was involved in at least some of these intrusions is deeply significant, and underscores how the digital integrity of elections is a matter of geopolitics as well as computer science. This intersection of technology and international affairs is a complex and vital one. The aim of this paper therefore is to consider, contextualize, and help mitigate the cybersecurity threats to American elections.

We argue that, while a foreign intelligence service is likely the most persistent and capable threat, a range of actors might have reason to try to interfere with the electoral process. Though actually swinging the result of a presidential election is a major challenge, even the appearance or allegations of improprieties are damaging. It is too late to fully mitigate this danger in 2016, but the cybersecurity of future elections should be a paramount concern. The paper's goal is neither to catalogue every possible danger, nor to provide a technical roadmap of solutions. Instead, this paper seeks to frame this issue and elevate it as a topic of importance. The risk simply isn't going away.

To make this argument, we have divided this paper into three sections, each linked to one of the above themes. The first section outlines categories of actors and their motivations for manipulating an election via cyber means. The second section offers a typology of different types of cyber threats to the election, building on excellent technical audits and work done by other researchers. The third and final section considers the difficulty of accomplishing such a task, but also the dangerous effects of perceived electoral irregularities, especially in the absence of verification mechanisms. We then conclude with five recommendations for improving the cybersecurity of elections.

[2] A bipartisan report on electoral fraud concluded that successful electoral manipulation was "rare." 'The American Voting Experience: Report and Recommendations of the Presidential Commission on Election Administration', Presidential Commission on Election Administration, 2014, 55.

Motivations

Who might seek to manipulate an election, and why? Though this list of possible actors is hardly exhaustive, this section aims to show the multiplicity of conceivable incentives for electoral interference, the variety of potential actors, and the range of levels—local, state, and federal—possibly affected.

Perhaps the most widely discussed possibility is the potential for a foreign state to manipulate an election to advance its broad geopolitical interests. Trade deals, diplomacy, and military affairs all depend in large part on the political leadership of nations. The leaders of one state may wish to influence whom its interlocutors are in another. For this reason, there is a well-documented history, long preceding the use of cyber capabilities, of states interfering with the elections of other states. From 1945 to 2000, the United States and Russia combined to intervene in 117 national-level foreign elections.[3] Sometimes this influence was overt, such as the American support for West Germany Chancellor Konrad Adenauer in 1953, but in many cases it was not. It is therefore entirely plausible, perhaps even likely, that cyber capabilities could play a role in similar modern efforts. For instance, hackers potentially linked to Russia attempted to interfere with Ukraine's 2014 election; the mechanics of that attack will be discussed below.[4]

Too frequently, though, the discussion of actors with the intent to interfere with an election ends here. This is a mistake that ignores other possible actors and their motivations. For example, a terrorist organization might attempt to undermine the legitimacy of an election. Such a group could have a preferred candidate, as demonstrated by the coordinated bombing of the Madrid subway in 2004. Those attacks killed 192 people three days prior to Spain's general election and helped usher in a Prime Minister who withdrew Spanish forces from the Iraq War.[5] A terrorist group also might

[3] Dov H. Levin, 'When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results', *International Studies Quarterly* (2016).

[4] Mark Clayton, 'Ukraine Election Narrowly Avoided 'Wanton Destruction' from Hackers', *Christian Science Monitor*, 17 June 2014.

[5] For more on the effects of the attack on the election, see William Rose, Rysia Murphy, and Max Abrahms, 'Does Terrorism Ever Work? The 2004 Madrid Train Bombings', *International Security* 32, no. 1 (2007).

want to meddle with or undercut the practice of democracy. The group may claim responsibility for the attempt or attempt to remain covert.

At home, a candidate and political party could attempt to rig an election. The incentive here is obvious. The candidate and party is likely to believe that their view on the issues is correct, that the other side would do damage—perhaps irreparably so—in vital areas, and that electoral impropriety in this case serves long-run national interests. There are practical incentives as well. Access to power, funds, and higher offices could also motivate self-interested fraud. It is possible a candidate could undertake such an interference effort on his or her own, without the knowledge of the political party, and vice versa.

If talented and persistent enough, an individual unaffiliated with a campaign might try to hack an election. This individual could be motivated by partisan concerns, by a passionate view on a single issue, by aspirations of notoriety, or even by a desire to demonstrate the insecurity of the electoral process and prompt reform. This individual might have particular expertise in elections, in computer systems, or both. For instance, it is believed that Bruce Ivins, a senior biodefense researcher for the United States government, carried out the 2001 anthrax attacks; one motivation psychologists identified for his behavior is that the attacks "elevate[d] his own significance" and brought greater attention to the importance of biodefense research.[6] A similar desire could prompt an individual to target the electoral system. Indeed, in 2016 the owner of a cybersecurity company was charged with hacking a Florida election system in order to highlight its vulnerabilities.[7]

Lastly, there is possibility of more attacks like those by the Rajneeshees, in which local groups, concerned with parochial interest, try to manipulate an election. This group could interfere with a local election, but have effects that reach further or are perceived to do so, especially if they live in a swing state or swing region.

[6] Gregory Saathoff *et al.*, 'Report of the Expert Behavioral Analysis Panel', Research Strategies Network, 2011. Scott Shane, 'Panel on Anthrax Inquiry Finds Case against Ivins Persuasive', *The New York Times*, 23 March 2011.

[7] Dan Goodin, 'How a Security Pro's Ill-Advised Hack of a Florida Elections Site Backfired', *Ars Technica*, 9 May 2016.

It is difficult to assess how many significant actors fall into each category. But, in the anticipation or aftermath of electoral irregularities, officials and analysts would do well to remember the broad range of possibilities rather than assume that a foreign government's hand lies behind every turn. Without such a broad view, a careful analysis of competing hypotheses is not possible. Furthermore, the broader range of actors reveals the limits of strategies such as deterrence through cost imposition as a primary means of securing elections; not every actor on the list above will be easily deterred, even by prison or by geopolitical consequences. While deterrence has an important role, particularly in thwarting sophisticated potential adversaries, the overall problem of election security is made more manageable by solid cybersecurity designs that guard against simpler threats from less capable actors.

Threats

Electoral interference can take many forms. The mechanics of carrying out election fraud via cyber means are crucial to understanding which threats are credible and which are not. This section defines the threat of electoral interference as the illegitimate manipulation of voters or votes in an effort to change the outcome of an election or undermine the credibility of the result. Since the focus of this paper is on cyber capabilities, the typology of different threats that follows is limited only to those that directly employ the use of such capabilities. These are usually network intrusions. General information operations, such as radio, television, and social media efforts, fall outside of the scope of this paper.

Computer scientists divide threats into three categories: those that target the confidentiality of data or systems, those that target their integrity, and those that target their availability. This framework is useful for assessing the potential for manipulation or interference with the American electoral process. It is also useful to distinguish between manipulating voters (causing them to a cast a ballot for a preferred candidate) and manipulating votes (causing an actual casted ballot to be discounted or changed). Manipulation of confidentiality, integrity, and availability of various systems and data is useful for both types of operations. This has long been true—the Rajneeshees' poisoning can be thought of as an attempt to limit voters' availability—but cyber operations offer some new and interesting possibilities in scale and impact.

One way in which an actor targeting voters can influence the election is by making public damaging confidential information obtained via network intrusions. Using this tactic, the actor seeks to influence voters into choosing the actor's preferred candidate or otherwise sows discord in the political process. The most prominent example comes from the summer of 2016, in which Russian actors released internal Democratic National Committee documents perceived as unflattering to the party. After the release of this information, Democratic National Committee Chairwoman Debbie Wasserman Schultz resigned, in part due to concerns that the committee had shown a preference during the primary nominating process. The actor or actors, using the pseudonym "Guccifer 2.0," also released additional documents, including the Democratic Party's opposition file on Donald Trump, a large number of internal emails and strategy documents, and private information on donors and party officials.[8]

Without cyber capabilities, this operation would have been much more difficult to complete. The private documents leaked throughout the summer of 2016 were apparently obtained via network intrusions into a variety of Democratic Party systems. By making confidential data public, the hackers may have intended to exert influence on the political process and on the election. Leaking the opposition file and strategy documents may have undercut future Democratic political efforts. The emails forced a distracting shake-up in party headquarters, while the personal details on donors and candidates may have a chilling effect on participation. But all of this includes some amount of speculation. It is too soon to say what many of the practical effects of the leaks are, what the motivation of the hacker or hackers might be, and—most importantly—whether or how voters take the resulting news stories into account. Influencing voters through the release of confidential information is a lengthy and uncertain undertaking.

A more direct tactic might be influencing voters by manipulating not just the confidentiality but also the integrity of information. Though it appears the documents from the Democratic Party were authentic, it would have been a challenge for the party to verify publicly the integrity, or lack thereof, if some documents were fake. In short, an actor could hack a targeted system, copy a large number of authentic documents, and then either manipulate those documents or add new ones with embarrassing—but untrue—information.[9]

Russian hackers appeared to try this in 2016. They broke into the Open Society Foundation's computer systems, copied budget and other documents, and posted them online. But before they did so, they added a line item to the budget suggesting that the foundation had given money to anti-corruption advocates in Russia, an allegation that appears to be false,

[8] For an overview of the case, see Thomas Rid, 'All Signs Point to Russia Being Behind DNC Hack', *VICE*, 25 July 2016.

[9] For one discussion of the possibilities, see Bruce Schneier, 'How Long until Hackers Start Faking Leaked Documents?', *The Atlantic*, 13 September 2016.

though one that generated discussion in the relevant communities.[10] This tactic appears to be a cog in the broader Russian disinformation machine, an apparatus that former NATO Supreme Commander Phillip Breedlove said was capable of "the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare."[11]

Even with the tactic of false information, influencing voters is an indirect and inexact effort. Hackers might find more direct alternatives more appealing. Rather than targeting fickle voters, they can target votes and the voting process itself. Simply put, the disparate voting infrastructure in the United States—much of which was revamped after the contested 2000 election—has not been designed with cybersecurity as a priority. Once again, the confidentiality-integrity-availability triad is useful for conceptualizing threats.

The most immediate risk is that a hacker might manipulate a voting machine so that a vote for one candidate counts for someone else. This is an obvious attack on integrity. One method is to access the tabulation function on the machine itself. Sometimes this requires gaining physical access to the device, and there are a wide variety of conceptual attacks of this kind that have been demonstrated by researchers.[12]

Other times this manipulation can be done using wireless networks, if the voting machines connect to them. A 2015 audit by the Virginia government of some of its voting machines revealed gaping vulnerabilities in this area. The systems used a wireless connection to communicate with one another that used a default password of "abcde" and an old standard of encryption. The machines' operating system was a 2002 version of Windows XP that was not patched with security updates and enabled attackers to exploit critical vulnerabilities and run their own code remotely. The Virginia testers were able to both bypass and crack the weak password used in the machines' voting databases—also five letters long—and directly

[10] Elias Groll, 'Turns Out You Can't Trust Russian Hackers Anymore', *Foreign Policy*, 22 August 2016.

[11] Neil MacFarquhar, 'A Powerful Russian Weapon: The Spread of False Stories', New York Times, 28 August 2016. Peter Pomerantsev, 'Russia and the Menace of Unreality', *The Atlantic*, 9 September 2014.

[12] For a seminal example, see Tadayoshi Kohno et al., 'Analysis of an Electronic Voting System', IEEE Symposium on Security and Privacy (2004). For a broad survey, see Lawrence Norden, 'The Machinery of Democracy', Brennan Center for Justice, 2006.

view and modify voting and tabulation data.[13] These particular machines have since been taken out of use, but they are not alone in exhibiting major flaws. A different series of voting machine audits of a variety of systems revealed a wide array of problems in access control, data processing, cryptography, and software design.[14]

Another risk is that hackers might target the availability of key parts of the voting infrastructure. By making it harder for some people to vote, they could undermine confidence in the election and perhaps influence its outcome. For instance, an effort to slow the voting process in urban centers in Ohio would disproportionately hurt Democrats, while a similar digital attack on conservative rural areas in Pennsylvania would hurt Republicans. Such an attack could target the voting machines themselves, either slowing their operation or rendering them unavailable. In a 2002 primary in Florida, voting machines malfunctioned—for reasons not related to hacking—locking out voters and resulting in hours-long lines.[15]

Or such an attack could target the verification systems used to ensure that individuals are eligible to vote, frustrating voters and forcing the use of provisional ballots. As voting rolls become digitized—some states such as Ohio have dramatically expanded their use of digital poll books on Election Day[16]—this is an attack vector that could be increasingly appealing. Some of these systems have already suffered attacks on confidentiality. It appears that hackers have partially copied at least one state's voting rolls, targeted more than 20 others, and prompted several states to temporarily

[13] 'Security Assessment of WinVote Voting Equipment for Department of Elections', Commonwealth Security and Risk Management: Virginia Information Technology Agency, 2015.

[14] For a sampling of high-quality audits, see Srinivas Inguva *et al.,* 'Source Code Review of the Hart InterCivic Voting System', Berkeley University of California: California Secretary of State, 2007; 'Everest: Evaluation and Validation of Election-Related Equipment, Standards and Testing': Ohio Secretary of State, 2007; 'Source Code Review of the Sequoia Voting System', Berkeley University of California: California Secretary of State, 2007; 'Source Code Review of the Diebold Voting System', Berkeley University of California: California Secretary of State, 2007; Ariel J. Feldman, J. Alex Halderman, and Edward Felten, 'Security Analysis of the Diebold AccuVote-TS Voting Machine', USENIX/ACCURATE Electronic Voting Technology Workshop, 2006.

[15] 'New Florida Voting Machines Malfunction, Cause Delays ', USA Today, 10 September 2002; Rebecca Mercuri, 'Florida Primary 2002: Back to the Future', *Forum on Risks to the Public in Computers and Related Systems*, 22, no. 24 (2002).

[16] Karen Farkas, 'Electronic Poll Books Will Be at Voting Locations across the State by November 2016', Cleveland Plain Dealer, 28 August 2015. Katy Owens Hubler, 'Electronic Poll Books', National Conference of State Legislatures, 21 May 2016.

take their voter registration systems offline.[17] While copying voter information is by itself not enormously significant—some interested parties can legally purchase some voting roll information without hacking—the relatively unsophisticated breaches demonstrate the low level of security in some voting roll systems.[18] The attacks on confidentiality may undermine voter confidence or may be a precursor to a more serious attack on the availability or integrity of voter rolls. Removing large number of voters on the rolls is a serious risk, and one that would cause substantial upheaval on Election Day.[19]

Tabulation mechanisms are another possible vector of attack. This category of operation recalls Josef Stalin's famous statement: "I consider it completely unimportant who in the party will vote, or how; but what is extraordinarily important is this — who will count the votes, and how."[20] The risk to tabulation systems has already been demonstrated in other cases. In Ukraine in 2014, attackers deleted key files from the election commission's vote tallying computers just days prior to the election, forcing officials to rely on backups.[21] The compromise was so total that one investigator later said, "Literally, nothing worked."[22] As outlined earlier, at the machine or precinct level, security audits show that variety of compromises can enable attackers to manipulate the tabulation of votes.

Lastly, the distribution of timely and credible election results is a final possible area of weakness. For example, if automated data streams are used to inform news organizations of the outcome, attackers might manipulate these to try to goad the press into reporting things that will later be undercut or withdrawn. Or they might take control of a reporting stream such as an official Twitter account and disseminate false results directly; this occurred in

[17] Michael Isikoff, 'FBI Says Foreign Hackers Penetrated State Election Systems', Yahoo News, 29 August 2016. Tami Abdollah, 'US Official: Hackers Targeted Election Systems of 20 States', Associated Press, 30 September 2016.

[18] For one perspective on the lack of sophistication in some of these breaches written by a veteran information security professional, see Chris Wysopal, 'Election System Hacks: We're Focused on the Wrong Things', InfoWorld, 20 September 2016.

[19] 'Testimony of Dr. Dan S. Wallach: Protecting the 2016 Elections from Cyber and Voting Machine Attacks', House Committee on Space Science & Technology, 2016.

[20] This quote appears in various forms. The best source appears to be the Russian-language book by Stalin's former secretary. Boris Bazhanov, Memoirs of the Former Secretary of Stalin (Moscow: III Tysiacheletie, 2002).

[21] Clayton, 'Ukraine Election Narrowly Avoided 'Wanton Destruction' from Hackers'.

[22] Massimo Calabresi, 'How Russia Wants to Undermine the U.S. Election', *TIME*, 29 September 2016.

2013 when hackers caused the Associated Press's Twitter account to report that there had been a bombing in the White House and President Obama had been injured.[23] Similar disinformation efforts could sow discord in the political process and undermine confidence in the election. The 2000 election, which featured news networks calling the key state of Florida for Al Gore before retractions and a bitter recount resulted in the eventual swearing-in of President Bush, might provide inspiration in this regard.

The 2014 attack on Ukraine also attempted to manipulate the reporting of election results to news networks. A Ukrainian official said, "Offenders were trying by means of previously installed software to fake election results in [a] given region and in such a way to discredit general results of elections of the President of Ukraine." Election officials thwarted the software just forty minutes before results were due to be reported; curiously, pro-Russian TV nonetheless reported the fake results exactly, suggesting the possibility of coordinating electoral interference with other kinds of information operations.[24]

All told, the range of attack vectors aimed at either voters or votes is broad and disparate. We believe that each of these categories of threats represents a plausible risk and could be exploited by a sophisticated actor, with negative effects. For future elections, redesigning systems and processes to guard against these categories of threats is an imperative.

[23] Darren Samuelsohn and Hadas Gold, 'Media Vulnerable to Election Night Cyber Attack', *Politico*, 19 October.

[24] Clayton, 'Ukraine Election Narrowly Avoided 'Wanton Destruction' from Hackers'.

Effects

Conceptualizing various threats, as the last section did, is doable. It is substantially harder to carry out those threats. Here it is worth differentiating two categories of actors. First are those who seek to actively manipulate the election so that their preferred candidate is illegitimately declared the winner. Second are those that seek to undermine confidence in the vote, so that a defeated candidate can protest the outcome in a way that prompts at least some doubt in the general populace. In neither case does the candidate who appears to benefit have to know of the manipulation to play along; it is only human nature to convince oneself of victory, to contest elections that look like they are close, or to believe in political opponents' capacity for foul play.

As the Rajneeshee case shows, electoral manipulation at a sufficient scale is a major challenge—and that was only a county election. Especially for a federal election, manipulation at a level required to swing the result is a significant undertaking. Historically, these challenges in scalability appear to have been a major check on the capabilities of outside actors to manipulate the voting process; possible exceptions are when the voting process itself was corrupted by local politics.[25] The less close an election is, the harder it is to undetectably flip it.

Computers might make this hurdle easier to clear, since they generally enable operations to scale more quickly. But while cyber operations probably are more scalable than other previous efforts at electoral manipulation, in important respects attacks on the electoral system are substantially less scalable than other kinds of cyber operations. For some methods of interference, manipulating 1,000 votes requires 1,000 times as much effort as manipulating one vote.[26]

Furthermore, there is no national voting system in the United States. Instead, state and local governments take the lead, involving a dizzying

[25] A canonical example is Lyndon Johnson's apparent manipulation of the vote in the 1948 Democratic primary runoff for the Texas Senate. For a definitive account, see Robert Caro, The Years of Lyndon Johnson: Means of Ascent (New York: Knopf, 1990). See also Martin Tolchin, 'How Johnson Won Election He'd Lost', *The New York Times*, 11 February 1990.

[26] Nicholas Weaver, 'Secure the Vote Today', *Lawfare*, 8 August 2016.

array of 8,000 entities across the country. A patchwork of technical systems—each with their own standards, safeguards, and quirks—matches this jurisdictional maze.[27] To have a broader effect on votes, many methods of attack require hackers to understand and penetrate a variety of different systems, which increases the complexity and time required for operations and reduces scalability. FBI Director James Comey has claimed that this represents a form of security, saying that the system is too "clunky" to be broadly hacked easily.[28] Naturally, the closer an election is, the fewer systems would need to be manipulated to change the overall result.

Nonetheless, some cyber operations do scale at least somewhat well. Finding a vulnerability in software used by a particular kind of voting machine might enable hackers to exploit that vulnerability in all areas that employ that kind of machine. Locating a central voter registration store could enable large numbers of voter records to be copied or manipulated at once. Pilfered documents with embarrassing information, real or fake, could go viral and influence voters, as might erroneous news reports. Vulnerabilities that affect the tabulation or reporting of votes, or that enable attackers to modify voting data at the end of the day are particularly worrisome. Security audits leave no doubt: many of America's voting machines have exhibited significant vulnerabilities in the past, and it is likely that some continue to do so. A capable actor could, for a variety of reasons, try to take advantage of these systems.

In guarding against these risks, the trendline is positive. In the United States, most machines today produce a voter-verifiable paper trail that would enable recounts and audits. After a wave of voting machine failures in the 2000s, more states have switched to optical scanning systems in which the voter marks a paper ballot that also serves as evidence for later verification. In 2000, less than 30 percent of voters used such a system; in 2012, 56 percent did.[29] Here the United States is following a global trend. Overseas, nations that had previously switched to less-verifiable electronic

[27] For a more detailed breakdown, see the Verified Voting Project.

[28] Yet computer scientists have long warned against placing too much faith in so-called "security by obscurity." Devlin Barrett, 'U.S. Voting System So 'Clunky' It Is Insulated from Hacking, FBI Director Says ', *The Wall Street Journal*, 8 September 2016.

[29] Ben Wofford, 'How to Hack an Election in Seven Minutes', *Politico*, 5 August 2016.

voting systems, such as the Netherlands, have reversed course.[30] Some critical elections, such as Britain's referendum on leaving the European Union, are counted entirely by hand.[31]

But the slope of this positive trendline is nonetheless too shallow. A sizable percentage of precincts still use systems that are potentially open to manipulation and that sometimes also lack a voter-verifiable paper trail.[32] Five states lack such paper trails entirely and in some states, including swing states like Pennsylvania, a majority of counties do not use machines with voter-verifiable paper trails.[33] Severe funding shortfalls prevent the updating of voting machines and means that they are often used well past their intended use date. In 2016, 43 states will use voting machines that are more than ten years old, many of which are no longer manufactured and are difficult to maintain.[34] The design flaws and security vulnerabilities of some of these machines are likely impossible to correct.[35]

The second category of actors and attacks—those that just seek to cast doubt—is thus much more plausible. There are several mechanisms through which this effect could be achieved. A hacking effort that creates some irregularities can foster a perception of illegitimacy. In the same way that long lines in Democratic areas of Ohio in 2004 caused some to question—likely incorrectly—that state's overall vote for President Bush, a hacking effort could raise doubts even when none should exist. Even evidence of an unsuccessful hacking attempt in some areas could provide an misperception that hackers were successful elsewhere.

Hackers can also try to create doubt directly. In order to raise doubts about legitimacy, they could provide evidence of their actions, such as videos of electronic vote manipulation or unauthorized access. These

[30] Ben Goldsmith and Holly Ruthrauff, 'Case Study Report on Electronic Voting in the Netherlands', National Democratic Institute, 2013.

[31] Camila Domonoske, 'It's Decision Time in the U.K.: Voters to Settle 'Brexit' Question', NPR, 23 June 2016.

[32] Weaver, 'Secure the Vote Today'.

[33] For one visualization, see Haley Sweetland Edwards and Chris Wilson, 'See How Likely It Is That Your Voting Booth Gets Hacked', *TIME*, 19 September 2016.

[34] Lawrence Norden and Christopher Famighetti, 'America's Voting Machines at Risk', Brennan Center for Justice, 2015.

[35] For more, see 'Written Testimony of Andrew W. Appel': House Subcommittee on Information Technology, 2016.

kinds of communications—part-boast, part-threat, part-influence operation—have gained such prominence as to become their own genre, appearing after the hacks of Sony, Aramco, Sands Casino, and many others. Most relevant, though, is that the online statements of Guccifer 2.0, the hacker or hackers of the Democratic Party, certainly fall into this category. One can imagine exclusive evidence of hacking given to news organizations on Election Day, mirroring the way in which Guccifer 2.0 has sometimes parceled out documents to relevant publications in the summer of 2016.[36]

Candidates themselves can exacerbate the problem of perceived illegitimacy. Faced with either evidence of hacking attempts or claims of manipulation, a losing candidate may seize on any irregularities as signs of broader foul play. This is possible even if the hackers did not actually flip the election, and perhaps even if there were no hacking incidents at all. By refusing to concede and by alleging impropriety, a candidate may do damage to the democratic process and to the incoming administration. One of the cornerstones of American politics, even in contested elections like 2000's, is the eventual concession by the candidate who is judged to have lost, even as a result of voting irregularities; the possibility of hacking, especially by a foreign power or political opponent, may make a peaceful transition of power more difficult.

The perception of illegitimacy is damaging. We believe that, in order to jeopardize the perceived legitimacy of an election, a hacker does not need to flip the results but only to cause doubt. Evidence of hacking-related irregularities, credible claims by hackers, and candidates quick to sense fraud all can threaten the perception of fairness that is central to the electoral process. In order to strengthen this perception in the face of such threats—and ensure the reality of an equitable and secure process—it is time to get serious about electoral cybersecurity.

[36] For example, see Joe Uchill, 'Guccifer 2.0 Releases New DNC Docs', The Hill, 13 July 2016.

Recommendations

We make five recommendations for improving electoral cybersecurity, drawing in part on research that has already been carried out by both computer and political scientists.

First, the federal government should identify election systems, including vote tabulation and official results dissemination mechanisms, as critical infrastructure. This is a subject of great debate, as some states fear that such a designation would increase federal control over elections.[37] We also recognize that American elections have long been run by local and state administrators, and think it should remain that way. We agree with one poll of security professionals in thinking that designating something as critical does not make it secure.[38]

Nonetheless, within the federal government, the designation of critical infrastructure is an important one that is reserved for systems of the highest importance. We think that, because of their central role in democracy, election systems qualify as critical infrastructure. The federal government should acknowledge as much under Section 9 of the 2013 Executive Order on cybersecurity. It should use this designation to make available to states and localities funding and other resources to assist their efforts to ensure the integrity of the process.[39] Federal assistance to locally-run elections sends a strong signal about the importance of the matter to both domestic and international audiences, even if it is not in itself a sufficient condition for achieving security.

Second, every vote should involve a paper ballot marked by—or at least verifiable by—the voter. A clear paper trail is vital for voter confidence and enables more credible audits and recounts. In exceptionally close races, such as the 2008 Minnesota Senate election, paper trails have been valuable in determining the winner of the election and ensuring

[37] Even without such a designation, some states have declined federal assistance for fear of losing control over the election. Aliya Sternstein, 'At Least One State Declines Offer for DHS Voting Security', NextGov, 25 August 2016.

[38] Jack Detsch, 'Influencers: Calling It 'Critical Infrastructure' Won't Protect the Vote', *Christian Science Monitor*, 21 September 2016.

[39] 'Executive Order -- Improving Critical Infrastructure Cybersecurity', The White House, 2013.

legitimacy. Historically, contested races without a paper trail have been more contentious and harder to resolve, a problem made only more serious by the increased risk of computer hacking.[40]

Election authorities have made progress on this front in recent years, but that progress must be accelerated. In 2016, around one-quarter of Americans will still vote using machines that lack such a paper trail.[41] Just as the 2000 election led to the removal of punch card machines and increased federal funding for new equipment, Congress should use the hacking threats of 2016 as an impetus for action. Additional funding for a voter-verifiable paper trail in all future elections is essential as a bulwark against perceptions of a hacked result.

Third, election authorities should encourage security audits and strengthen digital security practices for election systems. Many of the vulnerabilities discussed in this paper have only been found through the diligent efforts of academic researchers, sometimes working independently and sometimes contracted by state governments. It is essential that these pre-election audits be increased and that all voting systems are examined for weaknesses that could be exploited by hackers. Within the federal government, the Election Assistance Commission should highlight and advance credible security standards, in coordination with the National Institute for Standards and Technology.[42] States should dedicate resources to supplement federal funding and bolster their security posture.

The Department of Homeland Security has already begun work in this vein. In 2016, as the cybersecurity threats to elections became more apparent, the Department increased its cybersecurity assistance to states and localities. This assistance includes offering vulnerability scans, information on threats, and access to resources and tools relevant to election

[40] For more, see Mark Lindeman et al., 'Principles and Best Practices in Post Election Audits', Election Audits, 2008.

[41] Edwards and Wilson, 'See How Likely It Is That Your Voting Booth Gets Hacked'.

[42] For more on current efforts, see 'U.S. Election Assistance Commission: Agency Financial Report': U.S. Election Assistance Commission, 2015. For more detailed recommendations, see 'The American Voting Experience: Report and Recommendations of the Presidential Commission on Election Administration', Presidential Commission on Election Administration.

cybersecurity.[43] These sorts of steps are part of a baseline of effective defense and contribute to a deterrence strategy by partially denying adversaries the opportunity to do damage.

Fourth, post-election audits should be strengthened and should use more rigorous forms of statistical sampling. After every election, the relevant election commission should count a percentage of randomly sampled paper ballots. The percentage of ballots to be included in an audit depends on the margin of the election, with statistical models guiding the process. If a sufficient number of ballots are included, it is possible to verify with a high degree of certainty that, even if hacking or other irregularities occurred, it did not change the winning candidate; this is known as a risk-limited audit.

Current practices on post-election audits vary enormously by state and in general fall short of what is needed for mathematically-strong confidence.[44] The Election Assistance Commission should take a role in encouraging high standards to ensure rigorous chain of custody procedures, appropriate sampling, and risk-limited audits. Doing so would increase confidence in elections.

Fifth, the United States should put forth a declaratory policy on the vital importance of elections, vowing to impose costs on any state that interferes with the integrity of the process. We recognize that the previous four recommendations, though effective against many threats, may not be enough to thwart some of the most sophisticated adversaries, such as some foreign intelligence services. Against these sophisticated adversaries, which likely have their own interests that the United States could threaten, the United States should articulate a policy of deterrence through cost imposition.

[43] 'Readout of Secretary Johnson's Call with State Election Officials on Cybersecurity', Department of Homeland Security, 15 August 2016. Abdollah, 'US Official: Hackers Targeted Election Systems of 20 States'.

[44] Lawrence Norden et al., 'Post-Election Audits: Restoring Trust in Elections', Brennan Center for Justice, 2007; Lindeman et al., 'Principles and Best Practices in Post Election Audits', Election Audits; 'Post Election Audits', Verified Voting, 2016.

If one of these adversaries tries to interfere with the integrity of the electoral process, the United States should seriously explore means of retaliation. This policy would not necessarily apply to operations targeting confidentiality, such as acquiring voter or party information, which would be considered quasi-acceptable international espionage. It would be activated only if a foreign actor sought to tip an election to one candidate or introduce significant doubt as to the legitimacy of democracy. The integrity of the electoral process is vital to the United States and is worth defending.

Notes

Abdollah, Tami, ‘US Official: Hackers Targeted Election Systems of 20 States’, Associated Press, 30 September 2016, https://www.apnews.com/c6f67fb36d844f28bd18a522811bdd18/US-official:-Hackers-targeted-election-systems-of-20-states

‘The American Voting Experience: Report and Recommendations of the Presidential Commission on Election Administration’, Presidential Commission on Election Administration, 2014, https://www.supportthevoter.gov/files/2014/01/Amer-Voting-Exper-final-draft-01-09-14-508.pdf

Appel, Andrew W., ‘Written Testimony of Andrew W. Appel’, House Subcommittee on Information Technology, 2016, https://oversight.house.gov/wp-content/uploads/2016/09/2016-09-28-Appel-Princeton-Testimony.pdf

Barrett, Devlin, ‘U.S. Voting System So ‘Clunky’ It Is Insulated from Hacking, FBI Director Says’, Wall Street Journal, 8 September 2016, http://www.wsj.com/articles/u-s-voting-system-so-clunky-it-is-insulated-from-hacking-fbi-director-says-1473368396

Bazhanov, Boris, Memoirs of the Former Secretary of Stalin. Moscow: III Tysiacheletie, 2002.

Blaze, Matt, Arel Cordero, Sophie Engle, Chris Karlof, Naveen Sastry, Micah Sherr, Till Stegers, and Ka-Ping Yee, ‘Source Code Review of the Sequoia Voting System’, Berkeley University of California: California Secretary of State, 2007, http://votingsystems.cdn.sos.ca.gov/oversight/ttbr/sequoia-source-public-jul26.pdf

Calabresi, Massimo, ‘How Russia Wants to Undermine the U.S. Election’, Time, 29 September 2016, http://time.com/4512771/how-russia-wants-undermine-us-election/

Calandrino, Joseph A., Ariel J. Feldman, J. Alex Halderman, David Wagner, Harlan Yu, and William P. Zeller, ‘Source Code Review of the Diebold Voting System’, Berkeley University of California: California Secretary of State, 2007, http://votingsystems.cdn.sos.ca.gov/oversight/ttbr/diebold-source-public-jul29.pdf

Caro, Robert, The Years of Lyndon Johnson: Means of Ascent. New York: Knopf, 1990.

Clayton, Mark, ‘Ukraine Election Narrowly Avoided ‘Wanton Destruction’ from Hackers’, Christian Science Monitor, 17 June 2014, http://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers-video

Detsch, Jack, ‘Influencers: Calling It ‘Critical Infrastructure’ Won’t Protect the Vote’, Christian Science Monitor, 21 September 2016, http://www.csmonitor.com/World/Passcode/Passcode-Influencers/2016/0921/Influencers-Calling-it-critical-infrastructure-won-t-protect-the-vote

Domonoske, Camila, ‘It’s Decision Time in the U.K.: Voters to Settle ‘Brexit’ Question’, NPR, 23 June 2016, http://www.npr.org/sections/thetwo-way/2016/06/23/483212779/its-decision-time-in-the-u-k-voters-to-settle-brexit-question

Edwards, Haley Sweetland, and Chris Wilson, ‘See How Likely It Is That Your Voting Booth Gets Hacked’, Time, 19 September 2016, http://time.com/4498995/voting-hackers-safety-security-polling-station/

‘Executive Order -- Improving Critical Infrastructure Cybersecurity’, The White House: 2013, https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

Farkas, Karen, ‘Electronic Poll Books Will Be at Voting Locations across the State by November 2016’, Cleveland Plain Dealer, 28 August 2015, http://www.cleveland.com/metro/index.ssf/2015/08/electronic_poll_books_will_be.html

Feldman, Ariel J., J. Alex Halderman, and Edward Felten, ‘Security Analysis of the Diebold AccuVote-TS Voting Machine’, USENIX/ACCURATE Electronic Voting Technology Workshop, 2006, https://jhalderm.com/pub/papers/ts-evt07.pdf

Goldsmith, Ben, and Holly Ruthrauff, ‘Case Study Report on Electronic Voting in the Netherlands’, National Democratic Institute, 2013, https://www.ndi.org/files/5_Netherlands.pdf

Goodin, Dan, ‘How a Security Pro’s Ill-Advised Hack of a Florida Elections Site Backfired’, Ars Technica, 9 May 2016, http://arstechnica.com/security/2016/05/how-a-security-pros-ill-advised-hack-of-a-florida-elections-site-backfired/

Groll, Elias, ‘Turns Out You Can’t Trust Russian Hackers Anymore’, Foreign Policy, 22 August 2016, https://foreignpolicy.com/2016/08/22/turns-out-you-cant-trust-russian-hackers-anymore/

Hubler, Katy Owens, ‘Electronic Poll Books’, National Conference of State Legislatures, 21 May 2016, http://www.ncsl.org/research/elections-and-campaigns/electronic-pollbooks.aspx

Inguva, Srinivas, Eric Rescorla, Hovav Shacham, and Dan S. Wallach, ‘Source Code Review of the Hart InterCivic Voting System’, Berkeley University of California: California Secretary of State, 2007, http://votingsystems.cdn.sos.ca.gov/oversight/ttbr/Hart-source-public.pdf

Isikoff, Michael, ‘FBI Says Foreign Hackers Penetrated State Election Systems’, Yahoo News, 29 August 2016, https://www.yahoo.com/news/fbi-says-foreign-hackers-penetrated-000000175.html

Kohno, Tadayoshi, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach, 'Analysis of an Electronic Voting System'. *IEEE Symposium on Security and Privacy* (2004).

Levin, Dov H., 'When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results'. *International Studies Quarterly* (2016).

Lindeman, Mark, Mark Halvorson, Pamela Smith, Lynn Garland, Vittorio Addona, and Dan McCrea, 'Principles and Best Practices in Post Election Audits', Election Audits, 2008, http://electionaudits.org/files/best practices final_0.pdf

MacFarquhar, Neil, 'A Powerful Russian Weapon: The Spread of False Stories', New York Times, 28 August 2016, http://www.nytimes.com/2016/08/29/world/europe/russia-sweden-disinformation.html

McDaniel, Patrick, Matt Blaze, and Giovanni Vigna, 'Everest: Evaluation and Validation of Election-Related Equipment, Standards and Testing', Ohio Secretary of State, 2007, http://www.patrickmcdaniel.org/pubs/everest.pdf

Mercuri, Rebecca, 'Florida Primary 2002: Back to the Future'. *Forum on Risks to the Public in Computers and Related Systems,* 22, no. 24 (2002).

Miller, Judith, Stephen Engelberg, and William Broad, Germs: Biological Weapons and America's Secret War. New York: Simon & Schuster, 2002.

'New Florida Voting Machines Malfunction, Cause Delays', USA Today, 10 September 2002, http://usatoday30.usatoday.com/tech/news/techinnovations/2002-09-10-voting-machines_x.htm

Norden, Lawrence, 'The Machinery of Democracy', Brennan Center for Justice, 2006, https://www.brennancenter.org/sites/default/files/publications/Machinery_Democracy.pdf

Norden, Lawrence, Aaron Burstein, Joseph Lorenzo Hall, and Margaret Chen, 'Post-Election Audits: Restoring Trust in Elections', Brennan Center for Justice, 2007, https://www.brennancenter.org/sites/default/files/legacy/d/download_file_50227.pdf

Norden, Lawrence, and Christopher Famighetti, 'America's Voting Machines at Risk', Brennan Center for Justice, 2015,

Pomerantsev, Peter, 'Russia and the Menace of Unreality', The Atlantic, 9 September 2014, http://www.theatlantic.com/international/archive/2014/09/russia-putin-revolutionizing-information-warfare/379880/

'Post Election Audits', Verified Voting, 2016, https://www.verifiedvoting.org/resources/post-election-audits/

'Readout of Secretary Johnson's Call with State Election Officials on Cybersecurity', Department of Homeland Security, 15 August 2016, https://www.dhs.gov/news/2016/08/15/readout-secretary-johnsons-call-state-election-officials-cybersecurity

Rid, Thomas, 'All Signs Point to Russia Being Behind DNC Hack', Vice, 25 July 2016, https://motherboard.vice.com/read/all-signs-point-to-russia-being-behind-the-dnc-hack

Rose, William, Rysia Murphy, and Max Abrahms, 'Does Terrorism Ever Work? The 2004 Madrid Train Bombings'. *International Security* 32, no. 1 (2007): 185-92.

Saathoff, Gregory, Gerald DeFrancisco, David Benedek, Anita Everett, Christopher Holstege, Sally C. Johnson, J. Steven Lamberti, Ronald Schouten, and Joseph C. White, 'Report of the Expert Behavioral Analysis Panel', Research Strategies Network, 2011, https://www.med.unc.edu/psych/forensic/files/EBAP_Report_ExSum_Redacted_Version.pdf

Samuelsohn, Darren, and Hadas Gold, 'Media Vulnerable to Election Night Cyber Attack', Politico, 19 October http://www.politico.com/story/2016/10/media-vulnerable-to-election-night-cyber-attack-229956

Schneier, Bruce, 'How Long until Hackers Start Faking Leaked Documents?', The Atlantic, 13 September 2016, http://www.theatlantic.com/technology/archive/2016/09/hacking-forgeries/499775/

'Security Assessment of WinVote Voting Equipment for Department of Elections', Commonwealth Security and Risk Management: Virginia Information Technology Agency, 2015, http://elections.virginia.gov/WebDocs/VotingEquipReport/WINVote-final.pdf

Shane, Scott, 'Panel on Anthrax Inquiry Finds Case against Ivins Persuasive', New York Times, 23 March 2011, http://www.nytimes.com/2011/03/24/us/24anthrax.html

Sternstein, Aliya, 'At Least One State Declines Offer for DHS Voting Security', NextGov, 25 August 2016, http://www.nextgov.com/cybersecurity/2016/08/some-swing-states-decline-dhs-voting-security-offer/131037/

Tolchin, Martin, 'How Johnson Won Election He'd Lost', New York Times, 11 February 1990, http://www.nytimes.com/1990/02/11/us/how-johnson-won-election-he-d-lost.html

'U.S. Election Assistance Commission: Agency Financial Report', U.S. Election Assistance Commission, 2015, http://www.eac.gov/assets/1/Documents/FY 15 EAC Agency Financial Report Nov 13 2015 Final-website.pdf

Uchill, Joe, 'Guccifer 2.0 Releases New DNC Docs', The Hill, 13 July 2016, http://thehill.com/policy/cybersecurity/287558-guccifer-20-drops-new-dnc-docs

Wallach, Dan S., ‘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

Weaver, Nicholas, ‘Secure the Vote Today’, Lawfare, 8 August 2016, https://www.lawfareblog.com/secure-vote-today

Wofford, Ben, ‘How to Hack an Election in Seven Minutes’, Politico, 5 August 2016, http://www.politico.com/magazine/story/2016/08/2016-elections-russia-hack-how-to-hack-an-election-in-seven-minutes-214144

Wysopal, Chris, ‘Election System Hacks: We’re Focused on the Wrong Things’, InfoWorld, 20 September 2016, http://www.infoworld.com/article/3120325/application-development/election-system-hacks-were-focused-on-the-wrong-things.html

The Cyber Security Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138
www.belfercenter.org/cyber

Printed in the United States of America