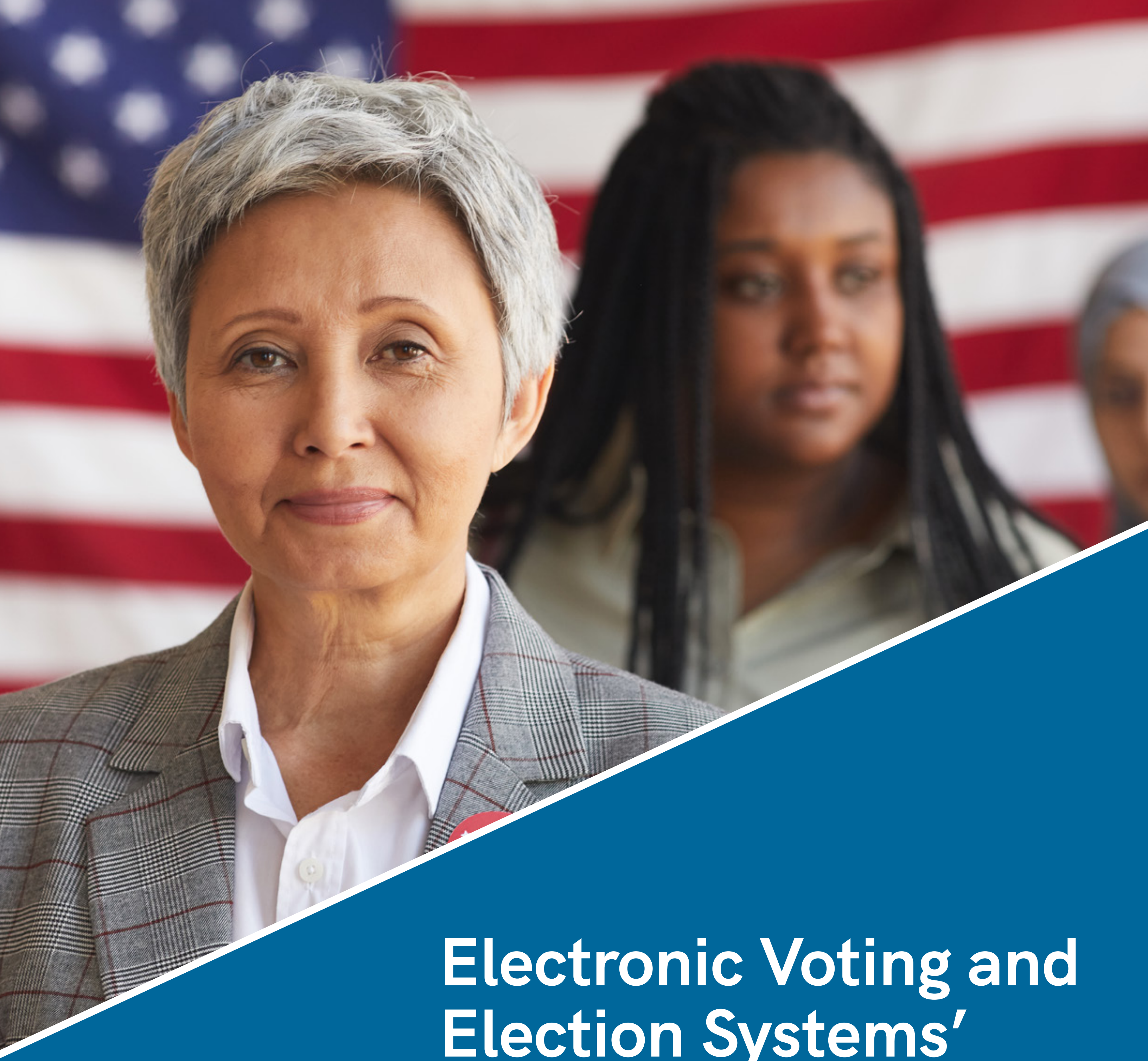


Electronic Voting and Election Systems' Vulnerabilities in the Information Age

Lessons Learned from 2016 and Beyond About the Potential to Influence Elections

PUBLISHED
NOVEMBER 2020

Jonathon Hauenschild, Policy Advisor

Rainey Center

Introduction

Secure election operations are challenging for republics and democracies. Citizens are willing to make some tradeoffs to have a voice in their governments. These tradeoffs include allowing inherent vulnerabilities in systems despite the constant need for mitigation. This paper examines the most common vulnerabilities[1] in U.S. voting and elections systems in order to equip state policymakers in their efforts to identify vulnerabilities and develop a framework for prioritizing the allocation of election security resources.

Prior to the advent of electronic voting and digitized voter registration, vulnerabilities included the ability to physically stuff ballot boxes, "hanging chads," or manipulating absentee voting procedures. Elections experts offered electronic voting machines and digitized processes as cures for "hanging chads", slow total reporting, and more. As states adopted electronic systems, funded and mandated primarily through the Help America Vote Act ("HAVA"), new

[1] In this paper, the term vulnerability simply refers to susceptibility to attack or harm. Within the context of elections, it means the variety of susceptibilities or weaknesses within given systems or processes.

vulnerabilities arose. States and the federal government exchanged one set of vulnerabilities for a new set — the potential for foreign actors to "hack" elections.

Hacking, while accurate, is a simple term for a complex security problem. The term "hack" is applied to a plethora of vulnerabilities, such as the ability to improperly access voting machine or influence the voting populous or in some way to potentially alter the outcome of the election. Operations to exploit vulnerabilities in voting systems are multifaceted. Foreign actors do not merely target the electronic voting machines; they will target state registration databases and sustain disinformation campaigns.

In the United States (U.S.), "Election Day" is as much a misnomer as the term "hack." Most voting occurs on one "general Election Day" in November. U.S. elections, however, are in practice the aggregate of thousands of state, county, and local election operations spread across several weeks when one considers early voting, absentee voting, and military voting. Each locality within a state, too, may use a voting system different from its neighbor.

This lack of standardization creates additional vulnerabilities while also providing a degree of resilience.[2] Foreign actors may not be able to understand the complexity, may not have the resources to attack the thousands of counties and local governments, or invest in a type of attack that is not as relevant as thought for a specific target. The lack of standardization allows experts and policy makers to triage and prioritize the most vulnerable aspects of voting systems. On the other hand, county and local governments' cyber security practices may not be as robust as the state or federal government and thus easier both to target and penetrate.

Limited state and local budgets, along with state elections procedures, require governments to triage and prioritize hardening vulnerable aspects of elections. The burden to harden voting systems and the elections process tends to fall primarily on state governments, with the federal government offering occasional assistance. Through HAVA, for example, the federal government has provided the states with $3.3 billion to upgrade voting systems.[3] Similarly, Congress recently appropriated $380 million "in grant money for the states to bolster cybersecurity and replace vulnerable voting machines."[4]

[2] As part of her testimony to the Senate Select Committee on Intelligence, DHS Assistant Secretary Jeannette Manfra emphasized that "we do have confidence in the overall integrity of our electoral system because our voting infrastructure is fundamentally resilient." *See*, U.S. Congress, Senate, Select Committee on Intelligence, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election; Volume 1: Russian Efforts Against Election Infrastructure with Additional Views*, 116th Cong., 1st sess., 2019, S. Rep. 116-XX, 38 (hereafter "*SSCI 2016 Election Report*, Vol. 1").

[3] Ballotpedia, "Help America Vote Act (HAVA) of 2002," accessed October 16, 2019, https://ballotpedia.org/Help_America_Vote_Act_(HAVA)_of_2002.

[4] SSCI 2016 Election Report, Vol. 1, at 4-5.

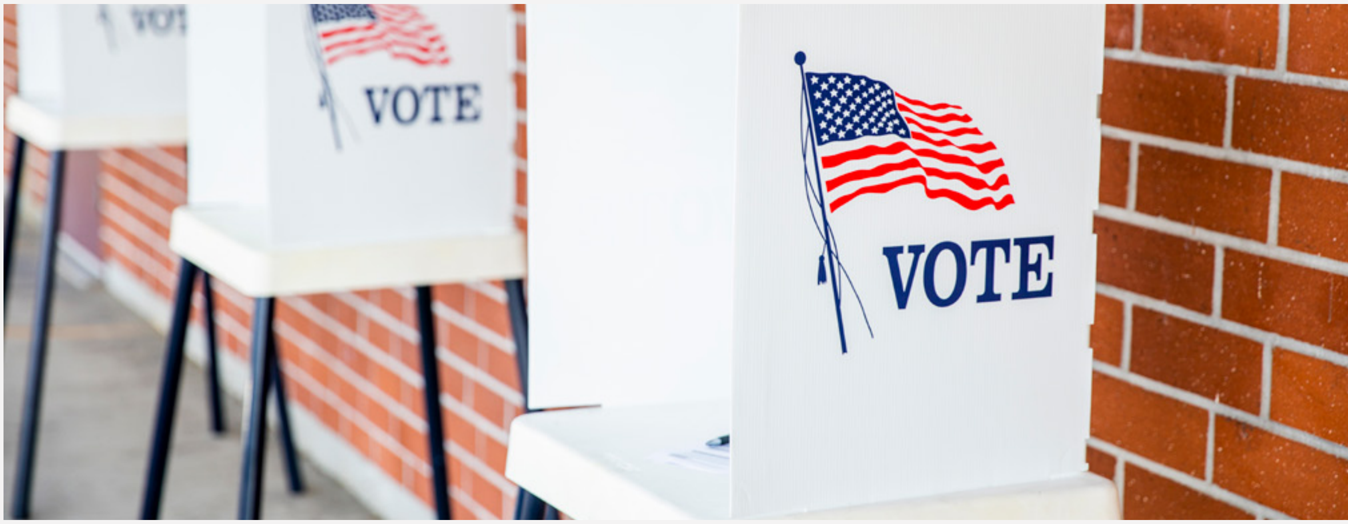
Elections vulnerabilities fit within two different buckets. One set of vulnerabilities primarily impacts "voting systems." The other set relates to cognitive issues and, for convenience, impacts the broader "election process."

"Voting systems" mean everything related to the way Americans vote, including:

- Voter registration
- Voter information databases (and electronic pollbooks or "e-pollbooks")
- Processes used to verify identities during the registration process
- Maintenance of voter registration databases
- The administration of elections at local polling places
- The machines upon which people vote
- Absentee, provisional, and military voting
- Voting result reporting
- Recounts
- Vote certifications
- Communications between elections officials at the state and local level

"Voting systems" are necessary for the "election process," but the "election process" is much more. "Election processes" include:

- Candidates
- Campaigns
- Political parties
- The way people consume information about candidates, share that information, and use that information to determine which candidate or party will receive their vote



Background

Prior to 2006, elections in the United States were primarily an analog process. Prospective voters filled out paper registration cards then mailed or personally delivered them to county elections departments. County elections departments, in turn, maintained paper copies of the registration databases. People voted on punch card or lever machines. Officials manually tabulated vote counts and included absentee ballots.

The 2000 presidential election brought to the forefront vulnerabilities associated with analog voting, such as the infamous hanging chads, the difficulty of managing recounts and the standards by which to judge votes cast for candidates. To address these risks, Congress enacted HAVA. Among other things, HAVA required each state to develop a single, centralized, and interactive computerized statewide voter registration list. This single, centralized list must be coordinated with other agency databases within the state, like driver's licenses, effectively requiring the digitization of other databases. HAVA also required states to replace analog machines with new, digital systems compliant with the HAVA standards.

Digital voting systems and election processes have advantages. Voter registration, list maintenance, voting, vote counting, campaign and party communications are more efficient and faster. Elections officials have registration databases at their fingertips. Candidates and campaigns can deploy get-out-the-vote efforts to areas where the data suggests those efforts have substantial impact.

Digitization trades one set of vulnerabilities, though, for another. Bad actors, consequently, need only focus their efforts on state or county registration databases rather than local governments. Theoretically, they could hack electronic voting machines, interfere with result reporting, and more.[5] Under the prior, analogue, systems bad actors could influence the count. Digitization of election assets allows bad actors to undermine the entire voting systems and elections process if policymakers and elections officials do not properly safeguard these assets.

Just as the 2000 election highlighted the risks in the analog system, President Trump's 2016 election brought them to public consciousness regarding digital systems. Prior to the election, intelligence and law enforcement officials noticed a spike in efforts by foreign actors—primarily Russian—to influence digital voting and elections systems. These efforts by malign foreign actors sought to discover, and potentially exploit, software, hardware, and human vulnerabilities. These efforts sought to sway voters through what was once known as "active measures."[6] Fortunately, though, these efforts, from an election integrity perspective largely failed. For now.

Before proceeding, a word of warning: experts are now aware of state-sponsored efforts to interfere with U.S. elections. The temptation may be to focus efforts on preventing the exact same type of attack, or an attack by the same country. While this is necessary, cyberattacks and active measures are never static. While Russia remains a constant threat, for example, intelligence officials warned recently that Iran, along with Russia, have obtained "voter registration information."[7] They constantly evolve to avoid detection. Future attacks on voting and elections systems could come from lone wolves, politically motivated groups, Russia, Iran, China, other state actors, or any number of other sources. They will seek to exploit the connectivity the internet provides including social media platforms such as Facebook, Twitter, or YouTube, but modify the tactics from 2016. Policymakers and elections officials should remain constantly vigilant and aware than anyone with a laptop and WiFi connection could seek improperly to influence U.S. elections.

[5] During the 2016 Presidential election, for example, the FBI and Florida Governor Ron DeSantis stated that hackers affiliated with the GRU, the Russian military intelligence unit, accessed voter databases in two Florida counties, but did not change or manipulate either the data or the election results. Illustrating the vulnerabilities of the digital age, the GRU gained access through spearfishing emails—emails it sent to 120 emails associated with elections officials across the state of Florida.

[6] "Active measures" broadly defined refers to "the manipulative use of slogans, arguments, disinformation, and carefully selected true information… used to try to influence the attitudes and actions of foreign publics and governments." U. S. Information Agency, *Soviet Active Measures in the "Post-Cold War" Era 1988-1991*, Washington, D.C., June 1992, http://intellit.muskingum.edu/russia_folder/pcw_era/.

[7] United States Office of Director of National Intelligence (ONDI), Washington, D.C., "DNI John Ratcliffe's Remarks at Press Conference on Election Security," October 22, 2020, https://www.dni.gov/index.php/newsroom/press-releases/item/2162-dni-john-ratcliffe-s-remarks-at-press-conference-on-election-security.

Triaging Vulnerabilities in Voting Systems

Registration, Databases, Voting Machines, Counts and Recounts[8]

The media likes to focus on security problems with electronic voting machines. Machines are an easy and relatable target. After all, most people use machines when they vote. Because of the media focus on machines, there are ample stories about vulnerabilities, perceived or real,[9] even in "off" election years. The media,

[8] The Defending Digital Democracy Project at the Harvard Kennedy School's Belfer Center for Science and International Affairs breaks down "election system[s]" into three levels: (1) Core systems that make elections run, such as voter registration databases, electronic poll books, vote capture devices and tally systems, and election night reporting systems; (2) Intermediary government functions that connect multiple election system components: other state and county-level systems, and election officials' internal communications channels; and (3) External functions that touch the entirety of the elections process: vendors, and traditional social media. "The State and Local Election Cybersecurity Playbook," Belfer Center for Science and International Affairs, Harvard Kennedy School, February 2018, https://www.belfercenter.org/sites/default/files/files/publication/StateLocalPlaybook%201.1.pdf. The three levels are somewhat logical but fail to make some critical distinctions. First, the levels do not allow for the division of vulnerabilities between cybersecurity and human. Second, "social media" are not external functions of the "elections process." Social media enables people to communicate with each other, enhancing the democratic process or, as discussed later, allowing for foreign actors to influence the process. Put simply, people vote; social media companies do not.

[9] A perceived vulnerability, for example, is "vote switching," when a voter attempts to select one candidate, but the machine selects that candidate's opponent. Often, this is a calibration error rather than a deliberate vulnerability.

for example, published stories about hackers at DefCon participating in an annual hack of voting machines at Voter Village. During the 2019 conference, participants managed to hack every single machine.[10]

DefCon Hackers used a variety of methods to access the voting machines. Despite the success, one thing stood out. All the hackers needed physical access to the machines. They needed to insert something into a port, unscrew the back, or similar actions as a predicate to the attack. This type of hardware-based attack, if successful, is unlikely significantly impact the result of an election. It would impact one machine in one precinct. Concentrating on machines is a relatively high-risk, low-reward proposition for bad actors. To impact election results, hackers would need physically to access multiple machines in multiple precincts, without getting caught by election officials. Elections officials, despite some caricatures portraying them otherwise, are individuals highly trained and competent. Put simply, they know how to run elections in their precincts and can frequently spot attempts to game the system. Any scheme would necessarily fail if an official recognized attempts to improperly access the machines and denied access to the polling location.

There are two basic categories of electronic voting machines: Direct Recording Electronic (DRE) or Optical Scan (OS). The former requires voters to make their selection on a touch screen and electronically records the vote. If there is a paper trail, it simply returns the aggregate vote totals and is not enough to audit the result of an election. The latter requires voters to fill out a paper ballot and then scans the results for the purpose of electronically tabulating the vote. With OS machines, there is an auditable paper trail. In the event of a recount, officials can manually count the ballots and compare that count to the electronic tabulations. Most states employ OS machines, with only a handful of states relying on DREs.[11]

While Defcon's Voter Village exercise illustrates the vulnerability of machines should bad actors physically access them, the bad actors may not need physical access. While machines are not connected to the internet during the voting or vote reporting process, they are connected to the internet at random intervals. The machines are nothing more than computers and require software and ballot updates. Not counting patches or updates to the operating systems, officials must

[10] DefCon's Voter Village does not "provide samples of every piece of voting equipment" in use in the United States, but "every piece of equipment at the Village is currently certified for use in at least one jurisdiction." Of those machines present in the Village, participants managed to "compromis[e] every one of the devices in the room…" Matt Blaze, Harri Hursti, Margaret Macalpine, et al. "Def Con 27 Voting Machine Hacking Village." Defcon. September 26, 2019. https://media.defcon.org/DEF%20CON%2027/voting-village-report-defcon27.pdf

[11] At least 11 states still use, in whole or in part, DRE machines that do not provide auditable paper trails. Most states use paper ballots with OS tabulation. Three states vote only by mail. See Ballotpedia, "Voting Methods and Equipment by State," https://ballotpedia.org/Voting_methods_and_equipment_by_state.

update machines to reflect the ballot at least twice a year—once each before primary and general elections.

Bad actors could theoretically maximize potential impact by attacking either the vendors or other entities responsible for updating ballots, operating systems, or patches. Bad actors could research the manufacturers and how the machines are coded. States may list the vendors,[12] either on a Secretary of State website or buried within state budgets or RFPs for election equipment. Bad actors can then identify the vendors and research specific vulnerabilities, custom design malware and install it either through the third-party vendors or other processes states utilize.

If these vulnerabilities are not concerning enough, electronic machines are not the easiest component of voting systems potentially to manipulate. Perhaps the most vulnerable components are voter registration databases and electronic pollbooks ("e-pollbooks").[13] In some respects, policymakers and state elections officials have very little discretion for creating and maintaining these databases. HAVA requires states to have a "single, uniform, official, centralized, interactive, computerized voter registration list."[14] States do, however, have discretion with cybersecurity standards including third-party access.

To assist with list maintenance, states must provide third-party access to the list other government agencies, such as vital statistics, the court system, and the state Department of Motor Vehicles.[15] Each third-party with access represents a vulnerability—a way for bad actors to obtain improper access to the system. A bad actor need not directly target state elections officials, for example. They may try to obtain access to the registration database through the Department of Motor Vehicles or through vital statistics.

Voter registration databases are nearly always online. Because they are online, bad actors can target them at any time. During the 2016 election, for example, US intelligence and law enforcement entities noticed that the Russians attempted to

[12] Vendors may be a weak point. While the U.S.'s federalist system mitigates vulnerabilities, that mitigation disappears when states use the same vendor provide the machines and related support. According the Belfer Center, "over 60 percent of American voters cast ballots on systems owned and operated by a single vendor. In the 2012 presidential election, this vendor produced over 100 million ballots in more than 4,500 election jurisdictions and 40 states. The same [vulnerability] can exist at the state level. For example, one state contracted with a single vendor to do all of its state maintenance and ballot definition files for the 2018 elections." *Election Cybersecurity Playbook*, 12.

[13] An e-pollbook is an electronic version of the voter rolls used by local elections officials to verify voter registration. Unlike voting machines, which are unconnected from the internet, e-pollbooks are often connected to the internet during the voting process and the voter rolls may be updated in real-time.

[14] 52 U.S.C. § 21083(a)(1)(A).

[15] According to HAVA, state officials must perform "list maintenance" to ensure that people who are imprisoned, dead, or who have moved are no longer listed as eligible voters. As part of this maintenance elections officials must "coordinate the computerized list with State agency records on felony status and… State agency records on death." *See* 52 U.S.C. §§ 21083(a)(2) and 20507(a)(3)-(4).

OFFICIAL ELECTION MAIL
OFFICIAL VOTE BY MAIL BALLOT ENCLOSED
(To be opened only by Canvassing Board)
NOTICE
Voted ballots may be hand delivered to the Elections Office or any polling place NO LATER THAN 8 p.m. ON ELECTION DAY. Ballots returned by mail must be postmarked before or on Election Day and received within 3 days of Election Day.

probe voter registration databases of at least twenty-one states.[16] These probes enjoyed varying levels of success, with some states noting nothing more than a "probe" and Illinois admitting voter information was exfiltrated. Ultimately, the Senate Select Committee on Intelligence found that the Russians were "developing and implementing capabilities to interfere with the 2016 elections," it also "found no evidence that vote tallies were altered or that voter registry files were deleted or modified."[17]

In 2016, efforts aimed at elections officials may not have been for the purpose of altering the outcome of an election. Most of the efforts are better described as "probes" than attacks. Some of the probes were not aimed directly at registration databases, as one state noted that foreign actors were able to access a portion of the Secretary of State's website relating to the reporting of election results. With that access, the actors could have changed the reporting of results, but not the results themselves. If utilized successfully, foreign actors could have created the illusion of a stolen election—the Secretary would appear to have reported a

[16] At least one expert testifying to the SSCI "personally concluded that the Russians had attempted to intrude in all 50 states." *SSCI 2016 Election Report*, Vol. 1, at p. 12.

[17] Ibid. at p. 5.

positive result for one candidate, only for the official result to "hand" the election to that candidate's opponent. The probes seem to support the conclusion in *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election; Volume 1: Russian Efforts Against Election Infrastructure*, which was that the efforts directed at elections officials are consistent with Russia's overall purpose to undermine confidence in democratic institutions and cause Americans to question the validity of election results.[18]

While no investigator uncovered evidence that foreign actors altered registration databases, it remains that they represent some of the most pressing vulnerabilities within voting systems. The largest threat to the integrity of voting systems is not what has transpired, but what could transpire. With foreign operatives probing state registration databases, if left unchecked or unsecured, these operatives could add or delete names, creating chaos during on Election Day. Operatives could alter the address, in states that mail ballots out, so that they receive ballots. Foreign operatives need not make any changes to create chaos, too. They could figure out who routinely votes absentee and request ballots on voters' behalf.[19]

Recent efforts by Iran and Russia, though, uncovered by the intelligence community, may shed some light on foreign actors' intentions. According to officials, Iran and Russia exfiltrated "some voter registration information." Both countries seem to be using the data in similar ways—they are using it to "attempt to communicate false information to registered voters" in efforts to "cause confusion, sow chaos, and undermine [ ] confidence in American democracy,"[20] rather than in ways to impact the outcome by manipulating specific votes. Specifically, actors in Iran and Russia are using the voter registration information to send fake emails to registered voters made to look like they are sent from a pro-Trump group known as "the Proud Boys." The emails threaten Democratic voters, demanding they vote for President Trump's reelection or the Proud Boys "will come after" the voter.[21]

Regardless of how Russia and Iran use the hacked data, it helps establish that some of the most vulnerable elements of voting systems are those that are

[18] According to former Homeland Security Adviser Lisa Monaco, "one of the motives that Russia was trying to do with this active measures campaign was to sow discord and lack of confidence in the voting process and the democratic process." Ibid at p. 35.

[19] Nor would operatives need to cast mail-in or absentee ballots to create chaos. In many states, for example, when a vote requests an absentee ballot, the county election officials notes the request in the poll book and if the voter appears in person on Election Day, the voter must either destroy the absentee ballot in front of elections officials or cast a provisional ballot.

[20] See "DNI John Ratcliffe's Remarks at Press Conference on Election Security, above, n. 7.

[21] Katie Shepherd, "DNI Ratcliffe said Iran aimed to hurt Trump with faked Proud Boy emails. Democrats are skeptical," The Washington Post, October 22, 2020, https://www.washingtonpost.com/nation/2020/10/22/democrats-election-trump-ratcliffe-iran/.

constantly online. Despite best efforts to protect the data, including the sharing of information between federal and state authorities, foreign actors will try to obtain access and use the information in efforts to undermine confidence in democratic institutions.

Some elements of voting systems represent greater vulnerabilities than others. Bad actors—especially foreign bad actors—are likely to focus efforts on what could obtain the greatest return on their investments with the smallest possible risk. This calculation tends to disfavor efforts physically to hack voting machines while favoring attempts to access online databases, create malware applicable at the operating system level, and so forth. With the risk/reward calculation in mind, policymakers will have a better idea of how to triage and respond to voting system vulnerabilities.

Priorities and Recommendations

The ultimate responsibility for mitigating voting system vulnerabilities falls primarily with state and local elected officials. When triaging vulnerabilities, officials should look at voting systems component parts, determine which vulnerabilities are the most likely to be exploited and which are least complex to mitigate.

First and foremost, policymakers should presume that their elections officials are targets for both foreign state and non-state actors. Because elections officials are targets, policymakers should focus on ensuring the security of voter registration processes and databases. Voter registration databases, for example, should always be encrypted. State employees should be trained on how to spot phishing and other attempts to procure network credentials. State elections officials, also, should have a designated cybersecurity official, such as a Chief Information Security Officer (CISO) who can identify attempts to improperly access databases and communicate those attempts with other states and the federal government.

Policymakers should also ensure that electronic voting machines have an auditable paper trail. In the wake of recounts in 2016, it became clear that many DRE machines lack the ability to have a paper trail that officials can audit in a meaningful way. Similarly, the recounts also established that many states lack a proper, uniform audit process. Two simple steps for states to take are: Replacing DRE systems and enacting sound audit procedures. As to the first, states should ensure that DRE systems are replaced with systems capable where the voter generates a paper trail rather than the system itself. To the extent any machines are internet enabled, this feature should be disabled prior to Election Day. As to the second step, states should enact widespread, statistically sound audit procedures and periodically engage in those audits even when nothing seems amiss.

States also must take steps to secure voter registration databases, e-pollbooks, and other online databases. Some solutions are easier, and faster, to implement than others. The two easiest solutions include requiring two-factor authentication for access, ensuring passwords are changed from default to strong, controlling and actively managing access to databases—limiting access only to those who absolutely need it—and backing-up systems routinely. Other solutions, which may take more time, include requiring third parties and vendors who need access to the system to develop and implement strong cybersecurity practices, conduct regular penetration testing (pen-testing) and regular audits, revising procurement practices and contracts to ensure the adoption of reasonable security practices, and more.

Despite the vulnerabilities, the U.S. federal system has so far fulfilled its core function: ensuring the overall integrity of the system. Any solution must involve states and the federal government cooperating, with states taking the lead running voting systems and the federal government ensuring adequate communication of known and potential threats.

The Election Information Vulnerabilities

People, Candidates, Campaigns, Parties, Voters and Active Measures

Where vulnerabilities in voting systems are primarily focused on hardware and processes, vulnerabilities within elections systems require a focus on humans. "Active measures," including disinformation campaigns, are designed to appeal to voters' decision-making processes. Practically speaking, bad actors often obtain access to candidate, campaign, or party email servers or campaign network because a staff member inadvertently provides access.

When bad actors gain access to databases, they can download troves of emails, export campaign data, find either contact information, and even jeopardize third-party databases. Most campaigns or parties contract with vendors to provide smartphone apps that provide volunteers walk lists, phone banking resources, and more. Behind these apps are extensive, proprietary databases with treasure troves of information, such as voters' names, age, addresses, voter score (the likelihood that the voter is to participate in a given election), demographic modeling and more. For foreign actors intent on interfering with an election, they may find access to the third-party databases easier to access than state-run databases.

The term "active measures," according to the United States Information Agency, refers "to the manipulative use of slogans, arguments, disinformation, and carefully selected true information… used to try to influence the attitudes and actions of foreign publics and governments."[22] Experts and the American public tend to associate the term "active measures" primarily with Russia, though other countries such as China and Iran may employ similar tactics for slightly different purposes.[23]

Employing active measures against the United States is not a new tactic for Russia—the Soviet Union employed them as a regular intelligence tactic against the U.S. since at least the 1950s. Two aspects of active measures have changed, though, since the days of the Soviet Union. First, active measure campaigns can now be delegated to private companies, making it harder to link them directly to the Russian government. Second, the advent of social media has eliminated communications barriers that previously existed, allowing foreign actors to engage directly with their intended targets at significantly lower risk and expense.

Russia's active measures efforts can be subdivided into two primary categories, at least as applied to the 2016 presidential elections:

- Efforts focused on dividing Americans along ideological, ethnic, or other similar fault lines
- Efforts focused on disseminating largely true information obtained through improper sources

While the efforts can be subdivided into two primary categories, the tactics are largely the same. The government outsourced many of the efforts to a private company called the Internet Research Agency ("IRA"), which was run by a close ally of Russian President Vladimir Putin, Yevginy Prigozhin. Thousands, if not tens-of-thousands, of fake social media accounts were created by the IRA on platforms

[22] United States Information Agency, Washington, D.C., Soviet Active Measures in the "Post-Cold War" Era 1988-1991 (June 1992). http://intellit.muskingum.edu/russia_folder/pcw_era/.

[23] *See*, United States Office of Director of National Intelligence (ONDI), Washington, D.C., "Statement by NCSC Director William Evanina: Election Threat Update for the American Public," ODNI Release No. 29-20, August 7, 2020. https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public.

such as Facebook, Twitter, Instagram, and YouTube. The IRA used these accounts to disseminate both fake news and real information obtained through improper sources. IRA operatives also created social media bots for the purpose of sharing information automatically. Both the automated and real accounts would magnify original posts, causing the information to go viral.[24]

Prior to the 2016 presidential election, the IRA sent operatives to the United States for several purposes. Chief among these purposes was to research the issues that would divide Americans. This research is consistent with the presumed goal of active measures: to cause Americans to question their institutions, such as the democratic selection of the country's leaders, to question the motives of fellow citizens of other political parties, and to doubt the outcome of the election.[25]

[24] "The spread of intentionally false information on social media is often exacerbated by automated, or 'bot' accounts." The Report further cited several studies, one of which concluded that "one-fifth of the political discourse around the 2016 election on Twitter may have been automated and the result of bot activity." Similarly, Twitter itself estimated that over 50,000 automated accounts linked to Russia were tweeting election-related content" during the 2016 election. *SSCI Report, Vol. 2* at 10, 18.

[25] Whether the Russians were successful in their operations depends on the perspective. Looking solely at the amount of ink, resources, and time spent analyzing the efforts, along with allegations of Trump's collusion with Russia, one could state that the efforts were resounding successes. For example, the Senate Select Committee on Intelligence found both that "the IRA sought to influence the 2016 U.S. presidential election by harming Hillary Clinton's chances of success and supporting Donald Trump at the direction of the Kremlin" and that Russia's efforts were "part of a broader, sophisticated, and ongoing information warfare campaign designed to sow discord in American politics and society." U.S. Congress, Senate, Select Committee on Intelligence, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election; Volume 2: Russia's Use of Social Media with Additional Views*, 116th Cong., 1st sess., 2019, S. Rep. 116-XX, 4-5 (hereafter "*SSCI 2016 Election Report*, Vol. 2"). The statistics, on the other hand, lead to some mixed results. First, for example, the SSCI Report notes, during the 2016 campaign, that there were over 9 billion

Consequently, the IRA crafted social media posts on both sides of divisive issues.

When viewed through the lens of the Russian's objectives, it makes sense that most of the IRA posts discussed both sides of immigration, racial tensions such as black lives matter and policing, stoked outrage against and defended Muslims, and so on. While much of the narrative in the media has focused on the Russian's opposition to Hillary Clinton, the evidence reveals that the Russians hardly spent any time discussing candidates.[26] Instead, the IRA spent time cultivating virtual relationships with Americans and used those relationships to further its messages.[27]

Russian intelligence units within the GRU stole documents from the Democratic National Committee (DNC) and Clinton campaign chairman John Podesta.[28] With respect to the latter, Podesta was the victim of a well-executed phishing attack. With respect to the former, it is unclear how the hackers obtained access to DNC servers, but another phishing attack is not out of the question.[29]

After obtaining documents through hacks, the Russian government distributed the documents to Wikileaks through known fronts, such as DCLeaks and Guccifer 2.0.[30] Once Wikileaks published the documents, the Trump campaign, media, and other social media platform users distributed the documents far and wide. President Trump, Senator Warren, and others relied on the leaked documents to divide the Democratic Party, showing a conspiracy against Sen. Bernie Sanders in the party's primary.[31]

Where the primary purpose for Russian interference in elections systems may be to create distrust in institutions and outcomes, the goals of other countries differ.

posts related to the campaign, of which 1.1 billion occurred in the final month. IRA operatives, during the 2016 presidential race, created over 61,500 Facebook posts, including a couple false stories that generated a combined 1.7 million interactions during the final three months of the election. That 1.7 million interactions represents about 1 percent of the total interactions during the final month of the campaign. Those 61,500 Facebook posts, though, may have led to over 30 million interactions touching as many as 126 million Americans. *Id*. at 45. The statistics may be misstated, since the report does distinguish between shares, likes, comments, and reactions; many of those interactions may be from the same Facebook users. It is unclear, further, what is meant by "come in contact with" the IRA posts, as some Americans could simply have scrolled past them without really reading or being influenced by them.

[26] "The overwhelming majority of the content disseminated by the IRA did not express clear support for one presidential candidate or another. Instead… most IRA content discreetly messaged narratives of disunity, discontent, hopelessness, and contempt of others, all aimed at sowing societal division." *SSCI 2016 Election Report*, Vol. 2 at p. 32. The evidence found in both the Senate Report on Russian Interference, Vol. 2 and the indictment of the IRA suggests that the Russians were opportunistic rather than leaning toward one candidate. During the primaries, for example, posts attributable to the IRA supported Senators Bernie Sanders, Ted Cruz, and Marco Rubio. *See, ibid*. at pp. 6, 37. *See also*, U.S Department of Justice, Office of Special Counsel, Washington, D.C., *Indictment, United States v. Internet Research Agency, et al.*, Robert S. Mueller, III, February 16, 2018, p. 17. https://www.justice.gov/file/1035477/download.

[27] *See, e.g., SSCI Report, Vol. 2*, 29-30, U.S. Department of Justice, Office of Special Counsel, *Report on the Investigation Into Russian Interference In the 2016 Presidential Election, Vol. 1* ("*Mueller Report*"), Robert S. Mueller, III, 21-22, and U.S Department of Justice, Office of Special Counsel, Washington, D.C. *Indictment, United States v. Internet Research Agency, et al*. Robert S. Mueller, III, 3.

[28] *SSCI Report, Vol. 2*, 63-64.

[29] It is also worth noting that Republican Party, Republican lawmakers, and other Republican affiliated organizations were also targeted. *See* "2016 Presidential Campaign Hacking Fast Facts," *CNN*, https://www.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html.

[30] *SSCI Report, Vol. 2*, 63-64.

[31] Scott Detrow. "Clinton Campaign Had Additional Signed Agreement With DNC In 2015." NPR, November 3, 2017. https://www.npr.org/2017/11/03/561976645/clinton-campaign-had-additional-signed-agreement-with-dnc-in-2015.

China, for example, “prefers that President Trump… does not win reelection” but rather than waging a Soviet-style disinformation campaign, seeks to “pressure political figures it views as opposed to China’s interests, and deflect and counter criticism of China.”[32]

China’s active measures focuses either on silencing criticism of the country and ruling communist party or on promoting positive stories to bolster its global reputation. China uses the Confucius Institute, for example, to control messages and academic material appearing on college campuses.[33] China uses its investments through Tencent and partnerships with United States sporting associations to tamp down criticism of how it handled protests in Hong Kong or the treatment of the Uyghurs.[34]

Despite these traditional efforts to influence public perception, there is evidence that Beijing is taking a more active role influencing elections in the mold of the Russians. According to the Washington Post, in 2018, Chinese operatives used fake digital accounts in a successful effort to promote a pro-Beijing politician in southern Taiwan.[35] The Chinese consulate in Houston was a hub for intelligence activities, including using sophisticated means to identify and recruit Black Lives Matter protestors.[36]

[32] Office of the Director of National Intelligence, Washington, D.C., “Statement of NCSC Director William Evanina: Election Threat Update for the American Public,” ODNI Release No. 29-20, August 7, 2020. https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public.

[33] Confucius Institutes “attract full-tuition-paying Chinese students, fund scholarships for American students to study abroad, and offer other resources. Universities with financial incentives to please China find it more difficult to criticize Chinese policies.” Additionally, Confucius Institutes tend to yield significant soft power and are able to encourage colleges and universities to “avoid Chinese political history and human rights abuses” along with presenting American students only one side of disputed topics. *See* Rachelle Peterson, *Outsourced to China: Confucius Institutes and Soft Power in American Higher Education*, National Association of Scholars, April 7, 2017. https://www.nas.org/reports/outsourced-to-china/full-report.

[34] China “demands that online platforms remove all objectionable content, including anything politically insensitive… [Chinese] [t]ech giants like Alibaba Group Holding Ltd. and Tencent Holdings Ltd. are developing sophisticated content-moderation systems that intentionally target political content.” Shan Li, “Made-in-China Censorship for Sale,” The Wall Street Journal, March 6, 2020. https://www.wsj.com/articles/made-in-china-censorship-for-sale-11583448433. *See also* Scott Simon, “NBA Sidelines Free Speech In Favor of China,” NPR, October 12, 2019. https://www.npr.org/2019/10/12/769578234/opinion-nba-sidelines-free-speech-in-favor-of-china.

[35] “There’s another expert player warming up to online election interference. We should worry,” Washington Post, September 22, 2019. https://www.washingtonpost.com/opinions/global-opinions/theres-another-expert-player-warming-up-to-online-election-interference-we-should-worry/2019/09/22/76c8c870-d990-11e9-bfb1-849887369476_story.html.

[36] Ted Galen Carpenter, “China Is Interfering in the 2020 Election. Beijing Wants Trump to Lose,” Cato Institute, September 4, 2020. https://www.cato.org/publications/commentary/china-interfering-2020-election-beijing-wants-trump-lose.

Solutions and Priorities

The election system vulnerabilities relate to human behavior. Email, for example, remains the most common point of entry for hackers, though the use of stolen credentials and identifying backdoors is growing.[37] Because the vulnerabilities relate to people, the solutions must also focus on people.

The best solutions are those focused on education for citizens. Society needs to educate citizens on how to identify phishing scams, introduce an abundance of caution for even the lowest level campaign staffer, teach people how to consume news critically and how to spot potential foreign interference efforts. Since the best solutions will focus on education, the government and private sector are equal partners. Many technology platforms are leading the way, with companies like Alphabet (Google and YouTube),[38] Facebook,[39] Twitter,[40] leading the way. Certainly, these technological innovations will help, but they cannot, and will not, completely solve problems of disinformation, mistake, or electronic subterfuge. The public will need to remain vigilant.

[37] "2019 Data Breach Investigations Report," *Verizon*, 2019. Accessed November 12, 2019. https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf.

[38] Google maintains an official "Civics" blog that "updates on [its] efforts to support democratic processes around the world. Anyone can find articles detailing how Google, for example, is "helping to safeguard elections," access authoritative information, and more. https://blog.google/outreach-initiatives/civics/.

[39] Facebook maintains a page dedicated to detailing efforts to "secur[e] [its] platforms, provid[e] transparency and empower[ ] people to vote." Among the projects listed are efforts to stop influence operations; identify and eliminate fake accounts; secure the accounts of elected officials, candidates, and their staff; and more. https://about.fb.com/actions/preparing-for-elections-on-facebook/.

[40] Twitter has a constantly evolving policy for safeguarding the election. Unlike Facebook and Alphabet, which tend to focus on stopping influence operations, identifying face accounts, and so on, Twitter's policy focuses more on misinformation. It includes in election-related misinformation topics such as COVID-19, declaring victory before official results, and so on. It also identifies candidates and campaigns as the potential source of misinformation and has banned "all political ads." Vijaya Gadde and Kayvon Beykpour, "Additional steps we're taking ahead of the 2020 US Election," Twitter Company Blog, October 9, 2020, https://blog.twitter.com/en_us/topics/company/2020/2020-election-changes.html.

Conclusion

The Information Age challenges democratic processes by providing opportunities for malign foreign actors to influence elections through either hacking voting systems inserting themselves into the elections process. Thus far, those attempts have met with limited success.[41] And thanks to publicity about active measures efforts in the 2016 presidential elections, the country and elections officials are keenly aware of the efforts.

The democratic process is rife with vulnerabilities. When the United States shifted from analog systems to electronic voting and elections systems, it swapped one set of vulnerabilities for another. Many of the vulnerabilities, though, are easily mitigated. Policymakers need to understand the vulnerabilities and learn how to prioritize the solutions, learning which ones may be undertaken with little-to-no cost and which may require more time and resources. The democratic process in the United States is second to none. With the right policy response, our elections process will remain that way.

[41] *SSCI Report, Vol. 1*, 3-5.

BIBLIOGRAPHY

CNN. "2016 Presidential Campaign Hacking Fast Facts." Accessed November 12, 2019. https://www.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html.

Ballotpedia. "Help America Vote Act (HAVA) of 2002." Accessed November 7, 2019, https://ballotpedia.org/Help_America_Vote_Act_(HAVA)_of_2002.

Ballotpedia. "Voting Methods and Equipment by State." Accessed November 8, 2019. https://ballotpedia.org/Voting_methods_and_equipment_by_state.

Matt Blaze, Harri Hursti, Margaret Macalpine, et al. "Def Con 27 Voting Machine Hacking Village." Defcon. September 26, 2019. https://media.defcon.org/DEF%20CON%2027/voting-village-report-defcon27.pdf.

Ted Galen Carpenter, "China Is Interfering in the 2020 Election. Beijing Wants Trump to Lose," Cato Institute, September 4, 2020. https://www.cato.org/publications/commentary/china-interfering-2020-election-beijing-wants-trump-lose.

Laurie Chen. "NBA in damage-control mode as more Chinese partners cut ties in Hong Kong protest tweet storm." South China Morning Post. October 9, 2019. https://www.scmp.com/news/china/society/article/3032164/nba-damage-control-mode-adam-silver-lands-china-hong-kong.

Peter Allen Clark. "What to Know about Blizzard, Hong Kong and the Controversy Over Politics in Esports." Time. October 21, 2019. https://time.com/5702971/blizzard-esports-hearthstone-hong-kong-protests-backlash-blitzchung/.

Scott Detrow. "Clinton Campaign Had Additional Signed Agreement With DNC In 2015." NPR, November 3, 2017. https://www.npr.org/2017/11/03/561976645/clinton-campaign-had-additional-signed-agreement-with-dnc-in-2015.

Jerry Dunleavy. "Mueller says Russia's GRU stole Clinton, DNC emails and gave them to Wikileaks." *Washington Examiner*. April 18, 2019. https://www.washingtonexaminer.com/news/mueller-says-russias-gru-stole-clinton-dnc-emails-and-gave-them-to-wikileaks.

Ron Elving. "The Florida Recount of 2000: A Nightmare That Goes On Haunting." *NPR*. November 12, 2018. https://www.npr.org/2018/11/12/666812854/the-florida-recount-of-2000-a-nightmare-that-goes-on-haunting.

BIBLIOGRAPHY

Vijaya Gadde and Kayvon Beykpour. "Additional steps we're taking ahead of the 2020 US Election." Twitter Company Blog. October 9, 2020. https://blog.twitter.com/en_us/topics/company/2020/2020-election-changes.html.

Shane Harris, Ellen Nakashima, and Craig Timberg. "Through email leaks and propaganda, Russians sought to elect Trump, Mueller finds." *The Washington Post*. April 18, 2019. https://www.washingtonpost.com/politics/through-email-leaks-and-propaganda-russians-sought-to-elect-trump-mueller-finds/2019/04/18/109ddf74-571b-11e9-814f-e2f46684196e_story.html.

Drew Harwell and Tony Romm. "TikTok's Bejing roots fuel censorship suspicion as it builds for a huge U.S. audience." *The Washington Post*. September 15, 2019. https://www.washingtonpost.com/technology/2019/09/15/tiktoks-beijing-roots-fuel-censorship-suspicion-it-builds-huge-us-audience/.

Elaine Kamarck. "State and localities are on the front lines of fighting cyber-crimes in elections." Brookings. August 15, 2019. https://www.brookings.edu/blog/fixgov/2019/08/15/states-and-localities-are-on-the-front-lines-of-election-security/.

Makena Kelly. "Russians hacked voting databases in two Florida counties in 2016, governor says." *The Verge*. May 14, 2019. https://www.theverge.com/2019/5/14/18623392/russians-ron-desantis-vote-database-hack-gru-ron-wyden-paper-ballots.

Peter Kelley. "Documents that Changed the World: 'Hanging chads' and butterfly ballots — Florida, 2000." *UW News, University of Washington*. March 14, 2016. https://www.washington.edu/news/2016/03/14/documents-that-changed-the-world-hanging-chads-and-butterfly-ballots-florida-2000/.

Shan Li. "Made-in-China Censorship for Sale." The Wall Street Journal. March 6, 2020. https://www.wsj.com/articles/made-in-china-censorship-for-sale-11583448433.

Paris Martineau. "Russia's Disinformation Was is Just Getting Started." *Wired*. October 8, 2019. https://www.wired.com/story/russias-disinformation-war-is-just-getting-started/.

BIBLIOGRAPHY

Lily May Newman. “Hackers Take on Darpa’s $10 Million Voting Machine.” *Wired*. August 9, 2019. https://www.wired.com/story/darpa-voting-machine-defcon-voting-village-hackers/.

Lawrence Norden and Edgardo Cortes. “What Does Election Security Cost?” *Brennan Center for Justice*. August 15, 2019. https://www.brennancenter.org/our-work/analysis-opinion/what-does-election-security-cost.

Rachelle Peterson, *Outsourced to China: Confucius Institutes and Soft Power in American Higher Education*, National Association of Scholars, April 7, 2017. https://www.nas.org/reports/outsourced-to-china/full-report.

Scott Simon. “NBA Sidelines Free Speech In Favor of China.” *NPR*. October 12, 2019. https://www.npr.org/2019/10/12/769578234/opinion-nba-sidelines-free-speech-in-favor-of-china.

Katie Shepherd. “DNI Ratcliffe said Iran aimed to hurt Trump with faked Proud Boy emails. Democrats are skeptical.” The Washington Post, October 22, 2020. https://www.washingtonpost.com/nation/2020/10/22/democrats-election-trump-ratcliffe-iran/.

“The State and Local Election Cybersecurity Playbook.” *Belfer Center for Science and International Affairs, Harvard Kennedy School*. February 2018. https://www.belfercenter.org/sites/default/files/files/publication/StateLocalPlaybook%20 1.1.pdf.

U.S. Congress. Senate. Select Committee on Intelligence. *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election; Volume 1: Russian Efforts Against Election Infrastructure with Additional Views*. 116th Cong., 1st sess., 2019, S. Rep. 116-XX.

U.S. Congress, Senate, Select Committee on Intelligence. *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election; Volume 2: Russia’s Use of Social Media with Additional Views*. 116th Cong., 1st sess., 2019, S. Rep. 116-XX.

U.S. Department of Homeland Security. *Foreign Interference Taxonomy*. Washington, D.C. July 2018. https://www.dhs.gov/sites/default/files/publications/19_0717_cisa_foreign-influence-taxonomy.pdf.

BIBLIOGRAPHY

U.S. Department of Homeland Security. *Social Media Bots Overview*. Washington, D.C. May 2018. https://www.dhs.gov/sites/default/files/publications/19_0717_cisa_social-media-bots-overview.pdf.

U.S. Department of Homeland Security. *The War on Pineapple: Understanding Foreign Interference in 5 Steps*. Washington, D.C. July 2019. https://www.dhs.gov/sites/default/files/publications/19_0717_cisa_the-war-on-pineapple-understanding-foreign-interference-in-5-steps_0.pdf.

U.S Department of Justice, Office of Special Counsel, Washington, D.C. *Indictment, United States v. Internet Research Agency, et al*. Robert S. Mueller, III. February 16, 2018. https://www.justice.gov/file/1035477/download.

U.S. Department of Justice, Office of Special Counsel, Washington, D.C. *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*, Robert S. Mueller, III, March 2019. https://www.justice.gov/storage/report.pdf.

U. S. Information Agency. *Soviet Active Measures in the "Post-Cold War" Era 1988-1991*. Washington, D.C. June 1992. http://intellit.muskingum.edu/russia_folder/pcw_era/.

United States Office of Director of National Intelligence (ONDI). Washington, D.C. "Statement by NCSC Director William Evanina: Election Threat Update for the American Public." ODNI Release No. 29-20. August 7, 2020. https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public.

United States Office of Director of National Intelligence (ONDI). Washington, D.C. "DNI John Ratcliffe's Remarks at Press Conference on Election Security." October 22, 2020. https://www.dni.gov/index.php/newsroom/press-releases/item/2162-dni-john-ratcliffe-s-remarks-at-press-conference-on-election-security.

Verizon. "Data Breach Investigations Report." Accessed November 12, 2019, https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf.

BIBLIOGRAPHY

Washington Post Editorial Board. "There's another expert player warming up to online election interference. We should worry," Washington Post, September 22, 2019. https://www.washingtonpost.com/opinions/global-opinions/theres-another-expert-player-warming-up-to-online-election-interference-we-should-worry/2019/09/22/76c8c870-d990-11e9-bfb1-849887369476_story.html.

Help America Vote Act, Pub. Law 107-252, 107th Cong., 1st sess., 2002. Codified at 42 U.S.C. §§ 15301, *et seq*. but transferred to 52 U.S.C. §§ 20901, *et seq*.

Rainey Center

317 A Street SE
Washington, DC 20003
(202) 350-1689
info@raineycenter.org
raineycenter.org