CYBERATTACKS AND ELECTION INTEGRITY

Daniel Barabander[*]

CITE AS: 4 GEO. L. TECH. REV. 665 (2020)

TABLE OF CONTENTS

I. INTRODUCTION

The Russian attacks on voter registration databases preceding the 2016 Election "changed the narrative" about election security, highlighting a new avenue for adversarial foreign nation-states to interfere with the U.S.'s elections: the cyberattack.[1] This Technology Explainer will analyze how cyberattacks function in elections, which election systems are most vulnerable to these attacks, and how cyberattacks hurt election integrity.

II. CYBERATTACK METHODS IN ELECTIONS

A cyberattack is "an attempt to gain illegal access to a computer or computer system for the purpose of causing damage or harm."[2] Some common cyberattack methods used on election systems are through denial-of-service (DoS) attacks, malware, Structured Query Language (SQL) injections, and phishing attacks.

[*] Georgetown University Law Center, J.D. Candidate 2021; Colgate University, B.A. in History and Geography 2013.

[1] Jacob Rush, *Hacking the Right to Vote*, 105 VA. L. REV. ONLINE 67, 74 (2019) https://www.virginialawreview.org/sites/virginialawreview.org/files/05.%20Final%20Rush.pdf [https://perma.cc/G6HX-U2FY].

[2] *Cyberattack,* MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/cyberattack [https://perma.cc/VTY3-T6HL].

DoS attacks interrupt or slow down access to a computer system for legitimate users by flooding the system with illegitimate traffic.[3] In elections, computer systems vulnerable to DoS attacks include e-pollbooks, electronic voting machines, voter registration databases, and electronic auditing systems.[4] The goal of a DoS attack is to render election technology unusable, thereby disrupting the election.[5]

Malware is malicious software that introduces worms, spyware, viruses, Trojan horses, and ransomware to a system.[6] Malware, like DoS attacks, can disrupt election technologies such as e-pollbooks, electronic voting machines, and electronic auditing systems.[7] However, attackers can also use malware to attack these election systems to produce a specific desired result, such as manipulating vote counts on a voting machine or changing a person's voting registration status on an e-pollbook..[8]

A SQL injection "is a code injection technique that hackers can use to insert malicious SQL statements into [user-facing] input fields for execution by the underlying SQL database."[9] Attackers can use SQL injections to access and destroy data in voter registration databases.[10]

A phishing attack is when an attacker, "masquerading as a trusted entity," sends an email or text to a victim that prompts the victim into providing the attacker with sensitive information for that "trusted entity," like a username and password.[11] Attackers can use the sensitive information they obtain from phishing attacks to gain access to otherwise restricted voting systems.[12]

[3] NAT'L ACADS. OF SCIS, ENG'G, & MED., SECURING THE VOTE: PROTECTING AMERICAN DEMOCRACY 86 (2018); Cybersecurity & Infrastructure Security Agency, *Security Tip (ST04-015): Understanding Denial-of-Service Attacks*, (Nov. 20, 2019), https://www.us-cert.gov/ncas/tips/ST04-015 [https://perma.cc/K4MY-9QTE].

[4] *Id.*

[5] *Id.*; Charles Stewart III, *The 2016 U.S. Election: Fears and Facts About Electoral Integrity*, 28 J. DEMOCRACY 50, 57 (2017), https://muse.jhu.edu/article/653376/pdf [https://perma.cc/V2EN-WJAP].

[6] NAT'L ACADS. OF SCIS, ENG'G, & MED., *supra* note 3, at 86.

[7] *Id* at 86–87.

[8] *Id.*

[9] UC BERKELEY, *How to Protect Against SQL Injection Attacks*, https://security.berkeley.edu/education-awareness/best-practices-how-articles/system-application-security/how-protect-against-sql [https://perma.cc/T5MK-WWKL].

[10] *Id.*; Marian K. Schneider, *Election Security: Increasing Election Integrity by Improving Cybersecurity*, *in* THE FUTURE OF ELECTION ADMINISTRATION 243, 252 (Mitchell Brown et al. eds., 2019).

[11] IMPERVA, *Phishing Attacks*, https://www.imperva.com/learn/application-security/phishing-attack-scam [https://perma.cc/24NM-XGQ9].

[12] *See* Matthew Cole et al., *Top-Secret NSA Report Details Russian Hacking Effort Days*

III. VOTING SYSTEMS VULNERABLE TO CYBERATTACKS

It is important to realize that any computerized voting system is vulnerable to cyberattacks.[13] This Technology Explainer focuses on two voting systems: (1) voting machines and (2) voter registration databases. These technologies are integral to our elections and highly vulnerable to cyberattacks because they can be connected to the Internet.[14]

A. Voting Machines

"Voting machines" are computers that cast and tabulate votes.[15] There are multiple ways in which a cyberattacker can access a voting machine, but this paper will focus on methods that utilize the Internet.[16]

First, although voting machines are not supposed to be connected to the Internet, they can be connected indirectly through election management computers, which are themselves connected to the Internet.[17] Election management computers contain software and ballot definition files that are loaded onto voting machines using a cartridge or memory card.[18] A cyberattacker could implant malware onto an election management computer via the Internet, and this malware could then be transferred to a voting machine by a cartridge or memory card.[19] From this voting machine, the malware could further be transmitted to other voting machines through in-precinct local

Before 2016 Election, INTERCEPT (June 5, 2017, 3:44 PM), https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election [https://perma.cc/M3B6-PD3T] (detailing phishing attacks on election systems in Arizona and Illinois).

[13] Judd Choate & Robert Smith, *Election Cybersecurity*, *in* THE FUTURE OF ELECTION ADMINISTRATION 279, 280 (Mitchell Brown et al. eds., 2019).

[14] Eric Manpearl, *Securing U.S. Election Systems: Designating U.S. Election Systems as Critical Infrastructure and Instituting Election Security Reforms*, 24 B.U. J. SCI. & TECH. L. 168, 173, 175 (2018).

[15] NAT'L ACADS. OF SCIS, ENG'G, & MED., *supra* note 3, at 39.

[16] Although generally not considered in the realm of cyberattacks, an attacker can also physically tamper with a voting machine, and studies have repeatedly shown how easy it is for an attacker with moderate levels of experience to corrupt a voting machine in person. *See* MATTHEW BLAZE ET AL., DEF CON 27: VOTING MACHINE HACKING VILLAGE 5 (2019), https://media.defcon.org/DEF%20CON%2027/voting-village-report-defcon27.pdf [https://perma.cc/88S3-MN4Z].

[17] Manpearl, *supra* note 14, at 175; NAT'L ACADS. OF SCIS, ENG'G, & MED., *supra* note 3, at 90–91; Schneider, *supra* note 10, at 255 (noting that "[a]lthough jurisdictions 'should' not connect those computers to a network or the Internet, no systematic efforts exist to ensure compliance with recommended security configurations.").

[18] Manpearl, *supra* note 14, at 175

[19] *Id.*

networks and as memory cards are exchanged.[20] Thus, through corrupting just one voting machine, the cyberattacker could corrupt the voting machines of an entire jurisdiction.[21]

Second, some voting machines can be errantly connected to the Internet. For example, up until 2014, twenty percent of Virginia's voting precincts were equipped with a wireless network to allow ballot programming and voter data exchange between voting machines.[22] The Virginia State Board of Elections investigated these machines and discovered that wireless cards on the voting machine permitted "an external party to access the [machine] and modify the data [on the machine] without notice . . . an attacker could join the wireless ad-hoc network, record voting data or inject malicious [data.]"[23]

Regardless of how the cyberattack is carried out, once a voting machine is breached, the attackers can choose their desired impact on the machine from a parade of horribles. These impacts include flipping the vote the computer casts in favor of the attackers' preferred candidate, destroying records required for auditing, or simply making the process of casting a vote more difficult.[24]

If the voting machine does not have a paper audit trail (meaning it is not "software independent"[25]), like Direct Recording Electronic (DRE) machines without a Voter Verified Paper Audit Trail (VVPAT), the only record of the vote is in the machine itself; in the event of tampering, there is no way to verify, audit, or recount the votes cast on that machine.[26]

[20] *Id.*; NAT'L ACADS. OF SCIS, ENG'G, & MED., *supra* note 3, at 90.

[21] Adam Aviv et al., *Security Evaluation of ES&S Voting Machines and Election Management System, in* EVT'08: PROCEEDINGS OF THE CONFERENCE ON ELECTRONIC VOTING TECHNOLOGY 4 (2008), https://www.usenix.org/legacy/event/evt08/tech/full_papers/aviv/aviv.pdf [https://perma.cc/87BW-Z3XH] ("a single circumvented piece of precinct hardware (such as a memory card returned from a precinct for vote tallying) can effectively 'take over' the county-wide back-end tally system, alter county-wide results reported in the current election, and then corrupt the installed firmware of additional precinct hardware in subsequent elections.").

[22] Manpearl, *supra* note 14, at 175–76.

[23] *Id* at 176.

[24] *Id.* at 179; NAT'L ACADS. OF SCIS, ENG'G, & MED., *supra* note 3, at 85–86.

[25] Ronald L. Rivest & John P. Wack, *On The Notion of "Software Independence" in Voting Systems*, 366 PHIL. TRANS. R. SOC. A 3759, 3759 (2008) https://royalsocietypublishing.org/doi/pdf/10.1098/rsta.2008.0149 [https://perma.cc/P9VV-L4L6] ("A voting system is software independent if an (undetected) change or error in its software cannot cause an undetectable change or error in an election outcome . . . .").

[26] Schneider, *supra* note 10, at 254; Kimberly Breedon & Christopher A. Bryant, *Counting the Votes: Electronic Voting Irregularities, Election Integrity, and Public Corruption*, 49 U. MEM. L. REV. 979, 990, 993 (2019).

B. Voter Registration Databases

A voter registration database is a "single, uniform, official, centralized, interactive computerized statewide voter registration list . . . that contains the name and registration information of every legally registered voter in the state . . . ."[27] Voter registration databases are considered "the most vulnerable part of U.S. election systems" because they are almost always directly connected to the Internet.[28] Direct connection to the Internet makes voter registration databases susceptible to a variety of cyberattacks, including SQL injections, DoS attacks, and phishing attacks.[29]

Cyberattackers of voter registration databases can generally accomplish four objectives. First, they can make voters ineligible to vote by, for example, marking them as felons in a state where felons are not permitted to vote.[30] In this way, the attacker could selectively disenfranchise voters to support their desired candidate.[31] Second, the attacker can delete voter entries in the database prior to, or on, Election Day.[32] In both of these scenarios, voters who cannot prove their registered status will be forced to cast provisional ballots, "leading to long lines, undermining faith in the fairness of an election, and creating a major administrative headache to accurately count votes after the polls closed."[33] Third, attackers could focus on vote-by-mail voting, changing address information of vote-by-mail voters or creating entries for voters that do not exist.[34] Vote-by-mail voters who have had their addresses changed will not receive their ballots and may never vote at all.[35] In the case of fictitious voters added to the database, it would be difficult for officials even

[27] 52 U.S.C. § 21083 (2002).

[28] Manpearl, *supra* note 14, at 173; Mike Orcutt, *How Hackers Could Send Your Polling Station into Chaos*, MIT TECH. REV. (Oct. 5, 2016), https://www.technologyreview.com/s/602484/how-hackers-could-send-your-polling-station-into-chaos [https://perma.cc/9VAU-JJ5R].

[29] Schneider, *supra* note 10, at 252.

[30] Eric S. Lynch, *Trusting the Federalism Process Under Unique Circumstances: United States Election Administration and Cybersecurity*, 60 WM. & MARY L. REV. 1979, 2001 (2019) https://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=3814&context=wmlr [https://perma.cc/RHD6-LAA4].

[31] Manpearl, *supra* note 14, at 173–74.

[32] Lynch, *supra* note 30, at 2001.

[33] LAWRENCE NORDEN & IAN VANDEWALKER, BRENNAN CTR. JUSTICE, SECURING ELECTIONS FROM FOREIGN INTERFERENCE 16 (2017), https://www.brennancenter.org/sites/default/files/publications/Securing_Elections_From_Foreign_Interference_1.pdf [https://perma.cc/E4GF-CVUU].

[34] Lynch, *supra* note 30, at 2001.

[35] Manpearl, *supra* note 14, at 174.

to recognize the problem without any in-person verification.[36] Finally, if a DoS attack is employed and takes down the registration database, the e-pollbooks connected to this database would not be able to check in voters, creating widespread disruption.[37]

IV. WHY CYBERATTACKS HURT ELECTION INTEGRITY

Cyberattacks hurt election integrity through both actual and perceived tampering. The Supreme Court has consistently reiterated that the Constitution requires that each person's vote is given "full and equal significance."[38] Both manipulating vote tallies and disrupting an individual's ability to vote denies these rights entrusted by the Constitution.[39]

However, an election's legitimacy does not only depend on accurate and equal vote counting; people must also believe that the election system in place upholds these qualities.[40] Disruptions created by cyberattacks in even a small number of jurisdictions can lead to a loss of confidence in the integrity of the election as a whole.[41] Doubts on vote-counting "crack the foundation on which the edifice of elections rests" and "may ultimately prove as destructive to the democratic processes as actual tampering."[42] Often casting doubt, rather than actually changing any election results, is the motive of a cyberattacker.[43] An election without public confidence is not a legitimate election.[44]

V. CONCLUSION

The Russian attack from 2016 shows that the prospect of a cyberattack by foreign nation-states on election systems should not be considered a possibility, but an inevitability.[45] Since 2016, the U.S.'s voting infrastructure is only becoming *more* dependent on voting technologies that are vulnerable to cyberattacks.[46] One of Russia's goals in the 2016 attack may have been to

[36] NORDEN & VANDEWALKER, *supra* note 33, at 16. For example, in 2012, hackers submitted online requests for thousands of vote-by-mail ballots in Florida, but thankfully the unusual activity was detected, and no disruption occurred. *Id.*

[37] Stewart III, *supra* note 5, at 57.

[38] Breedon & Bryant, *supra* note 26, at 983–84.

[39] *Id.*; Manpearl, *supra* note 14, at 174.

[40] Breedon & Bryant, *supra* note 26, at 984.

[41] NAT'L ACADS. OF SCIS, ENG'G, & MED., *supra* note 3, at 86.

[42] Breedon & Bryant, *supra* note 26, at 982, 984.

[43] *Id.* at 987.

[44] *Id.* at 984.

[45] Schneider, *supra* note 10, at 248–49 ("future attacks on American elections are inevitable.").

[46] *See* Choate & Smith, supra note 13, at 279–80.

learn about the U.S.'s election systems' vulnerabilities for future attacks.[47] The same cyberattackers behind the 2016 attacks also made successful attempts at penetrating the U.S.'s election systems before the 2018 midterms "and, by all accounts, will be back again in 2020."[48] This Technology Explainer has taken a first step in combating cyberattacks in our election systems by recognizing how they function in practice.

[47] S. REP. NO. 116-XX, pt. 1, at 4 (2019), https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf [https://perma.cc/7UKN-W74T].

[48] Thomas Hicks, *Accessible and Secure: Improving Voter Confidence by Protecting the Right to Vote*, *in* THE FUTURE OF ELECTION ADMINISTRATION 49, 49 (Mitchell Brown et al. eds., 2019).