MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

ELECTION 2020 FEARS WHAT'S REAL AND WHAT'S (PROBABLY) NOT

by Hannah Hess and Emily Frye

OCTOBER 2020

#20-2968 10-28-2020

Background

In 2016, the integrity of the United States' presidential election was compromised by foreign state interference, particularly by Russia. It is widely understood that there was foreign interference in the U.S. election process, but it is unknown to what extent this may have affected the outcome of the election (if at all), as there are no indications that votes were changed. According to the Mueller Report, Russian entities engaged in both the spread of disinformation through social media, as well as computer-intrusion operations to steal data and release stolen documents.[1] Public perception often mischaracterizes these events as "hacking" the election infrastructure. In this paper, we will examine the risks and realities of election "hacking" as currently reported. We will consider the a) fear, b) reality, and c) best possible mitigation for the hacking of voter registration, electronic poll books, voting machines, and election night reporting, as well as the overarching threat of ransomware.

[1] Mueller, Robert S. "Report on the Investigation into Russian Interference in the 2016 Presidential Election." U.S. Department of Justice, 2019.

What “Hacking” Really Means

To understand the risks and realities regarding hacking attempts on our election infrastructure, we have to define both “hacking” and “election infrastructure.” The term “election hacking” is often used to encompass many different kinds of malicious activity targeting elections, including efforts to steal information and disinformation campaigns. When election “hacking” is used in article headlines, it can refer to anything from port scans (like a burglar looking for an unlocked door or window in a house), which happen on average about every five seconds, to the manipulation of votes, which has not been proven to have occurred in any U.S. election to date. Most hacking attempts on the election infrastructure lie somewhere between, in both frequency and nature.[2]

Much of the “election hacking” portrayed in the media actually refers to attempts to steal information from campaigns and individuals associated with campaigns, influence voters through disinformation campaigns, and access accounts or steal information through phishing activities. Russia, China, and Iran have all engaged in these efforts to some extent over the past four years.[3] However, it is important to note that hacking into the email of an individual associated with a campaign is not a hack into the election infrastructure, and disinformation campaigns and phishing emails are not “hacking” at all. Actual election hacking refers to compromises of election infrastructure that are intended to manipulate voter information, modify a vote tally, or undermine credibility in tabulated results. This paper will focus on hacking efforts aiming to compromise election infrastructure. “Election infrastructure” comprises voter registration database systems, electronic poll books, vote capture devices, vote tally systems, election night reporting systems, election officials’ communication systems, state and county data processing systems, communication systems used for situational reporting, and vendor equipment and service architectures.[4]

Even when votes are not changed, hacking attempts can still affect the outcome of the election through disinformation, delays, long lines, votes not cast, and decreased public confidence in election integrity. Hacking attempts that result in voter suppression, including long lines and delays, disproportionately affect the working class and can impact their probability to vote in future elections.[5] These incidents are even more important in “swing” counties, such as Durham County, North Carolina, a blue county in a primarily red state, which experienced a 2016 e-poll book hack, leading to challenges in the days leading up to the election and on Election Day. Additionally, states that heavily rely on in-person voting as opposed to mail-in voting are more vulnerable to many of these hacking attempts.

Though there have been instances of unauthorized access to election systems, there is currently no evidence to suggest that the integrity of elections data has been compromised.[6] That being said, election systems are still vulnerable to a variety of attacks, and proper precautionary steps to mitigate these attacks and the impact they might have on the election process should be taken.

[2] Microsoft. “New Cyberattacks Targeting U.S. Elections.” 10 Sept. 2020, blogs.microsoft.com/on-the-issues/2020/09/10/cyberattacks-us-elections-trump-biden/.

[3] Kirby, Jen. “Are China and Iran Meddling in US Elections? It’s Complicated.” Vox, 15 Sept. 2020, www.vox.com/21418513/china-iran-us-election-meddling-russia.

[4] Carnell Council. “Can the Voting Process Be Hacked?” Security Magazine, 17 Sept. 2020, www.securitymagazine.com/articles/93385-can-the-voting-process-be-hacked.

[5] Pettigrew, Stephen. “The Downstream Consequences of Long Waits: How Lines at the Precinct Depress Future Turnout.” Electoral Studies, 30 June 2020, https://www.stephenpettigrew.com/articles/pettigrew-lines-and-turnout-es.pdf.

[6] Cybersecurity and Infrastructure Security Agency. “APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations.” 9 Oct. 2020, us-cert.cisa.gov/ncas/alerts/aa20-283a.

Hacking Voter Registration

Fear

The most serious effect of a hack to voter registration databases would be changed or deleted voter registration records, causing confusion and voter suppression on Election Day. Without knowing their registration had been altered, voters would show up to their polling locations and be informed that they were either ineligible to vote entirely because no record of their registration exists, or that they are at the wrong polling place. Even if the voter is simply at the wrong polling location, that requires they travel to the new location, wait in line again, and then finally vote. Many individuals, especially those who are required to be at work during most voting hours, do not have the time to do this, and consequently will not cast a ballot on Election Day. This fear is magnified for voters relying on mail-in ballots, because if their voter registration data is incorrect or deleted, they will not have the opportunity to correct this information or prove their identity as easily as those who are voting in person.[7]

Reality

In reality, the most likely results of hacks on voter registration databases are delays to the voting process, and theft of personal information.[8] There is no evidence to suggest that any malicious cyber activity would result in changed or deleted voter registration records, but it could result in temporarily preventing access to these databases, in turn causing delays at the polls.[9] Additionally, hackers could use personal information that was stolen from these databases to attempt to steal money from individuals, or to target individuals for the purposes of disinformation campaigns.

IN REALITY, THE MOST LIKELY RESULTS OF HACKS ON VOTER REGISTRATION DATABASES ARE DELAYS TO THE VOTING PROCESS, AND THEFT OF PERSONAL INFORMATION.

In 2016, databases in Illinois were accessed by hackers using malicious SQL queries, but this did not result in the alteration or deletion of records in the database, nor did it have any substantial effect on the election.[10] About 90,000 voter registration records were accessed,[11] which included names, addresses, birthdays, sex, and in some cases drivers' license numbers and the last four digits of individuals' Social Security number. Although this information was accessed by the

[7] Cybersecurity and Infrastructure Security Agency. "Mail-in Voting in 2020 Infrastructure Risk Assessment." 28 July 2020, www.cisa.gov/sites/default/files/publications/cisa-mail-in-voting-infrastructure-risk-assessment_508.pdf.

[8] Internet Crime Complaint Center. "Cyber Threats to Voting Processes Could Slow But Not Prevent Voting." FBI and CISA, 24 Sept. 2020, www.ic3.gov/Media/Y2020/PSA200924.

[9] Internet Crime Complaint Center. "Cyber Threats."

[10] Bruer, Wesley, and Evan Perez. "Officials: Hackers Breach Election Systems in Illinois, Arizona." CNN, 30 Aug. 2016, www.cnn.com/2016/08/29/politics/hackers-breach-illinois-arizona-election-systems/index.html.

[11] U.S. Senate Select Committee on Intelligence. "Illinois Voter Registration System Database Breach Report." 2016, www.intelligence.senate.gov/sites/default/files/documents/os-ssandvoss-062117_0.pdf

hackers, the Federal Bureau of Investigation (FBI) concluded that none of the information had been changed or deleted.[12] However, it could easily be used to target individuals for disinformation campaigns, or to try to steal money from them. Even if no records were actually changed, the fact that voter registration databases were successfully accessed casts doubt in the public mind as to how secure databases really are. In the future, these systems could be vulnerable to an attack that renders their services unavailable for a period of time, potentially resulting in voter suppression due to delays and long lines.[13]

Solutions

To protect voter registration databases from an attack, security control best practices can be implemented to minimize intrusions. First, there must be secure communications between organizations, authenticating communications with external systems to ensure that there are no entry points for attacks.[14, 15] Making use of up-to-date Virtual Private Networks (VPNs) that utilize multi-factor authentication can improve security.[16, 17] This software should be patched regularly.[18] Additionally, the number of people who have access to a database should be minimized—enforced through role-based access, multi-factor authentication, device access control, and blocked public access to vulnerable ports.[19] A contingency plan should be in place and tested prior to the election.[20] And finally, back-up methods including provisional ballots and back-up poll books should be in place and tested to ensure that the election can still be conducted in the event of a hack.[21]

[12] Bruer and Perez. "Officials."

[13] Internet Crime Complaint Center. "Cyber Threats."

[14] Visner, Samuel. "Securing Elections Starts with Securing Voter Registration." StateScoop, 30 Jan. 2020, statescoop.com/securing-elections-starts-with-securing-voter-registration/.

[15] "Recommended Security Controls for Voter Registration Systems." MITRE, Nov. 2019, https://www.mitre.org/sites/default/files/publications/pr-19-3594-recommended-security-controls-for-voter-registration-systems.pdf.

[16] CISA. "APT Actors."

[17] Visner. "Securing Elections."

[18] CISA. "APT Actors."

[19] CISA. "APT Actors"; Visner. "Securing Elections."

[20] Visner. "Securing Elections."

[21] Internet Crime Complaint Center. "Cyber Threats"; Visner. "Securing Elections."

Hacking E-Poll Books

Fear

Electronic poll books (e-poll books) are a tool that poll workers can use to check in voters and reference their voter registration to verify that they are eligible to vote.[22] If e-poll books are hacked, it could have a similar effect as a hack to voter registration databases, creating confusion and long lines, as well as forcing some voters to vote at different locations, or preventing them from voting at all. Consequently, voters may lose confidence in the integrity of the election results, leaving some to speculate if the outcome may have been different were it not for these delays and changes.[23]

Reality

In 2016, e-poll books in Durham County, North Carolina, were hacked, resulting in a variety of issues both in the days leading up to the election and on Election Day. In the days preceding the election, the software that downloads data about the voters onto flash drives for the poll workers to use was taking up to ten times longer than normal. On Election Day, the e-poll books experienced additional problems, including incorrect records that indicated voters had already cast a ballot when they had not yet, or that they needed to show ID despite voter ID being unnecessary in North Carolina, as well as instances of the software crashing or freezing.[24] Although none of these instances resulted in the alteration of votes, these problems nonetheless caused serious delays and confusion, in some cases preventing voters from casting ballots. Especially in swing districts like Durham County, the disruptions and the delays that the e-poll book interferences caused are often viewed as attempts to manipulate the results of the election through voter suppression.

When investigated by the Department of Homeland Security (DHS), it was found that none of the computers or flash drives used contained malware. However, these investigations took place at least one week after the election, rather than

IF E-POLL BOOKS ARE HACKED, IT COULD HAVE A SIMILAR EFFECT AS A HACK TO VOTER REGISTRATION DATABASES, CREATING CONFUSION AND LONG LINES, AS WELL AS FORCING SOME VOTERS TO VOTE AT DIFFERENT LOCATIONS, OR PREVENTING THEM FROM VOTING AT ALL.

[22] Zetter, Kim. "Software Vendor May Have Opened a Gap for Hackers in 2016 Swing State." POLITICO, 6 June 2019, www.politico.com/story/2019/06/05/vr-systems-russian-hackers-2016-1505582.

[23] Zetter. "Software Vendor."

[24] Zetter, Kim. "How Close Did Russia Really Come to Hacking the 2016 Election?" POLITICO, 6 Jan. 2020, www.politico.com/news/magazine/2019/12/26/did-russia-really-hack-2016-election-088171.

[25] Zetter, Kim. "Election Probe Finds Security Flaws in Key North Carolina County but No Signs of Russian Hacking." POLITICO, 2 Jan. 2020, www.politico.com/news/2020/01/02/north-carolina-voting-security-092209.

[26] Zetter. "How Close."

on the same day that the incident occurred, and only on a subset of the machines used.[25] Malware used on the machines could have been deleted in the time between the election and the investigation, or could have been installed on machines not in the subset that was analyzed. As Susan Greenhalgh, vice president of policy and programs for National Election Defense Coalition, remarked, "Absence of evidence shouldn't be mistaken for evidence of absence."[26] It is still possible that these devices contained malware on Election Day, and precautions need to be taken in the future to avoid a repeat of this scenario. According to the FBI and Cybersecurity and Infrastructure Protection Agency (CISA), malicious cyber activity could result in delays at the polls in the upcoming presidential election, but there is no evidence that such activity would result in any changed or deleted voter registration records.[27] However, a slowed voting process and the long lines that accompany it could still prevent voters from casting their ballot.

Solutions

Ultimately, Durham averted crisis by using paper back-up versions of the e-poll books to check in voters. Ensuring that paper back-ups are readily available so that poll workers are able to quickly adapt to any situations where e-poll books may have been hacked is essential to avoiding as much fallout as possible on Election Day.[28] Conducting investigations on the same day or within 24 hours of the suspected attack, and on each of the machines involved rather than a subset, could result in more complete information about the nature of the hack. This information could be used in the future to deter additional hacks from occurring. Finally, and perhaps most important, Durham could have prevented this entirely by not remotely accessing critical election infrastructure.[29] Formal best practices for accessing and using critical election infrastructure can be found at https://www.cisa.gov/election-security-library.

[27] Internet Crime Complaint Center. "Cyber Threats."

[28] Internet Crime Complaint Center. "Cyber Threats."

[29] Zetter. "Software Vendor."

Ransomware

Fear

Ransomware could halt the election process by preventing poll workers and officials from accessing crucial infrastructure.[30] Malicious actors could deploy ransomware to prevent access to voter registration lists (often stored in e-poll books), tools supporting the tabulation and reporting of votes, and poll worker scheduling tools.[31] This could result in understaffed polls, long lines and delays at polling locations, and confusion before, during, and after Election Day.

This is more of a concern for states that rely heavily on in-person voting, rather than states that primarily use vote-by-mail.[32] Many local jurisdictions rely on outsourced information technology (IT) maintenance and remote monitoring and management (RMM), because they do not have adequate resources for in-house maintenance.[33] Because many RMMs are web-based, they are easily accessed by anyone with the log-in credentials, which is how malicious actors access them and deploy ransomware.

A ransomware attack on voter registration lists would create a similar scenario as an attack on e-poll books or voter registration databases. However, in this scenario, without any back-up copy of the voter registration lists, voters may not be able to vote at all. Infrastructure supporting electronic tabulation and reporting of votes could be targeted to prevent state officials from being able to accurately and timely report votes to federal officials. Without electronic tabulation, poll workers would be forced to count by hand, which is not only extremely tedious and time consuming, but can also be much less accurate than electronic tabulation.[34] If state election officials are unable to report their results on time, then total tallies will be inaccurate and the validity of the election results will be unclear. If infrastructure supporting the organization and scheduling of poll workers and volunteers is not available, polling locations may be understaffed on Election Day, resulting in long lines and delays for voters. Any of these scenarios could result in the manipulation of the election results, as well as perpetuate disinformation that the election results are inaccurate.

RANSOMWARE COULD HALT THE ELECTION PROCESS BY PREVENTING POLL WORKERS AND OFFICIALS FROM ACCESSING CRUCIAL INFRASTRUCTURE.

[30] Fraiser, John, et al. "Ingalls Threat Intelligence Report." Ingalls Information Security, Jan. 2020, www.nass.org/sites/default/files/2020-01/white-paper-ingalls-nass-winter20.pdf.

[31] Mehrotra, Kartikay. "Is the 2020 U.S. Election Secure From Hackers Interference?" Bloomberg.com, 11 Feb. 2020, www.bloomberg.com/news/articles/2020-02-11/hacks-on-louisiana-parishes-hint-at-nightmare-election-scenario?sref=ixa22l65.

[32] Cassidy, Christina, et al. "Ransomware Feared as Possible Saboteur for November Election." Associated Press, 2 Aug. 2020, apnews.com/article/ap-top-news-technology-politics-elections-election-2020-b39a09fc9a1334e9ef78bd46a40db253.

[33] Fraiser et al. "Ingalls Threat."

[34] Cassidy et al. "Ransomware Feared."

[35] Mehrotra. "Is the 2020."

Reality

In November 2019, local jurisdictions in Louisiana fell victim to a ransomware attack on their election system one week before their state and local Election Day. It appears that the hackers had accessed the election system four months prior, but waited until one week before the election to deploy the malware.[35] Although election systems were not specifically targeted, it is believed that the hackers deployed their attack right before the election in order to opportunistically maximize the likelihood of receiving the ransom payments. The hackers were able to access the election systems through the remote IT management company that the parishes used, called Need Computer Help. After accessing the Need Computer Help network, hackers were able to use connections to the local parish networks to infiltrate those networks as well.[36] Ultimately, the ransom was negotiated down from the initial $3.5 million, and the computers with data that could not be recovered were unlocked.[37] Although the data was recovered, and the election ultimately unaffected, this instance exemplifies how a ransomware attack could be effectively executed to disrupt the election process, and reinforces that more needs to be done to protect against such an attack. If the data had not been recovered, local jurisdictions in Louisiana likely would have faced a largely slowed voting process, causing long lines, a reduced voter turnout, and skepticism over the accuracy of the results of the election.

Solutions

To prevent against successful ransomware attacks, various cybersecurity tools and techniques can be put in place, including advanced endpoint protection, network and endpoint threat detection, incident response planning, and log aggregation, analysis, and review.[38] Network systems, software, and VPNs should be kept up to date, and network traffic monitored to increase security of systems.[39] Additionally, preventions such as multi-factor authentication, comprehensive account resets, and spear-phishing training can be put in place to reduce the likelihood of the theft of log-in credentials. In the Louisiana scenario, the systems were ultimately breached only because of stolen log-in credentials.[40] Finally, ensuring that there is a paper trail of ballots can provide for audits of votes cast in the event that a hack casts doubt over the results of the election.[41] These back-up methods should be readily available, so that in the event of an attack there is a minimal delay in operationalizing the failover systems.

[35] Mehrotra. "Is the 2020."

[36] Mehrotra. "Is the 2020."

[37] Mehrotra. "Is the 2020."

[38] Fraiser et al. "Ingalls Threat."

[39] CISA. "APT Actors."

[40] CISA. "APT Actors"; Mehrotra. "Is the 2020."

[41] Mehrotra, Kartikay. "Louisiana Target of Attempted Ransomware Hack, Governor Says." Bloomberg, 18 Nov. 2019, www.bloomberg.com/news/articles/2019-11-18/louisiana-targeted-by-attempted-ransomware-attack-governor-says?sref=ixa22l65.

Hacking Voting Machines

Fear

A hack on voting machines could "flip" votes from one party to another—or not record them at all. This type of hack would have the largest direct impact on the election results by physically tampering with how votes are recorded. An attack of this nature could be exacerbated by jurisdictions with no paper back-ups of votes, which exist in at least four of the thirteen states that do not require paper back-ups.[42] In the event of a nation-wide hack of voting machines on Election Day, if the votes from four states cannot be verified with a paper trail, the outcome of the election will be unclear, even after tabulation of paper back-ups to audit the results.

There are two types of voting machines: optical voting machines, which use paper ballots, and direct recording electronic machines (DRE).[43] Of the two, DREs are more vulnerable to an attack, because they are accessible by the internet. Both types of voting machines could be susceptible to physical tampering of the machines that result in a distorted vote count, although this type of attack is likely to be noticed by poll workers and voters. DREs are vulnerable to various electronic hacks, including remote access of malicious code, taking over the voting machines through a targeted attack by connecting to the same Wi-Fi network, or creating fake election cards to be used multiple times.[44]

Reality

Many voting machines that are currently used are very old and do not have adequate or up-to-date cybersecurity measures in place. Most of them have no firewalls or other controls in place to protect against unauthorized remote access.[45] While these machines are clearly vulnerable to attacks, the complexity of the systems and the required sophistication to launch a successful attack without raising alarms is unlikely. The FBI and DHS CISA remain confident in the security of the upcoming election, and FBI Director Christopher Wray has commented that "We haven't seen cyberattacks to date this year on voter registration databases or on any systems involved in primary voting," and CISA Director Christopher Krebs has repeatedly commented, "This will be the most secure election in modern history."[46] There is no evidence to date to suggest that malicious cyber activity could result in any changes to vote tallies in the upcoming presidential election.[47] States have been working to

A HACK ON VOTING MACHINES COULD "FLIP" VOTES FROM ONE PARTY TO ANOTHER— OR NOT RECORD THEM AT ALL.

[42] National Conference of State Legislatures. "Voting System Paper Trail Requirements." 27 June 2019, www.ncsl.org/research/elections-and-campaigns/voting-system-paper-trail-requirements.aspx.

[43] Carnell Council, "Can the Voting Process."

[44] Carnell Council, "Can the Voting Process."

[45] Carnell Council, "Can the Voting Process."

[46] Seldin, Jeff. "No Signs of Cyberattacks Targeting US Election Systems." Voice of America, 16 Sept. 2020, www.voanews.com/2020-usa-votes/no-signs-cyberattacks-targeting-us-election-systems.

[47] Internet Crime Complaint Center. "Cyber Threats."

[48] Seldin. "No Signs."

improve the security of their elections, through both increased measures to detect malicious activity and ensuring that adequate paper back-ups exist for each vote.[48]

Solutions

Paper back-ups and provisional ballots can be used to audit each vote cast in the event of a hack on voting machines, verifying that how the ballot was recorded matches the voter's intent.[49] Machines such as DREs, that do not have any paper trails, do not allow for the auditing of votes, and accurate vote tabulation may not be possible in the event of a hack.[50] Although the auditing of paper ballots would be very tedious and time-consuming, it would allow for accurate tabulation of votes, as well as an audit of where errors or breaches occurred.[51] However, this likely would not mitigate the resulting lack of confidence in the election integrity, and measures can be put in place to prevent a hack from occurring in the first place.

Best practices for controls and defensive measures from Center for Internet Security and National Institute of Standards and Technology can be employed, and the advice of a cybersecurity and advisory consulting firm can help manage cybersecurity vulnerabilities.[52] Additionally, any old or obsolete operating systems on the same network as election systems create vulnerabilities and should be updated.[53] Voting machines should be single-purpose and minimize privileges to reduce the number of entry points for a hack.[54] Finally, cyber-maturity assessments should be conducted regularly to ensure that systems are up to date and controls are functioning as expected.[55]

[49] Internet Crime Complaint Center. "Cyber Threats."

[50] Gambhir, Raj Karan, and Jack Karsten. "Why Paper Is Considered State-of-the-Art Voting Technology." Brookings, 14 Aug. 2019, www.brookings.edu/blog/techtank/2019/08/14/why-paper-is-considered-state-of-the-art-voting-technology/.

[51] Gambhir and Karsten. "Why Paper."

[52] Carnell Council. "Can the Voting Process."

[53] Carnell Council. "Can the Voting Process."

[54] Singer, Ari. "5 Measures to Harden Election Technology." Dark Reading, 6 Feb. 2020, www.darkreading.com/risk/5-measures-to-harden-election-technology-/a/d-id/1336978.

[55] Carnell Council. "Can the Voting Process."

Hacking Election Night Reporting

Fear

If a hack were to occur on the election night reporting infrastructure, results of the presidential race could be delayed, and when results finally were published, the public would likely be very skeptical of the results, even if they were accurate. This type of hack could target the tabulation infrastructure, the infrastructure used to report results, or the final vote tally data, all of which would prevent timely tabulation and reporting of votes. Additionally, in the delay period prior to announcement of verified election results, foreign actors could disseminate disinformation to further undermine the integrity of the election. According to the FBI and CISA, these disinformation attempts could include "reports of voter suppression, cyberattacks targeting election infrastructure, voter or ballot fraud, and other problems."[56] In any of these scenarios, it is likely that no clear winner would be determined on election night. Even if the votes are eventually accurately counted and reported, the delayed reporting would degrade the integrity of the election results, casting doubt in the public mind over the accuracy of the tabulation process and final results.

Reality

In Tennessee, a website used to report election results crashed due to a denial-of-service attack in May 2018. It is suspected that malicious actors were attempting to access the backend vote database connected to the website.[57] No primary data was compromised, no vote tallies were altered, and the website was restored within about one hour.[58] If the website used to report these results was connected to a live database of the vote tallies, the hackers likely could have accessed and altered them.[59]

IN ANY OF THESE SCENARIOS, IT IS LIKELY THAT NO CLEAR WINNER WOULD BE DETERMINED ON ELECTION NIGHT.

However, if the underlying data systems are not directly linked to the websites, even if hackers are able to successfully manipulate election reporting websites, the internal data and systems will remain uncompromised.[60] Disinformation about the results, rather than an actual hack on the results, is a more likely scenario. Claims that election night reporting systems were hacked will have the same effect of casting doubt on the integrity of the election outcome as if these systems actually were hacked. Even if the vote tally systems in Tennessee were not accessed or altered, such incidents cause voters to doubt how sure the election officials are that databases were not accessed or tampered with, as well as question how confident they should be in the reporting system.

[56] Internet Crime Complaint Center. "Foreign Actors and Cybercriminals Likely to Spread Disinformation Regarding 2020 Election Results." FBI and CISA, 22 Sept. 2020, www.ic3.gov/media/2020/200922.aspx.

[57] Levine, Sam. "Hackers Tried to Breach a Tennessee County Server on Election Night: Report." HuffPost, 11 May 2018, www.huffpost.com/entry/knox-county-election-cyberattack_n_5af5ca21e4b032b10bfa56ee?guccounter=1.

[58] Syeed, Nafeesa. "Hackers May Be Behind Election Night Website Crash in Tennessee." Bloomberg.com, 2 May 2018, www.bloomberg.com/news/articles/2018-05-02/hackers-may-be-behind-election-night-website-crash-in-tennessee?sref=ixa22l65.

[59] Levine. "Hackers Tried."

[60] Internet Crime Complaint Center. "Foreign Actors and Cybercriminals."

Solutions

As with a hack to voting machines, the most important solution to mitigate the effects of a hack to election night reporting is to ensure that there exists a paper trail of all of the votes cast. In a worst-case scenario, the paper trail could be relied on to determine accurate results. Additionally, when reporting results on the internet, it is important that the website reporting the results is not directly linked to the live databases that are recording votes. As seen in the Tennessee incident, if reporting websites are directly linked to live databases with the vote tallies, hackers have direct access to these databases and can alter them as they please.[61] Lastly, the FBI and DHS CISA released a public service announcement detailing how to handle the anticipated disinformation regarding the 2020 election results, which includes guidance on how to find trustworthy information, as well as how to recognize and report suspicious social media posts.[62]

[61] Levine. "Hackers Tried."

[62] Internet Crime Complaint Center. "Foreign Actors and Cybercriminals."

References

Bruer, Wesley, and Evan Perez. "Officials: Hackers Breach Election Systems in Illinois, Arizona." CNN, 30 Aug. 2016, www.cnn.com/2016/08/29/politics/hackers-breach-illinois-arizona-election-systems/index.html.

Carnell Council. "Can the Voting Process Be Hacked?" Security Magazine RSS, Security Magazine, 17 Sept. 2020, www.securitymagazine.com/articles/93385-can-the-voting-process-be-hacked.

Cassidy, Christina, et al. "Ransomware Feared as Possible Saboteur for November Election." Associated Press, 2 Aug. 2020, apnews.com/article/ap-top-news-technology-politics-elections-election-2020-b39a09fc9a1334e9ef78bd46a40db253.

Cybersecurity and Infrastructure Security Agency. "APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations." 9 Oct. 2020, us-cert.cisa.gov/ncas/alerts/aa20-283a.

Cybersecurity and Infrastructure Security Agency. "Mail-in Voting in 2020 Infrastructure Risk Assessment." 28 July 2020, www.cisa.gov/sites/default/files/publications/cisa-mail-in-voting-infrastructure-risk-assessment_508.pdf.

Fraiser, John, et al. "Ingalls Threat Intelligence Report." Ingalls Information Security, Jan. 2020, www.nass.org/sites/default/files/2020-01/white-paper-ingalls-nass-winter20.pdf.

Gambhir, Raj Karan, and Jack Karsten. "Why Paper Is Considered State-of-the-Art Voting Technology." Brookings, 14 Aug. 2019, www.brookings.edu/blog/techtank/2019/08/14/why-paper-is-considered-state-of-the-art-voting-technology/.

Internet Crime Complaint Center. "Cyber Threats to Voting Processes Could Slow But Not Prevent Voting." FBI and CISA, 24 Sept. 2020, www.ic3.gov/Media/Y2020/PSA200924.

Internet Crime Complaint Center. "Foreign Actors and Cybercriminals Likely to Spread Disinformation Regarding 2020 Election Results." FBI and CISA, 22 Sept. 2020, www.ic3.gov/media/2020/200922.aspx.

Kirby, Jen. "Are China and Iran Meddling in US Elections? It's Complicated." Vox, 15 Sept. 2020, www.vox.com/21418513/china-iran-us-election-meddling-russia.

Levine, Sam. "Hackers Tried to Breach a Tennessee County Server on Election Night: Report." HuffPost, 11 May 2018, www.huffpost.com/entry/knox-county-election-cyberattack_n_5af5ca21e4b032b10bfa56ee?guccounter=1.

Mehrotra, Kartikay. "Is the 2020 U.S. Election Secure From Hackers Interference?" Bloomberg.com, 11 Feb. 2020, www.bloomberg.com/news/articles/2020-02-11/hacks-on-louisiana-parishes-hint-at-nightmare-election-scenario?sref=ixa22l65.

Mehrotra, Kartikay. "Louisiana Target of Attempted Ransomware Hack, Governor Says." Bloomberg, 18 Nov. 2019, www.bloomberg.com/news/articles/2019-11-18/louisiana-targeted-by-attempted-ransomware-attack-governor-says?sref=ixa22l65.

Microsoft. "New Cyberattacks Targeting U.S. Elections." 10 Sept. 2020, blogs.microsoft.com/on-the-issues/2020/09/10/cyberattacks-us-elections-trump-biden/.

MITRE. "Recommended Security Controls for Voter Registration Systems." Nov. 2019, www.mitre.org/sites/default/files/publications/pr-19-3594-recommended-security-controls-for-voter-registration-systems.pdf.

Mueller, Robert S. "Report on the Investigation into Russian Interference in the 2016 Presidential Election." U.S. Department of Justice, 2019.

National Conference of State Legislatures. "Voting System Paper Trail Requirements." 27 June 2019, www.ncsl.org/research/elections-and-campaigns/voting-system-paper-trail-requirements.aspx.

Pettigrew, Stephen. "The Downstream Consequences of Long Waits: How Lines at the Precinct Depress Future Turnout." Electoral Studies, 30 June 2020, https://www.stephenpettigrew.com/articles/pettigrew-lines-and-turnout-es.pdf.

Seldin, Jeff. "No Signs of Cyberattacks Targeting US Election Systems." Voice of America, 16 Sept. 2020, www.voanews.com/2020-usa-votes/no-signs-cyberattacks-targeting-us-election-systems.

Singer, Ari. "5 Measures to Harden Election Technology." Dark Reading, 6 Feb. 2020, www.darkreading.com/risk/5-measures-to-harden-election-technology-/a/d-id/1336978.

Syeed, Nafeesa. "Hackers May Be Behind Election Night Website Crash in Tennessee." Bloomberg.com, 2 May 2018, www.bloomberg.com/news/articles/2018-05-02/hackers-may-be-behind-election-night-website-crash-in-tennessee?sref=ixa22l65.

U.S. Senate Select Committee on Intelligence. "Illinois Voter Registration System Database Breach Report." 2016, www.intelligence.senate.gov/sites/default/files/documents/os-ssandvoss-062117_0.pdf.

Visner, Samuel. "Securing Elections Starts with Securing Voter Registration." StateScoop, 30 Jan. 2020, statescoop.com/securing-elections-starts-with-securing-voter-registration/.

Zetter, Kim. "Election Probe Finds Security Flaws in Key North Carolina County but No Signs of Russian Hacking." POLITICO, 2 Jan. 2020, www.politico.com/news/2020/01/02/north-carolina-voting-security-092209.

Zetter, Kim. "How Close Did Russia Really Come to Hacking the 2016 Election?" POLITICO, 6 Jan. 2020, www.politico.com/news/magazine/2019/12/26/did-russia-really-hack-2016-election-088171.

Zetter, Kim. "Software Vendor May Have Opened a Gap for Hackers in 2016 Swing State." POLITICO, 6 June 2019, www.politico.com/story/2019/06/05/vr-systems-russian-hackers-2016-1505582.

MITRE's Mission

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

OCTOBER 2020