[redacted]

NATIONAL INTELLIGENCE COUNCIL

MEMORANDUM

15 January 2020 NICM 2020-003

[redacted] Vulnerabilities in US 2020 Election Infrastructure

(U) Key Takeaway

[redacted] ***Scope Note:*** *This memo assesses the potential impact of cyber operations against US election infrastructure for the 2020 presidential election, including the voting process and integrity of results. It does not assess adversary intentions or views of US vulnerabilities.*

[redacted] We assess that at least Russia, China, Iran, and North Korea have the capability to access and potentially manipulate data in US election-related computer systems, but we do not know whether they have specific plans to interfere with the functioning of these systems.

- [redacted] We assess that centralized election-related data repositories, such as voter registration databases, pollbooks, and official election websites, are most vulnerable to exploitation, and adversaries could use access to these systems to disrupt election processes.
- [redacted] Systems that tabulate, transmit, or display election results are vulnerable to localized exploitation but would be difficult to manipulate on a wide enough scale to alter the election outcome.
- [redacted] Adversary claims of manipulation would be difficult to disprove and could undermine public confidence in election results.

[redacted] **We judge that US adversaries, including at a minimum Russia, China, Iran, and North Korea, as well as nonstate groups, have the capability to compromise US election infrastructure for the 2020 presidential election.** Adversaries gaining access to US election-related systems could disrupt the voting process, steal sensitive data, or undermine confidence in the election results, but we do not know whether any of them have specific plans to manipulate election-related systems.

- [redacted] Russia almost certainly reconnoitered all US state election networks during the 2016 election cycle, accessed election-related infrastructure in at least two states, and exfiltrated voter data from at least one state. Russia, China, Iran, and North Korea are all capable of conducting similar operations during the 2020 election cycle, judging from their known cyber capabilities and past operations.
- [redacted] The availability of sophisticated computer network intrusion or attack tools on the dark web gives additional countries and nonstate actors the potential capability to interfere in the election. We judge that cyber criminals and hacktivists could also target election infrastructure for financial or political reasons, based on past incidents possibly or definitely attributed to such groups.

(U) *This memorandum was prepared under the auspices of the National Intelligence Officer (NIO) for Cyber.* [redacted]

[redacted]

Classified By: [redacted] | Derived From: [redacted] | Declassify On: [redacted]

[redacted]

(U) Definitions of Cyber Terms

(U/[redacted]) **Attack.** A cyber actor attempts to degrade, destroy, disrupt, manipulate, or otherwise hinder the operation of a system or network. Manipulation or deletion of data solely to hide an intrusion is not considered an attack.

(U/[redacted]) **Compromise.** A cyber actor gains unauthorized access to collect data or execute demands or installs malware linked to a malicious Internet protocol address.

(U/[redacted]) **Exploit.** A malicious actor collects data, deploys additional malware, or establishes persistent access on a compromised system. Cyber actors may compromise more accounts and systems than they exploit, in part because of the availability of tools that automate the process of compromising vulnerable systems.

(U/[redacted]) **Scan.** A cyber actor sends a system specific network traffic and observes its responses to identify security vulnerabilities. Internet scanning is very common but may have only a modest success rate, meaning cyber actors scan far more systems than they actually affect.

[redacted] Centralized Data Repositories Most Vulnerable

[redacted] **We assess that adversaries could most easily exploit centralized election-related data repositories because of their ease of access and comparative lack of security.** These systems, which are used to collect, update, and store voter information, are designed for regular access, commonly through web portals, which makes them vulnerable to a range of malicious cyber activities. A committed adversary could exploit access to these systems to disrupt election processes across the country.

- [redacted] **Voter Registration Databases.** States house their voter registration databases predominantly on Internet-connected systems that are designed for easy access because maintaining up-to-date voter registration records is a nearly continuous process. Adversaries could alter data to potentially prevent individual voters or groups of voters from voting, causing delays on election day or forcing voters to use provisional ballots. Adversaries could also use the registration data—which in some cases is also available publicly or for purchase—to tailor other interference or influence efforts.

- [redacted] **Pollbooks.** Registration databases transfer voter registration information to e-pollbook devices or paper pollbooks used to check in voters at the precinct level. Some pollbooks are tied to Internet-connected databases that adversaries probably would be able to easily exploit to manipulate data, with effects similar to those from manipulation of registration databases.

- [redacted] **State and Local Election Officials' Websites.** These sites provide public information about voting locations or, in some states, are used to report voting results. Attacks on or compromises of these sites could deter individuals from voting or cast doubt on election results.

[redacted] Vote-Administering Systems Vulnerable to Localized Exploitation

[redacted] **We assess that systems designed to tabulate votes, transmit vote amounts, or display election results probably are vulnerable to localized exploitation but would be difficult to manipulate at scale.** For example, hackers have repeatedly demonstrated that some voting machines are easy to compromise.

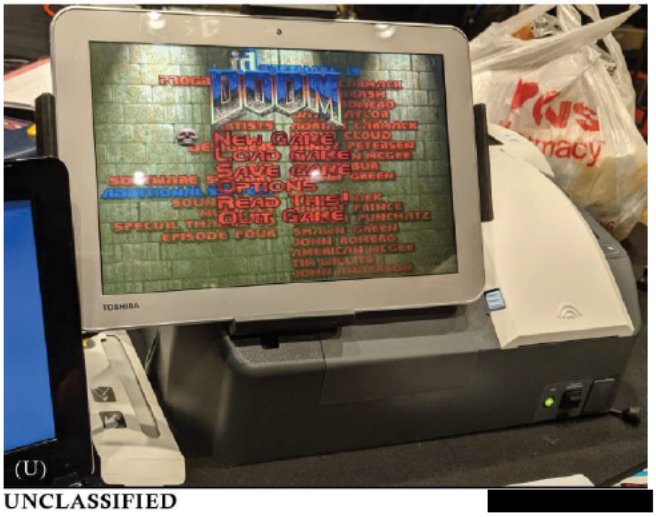
- [redacted] Direct recording electronic machines, which record and process votes digitally and store tabulation data in removable memory, are particularly vulnerable to cyber operations, especially machines with no paper backup. Such

machines, however, are used far less than other, more secure types of voting machines.

- [redacted] Adversaries who obtained physical access to voting machines could alter how they function, manipulate the data in them, or install malware, according to US state and academic investigations. At the 2019 DefCon cyber security conference, hackers demonstrated the ability to compromise more than 100 voting machines, all of which had been certified for use in at least one US voting jurisdiction.

(U) Pollbook Hacking Example

(U) A pollbook was modified at the 2019 Defcon Voting Machine Hacking Village to run the popular videogame Doom, according to press reporting.



(U)

UNCLASSIFIED [redacted]

- [redacted] Thirty-one states and the District of Columbia allow eligible voters to submit absentee ballots via Internet or fax, making these votes susceptible to disruption or manipulation. Four states allow voters to return absentee ballots via a web-based portal, seven allow some voters to return ballots via fax only, and one allows mobile voting secured with blockchain technology. Absentee votes, however, are small in number and typically closely monitored for anomalies.

[redacted] **We assess that vote tabulation systems would be difficult to manipulate on a wide enough scale to compromise election results.** The systems in each voting location are not connected to the Internet or to each other, and many methods for exploiting them rely on physical proximity. Although an adversary could manipulate voting results across multiple jurisdictions and enough states to influence a presidential election, we judge that conducting such a campaign would be difficult and that postelection audits and paper trails very likely would uncover such an effort.

- (U) A growing number of jurisdictions are using voter-verified paper backups and postelection

[redacted] Ballot and Voting Machine Preparation Vulnerabilities

(U//[redacted]) Ballot and voting machine preparation is vulnerable to cyber, supply chain, or insider threats. We judge, however, that security and mitigation measures used in these processes, and the distribution of voting machine storage facilities countrywide, would make it difficult for an adversary to coordinate a campaign to manipulate voting results across an entire state or multiple states.

- [redacted] **Ballot Preparation.** Creating paper or electronic ballots to upload to voting machines is usually outsourced to third-party vendors. Some use Internet-connected computer systems and lack password and encryption policies, which could allow malicious actors to corrupt ballot files. Logic and accuracy tests to ensure the machines function properly before election day, however, probably would detect such activity.

- [redacted] **Voting Machine Preparation.** Voting machines configured at a central location are vulnerable to insider threats. Malware introduced into the voting machines during this phase might affect multiple jurisdictions but also would be detectable during the preelection testing.

audits (now required in 38 states), which can alert election officials to manipulation or errors.

[redacted] **We assess that cyber operations targeting the electronic tabulation of results could delay results reporting from affected jurisdictions, potentially creating public uncertainty but probably not affecting the integrity of certified results.** Tabulated results are stored independently of copies displayed on results websites, although investigations of malicious activity could delay results and introduce public uncertainty about the validity of vote counts. Denial of service (DOS) attacks or manipulation of copies of the results in transit would delay public access to the results or make them difficult to access, creating the appearance of modified results.

- [redacted] The Blue Ribbon Commission on the vulnerabilities of Pennsylvania's election infrastructure found the transmission of preliminary results to public-facing websites is vulnerable to "man-in-the-middle" attacks, in which the attacker manipulates data mid-transmission. Such attacks would not alter separately stored certified copies of tabulation results, which are processed offline, but even short delays in reporting the results could introduce doubts about the security of the election or the validity of the results.

- [redacted]

- [redacted] In May 2019, unidentified cyber actors rendered a US county election website unavailable on the night of a mayoral primary; the incident did not affect the tabulation results, which were stored on a separate system not connected to the Internet.

[redacted] False Manipulation Narratives Could Undermine Public Confidence

[redacted] We assess that adversaries could also make false claims about their ability to manipulate US election infrastructure as part of a broader effort to undermine confidence in US democratic processes. Much of the voting public probably knows little about the process of administering US elections, which could allow false narratives to gain traction. Government efforts to investigate and publicly invalidate such claims could take weeks or months, providing time for concerns about election security to spread. Disproving claims would also be impossible if adversaries evaded US intelligence collection.

- [redacted] Adversaries could make wholly fabricated claims, such as announcing that they have compromised all US voting machines, a claim that would be difficult and time-consuming—or impossible—for the US Government to disprove.

- [redacted] Adversaries could also link an exaggerated claim—for example, about their ability to affect the election outcome—to actual operations, such as DOS attacks against election-related websites or intrusions into voter registration databases. Linking the two could introduce public doubts about the validity of the election, even if the actual cyber operations were unrelated to the casting, tabulating, and reporting of votes.

- [redacted] A widely publicized compromise of election infrastructure probably would undercut public confidence in the election, even if the compromise was not used to manipulate election-related data or systems.

[redacted] Mitigating Threats to Infrastructure

[redacted] We assess that enhancing the physical security and cyber protections of election systems and messaging the US public and adversaries could mitigate some of the vulnerabilities of the complex US election process. Potential measures include the following:

- [redacted] **Physical Security and Cyber Hygiene.** These terms refer to adopting best practices for the physical and cyber protection of election facilities and equipment. Basic security measures—replacing obsolete equipment, strengthening password policy and audit processes, and implementing network segmentation—might prevent less sophisticated adversaries from disrupting election processes but probably would be insufficient to deter the most advanced and determined nation-state actors.

- [redacted] **Third-Party Vendor Verification.** Establishing and refining screening procedures for vendors who manufacture or transship election infrastructure could reveal shared vulnerabilities or insider threats.

- [redacted] **Public Messaging and Education.** Public messaging would be vital to providing accurate and timely information about the effects and limited scope of low-impact cyber operations. Partnerships with state and local election officials, cyber security firms, and the media could help minimize commercial disruptions, as well as counter cyber-enabled information operations. Timely public messaging before the election would help to educate the public about adversary goals and make US officials the trusted source for information about the integrity of the election process, recovery efforts, and investigations into attempted cyber attacks.

- [redacted] **Messaging to Adversaries.** Privately messaging adversaries to emphasize that attempts to manipulate US election infrastructure are unacceptable and would have serious consequences could deter them from taking such steps.