In 2018, cyber attacks by Russian hackers have allegedly targeted multiple Congressional campaigns, including Senator Claire McCaskill.

**Vulnerability**

- **Serious risk to credibility of candidates**
- **Severe risk to voting process and election results**
- **Inconsistent**
- **Improving**

**Security**

- Cyber attacks on campaigns have been used for selective “doxing,” in which adversaries release potentially compromising data on candidates and campaigns. These attacks have undermined the credibility of candidates, exacerbated social, economic and political divisions among the U.S. electorate, and fueled fears of corruption and abuse by government officials.

- Ongoing attacks in 2018
- Threat
- Vulnerability
- Inconsistent
- Improving

- Cybersecurity practices for political campaigns remain inconsistent, although efforts by DHS and the FBI to provide cybersecurity training and support to campaigns have had some effect. Extremely tight budgets, mostly-volunteer staffs, poor cybersecurity awareness, and the use of distributed, ad-hoc systems by campaigns have made improving campaign security difficult in spite of significant publicity around attacks on campaigns and campaign officials, particularly for local and state elections.

**Risk**

- Severe

**Voter Registration and Election Management Systems**

- **Known attacks in 2016**
- **Severe risk to voting process and election results**
- **IMPROVING**
- **Vulnerability**
- **Risk**
- **Serious**

- Voter registration systems in at least 21 states were targeted by Russian hackers in the 2016 election, although there is no evidence that voter rolls were actually changed.

- Attacks on voter registration systems and e-pollbooks could be used to steal data on American voters, or affect Americans’ ability to exercise their right to vote if their voter registration is manipulated. Blocking certain voters from the polls could even alter the results of an election.

- Voter registration systems remain vulnerable to cyber attacks, but progress is being made on basic cybersecurity standards and training, and DHS is coordinating information sharing and incident response exercises with state election officials.

**Risk**

- Serious

**Voting Systems**

- **Demonstrated vulnerability**
- **Extreme risk to voting process and election results**
- **Improving**
- **Vulnerability**
- **Risk**
- **Serious**

- There is no evidence of foreign tampering with U.S. voting systems in 2018, but known vulnerabilities have been demonstrated in many of the most widely-used voting systems in the U.S.

- Cyber attacks on voting systems could be used to disrupt the voting process, or even to directly manipulate votes, perhaps the most widely-feared form of election manipulation.

- Vulnerabilities in voting machines and vote counting systems have received a lot of attention since 2016, but most voting systems are not connected to the internet, and getting physical access to a large number of machines would be challenging, particularly for a foreign adversary. Furthermore, most states have plans to replace aging voting systems and implement a paper audit trail for all votes.

**Risk**

- Serious

**Election Night Reporting**

- **Demonstrated vulnerability**
- **Serious risk to credibility of election results**
- **Weak**
- **Vulnerability**
- **Risk**
- **Serious**

- There is no evidence of foreign tampering with election night reporting systems, but exploitable vulnerabilities in official election websites, traditional and social media platforms could be exploited by foreign actors.

- While attacks on election night reporting systems cannot affect the actual outcome of the election, if reported vote tallies are manipulated it could call the real results into question, even if they are ultimately verified.

- Secure election night reporting has received comparatively little attention and resources relative to voter registration and voting systems, and known vulnerabilities in official election night reporting websites, traditional and social media platforms remain unaddressed.
A Path Forward to Secure and Resilient Elections

1. U.S. elections are vulnerable to cyber threats

99% of votes in the United States are cast or counted by computers.

Computerized voting has important advantages:
- Reduces miscounted or excluded votes due to voter error
- Helps voters with disabilities vote
- Improves access to voting for rural voters
- Speeds up delivery of results

But we have not invested in strong security

The average state election cybersecurity grade in a recent report.

The average grade for states with toss-up Senate races in 2018.

---

2. Foreign adversaries want to exploit these vulnerabilities

CSIS surveyed our network of cybersecurity experts to find out what nation-state threats they most worry about.

What Nation State Poses the Greatest Cyber Threat to U.S. Elections?

- A. Russia: 81%
- B. China: 10%
- C. Iran: 2%
- D. No Threats: 2%
- E. United States: 5%

Espionage and influence operations are a bigger threat than sabotage

What Tactics Will Nation State Adversaries Use to Manipulate the 2018 Elections?

- Influence Operations: 95%
- Attack VRDBs/Voting Systems: 67%
- Cyber Espionage Against Campaigns/Candidates: 55%
- Nothing: 43%

CSIS
CENTER FOR STRATEGIC & INTERNATIONAL STUDIES
TECHNOLOGY POLICY PROGRAM
3. Despite Dire Headlines, Progress is Being Made on Basic Standards Ahead of 2018

Number of States with Basic Best Practices for Election Cybersecurity

Voter Registration and Election Management Systems
- Access Control: 46 states
- Information Sharing: 50 states
- Regular Vulnerability Analysis: 43 states
- Intrusion Detection: 43 states

Voting Systems
- Voting Machines <10y Old: 9 states
- Paper Audit Trail for All Voters: 36 states
- WSG Compliance: 45 states
- Post-Election Audits: 33 states

44 states participated in a DHS exercise to practice cyber incident response plans and information sharing

These 40 states are implementing new cybersecurity measures

All 50 states are now members of MS-ISAC and 548 state and local election organizations are members of EI-ISAC

A Path Forward to Secure and Resilient Elections

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES | TECHNOLOGY POLICY PROGRAM
4. And Much is Being Done for 2020

By 2020, 46 states will have or be in the process of implementing VVPAT for all voters.

More than **$300 million** will be invested in election system upgrades and security improvements across all 50 states before the 2020 Presidential Election.

5. More is Needed

- **Universal VVPAT and Risk-Limiting Audits**
  - No protection is perfect, and preventing 100% of attacks is impossible, but a paper audit trail is a key first step in establishing resilience if election systems are compromised.

- **Budget for Meaningful Security**
  - Current funds are helping to implement basic security practices, but the full cost of robust security is far higher. Many states and counties have developed plans to upgrade or replace vulnerable systems, but lack funding to implement them.

- **Credibility is as Important as Accuracy**
  - Attacks on campaigns and ENR systems cannot directly disrupt or change the outcome of an election, but they can undermine the credibility of American democracy, and comparatively little money and effort is being put into securing these systems.

- **Leverage Partnership Opportunities**
  - Campaigns and election officials should leverage every available opportunity to partner with the FBI, DHS, EI-ISAC, MS-ISAC, and private pro bono initiatives from companies like Cloudflare, Jigsaw, Microsoft and others.