GlobalResearch
Center for Research on Globalization

As Americans Vote, Will Hackers Pounce?

By Laura Colarusso
Global Research, November 08, 2016
Havard Gazette 28 October 2016

Region: USA
In-depth Report: U.S. Elections

Panelists at Kennedy School discuss DNC attacks and wider vulnerabilities

In late April, the Democratic National Committee (DNC) suspected that something was wrong with their network and called in the cybersecurity firm CrowdStrike to investigate. A few weeks later, after routine testing, the suspicions were confirmed: The committee had been hacked by the Russians.

The DNC's system "lit up like a Christmas tree," said Dmitri Alperovitch, CrowdStrike's chief technology officer. The culprits were bad actors CrowdStrike had seen before and given nicknames. "Cozy Bear," Russia's Federal Security Service, had been attacking the DNC since the summer of 2015. "Fancy Bear," which refers to Russia's military intelligence unit, had started its infiltration shortly before CrowdStrike did its test.

As DNC documents were leaked throughout the summer and into the fall, the episode put the United States on notice that Vladimir Putin's government is intent on influencing the 2016 election, Alperovitch said during a panel discussion at Harvard Kennedy School (HKS). That could mean a couple of things, he said. Russia might try to hack voting machines or it could mount a disinformation campaign to discredit the eventual results.

"The fundamental objective here by the Russians is not necessarily to get one person or another elected as president," said Alperovitch. "The fundamental objective is actually much more nefarious, which is to undermine the very idea of a free and fair election — the cornerstone of our democracy."

The decentralized nature of the U.S. vote should protect against a widespread intrusion, said Pamela Smith, president of Verified Voting, a nonpartisan advocacy group. Each of the 9,000 election jurisdictions across the country has its own systems and procedures, meaning no single point of failure could disrupt the tally nationwide.

Additionally, many jurisdictions have mitigation systems that would help election officials reconstruct voters' intent if electronic voting machines break down or are compromised by an attack. At least 75 percent of voters casting ballots between now and Nov. 8 will do so on machines that have either a paper ballot or a paper backup.

Moderator and director of the Belfer Center's Cyber Security Project Michael Sulmeyer (from left), Pamela Smith, Dmitri Alperovitch, and Ben Buchanan at the John F. Kennedy Jr. Forum. "The fundamental objective [of the hack] … is to undermine the very idea of a free and fair election," said Alperovitch. Photo by Sarah Silbiger

However, five states — Delaware, Georgia, Louisiana, New Jersey, and South Carolina — have no paper trail whatsoever. Another nine, including swing state Pennsylvania, have some jurisdictions that rely on paperless voting.

Voting isn't the only vulnerability. Every state has a computerized voter registration database that could be susceptible to hacking. Already this year, two states — Arizona and Illinois — have seen their registration systems breached. The questions now, according to Smith, include: Can records of who is registered to vote be tampered with or deleted? And, if so, how does that affect the election?

"The breaches … in June and July of the voter registration systems coupled with the DNC hack of the emails really brought a lot of people up short and made them realize this is not so much theoretical," said Smith. "This is happening. We need to check our systems."

The Department of Homeland Security is collaborating with election officials in 40 states to provide vulnerability scans and cyber-risk assessments. Yet U.S. voting systems are not classified as critical infrastructure, a designation that would allow for enhanced security.

No less urgent, said the Belfer Center's Ben Buchanan, is the need for policymakers to assert consequences for bad actors intent on disrupting American voting.

"The United States needs to come out after this election and establish some kind of deterrent policy," said Buchanan, a postdoctoral fellow with the center's Cyber Security Project. "If you start to mess with the integrity of an election machine itself [or] the integrity of a voter registration database or of a dissemination system, we will take that very seriously, and we will retaliate. We consider elections so fundamental to our democracy that we are ready to defend them with force or whatever is required."

Articles by: **Laura Colarusso**