Ahead of US election, angst over hacking threats

October 7 2018

Hack attack. Wikipedia, CC BY-SA

At a Boston technology conference last month, computer scientist Alex Halderman showed how easy it was to hack into an electronic voting machine and change the result, without leaving a trace.

Halderman staged a mock election in which three conference attendees voted for George Washington, but an infected memory card switched the result to give a 2-1 victory to Benedict Arnold, the military officer who sold secrets during the Revolutionary War.

Halderman's demonstration was on a voting machine still in use in 20 US states, which had no paper ballots that could be compared to the electronic output, and thus no way to determine if vote totals had been altered.

"What keeps me up at night is the threat that a hostile nation-state could probe every swing state or swing district (and) find the ones most weakly protected, to silently change the results of a national election," the University of Michigan professor said.

A month ahead of the midterm congressional elections, security experts say the risks remain high for a hack on voting machines or other targets.

The vote comes two years after the US national election in which, according to intelligence officials, Russian agents probed voter registration networks in at least 20 states and accessed at least one.

Halderman said the Russians had the ability to destroy or alter voting records, which could have led to chaos on election day. He added however that, according to a Senate Intelligence Committee investigation, "they did not pull the trigger on that ability."

Other researchers have shown flaws which could allow hackers to penetrate voting machines or networks, and have stepped up calls for new methods to replace all-electronic systems with no paper backup, still in use for an estimated 20 to 25 percent of US voters.

The Defcon conference of security researchers discovered a voting

tabulator used in 23 states is vulnerable to a remote hack via a network attack and another machine used in 18 states could be hacked within two minutes.

More paper needed

A National Academy of Science report in September recommended that every effort should be made to use paper ballots in the 2018 election and that by 2020 "human readable" ballots should be standard.

States should mandate audits prior to the certification of election results, it said, getting enough data to ensure that any electronic totals match the ones on paper.

US elections are managed by state and local officials, meaning standards may not be uniform, and some states have resisted efforts to impose norms, claiming this would impinge on their authority.

In Georgia, a judge declined to order the replacement of electronic voting machines for the November 6 vote because it was too late, but warned that voters may have a case that their constitutional rights were violated.

Five states still use "paperless" systems without any form of backup, according to Joseph Hall, who heads an election security research team at the Center for Democracy and Technology.

Hall said that in addition to voting machines and election rolls, hackers may look at other targets such as candidates, or the networks of state or local officials who run the elections.

"We are increasingly worried about adversaries attacking the election system," Hall said.

In addition to possible attacks from nation-states, Hall pointed to opportunistic attackers who don't have political motives but want to "make a name for themselves."

Mike Murray, of security firm Lookout, said attackers could disrupt the election by hacking into mobile phones of candidates, staffers, activists and others—sometimes simply by sending a text message infected with malware.

"There's a whole electoral ecosystem" of people whose phones can be hijacked, Murray told a Capitol Hill briefing. "The mobile device has become one of the primary targets of nation-states."

Making strides

Congress this year allocated $380 million to states to improve election security. But lawmakers declined to pass a proposed Secure Elections Act that would have mandated security standards and audits.

The National Association of Secretaries of State, comprised of officials in charge of state election systems, has downplayed the risks from hacking demonstrations, saying they don't reflect real-world conditions.

Meanwhile US Homeland Security Secretary Kirstjen Nielsen said there have been "tremendous strides" in election security in the past two years.

Her agency, she said, is providing technical assistance to all 50 states, including the deployment of sensors that can detect network intrusions.

"We are really and truly throwing everything we have at it," Nielsen told a Washington Post cybersecurity conference.

But some analysts say even a minor incident can undermine credibility in

the election result.

Christine Santoro of the Open Source Election Technology Institute said adversaries are using a combination of direct and indirect attacks, combined with propaganda and disinformation efforts.

"They may not have to expend great effort to derail an election," she said in a blog post.

"With a little luck they can continue to sow seeds of mistrust and distrust in our vital democratic processes."