Hacking the election: questions and answers

October 8 2016

The US government's accusation that Russian government-directed hacking aimed to disrupt the November election comes amid fears about the security of the voting process.

The attacks have included breaches of emails of political organizations—blamed on Russia—as well as probes of state voter databases, for which US officials have said they cannot determine the source.

Here are some questions and answers:

Can hackers affect the November election results?

This is unlikely, voting experts say. There is no single, centralized hub to be hacked, and the system is comprised of over 100,000 precincts and polling places.

"While no system is 100 percent hack-proof, elections in this country are secure, perhaps as secure as they've ever been," David Becker of the Center for Election Innovation & Research told a recent congressional hearing.

"There isn't a single or concentrated point of entry for a hacker."

Voting machines undergo frequent tests, and are not connected to the internet, Becker said, adding that 75 percent of votes are either on a paper ballot or with a paper backup. Thirty-two of the 50 states require

printed ballots that can be audited in the case of questions.

So the election is secure?

It remains to be seen. A study last year by the Brennan Center for Justice at New York University found that "outdated voting equipment across the country presents serious security and reliability challenges."

Even if attacks do not affect a large number of ballots, "they can severely damage voter confidence, and would be particularly troubling in very close contests," the report said.

Dan Wallach, a computer science professor at Rice University who studies voting systems, told lawmakers the biggest vulnerability is voter registration databases.

Wallach testified at a House of Representatives hearing on election security that such an effort "can selectively disenfranchise voters by deleting them from the database or otherwise introducing errors."

Even if voting machines are not connected to the internet, he said, they "still interact with normal computers as part of their initialization phase (loading software and ballot definitions) and the tabulation phase (extracting castvote records and computing the totals)."

This can allow hackers to attack even "air gapped" machines that are not online, Wallach said.

What about online voting?

Thirty-two states and the District of Columbia home to the US capital Washington allow some form of internet voting, involving email, fax or online portal, mainly for overseas and military voters, according to a

study by the Verified Voting Foundation.

But many computer experts contend these ballots may not be secure, with a potential for being altered, and with secrecy not guaranteed.

"Will we ever be able to vote on the internet? Eventually, yes, but definitely not with today's computers, and not on today's internet," according to Wallach.

Internet voting is widely used in Estonia and has been tested elsewhere. But a group of computer experts in 2014 urged Estonia and other countries to discontinue the practice "until there are fundamental advances in computer security."

What other disruptions are possible?

Instead of targeting voting machines, hackers or other activists could take a different approach: disinformation through social media or emails to create confusion in the final days of the campaign.

"A dump of carefully crafted fictional emails to WikiLeaks could do this, without ever actually attacking any machine," said University of Iowa computer scientist Douglas Jones.

"Creating havoc is far easier than systematically corrupting the results."

What is motivating the attacks?

Russia's involvement is not a surprise, according to James Lewis of the Center for Strategic and International Studies.

The Russians "see themselves in a new conflict where control of information is a tool or even a weapon," he said.

"They feel that Western institutions dominate global perceptions, and they feel there's a need to push back."