thehill.com

Hacking an election requires more than compromising a machine

Alfredo Ortega

Last month, hackers decided to take an active role in the U.S. presidential election. At this point, they weren't just shedding light on the sad state of our outdated, insecure electronic voting machines — they were working to cast doubt on the election's outcome and trying to undermine confidence in American democracy.

In wake of these attacks, like the DNC email hacks and the hacking of voting systems in Illinois and Arizona, some researchers point fingers at Russia. But the truth is, as Donald Trump famously said in the most recent presidential debate, it could have been done by a lone hacker in his room. While Russia and most other powerful countries seem to have very competent and talented state-sponsored hackers, what most don't realize is that the vulnerable state of America's voting systems and machines isn't necessarily the issue.

Speaking as one who has been able to break into a voting machine before, I can tell you right now that focusing on the security of the devices themselves is not the big issue at hand. The fact is, every digital system can be hacked, and those who tell you otherwise are lying.

What are They Hoping to Accomplish?

There are numerous ways to tamper with voting systems without having to touch the physical ballots or voting machines. In fact, in Germany, where they used electronic voting machines that were not connected to the internet, hackers could read a person's vote from 20 to 30 meters away, remotely and wirelessly, by using a small antenna to listen for the machine's radio emissions. Simply put, that system did not maintain the anonymity of the voter.

In the Illinois voting systems case, hackers seemed more interested in taking, rather than changing information stored on state systems. The hackers managed to extract information from up to 200,000 voters' personal data. Though stealing personal information to commit identify theft could be a motive, it seems that these hackers aren't looking for credit card or bank information. They're looking for voting history and seeing if there's an opportunity to influence future votes through bribes or threats. As seen in Germany, they don't have to be too near to the voter to get this information.

Perhaps the biggest concern that can come out of election attacks is blurring the lines between winning and losing. For a voting system to work effectively, you have to convince the losing side that it actually lost, and lost fairly. This is where purely electronic systems — like those found in Pennsylvania and Virginia — are the most susceptible to questions of legitimacy. With a paper-based system, you at least have a way to recount and show the votes are legitimate. In a purely digital system, you have no backup or certainty. The suspicion of a hack will always be there, and the losing side can use its discontent to either criticize the winning side, or even try to bribe the winners in exchange for not appealing the results. The democratic system gets weaker if you use an unreliable system to vote.

What We Should Take Away from This?

Given what is known about the effort it takes to penetrate a system, these are not concerns that should be brought up only near

Election Day. With electronic voting, you're not going to be hacked on the day of the vote — you have to assume you've already been hacked. These kind of hacks, or programs that deliver these hacks, are usually set up or planted months, sometimes years, before an Election Day. So those defending the vote have to start well before an election. You can get machines off of all networks and ensure software is up to date, but you have to assume that come the day of the vote, you've already been compromised.

Cyber threats are only going to get worse. If the United States is lucky enough to avoid these threats now, it should try to prepare for the future. At this point, the only true defense against hacks such as these is to avoid the use of digital devices at all. While it may be impossible to move completely away from electronic voting methods, the U.S. could implement systems with a paper ballot backup that can be read for recounts. While even a paper-based system can be "hacked" in its own way, it's the most secure option currently available – at least as long as the right glue is used for the paper ballots, a problem that recently caused Austria to postpone its presidential elections.

Regardless of what happens this year, we have been forewarned and have received the message loud and clear. The most dangerous thing the U.S. can do right now is nothing — if Americans shrug and forget about this as the election passes, they're leaving their future elections, and even their democratic system, in serious jeopardy. This is a crisis that needs the utmost attention of U.S. election officials, lawmakers and everyday citizens. Hacking an election doesn't only require hacking a machine — it requires the inaction of those the attacks target.

Ortega is a backend developer at Avast Software.

The views expressed by authors are their own and not the views of The Hill.