theconversation.com

How vulnerable to hacking is the US election cyber infrastructure?

Richard Forno

Following the hack of Democratic National Committee emails and reports of a new cyberattack against the Democratic Congressional Campaign Committee, worries abound that foreign nations may be clandestinely involved in the 2016 American presidential campaign. Allegations swirl that Russia, under the direction of President Vladimir Putin, is secretly working to undermine the U.S. Democratic Party. The apparent logic is that a Donald Trump presidency would result in more pro-Russian policies. At the moment, the FBI is investigating, but no U.S. government agency has yet made a formal accusation.

The Republican nominee added unprecedented fuel to the fire by encouraging Russia to “find” and release Hillary Clinton’s missing emails from her time as secretary of state. Trump’s comments drew sharp rebuke from the media and politicians on all sides. Some suggested that by soliciting a foreign power to intervene in domestic politics, his musings bordered on criminality or treason. Trump backtracked, saying his comments were “sarcastic,” implying they’re not to be taken seriously.

Of course, the desire to interfere with another country’s internal political processes is nothing new. Global powers routinely monitor their adversaries and, when deemed necessary, will try to

clandestinely undermine or influence foreign domestic politics to their own benefit. For example, the Soviet Union's foreign intelligence service engaged in so-called "active measures" designed to influence Western opinion. Among other efforts, it spread conspiracy theories about government officials and fabricated documents intended to exploit the social tensions of the 1960s. Similarly, U.S. intelligence services have conducted their own secret activities against foreign political systems – perhaps most notably its repeated attempts to help overthrow pro-communist Fidel Castro in Cuba.

Although the Cold War is over, intelligence services around the world continue to monitor other countries' domestic political situations. Today's "influence operations" are generally subtle and strategic. Intelligence services clandestinely try to sway the "hearts and minds" of the target country's population toward a certain political outcome.

What has changed, however, is the ability of individuals, governments, militaries and criminal or terrorist organizations to use internet-based tools – commonly called cyberweapons – not only to gather information but also to generate influence within a target group.

So what are some of the technical vulnerabilities faced by nations during political elections, and what's really at stake when foreign powers meddle in domestic political processes?

Ohio citizens using electronic voting machines during the 2012 presidential election. Aaron Josefczyk/Reuters

Vulnerabilities at the electronic ballot box

The process of democratic voting requires a strong sense of trust – in the equipment, the process and the people involved.

One of the most obvious, direct ways to affect a country's election is to interfere with the way citizens actually cast votes. As the United States (and other nations) embrace electronic voting, it must take steps to ensure the security – and more importantly, the trustworthiness – of the systems. Not doing so can endanger a nation's domestic democratic will and create general political discord – a situation that can be exploited by an adversary for its own purposes.

As early as 1975, the U.S. government examined the idea of computerized voting, but electronic voting systems were not used until Georgia's 2002 state elections. Other states have adopted the technology since then, although given ongoing fiscal constraints, those with aging or problematic electronic voting machines are returning to more traditional (and cheaper) paper-based ones.

New technology always comes with some glitches – even when it's not being attacked. For example, during the 2004 general election, North Carolina's Unilect e-voting machines "lost" 4,438 votes due to a system error.

But cybersecurity researchers focus on the kinds of problems that could be intentionally caused by bad actors. In 2006, Princeton computer science professor Ed Felten demonstrated how to install a self-propagating piece of vote-changing malware on Diebold e-voting systems in less than a minute. In 2011, technicians at the Argonne National Laboratory showed how to hack e-voting machines remotely and change voting data.

Voting officials recognize that these technologies are vulnerable. Following a 2007 study of her state's electronic voting systems, Ohio Secretary of State Jennifer L. Brunner announced that

> the computer-based voting systems in use in Ohio do not meet computer industry security standards and are susceptible to breaches of security that may jeopardize the integrity of the voting process.

As the first generation of voting machines ages, even maintenance and updating become an issue. A 2015 report found that electronic voting machines in 43 of 50 U.S. states are at least 10 years old – and that state election officials are unsure where the funding will come from to replace them.

A rigged (and murderous) voting machine on 'The Simpsons' satirized the issue in 2008.

Securing the machines and their data

In many cases, electronic voting depends on a distributed network, just like the electrical grid or municipal water system. Its spread-out nature means there are many points of potential vulnerability.

First, to be secure, the hardware “internals” of each voting machine must be made tamper-proof at the point of manufacture. Each individual machine’s software must remain tamper-proof and accountable, as must the vote data stored on it. (Some machines provide voters with a paper receipt of their votes, too.) When problems are discovered, the machines must be removed from service and fixed. Virginia did just this in 2015 once numerous glaring security vulnerabilities were discovered in its system.

Once votes are collected from individual machines, the compiled results must be transmitted from polling places to higher election offices for official consolidation, tabulation and final statewide reporting. So the network connections between locations must be tamper-proof and prevent interception or modification of the in-transit tallies. Likewise, state-level vote-tabulating systems must have trustworthy software that is both accountable and resistant to unauthorized data modification. Corrupting the integrity of data anywhere during this process, either intentionally or accidentally, can lead to botched election results.

However, technical vulnerabilities with the electoral process extend far beyond the voting machines at the “edge of the network.” Voter registration and administration systems operated by state and national governments are at risk too. Hacks here could affect voter rosters and citizen databases. Failing to secure these systems and records could result in fraudulent information in the voter database that may lead to improper (or illegal) voter registrations and potentially the casting of fraudulent votes.

And of course, underlying all this is human vulnerability: Anyone involved with e-voting technologies or procedures is susceptible to coercion or human error.

Voting machines in the warehouse before they are sent out to local precincts. Chris Keane/Reuters

How can we guard the systems?

The first line of defense in protecting electronic voting technologies and information is common sense. Applying the best practices of cybersecurity, data protection, information access and other objectively developed, responsibly implemented procedures makes it more difficult for adversaries to conduct cyber mischief. These are essential and must be practiced regularly.

Sure, it's unlikely a single voting machine in a specific precinct in a specific polling place would be targeted by an overseas or criminal entity. But the security of each electronic voting machine is essential to ensuring not only free and fair elections but fostering

citizen trust in such technologies and processes – think of the chaos around the infamous hanging chads during the contested 2000 Florida recount. Along these lines, in 2004, Nevada was the first state to mandate e-voting machines include a voter-verified paper trail to ensure public accountability for each vote cast.

Proactive examination and analysis of electronic voting machines and voter information systems are essential to ensuring free and fair elections and facilitating citizen trust in e-voting. Unfortunately, some voting machine manufacturers have invoked the controversial Digital Millennium Copyright Act to prohibit external researchers from assessing the security and trustworthiness of their systems.

However, a 2015 exception to the act authorizes security research into technologies otherwise protected by copyright laws. This means the security community can legally research, test, reverse-engineer and analyze such systems. Even more importantly, researchers now have the freedom to publish their findings without fear of being sued for copyright infringement. Their work is vital to identifying security vulnerabilities before they can be exploited in real-world elections.

Because of its benefits and conveniences, electronic voting may become the preferred mode for local and national elections. If so, officials must secure these systems and ensure they can provide trustworthy elections that support the democratic process.
State-level election agencies must be given the financial resources to invest in up-to-date e-voting systems. They also must guarantee sufficient, proactive, ongoing and effective protections are in place to reduce the threat of not only operational glitches but intentional cyberattacks.

Democracies endure based not on the whims of a single ruler but

the shared electoral responsibility of informed citizens who trust their government and its systems. That trust must not be broken by complacency, lack of resources or the intentional actions of a foreign power. As famed investor Warren Buffett once noted, “It takes 20 years to build a reputation and five minutes to ruin it.”

In cyberspace, five minutes is an eternity.