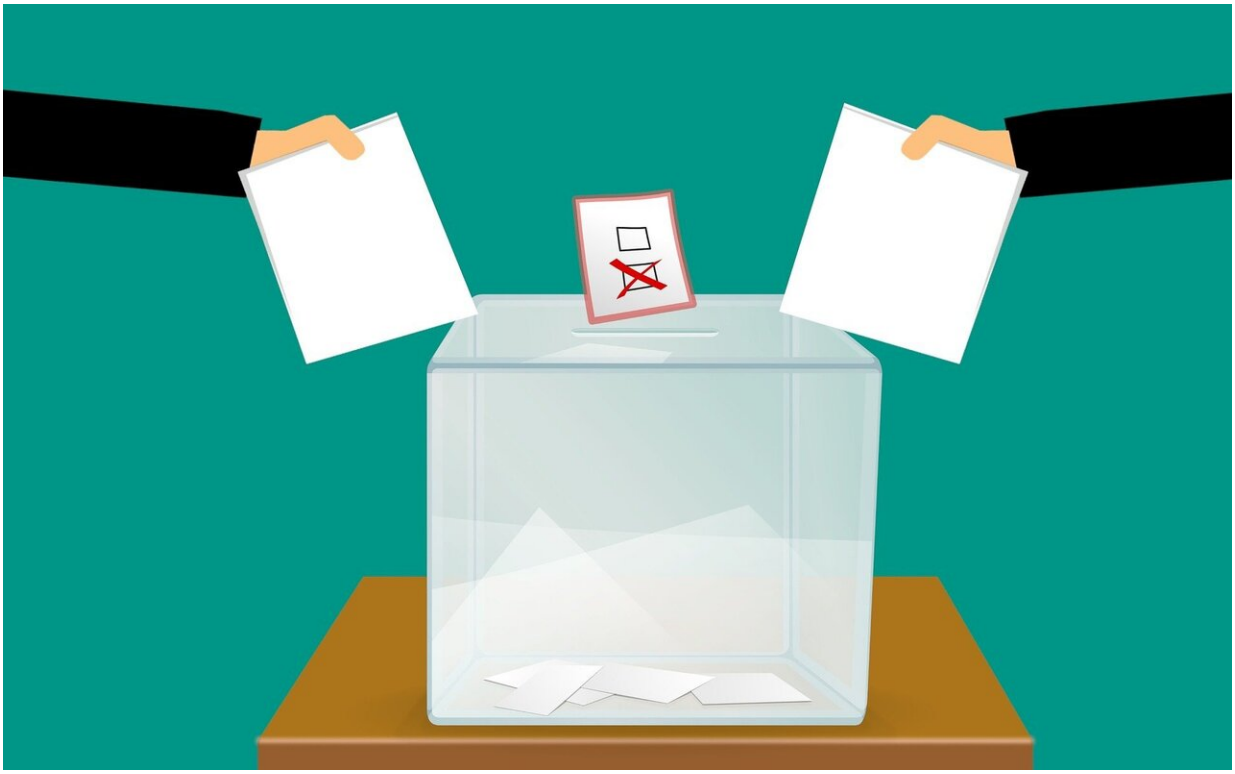
Here's why security officials are concerned about claims of a hacked (or stolen) election

November 4 2022, by Josh Meyer



Credit: Pixabay/CC0 Public Domain

Despite an unprecedented U.S. focus on preventing hackers from targeting the midterm elections Tuesday, there are still concerns that malicious cyber operatives could disrupt or influence the vote by penetrating polling stations, voter registration rolls, ballot counting

efforts and even the news reports that tell Americans who's winning state, local and federal elections.

But here's what really concerns public and private sector security analysts: malicious cyber actors who claim that the election was hacked or stolen even when nothing of the sort occurred. Such false claims, building on years of bogus election fraud narratives that began well before the 2020 presidential election, they say, could plunge the country into an unprecedented environment of political chaos and violence even worse than that which spawned the Jan. 6, 2021 attack at the U.S. Capitol.

"I'm quite concerned about the prospect for what folks are calling this cognitive hack around the elections; that there will be claims that the process was illegitimate and therefore the outcome is illegitimate," said Suzanne Spaulding, a former top Department Homeland Security official who headed the agency's election security efforts.

Despite the fact there are processes in place to verify voting and to do post-election audits, Spaulding worries that, "Conspiracy theories will take hold in a substantial segment of the population and could lead to additional political violence."

A senior FBI election security official agrees, telling reporters in a recent briefing that while the FBI was not aware of any foreign adversaries' cyber campaigns attacking the infrastructure of U.S. elections, authorities are concerned malicious cyber actors could seek to spread or amplify false claims of such compromises.

The official, one of several speaking anonymously under briefing conditions set by the FBI, said it's important for Americans to know that such claims of cyber compromises would neither prevent them from voting nor swing an election given the multiple layers of defenses

currently in place.

Still, as Spaulding noted, given the already explosively adversarial political climate in the United States these days, such false narratives could spread like wildfire and be hard to knock down.

Here are some cyber attack scenarios authorities are monitoring:

Hacking voting machines and registration rolls

There are three primary avenues cyber adversaries can use to hack a U.S. election: targeting voter registration, voting machines and voters themselves.

One potential method of cyber tampering with the vote count is to alter or delete voters aligned with a particular political party, so that "when people showed up to vote, they'd be turned away because they either weren't listed or their IDs didn't match the rolls," Spaulding said. "That could cause chaos that would undermine trust in the process."

In 2016, Russian cyberwarriors from the GRU military intelligence agency hacked voter registration databases in two Florida counties by sending phishing emails to county officials responsible for administering the election, federal authorities have said. That enabled the GRU to gain access to the network of at least one Florida county government, a Senate intelligence committee investigation later concluded. It said it found no evidence that vote tallies were altered or that voter registry files were deleted or modified, but also noted that the committee's and the overall U.S. intelligence community's "insight into this aspect of the 2016 election was limited."

While there are currently no indications of such activity this year, hackers could tamper with key databases like voter registration rolls,

shut down critically important websites like local election agency homepages or steal confidential voter information, according to F5 Labs, a threat intelligence and security firm.

Another hacking method is attacking voting machines.

Voting machine hacking has been a known issue for over 15 years. It was cited as a credible threat in former FBI director Robert Mueller's special counsel report on the investigation into Russian interference in the 2016 presidential election, which said Russia's GRU had also targeted state election offices and voting machine makers.

In all of these scenarios, though, federal, state and local election authorities have established layers of security measures and audit trails—including paper ballots and other backups—to help with detection and remediation.

The third avenue, and the one that most concerns many election officials , is using hacks and cyber attacks to deceptively influence voters. That includes creating or amplifying false narratives about particular candidates or, as Spaulding warns, about the integrity or fairness of the election itself.

Attacking the election itself

In 2016, U.S. officials confirmed that Russia was trying to hack the actual infrastructure and machinery of U.S. elections in ways that went beyond what it was trying to do in Florida. That included targeting voter registration data in an attempt to block some constituencies from voting and, more broadly, to undermine confidence in the overall elections process.

Overall, Russia-linked hackers targeted election systems in at least 20

states, trying to penetrate online systems like registration databases—but not the actual voting or tabulation machines that were to be used on Election Day, which are usually not tied to the Internet.

At the time, a senior DHS official described much of the Russian activity as "people poking at the systems to see if they are vulnerable." Even so, he said, "we are absolutely concerned. The concern is the ability to cause confusion and chaos."

Since then, election security agencies have invested significant time, resources and expertise to improve the security and resilience of U.S. election systems, according to the FBI officials, Spaulding and other current and former election security officials. By 2018, the federal government designated election systems as part of U.S. critical infrastructure, which added additional levels of protection and funding.

After Iran, Russia and other adversaries targeted the 2020 elections, federal authorities implemented another wave of improvements.

So far, in the run-up to the midterms, "there's not a huge uptick that we can see in terms of probing or access or anything that would indicate their direct attacks yet" by Russia or other foreign adversaries, said Ronald Bushar, the Global Government chief technology officer at Mandiant, a threat intelligence firm that is advising U.S. government agencies and local governments on election cyber protection.

But Bushar told U.S. TODAY that election security officials are on red alert that Russia in particular might try to penetrate election systems, perhaps as payback for U.S. aid to Ukraine that has helped it beat back Russian military advances. "That's their MO that we've seen before," he said, citing past Kremlin hacks of U.S. critical infrastructure and other cyberattacks that created chaos and confusion.

Jen Easterly, the director of the Cybersecurity and Infrastructure Security Agency, or CISA, said recently there are no specific or credible threats regarding the cyber disruption of election infrastructure in the Tuesday elections. But she said federal cybersecurity officials remain concerned about "a very complex threat environment," including potential efforts to interfere in the vote, both online and in person.

As such, CISA and other federal cybersecurity agencies have issued multiple warnings in recent weeks about election-eve threats, citing the prevalence of online extremism and fake and often maliciously circulated information about the strength of U.S. election security.

Sowing 'doubt, distrust and dissent' about the election

U.S. TODAY reported last week that China is stepping up its efforts to use cyber operations to influence the midterms, especially by creating false narratives online that undermine confidence in voting and in democracy itself.

More broadly, DHS and FBI officials have warned that Russia—and possibly Iran—are also seeking to spread disinformation about the elections in an effort to sow discord among Americans and undermine confidence in election integrity.

Such influence operations are nothing new. They were a central part of Russia's meddling in the 2016 presidential election, which ranged from promoting false narratives about the election and even hacking into the computers of the Democratic National Committee and releasing stolen emails aimed at embarrassing the campaign of Democratic presidential candidate Hillary Clinton. In July 2018, the FBI charged 12 Russian military intelligence officers in that case.

Authorities said the Russian operatives used phishing attempts to gain

access to campaign officials' computers, and authorities have since worked with campaigns to bolster their defenses against such attacks.

Iran was especially active in conducting such operations in the 2020 elections, U.S. intelligence agencies have concluded. Last November, for instance, the Justice Department charged two Iranian nationals for their part in allegedly targeting the 2020 election.

In the current election season, Iran has shown a continued willingness to "take advantage of election-integrity narratives that come up in the U.S. ecosystem," one of the senior FBI officials said at the recent election security briefing.

And Russia, on the ropes in its war against Ukraine, has resorted to ramped up disinformation campaigns in recent weeks, including pushing false narratives that seek to undermine election integrity, the senior FBI officials said.

Current and former election security officials say they are especially concerned that such disinformation efforts will find a receptive audience among conservatives who have spent the past two years since former President Donald Trump's electoral defeat claiming that U.S. elections have been rigged against their candidates and in favor of Democrats.

Numerous investigations have found no truth to those claims, but they are growing in intensity, according to Spaulding and others.

"What we see now is a more dynamic information environment that seeks to leverage doubt, distrust and dissent about the elections process, largely driven by untruths about how elections are run in the United States," said Matt Masterson, a former DHS cybersecurity official who is now director of Information Integrity at Microsoft.

Hacking the post-election landscape

Spaulding, director of the Defending Democratic Institutions project at the Center for Strategic and International Studies, isn't the only one worried about efforts to influence the outcome of the election through what she describes as "cognitive hacks," or efforts to use disinformation to covertly influence a target audience.

The FBI and DHS circulated a confidential briefing to state and local officials on Oct. 28 that warned about efforts to leverage the "enduring ideological grievances and perceptions of election fraud" that could cause a sharp spike in violence, just like it did after Trump falsely claimed he won the 2020 election and told his supporters to march on the Capitol on Jan. 6 and "fight like hell (or) you're not going to have a country anymore."

In their joint intelligence assessment, the FBI and DHS warned that domestic violent extremists pose a heightened threat to the 2022 midterm elections for a variety of reasons, including making physical threats to poll workers. One reason for that, they said, was that perceptions of election fraud would likely result in increased threats of violence—even if they have no merit and are based on disinformation campaigns.

Enduring perceptions of election fraud related to the 2020 general election continue to contribute to the radicalization of some violent extremists and likely would "increase their sensitivity to any new claims perceived as reaffirming their belief that U.S. elections are corrupt," the assessment said.

Numerous investigations have found no truth to those claims, but they are growing in intensity, Spaulding and others told U.S. TODAY. Spaulding and the FBI and DHS officials (including Easterly) said

"I still think the greatest threat is the cognitive hack; information operations that will undermine public trust and the legitimacy of the election—and that can take lots of forms," said Spaulding, a member of the federal government's Cyberspace Solarium Commission, which was established to develop a strategic U.S. approach to defending America against cyber attacks "of significant consequences."

Bad actors could try to sabotage the election through cyber means, including tampering with voter registration databases, she said, or they could simply claim that they—or others—did, and let the bots and paranoid activists on social media take it from there,

"It really wouldn't matter whether you were successful in actually changing any votes or even altering data," Spaulding said. "But you could claim that you had done something that creates doubts."

Government officials who are anticipating such activity would quickly beat back such accusations, and show how the vote count was transparent and unaltered in any way.

"But we have very fertile ground that has been laid for a segment of the population to be extremely skeptical, even of the state and local election officials who would be conducting these audits and reassuring people," she said. "So there's a greater risk than there's ever been, particularly since we have candidates who have already refused to say that they would accept the outcome of the election if they lose."