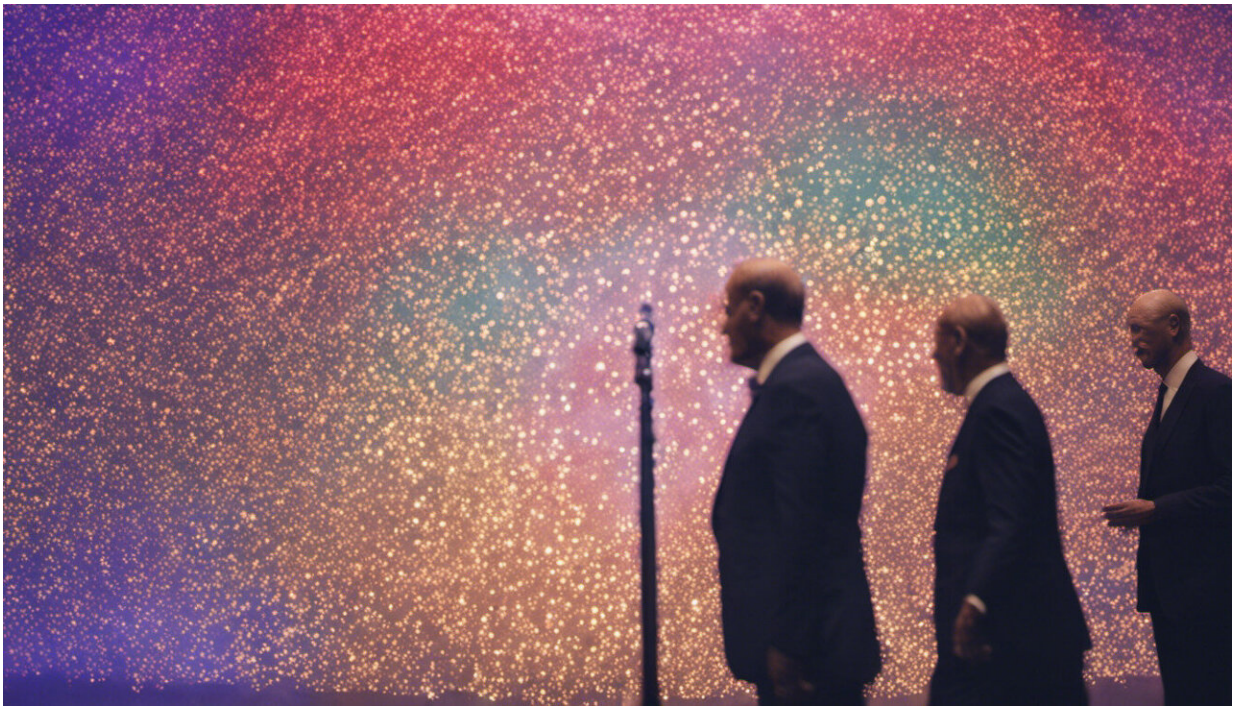
This election was not hacked – but it was attacked

November 9 2016, by Richard Forno



Credit: AI-generated image (disclaimer)

The presidential campaign of 2016 thankfully – and we can only hope officially – ended this evening. As of when this article was posted, there are no reports of widespread cyberattacks or other digital interference against state voting systems. Of course, since votes are still being tallied, we're not in the clear yet. But current indications are that this was a

fairly uneventful election, from a cybersecurity perspective at least.

So far, we've seen no public evidence of Russian hackers, 400-pound or otherwise, attacking individual voting machines from their bedrooms (to use a very tired old trope). There have been reports of brief computer problems, but they were easily remedied. And there's no indication that state voter registration databases were compromised by hostile third parties.

Nevertheless, cybersecurity units of several states' National Guard forces were mobilized ahead of the election, in a manner reminiscent of the reassuring and public show of force when airports reopened following 9/11. The military's hackers at U.S. Cyber Command reportedly stood ready to retaliate against cyberattacks on the election – in particular, from Russia as well.

These possibilities and preparations reinforce the need for America to place a greater emphasis on election-related cybersecurity, if not also cybersecurity more generally. Even though nothing suspicious appears to suggest the election was "hacked," we must still make improvements. At stake is the trustworthiness of the electoral systems and processes of the world's leading democracy.

Time for governments to act

Politically motivated digital attacks during the latter months of election 2016 raised concerns about the electronic security of the American electoral process. These events included the hacking of the Democratic National Committee and the ongoing Wikileaks disclosures of email accounts of Clinton advisers. These events increased public interest in cybersecurity beyond the effects of the revelations of NSA contractor Edward Snowden in 2013 and many high-profile data breaches.

In recent months, government agencies and experts (including myself) have recommended improvements to the electronic security of our hodgepodge collection of voting systems.

Among our suggestions are that states ensure their voting systems are modernized, properly updated, tested and secured from both physical and network-based tampering. States must continually ensure the integrity of their voter databases to help minimize the potential for voter fraud. And they must provide a trusted audit trail (for example, paper receipts) for election officials and the public to fall back on. There must be a way to clearly resolve questions about the security and integrity of the system, process or reported results.

All of this requires strong political will for meaningful action. It also means we'll need to ensure the necessary money and expertise are available to make it happen in communities all across the country – admittedly not an easy task during a period of widespread budget constraints.

These concerns align with the basic principles of cybersecurity that apply to any organization. Information resources and their data must remain available and accessible to authorized users, confidential from unauthorized users, and protected from intentional and accidental tampering or modification. In meeting these challenges, organizations must find the resources to implement those safeguards in a proactive, effective, and ongoing fashion.

But there is a crucial difference that makes these particular cybersecurity efforts especially important: Election systems are truly critical foundations for our nation's underlying social and political infrastructure.

Rhetoric attacked legitimacy

Although this election does not appear to be "hacked" in the manner that many predicted, I do believe that it was successfully and directly attacked, repeatedly. These attacks did not come in the form of hackers altering vote counts. Rather, the attacks on this election's integrity came from assorted and perhaps nontraditional threats, both foreign and domestic.

Over the past year, Republican Donald Trump repeatedly made vague claims of a "rigged" system, possibly related to unsubstantiated allegations of widespread voter fraud or Russian influence. In addition, politically sensitive information was regularly revealed by groups and organizations believing themselves to be above the rules of law and common sense. And, the media itself became the recurring target of scorn as enablers of the alleged election "rigging."

These claims targeted the public's behavioral and cognitive systems. Consequently, many Americans believe that the voting "system" in America cannot be trusted – even though there is no such thing. Rather, the country's elections operate on a patchwork of local and state rules, procedures and technologies.

To wit: Some states use fully electronic voting while others retain the traditional paper ballot. Polls open and close at different times across the country. Some states may offer a window for early voting while others do not. There is no unified national election "system" that could be attacked or disrupted in a single effort.

Unfortunately, refuting claims of vote-rigging or offering contrary views – even when based on documented evidence – was dismissed by believers as further proof of a "rigged" system.

Oddly, Trump made these "rigging" claims despite the fact that he was the nominee of a party whose own members oversee voting matters in

many states. That means his allegations suggested his own party's officials and election procedures were conspiring against him.

All this made it more difficult to discuss legitimate voting security concerns objectively, rationally or meaningfully. When everyone believes their own set of "facts," it is hard to address collective problems.

For these reasons, I believe election 2016 demonstrated the fragility of the American electoral process. It is susceptible to various types of attacks, overt and subtle, technical and nontechnical.

Protecting the voting system

Efforts to protect the American voting system can learn from the practice of cybersecurity. Cybersecurity professionals work to prevent attacks, and to respond to those that happen, in several ways. They identify threats and vulnerabilities in their systems and networks. They create and execute procedures to operate those systems. And they otherwise work to provide a secure cyberspace for their organizations.

They also share threat information and best practices across companies and government agencies. This is because they recognize that cybersecurity is a shared responsibility and collective efforts are more helpful than working alone.

The electoral equivalent of this problem involves much more than identifying and reducing the technical vulnerabilities with electronic voting machines from their assembly all the way to when they're used on Election Day. We must also ensure the integrity of all election data and systems, from the time a citizen submits their personal information when registering to vote, through casting their ballot, and on into counting the vote, tabulating it, and having it formally recorded by state election

officials.

Elections, like cybersecurity, are a shared effort involving many different people and organizations from industry and all levels of government. To carry the metaphor further, let's also take steps to ensure that the proverbial "window of vulnerability" is as small as possible. In the electoral process, reducing the potential time for an attacker to cause mischief is a valuable thing to consider. For example, is there really a need to have a multi-year presidential campaign that can be swayed regularly by any number of hacks in the cyber or cognitive domains?

Errors still happen

As of this evening, the process of voting appears to have encountered minimal, if any, cybersecurity-related problems. However, we may not learn about them immediately – unless attackers claim responsibility or government agencies make a public statement. Again, trust in the system, and trust in the people, processes and technologies, is crucial.

Yes, there will be human or procedural errors made in vote-casting and vote-counting. They, like any human process or organizational system, are not totally foolproof or errorproof. We must accept that fact. Will there be voter fraud somewhere? Perhaps. But in widespread numbers? Doubtful. And will votes be changed by overseas hackers? Probably not.

Certainly, there will be periodic and likely very minor errors, glitches, and hiccups in the overall election process – there almost always are. The media will report on them, social media will amplify them, and certain candidates or their supporters might use those reports as evidence of a larger conspiracy and evidence of a system "rigged" against them.

But even if tonight's vote count isn't hacked, the damage is done. We must acknowledge that the integrity of America's election system has

been attacked successfully. Accordingly, once people have recovered from election 2016, we must implement a series of bipartisan, nationwide, rational and objective discussions about our election processes and technologies so that citizen trust in this most cherished national infrastructure – and feature of American democracy – can be restored.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: This election was not hacked – but it was attacked (2016, November 9) retrieved 17 April 2024 from https://phys.org/news/2016-11-election-hacked.html