Researcher discusses likelihood of cyberattacks on the 2016 election

October 18 2016, by Molly Callahan

Credit: Northeastern University

It's clear that cybersecurity plays an increasingly important role in our daily lives. Need proof?

Just look at the news. In September it was revealed that hackers stole account information from at least 500 million Yahoo users. Earlier this month, a National Security Agency contractor was arrested and accused of stealing classified computer code. And, of course, there was the pre-Democratic National Convention bombshell that hackers, potentially orchestrated by the Russian government, stole documents from the DNC's computer system.

There's been chatter for months about vulnerabilities in the nation's registration databases and election systems. The recent hacks, combined with Republican presidential nominee Donald Trump's claims that the election is rigged against him, have pushed many across the nation toward deep unease.

We asked William Robertson, associate professor in the College of Computer and Information Science and an expert in systems, web, and mobile security, to weigh in on the state of domestic cybersecurity and how it relates to the election.

As our society increasingly becomes more global and interconnected, do you think hostile countries pose a greater risk to domestic cybersecurity? Is there a threat of international players influencing the outcome of a presidential election?

The short answer is yes and yes. One rather qualitative way of thinking about the risk and impact of cyberattacks is the idea of the "attack surface." That is, the more ways we give an attacker to inflict damage or steal information, the greater the attack surface and, consequently, the potential risk of successful attacks. It is simply logical that hostile countries will try to benefit from any weaknesses we expose, and the greater our attack surface, the greater the likelihood that weaknesses will

be found.

Along with the risk of security incidents, one should consider their potential impact. And so, the greater the criticality of the services that are exposed to the rest of the world—intentionally or not—the greater the potential impact of successful attacks. For example, one of the biggest emerging areas of concern at the moment is the growing exposure of critical infrastructure that, while once isolated in separate and dedicated networks, is now being exposed via the internet. Successful attacks against control networks for physical infrastructure could lead to incidents like widespread power failures or the shutdown of industrial processing plants, examples of which are already suspected to have occurred.

In the context of the electoral process, what is emerging as a particularly effective attack strategy is to illicitly obtain potentially damaging information via system penetration and then release this information through third parties (complicit or otherwise). The U.S. government has made an unprecedented concrete accusation against Russia in this regard and has now stated that it will consider a proportional response. It is unfortunate, to say the least, that this sort of sensitive information is not more carefully safeguarded. And, foreign attacks designed to influence the U.S. electoral process would certainly have a massive impact if those aims are achieved.

Some political figures have asserted that "rigged elections" could undermine the results on Election Day. How feasible is it that an agent would be able to hack into or attack either a system of voting machines or a voter list? Is the threat of a "rigged election" a real threat or concern?

Given that some aspects of our electoral process are partly electronic, it is conceptually possible that this could open the door to attacks that, for example, deny voting service in key precincts or create unaccountable errors in vote tabulation. I personally participated in two state-sponsored reviews in California and Ohio in the mid-2000s, both of which found multiple severe vulnerabilities in electronic voting machines. Those results led to the decertification of several models of electronic voting machines, but also raise the question of whether electronic voting is trustworthy enough for such a critical social function as voting.

However, the potential for attacks against electronic voting machines or other resources does not mean that such an attack is likely. In particular, I have not seen any factual basis for claiming that such an attack is imminent for the current election cycle. Ironically enough, if anything, the party currently claiming that the election is rigged is the one that benefits from the only actual substantiated report of election-related hacking we have seen.

Are there precautions that are being taken, or that should be taken, to reduce the risk of hacking on Election Day?

Prognosticating on future attacks is a difficult business; indeed, it is one of the most difficult aspects of security research. I will say that for the time being I would expect any efforts to influence or tamper with elections to remain in the vein of what we've already seen: hacking to obtain information that can be used to carry out traditional psychological warfare by influencing popular views on candidates in important races such as the presidency. This would be in line with the cyber cold war we are currently engaged in. Moving from attacks that simply leak sensitive information to attacks that have physical effects—such as disrupting traffic control systems on Election Day to make voting more

difficult—crosses a line. That line represents a dramatic escalation and is one that I hope all parties involved are not willing to cross in the context of electoral integrity.

Provided by Northeastern University