Expert says cyberattack worries could affect elections

11 August 2016, by Clifton B. Parker

A real possibility exists that foreign hackers could throw a monkey wrench into the outcome of the U.S. presidential election in the fall, a Stanford expert says.

Herbert Lin, senior research scholar for cyberpolicy and security at Stanford's Center for International Security and Cooperation and a research fellow at the Hoover Institution, said that electronic voting could be affected by hackers in the presidential race, especially if a candidate claims tampering. In recent months, hackers from outside the country reportedly infiltrated the Democratic National Committee and Hillary Clinton campaign computer networks, leading to data breaches that made headlines worldwide.

The Stanford News Service interviewed Lin on this subject:

How worried are you about possible cyberattacks that could influence the outcome of the November elections in the U.S.?

There are two kinds of things to worry about. One is an actual cyberattack that, for example, alters vote counts in a way that tilts the election away from the will of the voters. That kind of attack is hard to pull off, and I'm not very worried about that – though I worry about it some.

A second worry – much more serious in my opinion – is the possibility that an election loser might challenge the outcome of the election, alleging that the results were altered by a cyberattack, especially if the election were close. How would anyone ever prove that ballots, electronically cast with no permanent and auditable record, were accurately counted?

If the evidence that Russians hacked the Democratic National Committee and the Hillary Clinton campaign proves to be legitimate, how should President Obama respond to Russia and Vladimir Putin?

The U.S. has many response options, ranging from private diplomatic conversations to military action and everything in between. There are many things we could do to exact a price. But some of these things may be wise and others may be unwise. For example, an unwise option would be to threaten overt military action and otherwise do saber-rattling in response. The balancing act is calibrating a response that exacts a penalty but does not provoke a response that is unacceptable to us – and that's a hard thing to do.

Would the U.S. ever hack back at Russia in some way?

I would be utterly amazed if the U.S. were not hacking Russia, and every other major power in the world for that matter. And I would be amazed if every other major power in the world were not hacking the U.S. There's a baseline level of hacking that is going on all the time by everyone.

So, the question isn't hacking or not hacking, the question is hacking back versus hacking. And on that point, I suspect it would be really hard for the recipient – in this case, Russia – to distinguish between hacking that almost surely is going on already and hacking that was conducted in response to any putative Russian involvement in the Democratic National Committee hack.

Is the hacking symbolic of a poor relationship between the U.S. and Russian governments?

I would not say symbolic – but it's entirely consistent with a poor relationship.

Provided by Stanford University