US intelligence: Foreign hackers spying on campaigns (Update)

18 May 2016, by By Deb Riechmann

In this Feb. 9, 2016 file photo, Director of the National Intelligence James Clapper speaks on Capitol Hill in Washington. Clapper said Wednesday,May 18, 2016, that the U.S. has already seen evidence that cyber hackers, possibly working for foreign governments, are snooping on the presidential candidates, and government officials are working with them to tighten security as they expect the problem to grow as the campaigns intensify. (AP Photo/Alex Brandon, File)

The United States sees evidence of hackers, possibly working for foreign governments, snooping on the presidential candidates, the nation's intelligence chief said Wednesday. Government officials are assisting the campaigns to tighten security as the race for the White House intensifies.

The activity follows the pattern set in the last two presidential elections. Hacking was rampant in 2008, according to U.S. intelligence officials, and both President Barack Obama and Mitt Romney were targets of Chinese cyberattacks four years later. Nevertheless, cyber experts say Donald Trump and Hillary Clinton's campaign networks aren't secure enough to eliminate the risk.

"We've already had some indications" of hacking, James Clapper, director of national intelligence, said Wednesday at the Bipartisan Policy Center in Washington. He said the FBI and the Department of Homeland Security were helping educate the campaigns.

Of the attacks, Clapper predicted, "we'll probably have more."

The revelation comes after Clapper's office released a document this month saying foreign intelligence services tracked the 2008 presidential election cycle "like no other." The document was in a slide show used to warn incoming Obama administration officials that their new jobs could make them prey for spies.

Eight years ago, foreign intelligence services "met with campaign contacts and staff, used human source networks for policy insights, exploited technology to get otherwise sensitive data, engaged in perception management to influence policy," it said. "This exceeded traditional lobbying and public diplomacy."

Jonathan Lampe with InfoSec Institute, a private information security company in Chicago, said security hasn't improved significantly since then.

In October, he evaluated the security of 16 candidates' websites and wrote a pair of reports. Using the reconnaissance skills of a casual hacker, Lampe pulled full lists of site user names and technologies used on most sites. In some cases, he discovered which directories were accessible from the Internet and which weren't. He learned the software products Clinton's campaign used from a job posting soliciting a computer-wise staffer.

"Everybody was sitting with their pants down and by the time we looked at the sites in March, everybody had made fixes," Lampe said.

But countries are probably still snooping, he said: "The sites were open enough back in October that anyone who grabbed the information then and wanted to use it, could still use it now."

Some threats are publicly known.

The international group of activists and hackers known as Anonymous has declared cyberwar on Donald Trump, urging supporters to take down his website and expose private information. Weeks ago, a masked figure appeared on YouTube, saying, "Dear Donald Trump, we have been watching you for a long time and what we see is deeply disturbing."

The New York billionaire probably has the largest "attack surface" of the candidates, said John Dickson of the Denim Group, a San Antonio developer of secure software. "If it's the Bernie Sanders campaign, it's probably one website. If it's Donald Trump, it's his entire empire."

Dickson and other experts said they weren't privy to any incidents of foreign hacking of the campaigns. But as the political conventions and general election near, they worry about a well-timed, sophisticated attack by a government to help a candidate.

"Think of the Chinese. Think of the Iranians. They have the intelligence capabilities, obviously, and maybe even the desire to disrupt elections," Dickson said.

At the least, he said it must be taken for granted that foreign governments are trying to learn more about the candidates. "You would hope that the CIA is doing the same thing," he said. Indeed, the U.S. spies on allies and adversaries for political and commercial information.

The Clinton and Trump campaigns didn't respond to questions about cybersecurity.

Dickson said the campaigns focused more on computer security because of the investigation into Clinton's use of a private email server as secretary of state, and a breach of voter data at the Democratic National Committee. Last year, Sanders apologized after his campaign improperly gained access to the campaign data of his Democratic rival, and he fired a data director.

V. Newton Miller, chief executive officer of Milwaukee-based PKWARE, which provides encryption software and advises federal agencies on data security, said foreign spying on campaign sites was inevitable.

"These campaigns are not working on encrypted platforms," he said. "It's a matter of when and how serious of an impact it is going to have on this election."

Foreign hackers are more interested in sensitive, revealing emails and reports, especially with the unprecedented mudslinging of this campaign, rather than acts of cyber vandalism, Miller and other experts said.

"If they shut down a candidate's website," Miller said, "so what? It impacts fundraising for 24 to 48 hours."

Hackers sabotaged a website for Romney's presidential campaign for a few hours in 2012, costing the campaign potential donations.

In the 2008 race, Obama and the Republican candidate, Sen. John McCain, were targeted.

One letter obtained by hackers showed McCain expressing support for Taiwan. China's government presumably backed the hack. A Chinese diplomat called the campaign to complain about the letter—before it was even sent.