The Washington Post

We asked experts to compare Trump's and Clinton's cybersecurity policies. Here's what they said.

Andrea Peterson

August 17, 2016

Cybersecurity is now a top national security problem — some officials even call it a bigger threat than terrorism. But both major presidential candidates have hit hurdles on the campaign trail that raised questions about how they would try to keep U.S. computers safe if elected.

Just last month, Democratic nominee Hillary Clinton escaped criminal prosecution for using a private email server for work as secretary of state — but got a tongue-lashing from the director of the FBI for being "extremely careless" by using it. Then emails from the Democratic National Committee were released by WikiLeaks, exposing politically embarrassing information.

As that scandal unfolded, GOP candidate Donald Trump seemed to urge Russian government hackers to hack Clinton. Although he played down his comments as sarcastic, the idea of a presidential candidate inviting a foreign power to hack a U.S. citizen raised flags for some. Trump's remarks also put a microscope on his apparently cozy relationship with Russian President Vladimir Putin — whose government many say was behind the Democratic National Committee hack.

How seriously should voters take those high-tech hiccups? And what will a Clinton or Trump victory mean for the United States' ability to fend off the rising tide of digital attacks?

To answer those questions, The Washington Post reached out to cybersecurity policy experts, including academics, think-tankers and officials from previous Republican and Democratic administrations and asked them evaluate both candidates' cybersecurity policy strategies and whether they were more concerned about Clinton's private email server or Trump's hacking comments.

Here's what they said:

Gen. Michael Hayden

Former CIA and NSA director who worked in high-level posts during the Bill Clinton, George W. Bush, and Obama administrations. Now a principal at the Chertoff Group.

Hayden said he found Clinton's "email faux pas" and Trump's comments about Russian hackers "equally off-putting." However, he hadn't seen enough from either campaign to evaluate their overall cybersecurity strategies.

One area he wanted to hear more about was how the candidates would act on the encryption debate if elected. During the debate between Apple and the FBI over the San Bernardino, Calif., phone, Clinton largely sidestepped the issue while Trump called for a boycott of Apple.

"For the record, I shade toward Apple because I believe the private sector will be the main effort when it comes to cyberdefense," Hayden said. "The Trump answer was vintage … bold, clear and wrong," he said.

Stewart Baker

Former NSA general council and Department of Homeland Security assistant secretary for policy during the George W. Bush administration. Currently a partner at law firm Steptoe & Johnson.

"Hillary Clinton's use of a home-brew email server with laughably bad security was appalling and irresponsible," Baker said. "It looks as though she was more afraid of Republicans and prosecutors than of Russian and Chinese intelligence agencies."

He thought Trump was joking when he made the Russian hacker comment, "but it was a joke with a sharp point for Clinton because in fact the Russians probably had better access to those emails than the FBI; after all, Clinton's lawyers had aggressively wiped the servers by the time the FBI got there." The claim that he was asking Russia to commit cyberespionage "is a symptom of the press's Trump Derangement Syndrome," he said.

Baker said the candidate's positions on cybersecurity mirror over campaign strategies: "Clinton's position is cautious, incremental, sober and boring: a cybersecurity third term for President Obama. She is proposing nothing that President Obama hasn't already proposed," he said. Trump's position, on the other hand is "impressionistic and focused on American decline," according to Baker. "He doesn't like our current posture and might do something dramatic to change it. Whether he will, and what that might be, who knows?"

On encryption, the two parties' official stances are "indistinguishable," he said — with both party platforms calling for a "balanced" solution. However, "Trump's actual unfiltered statements are quite different from the massaged language of the GOP platform; on the whole he is more friendly to government and law and order and crime victims than to West Coast billionaires," Baker said.

Susan Landau

Former senior staff privacy adviser at Google and current professor at Worcester Polytechnic Institute.

Landau declined to weigh in on whether she was more concerned about Clinton's use of a private email server or Trump's Russian hackers comment. But she had plenty of thoughts about how to evaluate what we know about the candidates' cybersecurity strategies.

"There are three different aspects to consider: the two candidates' views on cybersecurity initiatives, the party platforms and the issue of cryptography policy," she said. "Cyber is a hard problem," involving economic, technical and policy issues, she said, and "on this count, Clinton certainly has the advantage: she understands complex negotiations with many moving parts."

But Trump's response to David Sanger in a New York Times interviewearlier this year — in which he claimed that the United States was way behind on cybersecurity — seemed to show Trump was unaware of things like the Stuxnet attack, a cyberattack on Iranian nuclear facilities thought to be the work of the United States and Israel, she said.

Neither candidate has laid out too much of a cybersecurity plan so far, she said, nor did party platforms weigh in on the encryption debate. But Trump's response to the Apple-FBI legal battle — calling for a boycott of Apple — wasn't a good sign, according to Landau. "By providing a more secure system for online access, Apple's secured phone is an excellent step in the right direction for cybersecurity, something that candidate Trump does not seem to grasp," she said.

"I would say that the Clinton/Democratic proposals are a B/B-plus at present, while the Trump/Republican direction is a D/D-minus at best," Landau concluded.

Peter Swire

Former chief counselor for privacy in Office of Management and Budget during the Bill Clinton administration. Now a law professor at Georgia Tech.

Swire's response focused more on Trump's comments than Clinton's email server situation. “Urging a Russian attack is directly contrary to his party’s platform, which says 'an attack will not be tolerated,'" he said.

Although neither Trump nor Clinton are tech experts themselves, Clinton helped greatly expand the State Department's cybersecurity portfolio when she was secretary of state "and that continues today," he said.

“There is no magical solution for cybersecurity, no matter who is president," Swire added. "Instead, it takes funding, persistence and building a large team that can defend against a world full of threats. Based on the conventions if nothing else, Clinton builds and leads that sort of team far more than Trump.”

Paul Rosenzweig

DHS assistant secretary for policy during the George W. Bush administration. Current Principal at Red Branch Consulting.

"Secretary Clinton is really offering us more of the same — it's the Obama policy continued forward and improved," Rosenzweig said. "I would say that I would not expect Secretary Clinton to have any grand new initiatives, although circumstances might drive something new. To some degree that's a little disappointing because I think we've reached a bit of a stasis point: We're playing a lot of defense and we don't have too much offensive strategy," he continued.

But when it comes to Trump, Rosenzweig said he has "no real idea what he would do."

When it came to the Clinton email scandal vs. Trump's Russian hacker comments, he seemed more focused on the comments. "[Trump] says we have to get more aggressive, but then he perhaps jokingly invites information operations against his own country. I don't know what to make of it," Rosenzweig said. "I suspect his policy would come with a blind spot to Russian adventurism that would be disadvantageous to American interests," he added.

"My hope would be that [cybersecurity] would be one of the areas where [Trump] wouldn't be paying too much attention" and instead bring in experts to guide policy, he said. "That would probably be more of the same as well, although there might be some evolution because he'd be willing to let people break more china — the dishes, not actual China," Rosenzweig said.

But Rosenzweig also said there wasn't a lot to go on to judge Trump's strategy. "There's no information out there or theory that underlies his foreign policy. If I had a sense of what he was doing in the physical world, I could probably extrapolate to the digital world, but there's really nothing there," he said.

Julian Sanchez

Senior fellow focused on technology and civil liberties at the Cato Institute.

Sanchez said both Clinton's email server situation and Trump's Russian hacker comments were "pretty bad, but probably somewhat overblown."

"Even on the charitable premise that Trump was attempting to make a joke, it’s obviously irresponsible for a major party presidential candidate to signal winking approval of foreign cyberattacks on the opposing party, because even the act of joking about it suggests you’re not terribly serious about imposing costs on Russia if it continues its current conduct," he said.

On Clinton's email, Sanchez was more concerned about transparency than national security implications. "I don’t think anyone buys the idea that she set up a private server for 'convenience' rather than to retain control over correspondence legally subject to Freedom of Information requests," he said.

When it comes to overall cybersecurity strategy, Sanchez says it's hard to judge Trump "because he doesn’t appear to have one, unless welcoming Russian hacks counts. "Clinton, on the other hand, has made it "fairly clear that her approach to cyber would represent a continuation of the Obama administration’s Cybersecurity National Action Plan, with a focus on information sharing

with the private sector and an integrated approach across federal networks under the stewardship of a federal chief information security officer," he said.

"As far as a comparison of the two goes, I suppose 'having a plan' beats 'not having one,'" Sanchez concluded.