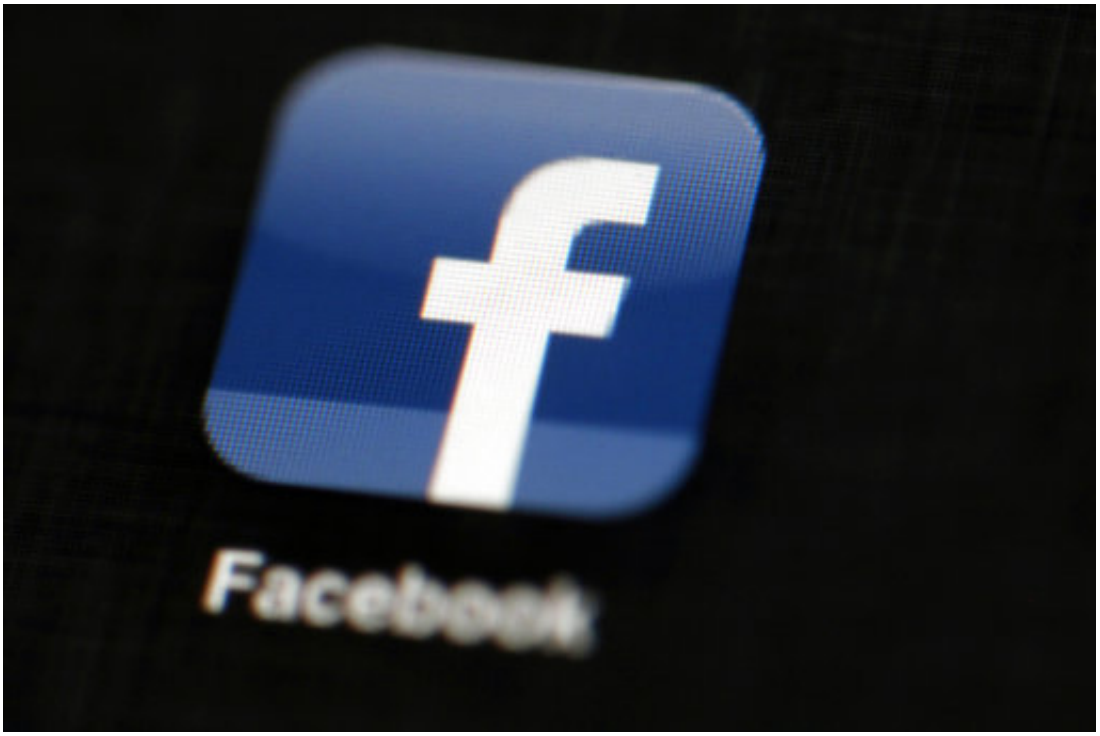
Campaigns on their own as cyber threats roil midterms

August 3 2018, by Steve Peoples And Christina A. Cassidy



In this May 16, 2012, file photo, the Facebook logo is displayed on an iPad in Philadelphia. Intelligence officials warn that foreign adversaries continue to wage cyber warfare against the U.S. election systems. But with the midterm elections just three months away, political campaigns report that they're largely on their own in the increasingly challenging task of protecting sensitive information and countering false or misleading content on social media. (AP Photo/Matt Rourke, File)

Kamala Harris has been the target of social media misinformation

campaigns since she became a U.S. senator.

Every month for the last 18 months, her office has discovered on average between three and five fake Facebook profiles pretending to be hers, according to a Harris aide. It's unclear who creates the pages, which are often designed to mislead American voters about the ambitious Democratic senator's policies and positions.

The aide spoke on the condition of anonymity, like more than a half dozen campaign officials contacted for this story, for fear of attracting unwanted attention from adversaries or scrutiny on the Senate office's evolving cybersecurity protocols.

Such internet mischief has become commonplace in U.S. politics. Facebook announced earlier this week that it uncovered "sophisticated" efforts, possibly linked to Russia, to influence U.S. politics on its platforms. Senior intelligence officials declared Thursday that foreign adversaries continue waging a quiet war against U.S. campaigns and election systems.

Still, one thing has become clear: With the midterm elections just three months away, campaigns are largely on their own in the increasingly challenging task of protecting sensitive information and countering false or misleading content on social media.

The Democratic National Committee has worked to strengthen its own internal security protocols and encouraged state parties to do the same, according to Raffi Krikorian, who previously worked for Uber and Twitter and now serves as the DNC's chief technology officer.

But in an interview, he acknowledged there are limits to how much the national party can protect the thousands of Democratic campaigns across the country.

"We're providing as much assistance to campaigns as we can, but there's only so much we can do," Krikorian said.

"For all the high-level campaigns I'm worried, but at least there are people to talk to," he continued. "The mid-sized campaigns are at least getting technical volunteers, but the truly down-ballot campaigns, that's where the state parties and coordinated campaigns can help, but there's no doubt that this is an uphill battle when we're dealing with a foreign adversary."

Officials in both political parties have intensified cybersecurity efforts, although the known cases of interference have so far overwhelmingly focused on Democrats.

The DNC now has a staff of 40 on its technical team, led by Krikorian and other Silicon Valley veterans hired in the months after Russians hacked the party's email system and released a trove of damaging messages in the months before President Donald Trump's 2016 victory.

Top U.S. intelligence and homeland security officials raised new alarms Thursday about outside efforts to influence the 2018 and 2020 elections during a White House press briefing.

Homeland Security chief Kirstjen Nielsen said: "Our democracy is in the crosshairs," while Director of National Intelligence Dan Coats added: "We continue to see a pervasive messaging campaign by Russia to try to weaken and divide the United States."

Facebook said it removed 32 accounts from its site and Instagram because they were involved in "coordinated" political behavior and appeared to be fake. Nearly 300,000 people followed at least one of the accounts, which featured names such as "Black Elevation" and "Resisters" and were designed to manipulate Americans with particular

ethnic, cultural or political identities.

In many cases, House and Senate political campaigns said they're just beginning to adopt basic internal security protocols, such as two-step verification for all email, storage and social media accounts and encrypted messaging services such as Wickr.

There is no protocol in place for campaigns or national parties to monitor broader social media misinformation campaigns, however. Nor is there any sign that law enforcement is playing a proactive role to protect campaigns from meddling on a day-to-day basis.

The FBI has set up a Foreign Influence Task Force and intelligence agencies are collecting information on Russian aggression, but campaigns report no regular contact with law enforcement officials.

"At the end of the day, the U.S. government is not putting any type of a bubble around any (campaign). They do not have the authority, capacity or capability to do it," said Shawn Henry, a former senior FBI official who now leads the cybersecurity firm CrowdStrike, which works with political campaigns. "NSA is not sitting in the ISPs filtering out malicious traffic."

Henry added: "They've got to take pro-active actions themselves."

Earlier this month, Microsoft said it discovered a fake domain had been set up as the landing page for phishing attacks by a hacking group believed to have links to Russian intelligence. A Microsoft spokesman said this week that additional analysis confirmed the attempted attacks occurred in late 2017 and targeted multiple accounts associated with the offices of two legislators running for re-election. Microsoft did not name the lawmakers.

Sen. Claire McCaskill, D-Mo., said Russian hackers tried unsuccessfully to infiltrate her Senate computer network in 2017. Former Democratic U.S. Rep. Brad Ashford of Nebraska also recently confirmed that his 2016 campaign emails had been hacked by Russian agents.

Ashford, who narrowly lost his seat to Republican Don Bacon that year, said hackers obtained all of his campaign email correspondence with the Democratic Congressional Campaign Committee. He said he was notified of the breach in late July or early August 2016 by House Democratic Leader Nancy Pelosi's office.

Ashford has said he doesn't believe any of the stolen information ever went to Bacon or the Republican Party, and he doesn't know whether it made a difference in his race. He did face a series of anonymous political attacks on social media.

By their very nature, U.S. political campaigns can be a challenge to defend from a cybersecurity standpoint. They are essentially pop-up organizations that rely heavily on volunteers and are focused on a singular task—winning. In addition, high-level IT expertise costs money and campaigns typically run on tight budgets.

Some 2018 House campaigns have yet to hire basic communications staffers.

In the case of California Sen. Harris, who is considered a 2020 presidential prospect, her office plans to continue rooting out fake social media profiles on its own. They have had no contact with the FBI. They have reported the issue to Facebook in every case—not the other way around.

"It's on the forefront of everybody's mind," said Patrick McHugh, a former Senate campaign official who now leads the Democratic-aligned

super PAC Priorities USA.

He acknowledged the tremendous challenge for many campaigns.

"All it takes is one person on a campaign to make a mistake," McHugh said. "You're up against a foreign country. That's a pretty big adversary that can and will go to all ends to get in."