The Washington Post

Look for conservatives to go after DHS counter-disinformation work

Tim Starks

November 3, 2022

Welcome to The Cybersecurity 202! Halloween always generates talk about bad confections, complete with one city that has an Emperor of Acceptable Candy who makes rulings. You know what's a good candy that's hard to find? Jum-Blo.

Below: Election jurisdictions are waiting for cybersecurity help from CISA, and Emotet returns. First:

Here's another topic Republicans could probe if they seize control of the House : the Department of Homeland Security's initiatives to counter misinformation online by monitoring speech it considers dangerous.

- "Simply put: The American People do not approve of the Department engaging in unclear, unaccountable, and opaque efforts led by the Biden administration's ever-changing definition of 'truth,'" Rep. **John Katko** (R-N.Y.), the top Republican on the panel, said in a statement Tuesday. "Homeland Republicans continue to engage DHS to get answers and will continue to conduct intense oversight. We will continue to demand the highest levels of transparency by DHS with Congress and the public."

Katko is one of the more moderate members of his caucus and is retiring next year. **That he spoke out suggests how deeply Republicans are concerned about the DHS efforts, which they label censorship. The American Civil Liberties Union also raised concerns on Twitter:**

Meanwhile, Democratic lawmakers have largely supported the efforts, calling them important moves to counter online dis-information and misinformation.

The DHS efforts, especially under the Cybersecurity and Infrastructure Security Agency, aren't new. CISA launched its "Rumor Control" website for the 2020 election, and a Countering Foreign Influence Task Force began its work in 2018 (and later continued under another name).

Katko's statement came one day after the Intercept published a story on the DHS efforts to counter disinformation, which largely drew upon documents released in a federal lawsuit filed by conservatives trying to draw out information about the extent to which the government is monitoring onine discourse. **That story fired up conservatives and some liberals on Twitter, just as it drew criticism from people who work in the field to battle disinformation.**

The Intercept's story and Meta CEO **Mark Zuckerberg's** recent appearance on the "Joe Rogan Experience" podcast — where he discussed interactions with the FBI over a story about **Hunter Biden**'s laptop — attracted a lot more attention from the right to the issue, **Will Duffield**, a policy analyst at the libertarian Cato Institute think tank, told me.

- "Whether it comes from a lawsuit, whether it comes from a leak, whether it comes from Zuckerberg disclosing something, these weren't public communications between government and platforms in the first place," said Duffield, who studies speech and internet governance. "It's the hint of an iceberg" that makes people wonder what else might be happening, he said.

The defenders

Some people involved in CISA's counter-disinformation work rejected the notion that anything secretive was happening. Here's **Kate Starbird**, a disinformation expert at the University of Washington:

The former director of CISA, **Chris Krebs**, poked fun at a Fox News chyron about CISA's "Rumor Control" website. The site existed when Krebs served under **President Donald Trump**, and disputes about it with the White House contributed to Trump firing him. (He has since co-founded a consulting firm).

One of the writers of the Intercept story wasn't on board with how some others were receiving it. Here's Ken Klippenstein, who has said the left should also be concerned about the reporting:

Even before the agitation the Intercept story stirred up, **DHS has at times nonetheless felt compelled to back away from its disinformation work** amid largely conservative backlash. It scrapped plans for a Disinformation Governance Board.

Criticism of that board "spooked" DHS, according to **CNN's** Sean Lyngaas, after which DHS rejected a proposal that would partially spend money to counter election-related dis- and misinformation. A subsequent **ProPublica** story by Andrea Bernstein and Ilya Marritz detailed other abandoned efforts from a Biden administration that originally said it would make countering conspiracy theories a priority.

- A DHS spokesperson told ProPublica that it hasn't backed down from working "for over a decade to address disinformation that poses a threat to that security."

Should Democrats retain control of the House, they're likely to go the opposite direction of conservatives. Rep. **Yvette D. Clarke** (D-N.Y.), who chairs the Homeland Security Committee's cybersecurity panel, has said she favors legislation that would authorize DHS efforts like "Rumor Control" into law.

"The Federal government — and CISA in particular — has a role to play in confronting the mis- and disinformation narratives that jeopardize our faith in free and fair elections, and other issues that threaten our national security, public health and safety," she said at a January hearing.

The keys

The jurisdictions have sought help with election system cybersecurity through voluntary services offered by CISA like risk assessments and penetration tests, **NBC News**'s Julia Ainsley and Kevin Collier report. The waits have come because CISA is short-staffed, two people familiar with the delays told NBC News.

"The vast majority of voting machines are not connected to the internet, meaning a credible threat from foreign hackers on the election system as a whole is practically impossible," Ainsley and Collier write. "But some election information does run through the internet, like voting registration, official information about how and where to vote, and election officials' email systems. So it could be possible to delete voters from rolls or change the way a website projects an election winner, creating chaos and confusion."

In a statement to NBC News, CISA didn't deny the backlog and said it provided free cyber hygiene tests to 425 "election-related entities" across every U.S. state, Washington, D.C., and U.S. territories. The cyber hygiene tests are less labor intensive than the other tests.

Emotet is back

The notorious malware operation stopped sending malicious spam emails in mid-June, but it is back after nearly five months, **Bleeping Computer**'s Lawrence Abrams reports. The latest emails appear to be hijacking email reply chains to share Microsoft Excel attachments that are actually malicious.

"Emotet is a malware infection distributed through phishing campaigns containing malicious Excel or Word documents. When users open these documents and enable macros, the Emotet DLL will be downloaded and loaded into memory," Abrams writes. "Once loaded, the malware will search for and steal emails to use in future spam campaigns and drop additional payloads such as Cobalt Strike or other malware that commonly leads to ransomware attacks."

Emotet has been linked to ransomware families like Ryuk, Conti, BlackCat and Quantum. Those ransomware variants appeared to use Emotet to get into devices and networks, Abrams reports.