Digital threats multiply ahead of 2020 US elections

September 22 2019, by Rob Lever

Digital threats including misinformation and ransomware could threaten the integrity of the 2020 US election, security researchers say

It could be a manipulated video embarrassing a candidate. Or a computer voting system locked by ransomware. Or doubts about electronic voting

machines with no paper backups.

As Americans prepare for 2020 elections, digital threats to election security are multiplying, stoking fears of a tainted outcome.

Worries are running high following revelations of a wide-ranging misinformation campaign on Facebook and other social platforms, largely directed by Russian operatives, in 2016.

This was described in detail by special counsel Robert Mueller, whose office obtained several indictments for election interference.

Cyber interference and disinformation operations surrounding elections "are part of a much larger, ongoing challenge to democracies everywhere," said a report from Stanford University's Cyber Policy Center.

Maurice Turner, an election security specialist with the Washington-based Center for Democracy & Technology, said these threats could lead to "a negative impact on voter confidence" in 2020.

Deepfakes, nudes

The newest threat may be "deepfake" video and audio manipulated with artificial intelligence which can put words in the mouths of candidates.

It might even show "unflattering or abusive images of women and minority aspirants in an effort to discredit them," said Darrell West with the Brookings Institution's Center for Technology Innovation, in an online report.

Social media platforms like Facebook and Twitter will be closely scrutinized on how well they counter misinformation and manipulation during the 2020 US presidential election

"It is easy to manipulate still images or video footage to put someone in a compromising situation," West wrote.

Danielle Citron, a Boston University online safety expert, told a recent TedSummit talk that deepfakes "can exploit and magnify the deep distrust that we already have in politicians, business leaders and other influential leaders."

Deepfakes "can reinforce an idea for those who want to believe it and be

a distraction in the news cycle" even if they are debunked, Turner said.

Hardening defenses

Social media platforms like Facebook and Twitter will be closely scrutinized on how well they counter misinformation.

Experts say it will be increasingly difficult to counter automated accounts or "bots" that can amplify false news.

The failure to take a hard stand against manipulation in 2016 has likely "emboldened Russia to try again in 2020," wrote Stanford professor and ex-Facebook security chief Alex Stamos. Other efforts might come China, Iran or North Korea, he said.

Facebook, Google, Microsoft and Twitter security teams met this month with FBI, homeland security and intelligence officials to discuss collaboration on election threats.

It will be important to anticipate new threats, and not simply use methods from the past.