

NATO warned Russian election meddling an evolving threat that must be met

U.S. now believes other states, including China, are emulating Russia's tactics, Halifax forum told



A computer expert operates at the NATO Computer Incident Response Capability (NCIRC) technical centre, at NATO's military headquarters in Mons, southwestern Belgium. (Yves Logghe/Associated Press)

A NATO draft report says the problem of Russian meddling in democratic elections continues to evolve and alliance members must be ready to meet the threat.

U.S. Democratic congresswoman Susan Davis told NATO's science and technology committee meeting in Halifax that Russian interference continued in the early stages of the recent mid-term elections in her country, although not on the scale seen during the 2016 presidential election.

- The House: Threat assessment at Halifax International Security Forum

- Canada joins allies in condemning ‘malicious’ Russian cyberattacks

Davis says technology companies shut down hundreds of fake accounts aiming to disrupt the elections.

She says some of the accounts identified and deleted were also Iranian, and the U.S. government now believes other states, including China, are emulating Russia’s tactics.

Russians still ‘a step ahead of us’

Giorgi Kandelaki of the delegation from Georgia, which is seeking closer ties to NATO, told the committee that he was the victim of a Russian-inspired disinformation campaign that popped up on Facebook news feeds.

Kandelaki says his experience taught him that the Russians are still “a step ahead of us” and he added that so far the threat response has been largely through “conferences and seminars.”

The report was presented as part of the NATO Parliamentary Assembly meeting in Halifax.

Defending against cyberattacks

James Stavridis, a retired U.S. Navy admiral who once served as the top NATO commander, spoke to CBC’s Wendy Mesley on *The Weekly* about the new NATO Cyber Operations Centre in Belgium, which NATO defence ministers agreed to create last year.

Canada hasn’t signed on so far in the alliance’s bid to get ready for cyber warfare. Defense Minister Harjit Sajjan has said he first wants to make sure Canada has “the right capabilities so we are able to contribute appropriately as well.”

Vulnerabilities in cybersecurity could leave electric grids open to attack, Stavridis said

He said the new centre is to be staffed by military personnel and civilians from each of the 29 nations in NATO and will begin by protecting NATO military cyberactivities. Over time, the idea is to expand it, so it can participate in the

defense of the electrical grid in any of the NATO countries.

As for social media meddling in the 2019 Canadian general election, Stavridis said it should be expected.



Retired U.S. Navy admiral James Stavridis, former supreme allied commander of NATO, said the new cyber operations centre in Belgium is a 'big, bold idea' that is 'just starting out' to protect NATO countries against cyberthreats. (CBC)

"One of Russia's principle, strategic objectives is to break that transatlantic link, to force the U.S. and Canada away from European partners and weaken the alliance," he said.

Stavridis said one message track that could be spread throughout the electoral process is that involvement in NATO is not necessary, and he predicted "Russian activity will play that way in the social networks."

With files from CBC News

CBC's Journalistic Standards and Practices|About CBC News

Source: <https://www.cbc.ca/news/canada/nato-summit-draft-report-russian-election-meddling-1.4910748>

[Disclaimer]