Cyberattacks on US healthcare raise alarms among senators

April 23 2020, by Gopal Ratnam, Cq-Roll Call

Credit: CC0 Public Domain

A bipartisan group of senators wrote to the top U.S. cybersecurity officials asking them to step up monitoring, warnings and, if needed, counterstrikes against a host of foreign hackers targeting the U.S. health

care system and pharmaceutical companies through cyberattacks.

In an April 20 letter to Gen. Paul Nakasone, head of the military's U.S. Cyber Command, and Christopher Krebs, the top Homeland Security Department official at the Cybersecurity and Infrastructure Security Agency, the lawmakers said they were alarmed at a spate of recent reports from private threat intelligence companies that "Russian, Chinese, Iranian, and North Korean hacking operations have targeted the healthcare sector and used the coronavirus as a lure in their campaigns."

The lawmakers include Sens. Richard Blumenthal, D-Conn., Mark Warner, D-Va., Edward J. Markey, D-Mass., Tom Cotton, R-Ark., and David Perdue, R-Ga.

Chinese attackers are staging espionage campaigns aimed at health care and pharmaceutical companies that are responding to the COVID-19 pandemic, the lawmakers said, citing recent reports by FireEye and other private companies that gather intelligence on cyber threats.

"The cybersecurity threat to our stretched and stressed medical and public health systems should not be ignored. Prior to the pandemic, hospitals had already struggled to defend themselves against an onslaught of ransomware and data breaches," the lawmakers said in their letter.

They wrote that Cyber Command and CISA should share threat intelligence and indicators of compromise with the health care sector, coordinate with officials from the Department of Health and Human Services, the FBI, and the Federal Trade Commission to raise public awareness on cyberattacks, and brief state National Guard teams on threats so they can defend critical health care infrastructure from breaches.

If necessary, the Cyber Command must be prepared "to defend forward

in an attempt to detect and deter attempts to intrude, exploit, and interfere with the healthcare, public health, and research sectors," the lawmakers said.

Defending forward is another term for counterattacking in cyberspace that includes dismantling infrastructure used by adversaries to stage attacks on U.S. interests.

Congress and President Donald Trump have expanded Cyber Command's powers to conduct such offensive operations, and the military carried out similar efforts ahead of the 2018 midterms to shut down Russian intervention.

Code-named Operation Synthetic Theology, Cyber Command sent teams of cyber experts to Macedonia, Ukraine and Montenegro to monitor Russian internet traffic and sent direct messages to Russian agents involved in trying to interfere in the 2018 midterms, warning that they were identified and being monitored. The command also temporarily shut down the Internet Research Agency, a Kremlin-backed troll farm in St. Petersburg.