Senate Panel to Hold Hearing on Suspected Chinese Hacking Incidents

By David Shepardson | November 19, 2024

Email This Subscribe to Newsletter

Article **0 Comments**

Ouça este artigo
3 min

A U.S. Senate Judiciary subcommittee overseeing technology issues will hold a hearing Tuesday on Chinese hacking incidents, including a recent incident involving American telecom companies.

The hearing to be chaired by Senator Richard Blumenthal will review the threats “Chinese hacking and influence pose to our democracy, national security, and economy,” his office said, adding the senator plans “to raise concerns about Elon Musk’s potential conflicts of interest with China as Mr. Musk becomes increasingly involved in government affairs.”

Musk, the head of electric car company Tesla TSLA.O, social media platform X and rocket company SpaceX, emerged during the election campaign as a major supporter of U.S. President-elect Donald Trump. Trump appointed him as co-head of a newly created Department of Government Efficiency to "slash excess regulations, cut wasteful expenditures, and restructure Federal Agencies."

Musk, who was in China in April and reportedly proposed testing Tesla's advanced driver-assistance package in China by deploying it in robotaxis, did not immediately to requests for comment.

The hearing will include CrowdStrike Senior Vice President Adam Meyers and Telecommunications Industry Association CEO David Stehlin, Strategy Risks CEO Isaac Stone Fish and Sam Bresnick, research fellow at the Center for Security and Emerging Technology at Georgetown University,

Last week, U.S. authorities said China-linked hackers have intercepted surveillance data intended for American law enforcement agencies after breaking in to an unspecified number of telecom companies, U.S. authorities said on Wednesday.

The hackers compromised the networks of "multiple telecommunications companies" and stole U.S. customer call records and communications from "a limited number of individuals who are primarily involved in government or political activity," according to a joint statement released by the FBI and the U.S. cyber watchdog agency CISA.

The announcement confirmed the broad outlines of previous media reports that Chinese hackers were believed to have opened a back door into the interception systems used by law enforcement to surveil Americans' telecommunications.

It follows reports Chinese hackers targeted telephones belonging to then-presidential and vice presidential candidates Donald Trump and JD Vance, along with other senior political figures, raised widespread concern over the security of U.S. telecommunications infrastructure.

Beijing has repeatedly denied claims by the U.S. government and others that it has used hackers to break into foreign computer systems.

Last month, a bipartisan group of U.S. lawmakers asked AT&T T.N, Verizon Communications VZ.N and Lumen Technologies LUMN.N to answer questions about the reporting hacking of the networks of U.S. broadband providers.