Democracy Dies in Darkness

Congress funds removal of Chinese telecom gear as feds probe home router risks

Legislative and executive branch actions highlight concerns that phone and internet networks are vulnerable to Beijing-sponsored hackers.

Today at 7:05 a.m. EST

7 min 46

By Eva Dou, Cate Cadell and Joseph Menn

Congress approved $3 billion Wednesday for a long-languishing project to cull Chinese equipment from networks nationwide over fears they are vulnerable to cyberattacks, underscoring the risk Beijing-sponsored hackers pose to phone and internet networks.

The new funding comes as the Commerce Department reviews whether to ban routers made by the Chinese-owned company TP-Link, which account for more than half of the U.S. retail router market.

The actions reflect the heightened attention among Washington policymakers to the threat posed by Chinese state-linked hackers. U.S. officials revealed the “Volt Typhoon” hack last year and in recent months have expressed alarm over the even bigger “Salt Typhoon” hack. In both cases, Chinese government hackers successfully penetrated major U.S. phone networks and critical infrastructure facilities, and U.S. officials said they still have not been able to expel the Salt

Typhoon interlopers.

The Justice, Defense and Commerce Departments have all been scrutinizing TP-Link, the most widely used home router in the United States, with Commerce considering a potential ban of the devices, two people familiar with the matter said Wednesday, speaking on the condition of anonymity because of the matter's sensitivity, and confirming an earlier report by the Wall Street Journal.

"The Biden administration is under significant pressure to demonstrate strength and take decisive action," said Craig Singleton, senior China fellow at the Foundation for Defense of Democracies think tank.

There is growing bipartisan support in Washington for decoupling the U.S. telecommunications sector from China's factory floor to reduce the risk of Beijing-sponsored cyberattacks and to support U.S. industry, an approach that just five years ago was widely considered economically and diplomatically unfeasible. The drive began under the first term of President-elect Donald Trump, who is expected to take it up again, in a rare point of policy continuity with the Biden administration.

"We have to get the horses back in the barn," Brendan Carr, Trump's pick for Federal Communications Commission chairman, said at this month's commission meeting, pledging to prioritize battening down communications networks. "Job One needs to be … closely coordinating with all of these other cyber-related agencies, focused very narrowly on getting this thing under control."

As part of the annual defense budget green-lit on Wednesday, Congress approved $3 billion to complete the "Rip and Replace" program to remove equipment made by the Chinese telecommunications manufacturing giants Huawei Technologies and ZTE from rural U.S. phone networks. The initiative was begun in 2020 by the Trump administration, but FCC officials soon realized they needed more than double the original funding to finish the job, largely stalling the program.

Sen. Maria Cantwell (D-Washington) praised the funding for helping to “ensure small and rural providers can finally remove these vulnerable systems, secure their networks, and close potential back doors to foreign adversaries.” She said Washington state still has 63 sites with unsecured equipment, with other states facing similar situations.

Marc Martin, partner at Perkins Coie and a former FCC official, said there was little historic precedent for the rip-and-replace program, with China’s strength in manufacturing advanced technologies only emerging as a concern in recent years.

“It’s not like in the Cold War that Russia was making sophisticated telecom network equipment commercially,” he said. “Whatever they were making wasn’t really competitive. It has been a more recent development with China.”

Lawmakers and agencies have also been combing through the tech industry more broadly, zeroing in on areas where Chinese firms command a majority share in U.S. consumer technology products.

The Commerce Department’s recently formed Office of Information and Communications Technology and Services program, under the Bureau of Industry and Security, is taking a key role in the probes, the people said. The program was formed under the authority from a 2019 Trump executive order in which he declared foreign infiltrations into U.S. telecom networks a national emergency.

While encouraged that the government is paying attention, some experts said they had concerns about consistency given the poor state of router security in general. “This would be stronger if coupled with policy that requires baseline security considerations for consumer devices, as well as a means to automatically update them,” said James Shank, director of product, data and analytics at security firm SpyCloud.

Commerce leading the charge suggests that market factors could be playing as much of a role as current security issues, security professionals said. The

department is acting under a lower threshold, they said, looking at possible supply-chain risks from China rather than urgent national-security threats.

The three agencies declined to comment on Wednesday. TP-Link did not respond to a request for comment.

“The recently announced federal investigations into this company are a step in the right direction, and I hope the executive branch will take action to protect our country,” said Rep. John Moolenaar (R-Michigan), chairman of the House Select Committee on the Chinese Communist Party, who had called for the Commerce Department to probe TP-Link earlier this year.

The Chinese Embassy in Washington did not respond to a request for comment on the rip-and-replace funding or the TP-Link probes. Beijing’s Foreign Ministry has previously decried such actions, accusing Washington of using national security as a pretext for suppressing Chinese companies in the U.S. market.

TP-Link is owned by TP-Link Technologies Co., Ltd., a company headquartered in Shenzhen, China, and says its routers are shipped to more than 170 countries worldwide.

TP-Link has faced increasing scrutiny over its ties to Beijing. The company’s dominance in the home internet router market, coupled with its rapid growth in recent years, has raised alarms among U.S. lawmakers and national security experts about potential vulnerabilities in its products.

The firm has a history of security flaws, and users have complained that it is hard to change configurations to make the routers more secure. In addition, some fault TP-Link for failing to consistently correct flaws once they have been discovered.

In October, Microsoft said TP-Link small home and office routers had been targeted by a Chinese-linked hacking group that successfully stole the credentials from multiple Microsoft customers.

No officials have publicly asserted any link between the devices and the Volt Typhoon and Salt Typhoon hacks, the latter of which led to the deep penetration of U.S. telecommunication providers including AT&T and Verizon. Those attacks allowed Chinese spies to listen in on conversations by political leaders and relied on out-of-date and therefore unpatched equipment from Cisco Systems and other U.S. vendors.

In August, Moolenaar's committee sent a letter to Commerce Secretary Gina Raimondo, urging a formal investigation into TP-Link. The committee highlighted the sale and use of TP-Link devices on U.S. military bases, warning that it could allow state-linked hackers to target sensitive defense information.

Analysts say actions like rip and replace and the TP-Link probes highlight a shift in how agencies handle cyberthreats — particularly from China.

"It underscores a broader evolution in how agencies approach cybersecurity — focusing on preemptive strategies to mitigate risks from state-sponsored cyberthreats, particularly from China," said Cliff Steinhauer, director of information security and engagement at the nonprofit National Cybersecurity Alliance.

While funding for the rip-and-replace program was approved as part of the defense budget on Wednesday, the legislation passed without including the Countering CCP Drones Act, despite strong advocacy from lawmakers. The proposed act would have banned the Chinese drone giant DJI from operating or selling its products in the United States.

Ellen Nakashima contributed to this report.