CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

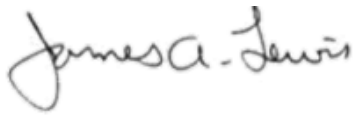
March 22, 2024

The Honorable Robert E. Latta
House Committee on Energy and Commerce
Subcommittee on Communications & Technology
2125 Rayburn House Office Building
Washington, DC 20515-6115

Dear Chairman Latta,

Thank you for the opportunity to testify before the Subcommittee on Communications and Technology on Thursday February 15, 2024, at the hearing entitled, "Securing Communications Networks from Foreign Adversaries". Please find below my responses to the additional questions submitted by Rep. Russ Fulcher and Rep. August Pfluger.

Sincerely,



James A. Lewis
Senior Vice President; Pritzker Chair
Director, Strategic Technologies Program

WWW.CSIS.ORG
1616 RHODE ISLAND AVENUE NW
WASHINGTON, DC 20036
TEL: (202) 887.0200
FAX: (202) 775.3199

The Honorable Russ Fulcher

1. Mr. Lewis, when I asked about China's potential to undermine reliability and/or quality of U.S. water and power systems through entry of malware (like "Volt Typhoon") through older WiFi routers, modems, and other network equipment, you noted not only to be "nervous" if those routers, modems, and other network equipment were more than three years old, but that this is part of a larger strategy by China against U.S. critical infrastructure. You also noted the targeting of smaller subcontractors to these water and power providers as especially vulnerable to malware that gets in and infects a network through connections to it. Why did you highlight smaller subcontractors?

    a. Does NTIA have adequate understanding of the risks when it comes to determining the scale of this problem, especially when it comes to smaller contractors?

    b. I am thinking particularly of the ability of hackers to flood routers with Distributed Denial of Service attacks, credential stuffing, and other problems. Is it these or other concerns, or both?

Unsurprisingly, attackers prefer to go after less well defended targets. This is not a new tactic, but the Administration has reported that China has gained access to less-well defended Small office/ Home office (SOHO) routers to enter the networks of critical American critical infrastructure. Individual and smaller contractors do not have the resources that may be required to defend against a large, well-resourced, and skilled opponent.

2. The ROUTERS Act asks the Assistant Secretary of Commerce to conduct a study on the national security risks posed by "routers, modems, and devices that combine a modem and router" …that come from China or one of the other "covered countries."

    a. Do you envision this study creating a requirement for CFIUS review of this equipment?

    b. Do you think including risks that come from connected software applications could also be helpful? I am thinking of building on Executive Order 14034 that directed the Secretary of Commerce to look at "connected software applications" to such network equipment, as well as Executive Order 13872 that declared the "exploitation" of Information and Communications Technology and Services (ICTS) due to risks to the "resiliency of critical infrastructure."

The ROUTERS Act would usefully require Department of Commerce to study the national security risks posed by "routers, modems, and devices that combine a modem and router" that come from China or one of the other "covered countries." This would allow us to gage the risk of the problem. Some sources suggest that China subsidizes the cost of home routers, and if true, this would be consistent with the long-standing Chinese practice to use subsidies to gain commercial and intelligence advantage.

The Department's new office Information and Communications Technology and Services (ICTS) can use the authorities of the Defense Production Act to undertake this survey. There is undoubted risk

and the issue for the Administration is to accelerate data collection and devise remedies, perhaps using CFIUS or the regulatory authorities of the ICTS Office, should be accelerated.

3. When I asked about Russia's similar behavior as China when it comes to breaking into routers, modems, other network equipment, you said that in some ways Russia is both "more aggressive" and "more skilled" than China, and that Russia has both interfered with U.S. critical infrastructure. Can you expound upon that, and how what questions would you want to see from a risk assessment?
    a. Any different questions or inquiries if we are talking about breaking into routers, modems, or other network equipment if we are talking about private U.S. company data operating here or the EU versus U.S. government agency data?

Russian entities (such as GRU Military Unit 26165) have taken advantage of SoHo routers to create botnets, aggregating number of home computers into botnets they control and can use for either disruption or espionage. Russia remains the most formidable of our opponents in cyberspace (although China, Iran and North Korea have all improved significantly). Russia has the benefit, however, of being able to use Russian cybercrime gangs to complement efforts by the GRU and other Russian agencies. While the FBI and the Department of Justice have recently undertaken actions to remove Russian-installed malware on SOHO devices, older systems remain vulnerable. This problem will grow as more devices connect to the internet via routers.

The Honorable August Pfluger

In 2023, CSIS conducted several wargames for a Chinese invasion of Taiwan and has concluded that the United States, Taiwan, and Japan could defeat a conventional amphibious invasion from China, but at a high human, economic, military, and political costs. CSIS set this conflict for 2026 and limited each side to its real life demonstrated military capabilities. Other specialists have speculated that an invasion could happen anywhere from 2027 to 2036. It is my belief that due to President Biden's weak foreign policy strategy of appeasement, the likelihood of some level of conflict from China in Taiwan is likely more in the near term than 2036.

1. In your opinion, what is the likelihood of a Chinese invasion of Taiwan in the near future?
2. In your wargame exercises, what was the prevailing thought of how China would target telecommunications networks?
3. Do you agree that the technology space is a key area from China to move ahead of the US?

China is unlikely to invade Taiwan. China has studied the Russian experience in Ukraine and has gathered that invasions do not always go smoothly. China has reportedly gamed out the effect of Ukraine-style sanctions and determined that even a less robust set of sanctions levied against it I response to an innovation of Taiwan could do unacceptable harm to its already weak economy. While Russia and Putin have friends in the United States, China realizes it has none and is likely to face unified American opposition. Attacking Tawain would badly damage its international standing and rally many more countries against it. There are anecdotal reports that Chinese leaders have privately signaled to Taiwan that if it does not declare independence, they

will not invade. Of course, an uncontrollable surge of nationalist sentiment in China could force Xi to take action against Taiwan and a perception of disarray in the United States could increase risk, but China probably hopes that its efforts to undermine Taiwan politically can lead unification without the use of force. One caveat to this is that if Xi has decided he will be the leader of China who regains Taiwan, since his third term (if he does not decide to continue in office) expires in a few years.

As addressed during the hearing, there are several steps this Congress can take to address outstanding national security threats, one of which is funding the Rip and Replace. program to remove untrusted Chinese telecommunications technology in our systems.

1. Why do you agree that this is a vital national security issue?
2. How could the CCP exploit these vulnerabilities and unnecessary gaps in our national security?
3. What enhancements to national security would be realized if Congress immediately prioritized full funding for the FCC's Rip and Replace program?

Rip and Replace has made considerable progress in the US but a number of smaller telecom companies (some located near and servicing customers from sensitive government facilities) continue to rely on Huawei infrastructure equipment and cannot afford to replace it. Continued use of Huawei equipment creates opportunities for China to exploit or disrupt traffic and data on those networks. Continuing Rip and Replace, although costly, is essential to eliminate this risk.