Documents for the Record – 04.30.25

1. A letter from Graphiant to Committee on Energy and Commerce leadership.
2. A March 24, 2025, statement entitled, “China Unveils Game-Changing Weapon That Could Decide Future Wars.”
3. An April 30, 2025, letter from Members of Congress to FCC Chairman Brendan Carr.

graphiant

The Honorable Richard Hudson
Chairman
Subcommittee on Communications and Technology
House Committee on Energy and Commerce
2112 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Doris Matsui
Ranking Member
Subcommittee on Communications and Technology
House Committee on Energy and Commerce
2206 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Brett Guthrie
Chairman
House Committee on Energy and Commerce
2161 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Frank Pallone, Jr.
Ranking Member
House Committee on Energy and Commerce
2107 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Hudson and Ranking Member Matsui,

Thank you for holding today's hearing, *Global Networks at Risk: Securing the Future of Telecommunications Infrastructure*. Below, find my statement for the record.

Sincerely,

Ali Shaikh
Chief Product Officer
Graphiant

The Problem

In 2025, the United States continues to face the two-fold problem of cyber security risks: threats to our national security and threats to our business landscape. Data is the lifeblood of innovation as well as the means to attack the nation. Inappropriate use of applications with sensitive data can be exploited, foreign adversaries can get into our critical infrastructure and take advantage of unclosed weaknesses, and we will have no means of enforcing compliance and audit if we do not upgrade our critical infrastructure.

A Solution

These are solvable problems; US companies have a range of solutions to meet the needs of our government and our citizens. It is of the highest importance that we advocate for the accelerated deployment of key capabilities that give us the abilities to ensure compliance and audit for our

regulators and oversight bodies, protect our national interests from threats, and deliver a better infrastructure for individuals and businesses to have better trust.

The best analogy to describe what we should expect as an outcome is that like we use services like Google Maps and Apple Maps that in real-time allow us to see where we are on the planet, and even allow us to see our loved ones travel safely, we should expect real-time ability to see what is happening to our data. We should expect from our infrastructure to tell us where is our data, where it's going and did it safely go from point A to point B without breaking any laws or being stolen.

Key Capabilities

1. Real-Time Oversight: Provide continuous monitoring of network traffic, allowing teams to detect and respond to threats promptly.

2. Advanced Profiling: Utilize sophisticated techniques, identify and categorize data flows, ensuring that sensitive information is handled appropriately.

3. Data Sovereignty: Ensure that data remains within approved geographic boundaries is crucial for compliance with data sovereignty laws.

About Graphiant

Graphiant is a US company that focuses on providing Data Assurance. These are services designed to provide comprehensive visibility, control, and compliance. Graphiant offers visibility into network traffic, enabling real-time monitoring and management. Graphiant employs advanced profiling methods and real-time telemetry to ensure that data is secure, efficient, and compliant.

Conclusion

Graphiant offers comprehensive solutions for modern networking challenges to deliver Data Assurance. By providing real-time visibility, advanced profiling, and compliance management, Graphiant empowers the United States to mitigate risks, enhance performance, and maintain control over their networks. These critical capabilities are essential for dealing with dynamic threats, increasing data complexity, and meeting regulatory requirements to fix our national security crisis.

China Unveils Game-Changing Weapon That Could Decide Future Wars

Published Mar 24, 2025 at 11:31 AM EDT Updated Mar 24, 2025 at 9:10 PM EDT

https://www.newsweek.com/china-unveils-game-changing-weapon-that-could-decide-future-wars-2049477

China has developed a device capable of cutting reinforced undersea cables thousands of feet below the ocean's surface.

The innovation comes amid concerns that Chinese vessels are targeting subsea infrastructure—threatening not only civilian but also military communications during a crisis.

Newsweek reached out to the Chinese embassy in Washington, D.C. with an emailed request for comment.

Why It Matters

Since early 2024, Chinese ships have been implicated in several cases of suspected cable sabotage, including in the Baltic Sea and around Taiwan, the self-ruled island claimed by China. The vessels were discovered to be in the area when the damage occurred, with investigators citing evidence such as anchor dragging as a likely cause.

Meanwhile, China has seen a rise in patent filings for tools designed to cheaply and efficiently sever submarine cables—vital infrastructure that carries more than 95 percent of global communications.

What To Know

The new invention was designed by the China Ship Scientific Research Center and its partner, the state-owned Laboratory of Deep-Sea Manned Vehicles, the *South China Morning Post* reported Saturday.

It can reportedly slice cables at depths of up to 4,000 meters (13,123 feet)—twice as deep as the deepest underwater cables currently in use.

The tool was first made public last month in the Chinese-language journal *Mechanical Engineer*.

The report marks the first time this capability has been unveiled by any country, despite its stated purpose of enabling civilian salvage and mining operations on the ocean floor.

Developed specifically for deployment on submersible vehicles such as the *Fendouzhe* and *Haidou-1*, the device's titanium alloy covering and specialized seals can withstand the intense pressures of that depth for long periods, *Interesting Engineering* cited the authors as saying.

A grinding wheel covered in diamond edges, spinning at a rapid 1,600 revolutions per minute, gives the device the ability to make short work of the protective steel layer encasing a cable.

he device has put China watchers on alert over its potential for more aggressive use, as well as the Chinese government's legal ability to compel cooperation from private companies—raising fears about the disruption of U.S. military communications across the network of Pacific bases including Guam, *SCMP* wrote.

What's Been Said

Bonnie Glaser, the managing director of the U.S. Indo-Pacific Program's German Marshall Fund, wrote on X, formerly Twitter: "Beijing insists it isn't responsible for cutting undersea cables. So why did it just unveil a powerful deep-sea cable cutter that can sever lines at depths of up to 4,000 meters?"

Theresa Fallon, founder and director of the Centre for Russia Europe Asia Studies in Brussels, wrote on X: "Beijing's underwater deep-sea, cable-cutting device makes explanations of 'it was just an accident' far harder to swallow."

Chinese embassy spokesperson Liu Pengyu told *Newsweek*: "We oppose unfounded attacks and smears against China. This tool, developed by China independently, is used in marine scientific research. The U.S. and some European countries also have similar technology. China attaches great importance to protecting undersea infrastructure and has been and will continue to work with the international community to protect undersea cables."

What's Next?

Investigations into suspected Chinese cable sabotage are ongoing, including a recent incident involving a Chinese-crewed vessel sailing under a Togo flag of convenience.

The ship was detained by Taiwanese authorities in February near where a cable linking Taiwan's main island with outlying Penghu County had been damaged.

Update 3/25/25, 1:10 p.m. ET: This article has been updated with a comment from the Chinese embassy.

Congress of the United States
House of Representatives
Washington, DC 20515–4311

April 30, 2025

The Honorable Brendan Carr
Chairman
Federal Communications Commission
45 L Street NE
Washington, D.C. 20554

Dear Chairman Carr:

Firstly, we write to commend your decision to establish the new Council for National Security within the Federal Communications Commission (FCC), a crucial step in safeguarding America's telecommunications infrastructure. Congress stands ready to work with you on this initiative to reduce America's dependence on foreign adversaries, mitigate cyberattack vulnerabilities, and ensure U.S. supremacy in critical technologies.

As you know, the House Energy and Commerce Committee has worked diligently to combat the People's Republic of China's (PRC) efforts to leverage private companies to create backdoors in our telecommunications infrastructure. For example, the House of Representatives just recently passed H.R. 866, the ROUTERS Act, to safeguard Americans' communications networks from foreign-adversary controlled technology, including routers, modems, or devices that combine both. Additionally, in the 118th Congress, the House passed H.R. 7521, the Protecting Americans from Foreign Adversary Controlled Applications Act, which prevents foreign adversary-controlled applications from targeting, surveilling, and manipulating Americans through online applications like TikTok. Congress also worked to ensure that the Secure and Trusted Communications Networks Reimbursement Program, or the "Rip and Replace" program, received proper funding to remove untrusted equipment such as Huawei and ZTE from our networks.

Last year, the House Committee on Homeland Security and the Select Committee on the Chinese Communist Party released their Joint Investigation report into Shanghai Zhenhua Heavy Industries Company (ZPMC), a PRC-owned and operated company. The investigation yielded that ZPMC, or a third-party company contracted with ZPMC, installed cellular modems onto STS cranes currently operational at U.S. ports. These installations fall outside the scope of any contract between the affected U.S. ports and ZPMC. The modems created an obscure method to

collect information and bypass firewalls in a manner that could potentially disrupt port operations.[1]

Even more recently, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) reported that the Chinese-made Contec CMS8000 patient monitors contained a hard-coded IP address linked to an unidentified third party, allowing for reverse backdoor functionality.[2] This vulnerability allows for remote access of the medical device and may allow for potential manipulation, risking patient safety and compromising sensitive health data.

These are just a few examples of how the CCP will use every tool at its disposal to undermine U.S. economic and national security interests to further its agenda. The recent proliferation of cybersecurity incidents underscores the need for the entire federal government to work together to address and deter cyber threats. We write to you today because we believe there is more the FCC can do to reduce the likelihood of such incidents.

As the backbone of the Internet, routers play a critical role in securing communications for consumers and businesses. When these devices are insecure, they can serve as gateways for cyberattacks. For example, weak, default, or easily predicted passwords make routers vulnerable to exploitation. Malicious actors can exploit these vulnerabilities in routers to disrupt service, steal sensitive data, or even launch attacks against critical infrastructure.

It has been reported that TP-Link, a Chinese company, owns roughly 65% of the routers used in U.S. homes and small businesses. Additionally, the Department of Defense and other federal government agencies have used TP-Link Routers before.[3] Multiple TP-Link routers have been added as to the National Institute of Science (NIST) National Vulnerability Database for containing a directory traversal vulnerability, allowing unauthenticated remote attackers to access sensitive files by sending specially crafted requests.[4]

We are increasingly concerned about the prevalence of these devices and that unsecure routers may allow the CCP to surveil American data or disrupt our networks. Although the Department of Commerce is reviewing whether or not to ban routers made by Chinese-owned companies in

---

[1] U.S. House of Representatives Committee on Homeland Security, Subcommittee on Transportation and Maritime Security and U.S. House of Representatives Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party. *Handling Our Cargo: How the People's Republic of China Invests Strategically in the U.S. Maritime Industry*. Washington: Select Committee on the CCP, 12 September 2024. https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/Joint%20Homeland-China%20Select%20Port%20Security%20Report-compressed.pdf

[2] U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency. *Contec CMS8000 Contains a Backdoor*, 30 January 2025. https://www.cisa.gov/sites/default/files/2025-01/fact-sheet-contec-cms8000-contains-a-backdoor-508c.pdf

[3] Somerville, Heather, et al. "U.S. Weighs Ban on Chinese-Made Router in Millions of American Homes." Wall Street Journal, 24 Dec. 2024. https://www.wsj.com/politics/national-security/us-ban-china-router-tp-link-systems-7d7507e6

[4] U.S. Department of Commerce, National Institute for Standards and Technology. "CVE-2015-3035 Detail." *National Vulnerability Database*, 21 April 2015. https://nvd.nist.gov/vuln/detail/CVE-2015-3035

the future, many of these devices remain on our networks, which nefarious actors could still leverage.

With the new Council for National Security, the FCC can take various actions to mitigate cybersecurity risks associated with unsecure routers. The FCC could leverage equipment authorization through the Telecommunications Certification Body to require routers to allow only uniquely identifiable devices known to the household and securely authenticated by the network owner onto a customer's network. These steps represent broadly accepted minimum security practices under NIST guidance and are necessary first steps toward protecting our nation's consumers and networks from cyber risks. Other immediate-term options, such as prohibiting any new sales of TP-Link routers, or requiring ISPs to block new TP-Link routers from being added to home networks, would stop the influx of these devices on networks. Additionally, as we think beyond TP-Link routers, ISP authentication will strengthen U.S. networks' ability to defend themselves against future untrusted Internet of Things (IoT) devices joining their networks.

We are confident that, under your leadership, we can advance national cybersecurity initiatives and create robust strategies to strengthen U.S. networks against cybersecurity threats. Together, we can foster a secure digital environment that instills trust and confidence among users nationwide.

Sincerely,

August Pfluger
Member of Congress

Robert E. Latta
Member of Congress

Earl L. "Buddy" Carter
Member of Congress

Jay Obernolte
Member of Congress

Nathaniel Moran
Member of Congress

Russ Fulcher
Member of Congress

Gus M. Bilirakis
Member of Congress

Nicholas A. Langworthy
Member of Congress

Troy Balderson
Member of Congress

Erin Houchin
Member of Congress