COMMITTEE ON HOMELAND SECURITY

Ranking Member Bennie G. Thompson

FOR IMMEDIATE RELEASE

Hearing Statement of Cybersecurity & Infrastructure Protection Subcommittee Rep. James Walkinshaw (D-VA)

Securing Global Communications: An Examination of Foreign Adversary Threats to Subsea Cable Infrastructure

November 20, 2025

Approximately 97 percent of global data traffic travels through subsea cables. Subsea cables support $9 trillion worth of trade each day, carry sensitive communications for national defense and intelligence operations, and ensure critical functions continue to seamlessly operate.

However, many subsea cables are poorly protected and are primarily vulnerable to accidents or negligence. Although a limited number of malign actors can deliberately disrupt cables, as the price of unscrewed underwater vehicles decrease, these vehicles may fall into the hands of non-state actors enabling them to dismantle essential global networks.

The urgency of better securing undersea cables hits close to home. According to a recent study by the Joint Legislative Audit and Review Commission in Virginia, an estimated seventy percent of global internet traffic passes through networks in Northern Virginia.

That makes our region one of the most important digital exchange points in the world, connecting federal agencies, critical industries, and global communication pathways. The information moving through these networks depends on the steady and secure operation of subsea cables that come ashore along the East Coast. Regardless of the cause, when those links are disrupted abroad, the strain is felt here at home. U.S. adversaries also continue to seek mechanisms to disrupt the entire system and ensure their targets remain vulnerable to threats.

Russia has spent money to develop platforms to target undersea infrastructure and the People's Republic of China has targeted subsea cables to sabotage Taiwan. In late 2024, two subsea cables in the Baltic Sea were severed in close succession, cutting connections between several European nations.

Officials in the region described the events as hybrid attacks and pointed to suspicious activity by vessels tied to Russia's shadow fleet. The interruption triggered rerouting of data traffic across alternative paths, which produced congestion on major routes that ultimately connect to the communications infrastructure serving Northern Virginia. Soon after, another rupture between Estonia and Finland affected both telecommunications and energy transmission. Authorities identified abnormal maritime behavior by a Russian linked vessel as a likely cause.

And earlier this year, Taiwan detained the crew of a Chinese operated ship after one of its critical cables near the Matsu Islands was cut. That incident followed recurring patterns of anchor dragging and location spoofing by vessels operating near sensitive undersea infrastructure. These events reveal a troubling pattern. Foreign adversaries with both capability and intent are increasingly probing or threatening these networks. Some incidents may have been deliberate acts, while others may represent

reckless behavior intended to signal strategic pressure. In either case, the vulnerabilities exposed are clear.

The United States must ensure that our defenses and preparedness match the scale of the threat. The Department of Homeland Security, CISA, the Coast Guard, and our interagency partners all have essential roles, but current efforts remain fragmented. Responsibilities are divided across multiple federal entities and private operators, which complicates coordination and slows action during emergencies. In considering the roles of these critical agencies, it is also important to acknowledge the strain placed on their missions when resources are diverted away from core security responsibilities.

The Trump administration has repeatedly proposed cuts to critical infrastructure protection programs within the Department of Homeland Security and is shifting personnel and funding toward large-scale deportation efforts. Those proposals include reductions to CISA's cybersecurity programs and cuts to Coast Guard operations that are responsible for monitoring unusual maritime activity around sensitive infrastructure.

This administration's singular and cruel focus on ripping apart families is jeopardizing the very capabilities to protect our nation's communications networks. At a time when foreign adversaries are probing undersea cables and testing our resilience, we cannot afford to divert attention or resources away from these priorities.

This hearing provides an opportunity for bipartisan leadership. Protecting the systems that carry our communications, financial transactions, and public safety information is a shared priority. Every community in this country relies on secure connectivity, and regions like Northern Virginia have especially high stakes and are home to key stakeholders.

I look forward to working with my colleagues on both sides of the aisle to strengthen federal coordination, support responsible investments, and ensure that the United States is prepared to protect this critical infrastructure against emerging threats.

# # #

Media contact