Policy Brief
*January 29, 2025*

# China, Russia and Undersea Cable Vulnerability: Shoring Up Protection

*Niklas Swanström*

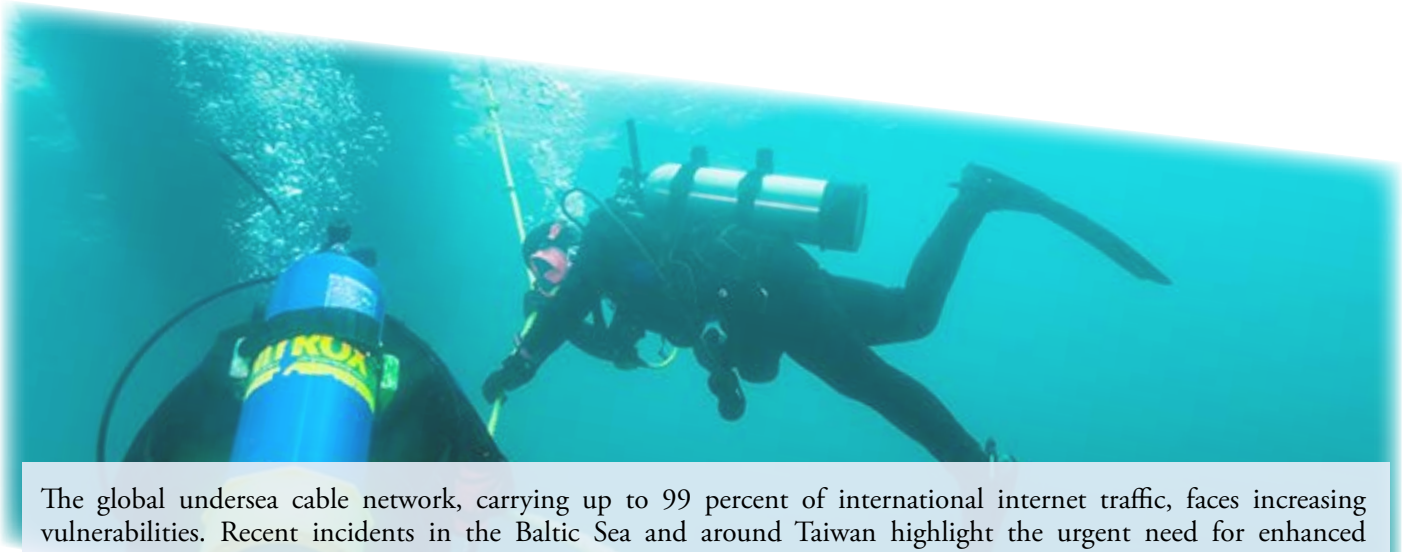

*Photo credit: Focused Adventures / Shutterstock*

The global undersea cable network, carrying up to 99 percent of international internet traffic, faces increasing vulnerabilities. Recent incidents in the Baltic Sea and around Taiwan highlight the urgent need for enhanced protection measures and international cooperation. The mere possibility of cable interference can create significant anxiety in financial markets and erode public confidence in critical infrastructure, having a huge psychological impact. Russia and China are developing alternative cable routes and systems that could reduce Western control over global communications infrastructure. The competition extends to technical standards and protocols, with both nations pushing for more significant influence in international standards bodies. If successful, this creates potential long-term vulnerabilities, as control over technical standards could facilitate future exploitation. China's approach to undersea cable warfare combines technological sophistication with strategic infrastructure development. China has significantly expanded its influence over global cable infrastructure under the Digital Silk Road initiative. Both Russia and China have invested heavily in dual-use marine research and operative infrastructure that can support cable interference operations. Maritime assets like oceanographic research vessels, deep-sea submersibles, and sophisticated mapping capabilities provide plausible deniability for the aggressor, while maintaining significant operational capabilities. Developments in quantum sensing and autonomous underwater vehicle technologies present new hurdles for cable protection. The combination of physical vulnerability, technical sophistication, and geopolitical complexity creates unique challenges that require innovative solutions and unprecedented international cooperation.

- Early warning systems powered by sophisticated detection and monitoring tools need to be supported by enhanced information sharing among allies and improved coordination between commercial operators and national security entities.
- Greater international cooperation includes joint monitoring operations, shared response protocols, and coordinated legal frameworks for attribution and response, as well as setting up multinational cable protection zones.
- The legal framework for cable protection should include development of clear attribution protocols, establishment of multinational response mechanisms, and creation of effective deterrence frameworks. The legal structure must balance the need for cable protection with commercial operational requirements and international maritime law.
- Accelerate investment in next-gen cable technologies and development of alternative communication technologies.
- There is urgent need for enhanced backup systems and alternative routing capabilities while developing protocols for operating under degraded connectivity conditions. This includes the establishment of distributed data centers with multiple redundant connections and a development of async transaction processing capabilities for critical systems
- Nations must develop comprehensive economic defense frameworks integrating cable protection with broader financial system security.

## Introduction

Undersea cables form the backbone of global digital infrastructure, facilitating trillions of dollars in daily financial transactions and carrying vital government communications. Due to the indispensable nature of the infrastructure, they have been eyed by malign states that view it as an easy and relatively cost-effective target. Stretching over 1.5 million kilometers and often in international waters, they are challenging to protect, which has become very apparent in the Baltic Sea and around Taiwan. In 2023, there were more than 200 failures in the underwater cable system, according to the International Telecommunications Union (ITU), primarily due to aging infrastructure, natural hazards, or human accidents.[1] Still, this policy brief is about deliberate attacks on undersea infrastructure. Their vulnerability represents a critical national security concern that demands immediate attention and coordinated international response. The increasing frequency of cable disruptions, and the threats thereof, due to malign interference, not least in the Baltic Sea and Taiwan, coupled with the emergence of sophisticated underwater capabilities among potential adversaries, creates an urgent need for enhanced protection frameworks.

The instinctive perception is that the primary threat to the cable network lies in direct attack on its physical structures. However, the impact extends far beyond the obvious disruptions. This policy brief discusses how China and Russia could utilize the vulnerabilities of the cable structures and how the EU and Taiwan could respond to this threat. The analysis examines the multifaceted threats to submarine cable infrastructure and their strategic implications and proposes policy recommendations for strengthening global cable security.

## Psychological Warfare and Information Operations

As noted, the apparent threat is the cutting of cables to directly damage the cable infrastructure. However, the psychological impact of cable vulnerabilities extends far beyond direct communication disruptions. The mere possibility of cable interference can create significant anxiety in financial markets and erode public confidence in critical infrastructure. The November 2024 cable incident in the Baltic Sea is a case in point, where any incident is automatically connected to adversaries and a growing insecurity is playing out in official media and national security organizations. This psychological vulnerability can be exploited through carefully orchestrated campaigns combining cable disruptions with information operations and economic pressure.

This strategy has become obvious in the Baltic region and Taiwan, where public opinion is seriously debating what individual states can do to counter such actions and if the malign states are not better equipped to act, despite, for example, Finland's quick response in the case of the November 20 incident that has potentially proven not to be a government orchestrated operation, this time.[2] Russia and China have effectively used the fear of disconnection to influence national decision-making and public opinion, as well as flaunting what they possibly could do. The psychological impact is particularly pronounced in highly digitized economies, such as Taiwan and the extended Baltic region, where brief interruptions in connectivity can trigger widespread panic and economic disruption. This creates a form of psychological leverage by authoritarian actors that has been exploited without requiring large-scale cable damage.

Additionally, cable disruptions can be synchronized with disinformation campaigns to amplify their psychological impact, i.e. weakness of the political system, military capability, etc. By targeting specific cables during periods of social or political tension, adversaries could create information vacuums that facilitate the spread of disinformation, even if it also would decrease the attacker's ability to use digital means for disinformation. The resultant uncertainty and confusion could be exploited to undermine public confidence and social cohesion. Many vessels involved in the attacks are under a different flag than the suspected attacker. For example, the attack on Taiwan cables in January 2025 was done by a commercial ship owned by Jie Tan Trading Limited of Hong Kong, headed by Guo Wenjie, a Peoples Republic of China (PRC) citizen, but the ship is

registered in Cameroon.[3] While the use of a different flag deceives no one, this particular practice creates insecurity that harms citizens and complicates effective responses.

The psychological effects are often asymmetric, with even minor disruptions causing disproportionate public reactions. The perceived attacks on the underwater cables in the Baltic Sea in 2024 and Taiwan in 2025 are evidence of actions that seemingly do not directly impact but outline the relative weakness of the impacted actors. This asymmetry makes cable attacks particularly attractive for actors seeking to maximize psychological impact while minimizing physical infrastructure damage. The attribution challenges associated with cable attacks further compound these psychological effects, as uncertainty about the source of disruptions can amplify public anxiety and political tension.

## Economic Warfare and Financial System Vulnerability

The economic implications of cable disruptions extend throughout the global financial system. Modern financial markets rely on ultra-low latency connections for trading and transaction processing. Even millisecond delays can trigger algorithmic trading responses that cascade through markets, potentially causing significant financial losses. The Bank for International Settlements (BIS) estimates that a significant cable disruption could affect trillion dollars in daily financial flows. Disruptions to undersea telecommunications cables can profoundly affect cryptocurrency operations, exposing the networks' decentralized architecture and their dependence on physical internet infrastructure. When these critical arteries of global connectivity are compromised, the repercussions ripple through the entire cryptocurrency ecosystem, manifesting in multiple forms of operational degradation. Financial markets face particular vulnerability during these events. Major cryptocurrency exchanges, despite their sophisticated infrastructure, may experience service interruptions that trigger heightened market volatility. The impact extends beyond traditional cryptocurrency trading to the broader decentralized finance ecosystem, where smart contracts and automated market makers require continuous, reliable internet connectivity to function effectively. While blockchain technology was conceived as a resilient, distributed system, the reality of its implementation reveals a critical dependency on the physical architecture of global internet infrastructure. This vulnerability becomes particularly acute during cable disruptions, highlighting the need for robust contingency measures and infrastructure redundancy in the cryptocurrency sector.

Key vulnerable sectors include, but are not limited to:

- High-frequency trading operations which require constant, low-latency connectivity
- International banking systems and SWIFT network operations
- Cloud-based services and data centers
- Global supply chain management systems
- International payment processing networks

Attacking these areas in the economic system could indeed be a crude instrument if one depends on the international financial system, and especially as China is trying to diversify its reliance on the currently U.S.-dominated system. Still, for actors outside the global monetary system, such as Russia or Iran, as two examples, they would be cost-effective measures that impact the adversary to a higher degree.

Sustained or repeated cable disruptions can affect economic behavior and investment patterns. Companies may begin to factor in connectivity risk when making investment decisions, potentially leading to market distortions and altered capital flows. The insurance market for cable infrastructure has already seen significant changes, with higher premiums reflecting increased risk perception.

Sophisticated actors can use cable disruptions for targeted economic warfare. By identifying and disrupting specific cable routes, attackers can:

- Create artificial latency advantages in financial trading

- Force traffic onto more easily monitored backup routes
- Disrupt specific economic sectors or geographic regions
- Manipulate market behavior through strategic timing of disruptions

Targeting multiple cables simultaneously or coordinating disruptions with other forms of economic pressure can magnify the financial impact. This compound effect can overwhelm standard market resilience mechanisms and challenge traditional economic security frameworks. This behavior also increases the weakness of economic systems, and it would not be hard to imagine rogue states forcing commercial activities into less secure backup routes to skim money out of transactions.

## How Russia and China have used the Cable War

Russia and China are developing alternative cable routes and systems that could reduce Western control over global communications infrastructure. In particular, China's Digital Silk Road initiative represents a significant challenge to traditional Western dominance in this sector. In combination with the development of alternative economics and payment systems this could increase the risks for liberal economic systems. The competition extends to technical standards and protocols, with both nations pushing for more significant influence in international standards bodies. If successful, this creates potential long-term vulnerabilities, as control over technical standards could facilitate future exploitation.

Russia's approach to undersea cable warfare reflects its broader doctrine of hybrid warfare and strategic deterrence. The Russian Navy maintains specialized vessels and submersibles capable of deep-sea operations, including the Main Directorate of Deep-Sea Research (GUGI) fleet.[4] GUGI has increased its operational capability in the Baltic region and the North Sea, which should be a concern. Russia has been known to sabotage and disrupt these networks, at least since 2014.[5] The assets within GUGI provide Russia with sophisticated cable interference capabilities that extend well beyond simple physical disruption and include information gathering and possible psychological warfare.

The Russian doctrine emphasizes the integration of cable operations with broader information warfare strategies. The country's geographic position provides unique advantages in the Baltic Sea and Arctic regions, where environmental concerns limit cable routes. Recent incidents suggest a pattern of testing Western detection and response capabilities through calibrated interference operations. It is not that the concerned states, and their NATO allies, are inactive; rather they are facing increasingly sophisticated and targeted threats that are complicated to fully counter. Still, Russia has moved into a wartime mentality. It utilizes the opportunities in a way that makes it hard to defend without stepping up the corresponding wartime mentality in NATO.

Key elements of Russian strategy include, but are not limited to:

- The development of sophisticated underwater reconnaissance capabilities
- Integration of cable operations with electronic warfare systems
- Use of civilian vessels and commercial activities as cover for surveillance
- Deployment of specialized underwater vehicles for cable interference
- Strategic positioning of "research vessels" near critical infrastructure

## Chinese Capabilities and Strategy

China's approach to undersea cable warfare combines technological sophistication with strategic infrastructure development. China has significantly expanded its influence over global cable infrastructure through direct ownership, and companies like HMN Tech (formerly Huawei Marine Networks) under the Digital Silk Road initiative. This creates persistent concerns about potential surveillance capabilities

built directly into cable systems. The 14th Five-Year Plan (2021-2025) outlined that deep-sea engineering, including the maritime information industry, should be a national focus.

Chinese military modernization includes significant investment in underwater capabilities, including advanced autonomous underwater vehicles (AUVs) and cable-laying ships. The People's Liberation Army Navy (PLAN) has demonstrated increasing sophistication in underwater operations, particularly in the South China Sea and around Taiwan. That said, the PLAN is not necessarily directly involved in all operations. The October 2023 incident was conducted by the commercial Hong Kong-based NewNew Polar Bear, and the second was operated by the Chinese cargo ship Yi Peng 3.[6] However, China has been known for including commercial vessels into its military operations for a long time, so it is only one of the strategies that Beijing has at its disposal.[7]

Additional Chinese strategic elements include, but are not limited to:

- Development of dual-use technologies for cable operations
- Strategic investment in cable infrastructure globally
- Integration of cable systems with broader maritime domain awareness
- Advanced capabilities in quantum communications and sensing
- Sophisticated cyber capabilities for network exploitation

Both Russia and China have invested heavily in dual-use marine research infrastructure that can support cable interference operations. This includes oceanographic research vessels, deep-sea submersibles, and sophisticated mapping capabilities. These maritime assets provide plausible deniability for the aggressor, while maintaining significant operational capabilities.

Both nations' development of quantum sensing technologies presents new challenges for cable protection. These technologies could potentially enable more sophisticated tapping operations that are harder to detect using conventional means. Similarly, advances in autonomous underwater vehicle technology create new vectors for cable interference that are difficult to attribute and counter.

## Strategic Context and Geopolitical Implications

The global submarine cable network represents a paradox in modern infrastructure: it is simultaneously critical for our security and vulnerable to external threats. Unlike traditional strategic assets that can be physically hardened or relocated, submarine cables follow largely fixed routes dictated by geography and technological constraints. The strategic significance of these cables extends beyond mere communication capacity; they represent critical chokepoints in the global economy and international security architecture.

Recent incidents have demonstrated how submarine cables can become instruments of hybrid warfare. The strategic positioning of cable disruptions can serve multiple objectives: degrading regional communication capabilities, forcing traffic onto monitored routes, or creating economic pressure through targeted service disruptions. The asymmetric nature of cable attacks makes them particularly attractive to actors seeking to exert influence while maintaining plausible deniability.

In the Baltic context, cable vulnerabilities intersect with broader regional security concerns. The limited number of cable routes and their concentration in relatively shallow waters create natural chokepoints that can be exploited for strategic advantage. The October 2023 Baltic connector incident, a suspected sabotage of an undersea gas pipeline connecting Finland and Estonia in the Baltic Sea,[8] demonstrated how cable attacks could be integrated into broader hybrid warfare strategies, combining infrastructure targeting with information operations and political pressure.

The Taiwan situation presents even more complex challenges. The concentration of cables in the

Taiwan Strait creates a critical vulnerability that could be exploited during periods of tension. The deep water environment around Taiwan presents different technical challenges for both attackers and defenders, while the presence of multiple state actors with competing interests complicates protection efforts. The potential for cable disruption serves as a form of strategic leverage, enabling subtle pressure through selective interference or the threat of comprehensive disconnection.

## Detection and Response Challenges

Modern cable attacks range from crude physical disruption to sophisticated operations using advanced underwater technologies. Simple anchor dragging remains an effective attack vector, providing plausible deniability through apparent commercial shipping accidents. However, more sophisticated approaches are emerging, including using AUVs capable of precise cable location and interference.

The development of cable tapping capabilities represents a particularly concerning trend. Advanced technical capabilities enable data extraction without physical cable damage, potentially allowing long-term surveillance operations to go undetected. The emergence of quantum sensing technologies may provide new detection capabilities and create new vulnerabilities that sophisticated actors could exploit.

Current cable protection systems face significant limitations in both detection and response capabilities. Traditional monitoring systems often rely on signal degradation to detect interference, potentially allowing sophisticated attacks to go unnoticed. The vast geographic scope of cable networks, combined with limitations in underwater surveillance capabilities, creates substantial monitoring challenges.

Response capabilities are further constrained by the limited availability of specialized repair vessels and the complex legal framework governing international waters. The time required for cable repairs can extend from days to weeks, depending on weather conditions, water depth, and geopolitical circumstances. This repair window creates opportunities for strategic exploitation, particularly in scenarios where multiple cables are targeted simultaneously.

The legal framework for cable protection, primarily based on the UN Convention on the Law of the Sea (UNCLOS) and domestic legislation, has proven inadequate for addressing modern threats. While UNCLOS provides basic protections for submarine cables, it lacks specific provisions for addressing state-sponsored attacks or sophisticated interference methods. The convention's enforcement mechanisms are particularly weak in international waters, where most cable vulnerabilities exist.[9] There are new legislations in the process, and UN has taken several actions to monitor the situation, but the situation does not seem to be changing enough to ensure security.

The private ownership of most submarine cables creates additional complexity in protection efforts. For example, HMN Tech is closely connected to the Chinese Communist Party by government representation and Chinese legislation. While cables carry vital national security communications, their operation and maintenance typically fall under commercial jurisdiction. This split between national security interests and commercial operations creates coordination challenges and potential gaps in protection frameworks.

## Policy Recommendations

There are a number of changes that need to be implemented, multilaterally if possible but more likely with like-minded nations. As long as democratic states do not play with the same cards as authoritarian states, they will always be one step behind. The tension in the field of critical international infrastructure can only be thwarted on a level playing field.

Modern cable protection requires a sophisticated approach to **detection and monitoring**. Integration of acoustic sensors, quantum detection systems, and AI-powered analysis tools can provide early warning of potential interference. These technical capabilities must be supported by enhanced information sharing among allies and improved coordination between

commercial operators and national security entities.

Effective cable protection requires unprecedented levels of **international cooperation**. This includes joint monitoring operations, shared response protocols, and coordinated legal frameworks for attribution and response. Establishing multinational cable protection zones, particularly in strategic areas like the Baltic Sea and Taiwan Strait, could provide models for broader international cooperation.

**Investment in next-generation cable technologies** must be accelerated. This includes development of physically hardened cables, improved monitoring capabilities, and alternative communication technologies. Quantum communication networks, while still in development, may provide new options for secure communication in critical scenarios. It will be crucial to **control and own infrastructure,** unilaterally or in cooperation with like-minded states, and keep authoritarian states out of new infrastructure projects.

The international **legal framework for cable protection** must evolve to address modern threats. This includes development of clear attribution protocols, establishment of multinational response mechanisms, and creation of effective deterrence frameworks. The legal structure must balance the need for cable protection with commercial operational requirements and international maritime law.

The future of cable protection requires a **fundamental rethinking of current approaches**. The development of alternative communication technologies, including new satellite systems and quantum networks, may reduce reliance on physical cables. However, the physical advantages of fiber optic cables suggest they will remain critical infrastructure for the foreseeable future.

Developing robust financial system resilience requires a multilayered approach that combines technical, operational, and regulatory measures. Financial institutions must implement **enhanced backup systems and alternative routing capabilities** while developing protocols for operating under degraded connectivity conditions. This includes the establishment of distributed data centers with multiple redundant connections and a development of async transaction processing capabilities for critical systems

Nations must develop **comprehensive economic defense frameworks** integrating cable protection with broader financial system security.

The protection of undersea cables represents one of the most critical yet challenging aspects of modern national security. The combination of physical vulnerability, technical sophistication, and geopolitical complexity creates unique challenges that require innovative solutions and unprecedented international cooperation. Success in this domain will require sustained investment, technical innovation, and political will to implement comprehensive protection frameworks.


## Author –

***Dr. Niklas Swanström*** *is the Executive Director of the Institute for Security and Development Policy, and one of its co-founders. He is a Fellow at the Foreign Policy Institute of the Paul H. Nitze School of Advanced International Studies (SAIS) and a Senior Associate Research Fellow at the Italian Institute for International Political Studies (ISPI).*





### About ISDP

*The Institute for Security and Development Policy is a Stockholm-based independent and non-profit research and policy institute. The Institute is dedicated to expanding understanding of international affairs, particularly the interrelationship between the issue areas of conflict, security and development. The Institute's primary areas of geographic focus are Asia and Europe's neighborhood.*

www.isdp.eu

## Endnotes


1 Emma Fargo, "UN Body to protect 'vulnerable' submarine cables after ruptures," Reuters, December 12, 2024, https://www.reuters.com/technology/un-body-protect-vulnerable-submarine-cables-after-ruptures-2024-12-12/.

2 Greg Miller, Robyn Dixon and Isaac Stanley-Becker, "Accidents, not Russian sabotage, behind undersea cable damage, officials say," The Washington Post, January 19, 2025, https://www.washingtonpost.com/world/2025/01/19/russia-baltic-undersea-cables-accidents-sabotage/.

3 Tom Nicholson, "Taiwan Suspects China of Latest attack on Undersea Cables," Politico, January 5, 2025, https://www.politico.eu/article/taiwan-china-undersea-cables-attack-international-telecom-cargo-ship-eu-russia/.

4 Andrii Ryzhenko, "Russia looks to Target Achilles' _Heel of Western Economies on Ocean Floor, Eurasia Daily Monitor," The Jamestown Foundation, September 17, 2024, https://jamestown.org/program/russia-looks-to-target-achilles-heel-of-western-economies-on-ocean-floor/.

5 Sam Clark, "The West has a plan to keep China, Russia our of subsea data pipes," Politico, September 12, 2024, https://www.politico.eu/article/china-russia-submarine-data-cables-security-united-states-european-union/.

6 Sophia Besch and Erik Brown, "A Chinese-Flagged Ship cut Baltic Sea internet cables," Carnegie Endowment, December 3, 2024, https://carnegieendowment.org/emissary/2024/12/baltic-sea-internet-cable-cut-europe-nato-security?lang=en.

7 Niklas Swanström, "The role of the People's Armed Forces Maritime Militia: Implications for Maritime Security and European interests," EuroHub4Sino Policy Paper 2024/10, https://doi.org/10.31175/eh4s.2014.10.

8 Li Beiping, "China's 'accidental' damage to Baltic pipeline viewed with suspicion," August 17, 2024, https://www.voanews.com/a/china-s-accidental-damage-to-baltic-pipeline-viewed-with-suspicion/7746569.html.

9 Amy Paik and Jennifer Counter, "International law doesn't adequately protect undersea cables," Atlantic Council, January 25, 2024, https://www.atlanticcouncil.org/content-series/hybrid-warfare-project/international-law-doesnt-adequately-protect-undersea-cables-that-must-change/.