The Hague Centre for Strategic Studies

NATO Seminar on Seabed Security

Strengthening Taiwan's Sea Cable Security

Dr. Kenny Huang

March 2025

The Hague Centre for Strategic Studies

Strengthening Taiwan's Sea Cable Security

Author:
Dr. Kenny Huang
Chair, Taiwan Network Information Centre

Editor:
Michel Rademaker

March 2025

This HCSS paper is part of a series of guest contributions following the NATO Seminar on Seabed Security, organised by TNO and HCSS, in close cooperation with the Dutch Ministries of Defence and Infrastructure & Water Management, on March 27, 2025.

Table of Contents

Abstract

Sea cables are a critical pillar of global digital infrastructure, carrying over 95% of international data traffic, including financial transactions, business communications, government intelligence, and everyday internet applications. In today's highly interconnected world, sea cables not only support the functioning of the global economy but are also closely tied to national security. For example, cross-border banking transactions, cloud computing, and military communications all rely on a stable and secure sea cable network. Any disruption or attack on these cables could have severe consequences for international communications, economic activities, and national security systems.

In recent years, multiple sea cable disruptions have highlighted the vulnerabilities of this infrastructure.In 2023, sea cables between Taiwan and its offshore islands were severed due to human activities, affecting local residents and businesses. In 2024, a Chinese-flagged vessel caused damage to Europe's sea cable infrastructure in the Baltic Sea, raising concerns about potential surveillance and sabotage by Beijing (Jakub Janda, 2024). As geopolitical tensions escalate, some nations have intensified monitoring or restricted certain companies from participating in sea cable construction, increasing the strategic sensitivity of these networks.

This paper examines the security challenges and response strategies related to sea cables. It covers an overview of sea cable technology, key routes and maintenance challenges, security risks faced by sea cables, international and regional governance, and technical and strategic measures to enhance sea cable security. It also explores Taiwan's specific challenges and response strategies. This paper aims to enhance understanding of sea cable security and provide concrete recommendations to ensure global internet stability and the sustainable development of the digital economy.

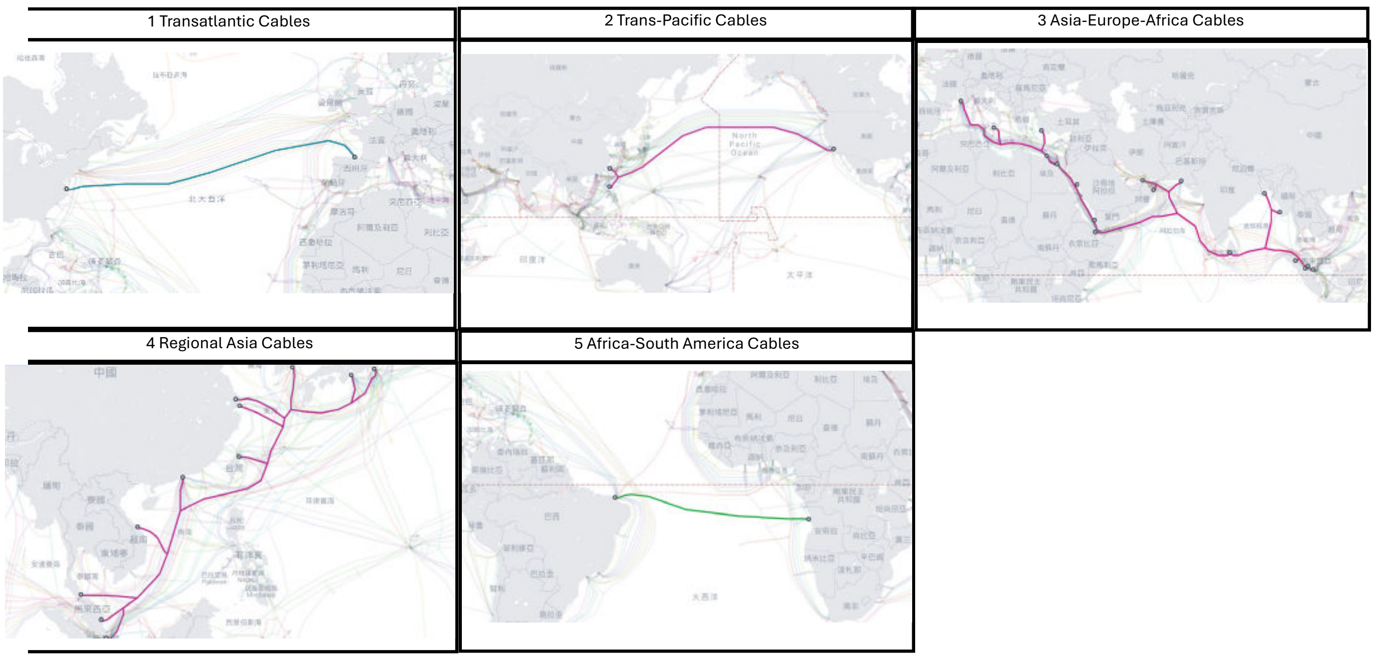
1. Sea Cable Overview

Sea cables are the backbone of global internet and international communications infrastructure, carrying over 99% of cross-border data transmissions (Telegeography, 2025). These cables are typically laid on or buried beneath the seabed to ensure high-speed and stable communication.

Sea cables span across continents, connecting major global economies and communication hubs. Some of the key global sea cable routes include : Transatlantic Cables, which connect North America and Europe, such as MAREA and AEC-2; Trans-Pacific Cables, like PLCN and JUPITER, linking the U.S., Japan, Taiwan, and Southeast Asia, serving as the main gateway for trade and financial data between the Asia-Pacific and North America; Asia-Europe-Africa Cables, including SEAMEWE Cables (Southeast Asia-Middle East-Western Europe), which connect major markets in Europe, the Middle East, and Asia; Regional Asian Cables, such as AAG (Asia-America Gateway) and APG (Asia-Pacific Gateway), strengthening interconnectivity between East and Southeast Asian nations; Africa & South America Cables, like SACS (South Atlantic Cable System) and ACE (Africa Coast to Europe), enhancing connectivity for emerging markets.

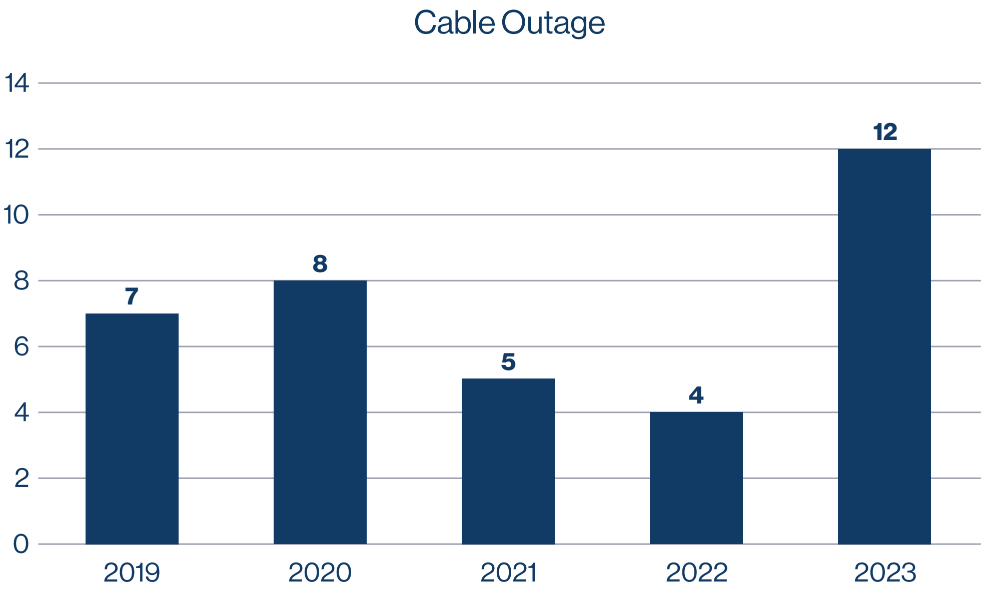
As a key sea cable hub in the Asia-Pacific region, Taiwan hosts multiple critical sea cables connecting Japan, the U.S., Southeast Asia, and China, including APCN-2, TPE, and FASTER, ensuring the stable operation of digital infrastructure.

Figure 1. Sea Cables Maps (submarinecablemap.com)



The deployment and maintenance of sea cables are influenced by various factors, including technology, environmental conditions, regulations, and geopolitical challenges. For instance, complex terrains such as deep-sea trenches, volcanic zones, and underwater canyons increase the difficulty of deploying sea cables. Natural disasters like earthquakes and tsunamis pose significant risks to sea cable infrastructure. A notable example is the 2006 earthquake south of Taiwan, which caused severe damage to multiple sea cables.

Figure 2. Outage statistics for Taiwan domestic sea cables (National Audit Office)



The earthquake killed two people and injured 42 others in Taiwan (TVBS, 2006). The earthquake damaged at least eight major submarine cables in the Luzon Strait, one of the world's most critical undersea communication hubs. Taiwan, Hong Kong, China, Japan, South Korea, Singapore, and even parts of the U.S. and Europe experienced severe internet slowdowns or disruptions. Taiwan's internet access was disrupted. Hong Kong's stock market operations slowed down. South Korea reported that 99% of its international internet traffic was cut off . The following table shows the significant impact of the earthquake.

Table 1. Significance of the 2006 Taiwan Earthquake (Dr. Kenny Huang)

Impact Type	Descriptions
Human Casualties	2 dead, 42 injured
Internet Disruptions	Widespread outages in East Asia
Affected Countries	Taiwan, Hong Kong, China, Japan, South Korea, Singapore, U.S.
Financial Impacts	Slowed stock trading, banking disruptions
Repair Time	2 weeks to 1 month for full restoration

Sea cable maintenance requires specialized vessels and skilled personnel, and repair operations can take weeks to months, making maintenance costs extremely high. To address these challenges, global organizations such as the International Cable Protection Committee (ICPC) establish maintenance standards and emergency response plans. Additionally, the United Nations Convention on the Law of the Sea (UNCLOS) provides a legal framework for sea cable installation and maintenance. Beyond international regulations, some countries conduct security reviews on new sea cable projects. For example, the U.S. government remains highly cautious about Chinese investments in sea cable infrastructure.

The U.S. fears that Chinese-backed companies involved in undersea cable construction and maintenance could enable the Chinese government to intercept data or conduct cyber espionage. In 2020, the Pacific Light Cable Network (PLCN)—a planned cable between the U.S. and Hong Kong funded by Google, Meta, and China's Dr. Peng Group—was forced to bypass Hong Kong after pressure from U.S. regulators. In the event of heightened geopolitical conflict (such as over Taiwan or the South China Sea), the risk of cable sabotage or access restrictions becomes a major concern (The Guardian, 2020).

2. Sea Cable Challenges

As a critical infrastructure for global data transmission, sea cables face multiple risks from natural disasters, human activities, and cybersecurity threats.

2.1. Natural Factors

Sea cables are often laid in earthquake-prone zones, such as the Pacific Ring of Fire, where earthquakes and underwater landslides can cause cable ruptures. A notable case was the 2006 earthquake south of Taiwan, which severed multiple sea cables, significantly disrupting communications between Asia and the Americas. Typhoons and strong ocean currents can shift seabed sediments, increasing the risk of cable exposure and damage.

Marine life can also pose a threat. While rare, sharks have been observed attacking sea cables.). Shark attacks on undersea cables have been observed, but they are not widespread or region-specific. Additionally, changes in underwater ecosystems, such as coral reef growth or sediment movement, may affect cable stability (David Sachs, 2023). Coral reef growth and sediment movement are typical particularly in tropical and subtropical coastal areas, where ocean conditions support reef development and sediment transport. These natural processes can impact sea cables and coastal infrastructure.

2.2. Human Factors

Trawling and large anchoring vessels are the leading causes of human-induced cable damage, accounting for over 60% of incidents. High-risk areas include major shipping routes and fishing zones, particularly in the waters around Southeast Asia and China.

Sea cables have also become targets in geopolitical conflicts, where certain nations or groups may attempt to sever cables to disrupt communications. For instance, the 2013 sea cable sabotage in Egypt caused a large-scale internet outage in the region. China has been suspected of developing capabilities to disrupt undersea cables in a conflict scenario (e.g., Taiwan Strait). In 2023,. Chinese ships were suspected of damaging two sea cables connecting Taiwan to the Matsu Islands raising espionage concerns (Su Si Yun, 2023). The Togolese-flagged cargo ship *Hong Tai*, which has Chinese capital background, was involved in severing the third sea cable between Taiwan and Penghu on 25 Feb. 2025 (LAI,YU-CHEN, 2025). Taiwan Presidential Office stated that the possibility cannot be ruled out that damaging sea cables has become a means of "gray zone" interference. In response, the government will not only impose heavier penalties and fines for damaging sea cables but will also continue to improve reporting and law enforcement procedures.

Malicious actors may conduct espionage activities through sea cables, and similar cases are becoming increasingly common. In response, many governments have tightened scrutiny over new sea cable projects to mitigate potential national security threats.

2.3. **Cybersecurity Risks**

Sea cable fiber optic signals can be intercepted, and some governments and agencies have been accused of using this method for surveillance. The Snowden revelations exposed U.S. intelligence agencies' monitoring of undersea cables.

In early 2025, Taiwan detained the *Hongtai*, a Togolese-flagged cargo ship with a Chinese crew, on suspicion of damaging an undersea cable connecting Taiwan to the Penghu Islands. This incident highlights concerns about Chinese vessels potentially disrupting critical undersea infrastructure in the region(LAI,YU-CHEN, 2025).

While most sea cable data is encrypted, advances in quantum computing could eventually render current encryption methods obsolete. To address this, global research efforts are underway to develop quantum encryption technologies to enhance sea cable security.

Control over sea cables also raises concerns about global surveillance and privacy protection. Many governments are increasingly monitoring the flow of data through sea cables, and international discussions continue on how to balance security and individual privacy.

The security of sea cables is threatened by natural disasters, maritime activities, geopolitical tensions, and cyber risks. To safeguard global data transmission, governments and enterprises must strengthen international cooperation, invest in technological innovation, and enhance maintenance mechanisms. By doing so, they can ensure the stability, security, and resilience of the global communication infrastructure.

3. Security Governance of Sea Cable

The security and development of sea cables involve multiple international organizations, treaties, and national policies. Multilateral cooperation and regulatory frameworks are essential to ensuring their stability and protection.

3.1. Key International Organizations and Standards

Several major international organizations oversee sea cable security and development. ITU (International Telecommunication Union) is responsible for global telecommunications standards, including sea cable technical specifications and operational guidelines. ICPC (International Cable Protection Committee) focuses on sea cable protection, issuing best practice guidelines and working with governments and enterprises to reduce risks. APNIC (Asia Pacific Network Information Centre): Oversees IP address allocation and policy in the Asia-Pacific region, with a focus on critical infrastructure development and security, including sea cables.

3.2. International Conventions and Regulations

UNCLOS (United Nations Convention on the Law of the Sea) establishes the legal framework for laying and maintaining sea cables, defining coastal states' jurisdiction over sea cables. It also prohibits unauthorized interference with other countries' cables.

Many nations cooperate on sea cable protection, implementing cross-border law enforcement mechanisms to prevent illegal cable disruptions.

3.3. National Policies and Strategies

Countries have developed policies to strengthen sea cable security and protect national data sovereignty. For example, U.S. developed Secure and Trusted Communications Networks Act restricts companies from certain countries from participating in U.S. sea cable projects. U.S. also imposed strict regulation of cable landing stations prevents foreign influence over U.S. data transmission. European Union developed Europe's Digital Decade initiative enhances sea cable security and intra-European connectivity. EU also establishes cybersecurity standards, requiring cable operators to implement encryption and monitoring measures. China developed Belt and Road Initiative (BRI) promotes global sea cable projects, expanding China's influence in telecommunications infrastructure. China's regulations restrict foreign investment in critical telecom infrastructure.

Taiwan has compiled a blacklist of 52 Chinese-owned ships operating under flags of convenience, which it will monitor and proactively inspect as part of its efforts to regulate a rapidly growing "shadow fleet" that poses global security concerns (Kathrin Hille, 2025). In response to frequent sea cable disruptions, Taiwan is strengthening its national resilience by developing a robust and redundant system capable of fully switching to satellite communications if necessary (Jane Rickards, 2025)

As a regional hub for Asia-Pacific sea cables, Taiwan actively engages in international cooperation to ensure communication resilience. Recent efforts focus on integrating sea cables with satellite communication to enhance network diversity and security.

The Ministry of Digital Affairs (MODA) launched the "International Sea Cable Landing Station Resilience Construction Subsidy Program" last year, allowing operators to apply for subsidies for the construction of new sea cable landing stations and two backup facilities, covering expenses such as power and security protection equipment. So far, MODA has granted NT$1.9 billion to Chunghwa Telecom for the construction of a new international sea cable landing station and backup facilities to enhance Taiwan's international sea cable connectivity. Additionally, in cases where sea cables or microwave links are unavailable, MODA has planned to use SES medium-Earth orbit (MEO) satellites and the OneWeb low-Earth orbit (LEO) satellite system as backup solutions to ensure uninterrupted communication for military and government command systems (Su Si Yun, 2025).

International and regional governance of sea cables involves standards, treaties, and national policies. Strengthening cooperation, technological innovation, and regulatory frameworks is key to ensuring the security and stability of global data transmission.

4. Strengthening Sea Cable Security

Ensuring the security of sea cables requires a combination of physical protection measures and cybersecurity strategies. These efforts minimise risks from natural disasters, human interference, and cyber threats.

4.1. Physical Protection Measures

Safe route planning avoides earthquake-prone zones, active underwater volcanoes, and high maritime traffic areas reduces the risk of natural and human-induced damage. Historical data and geological surveys help identify optimal cable-laying routes to extend cable lifespan.

Modern sea cables are designed with multi-layered protective structures, including steel-wire armouring and high-strength polymer casings to resist fishing nets and anchor drags. Advanced seabed installation techniques such as trenching and sand burial enhance cable concealment and protection.

Autonomous Underwater Vehicles (AUVs) and Remotely Operated Vehicles (ROVs) conduct regular inspections to detect wear, displacement, or suspicious activity. Seabed sonar and sensor networks monitor for abnormal vibrations or external impacts, enabling early warnings and rapid maintenance response.

4.2. Cybersecurity Technologies

End-to-End encryption protects sensitive data transmitted through sea cables requires high-strength encryption, ensuring that even if intercepted, the data remains unreadable. Deploying advanced protocols such as TLS (Transport Layer Security) and IPsec (Internet Protocol Security) to prevent Man-in-the-Middle (MITM) attacks. Conducting regular vulnerability assessments and security updates maintain system resilience. Multiple parallel cables ensure backup routes in case of failures, preventing disruptions to global communication. Geographically distributed backups and cloud storage protect critical data from single points of failure, enhancing overall network resilience.

A multi-layered security approach combining robust physical protection and advanced encryption is essential to safeguarding global communications and data transmission. By continuously improving monitoring, encryption, and redundancy strategies, nations can ensure the stability and security of the sea cable infrastructure.

5. Taiwan's sea cable security challenges and strategies

5.1. Taiwan's strategic role as an Asia-Pacific sea cable hub

Taiwan is located in a key position in the western Pacific Ocean and is a core sea cable hub connecting East Asia with Southeast Asia and North America. Many international sea cables such as APG (Asia Pacific Gateway), FASTER, and TPE (Taiwan-United States) pass through Taiwan, making it an important node for regional communications. However, this strategic position also exposes Taiwan to higher security risks, including geological disasters, man-made sabotage, and nation-state cyber threats.

5.2. Recent sea cable security incidents affecting Taiwan

In recent years, Taiwan's sea cables have been damaged many times (Huizhong Wu, 2024), including natural disasters, ship damage, and malicious attacks. Taiwan is located in the Pacific Rim seismic belt, and earthquakes have caused sea cables to break many times in history. For example, the 2006 Pingtung earthquake damaged several sea cables in East Asia, causing regional network outages for several days. Illegal trawlers and ship anchoring are the main man-made factors causing damage to Taiwan's sea cables. In 2023, several sea cables connecting outlying islands were damaged due to fishing activities, affecting local communications. In recent years, Taiwan has faced increasingly severe cyber security threats (Keoni Everington, 2024). In 2023, some sea cables were suspected to have been interfered with by unknown forces, resulting in unstable communications, showing the sensitivity of sea cables in international competition and conflict.

5.3. Policy recommendations and directions for international cooperation

Policy recommendations include strengthening the physical protection and monitoring mechanism of sea cables, establishing a diversified backup mechanism, and strengthening international cooperation. Measures to strengthen the protection and monitoring mechanism of sea cables include increasing the proportion of deep-sea cable laying and reducing risk exposure in shallow water areas. Establish AUVs (Autonomous Underwater Vehicle) patrol and seabed monitoring system to detect abnormal situations early. Strictly implement the management of sea cable protection areas, and strengthen supervision and penalties for fishing vessels and ships that operate in violation of regulations.

The diverse backup protection measures include developing more low-orbit satellites (LEO) as emergency communication solutions when sea cables are disconnected, such as OneWeb's plans to communicate with other low-orbit satellites. Promote cooperation between Taiwan and international telecommunications operators to increase the diversity of sea cable routes and reduce the risk of single point failures.

Measures to strengthen international cooperation include establishing a sea cable security alliance with countries in the Asia-Pacific region (such as Japan, Singapore, and the United States) to enhance intelligence sharing and rapid repair capabilities. Participate in international organization meetings such as ICPC (International Cable Protection Committee), ITU (International Telecommunication Union), and APNIC (Asia Pacific Network Information Centre) Internet governance meetings to strengthen Taiwan's role in international sea cable management. Learn from European and American sea cable safety standards, formulate Taiwan's sea cable safety regulations, strengthen public-private sector cooperation, and jointly maintain critical infrastructure.

As the sea cable hub of the Asia-Pacific region, Taiwan faces the dual challenges of natural disasters and man-made threats. Through physical protection, backup mechanisms, and international cooperation, it can effectively enhance sea cable security and network resilience, ensuring stable communications and national security.

6. Conclusion and Policy Recommendations

6.1. Conclusion

With the development of the global digital economy, sea cables have become the cornerstone of international communications and economic activities. However, the security risks and challenges facing sea cables are also increasing. Geopolitical risks may affect the construction and maintenance of new sea cables. Some countries may impose restrictions on foreign investment or companies from specific countries participating in sea cable projects for national security reasons. In addition, cyber attacks and data theft remain key concerns, especially as deep monitoring and interception technologies continue to advance.

Global awareness of protecting sea cable infrastructure is gradually increasing. Countries have strengthened regulations and supervision, and international organizations such as the ITU (International Telecommunication Union) and ICPC (International Cable Protection Union) continue to promote stricter security standards and policies. In the future, sea cable security will not only be a technical challenge, but also an issue of international cooperation and policy coordination.

Technological innovation plays a key role in improving the safety of sea cables, and many innovative technological developments will have a significant impact on the safety of sea cables. For example, AI and machine learning technologies can be used to monitor the status of sea cables, analyze abnormal signals, and predict possible cable break risks, thereby improving early warning and maintenance efficiency. AUVs (Autonomous Underwater Vehicle) technology can automatically inspect and repair sea cables, reducing the risks and costs of manual maintenance. Traditional end-to-end encryption technology still has the possibility of being intercepted, while quantum encryption technology will provide higher-level security protection for sea cable communications. In terms of satellite communications, projects such as Starlink and OneWeb provide additional communication backup to ensure minimum network connectivity when sea cables are damaged.

6.2. **Policy Recommendations**

To enhance the protection of critical sea cable infrastructure, it is recommended that governments, enterprises and international organizations should take the following measures:

1. Strengthen regulations and supervision

Formulate and enforce stricter sea cable protection regulations, such as requiring ships to avoid sea cable areas and mandatory reporting of maintenance plans.

Establish national sea cable safety standards to ensure that newly built sea cables meet the highest safety regulations.

2. Improve technical protection capabilities

Invest in the development of AI monitoring and unmanned maintenance technologies to enhance the ability to monitor sea cable status in real time and quickly repair them. Promote the application of fiber optic encryption and quantum communication technology to prevent the risk of data interception.

3. Strengthen international cooperation

Incorporate sea cable protection into the regional security agenda and study feasible technologies and measures to effectively protect sea cables. At the same time, we will promote the International Sea Cable Safety Alliance to strengthen collective protection measures, such as the sea cable emergency coordination line, and adopt a transparent and consistent approach to reporting and handling when a cable break occurs. Establish intelligence sharing and protection with other countries, and establish a malicious ship monitoring and early warning system. Through international cooperation to study and examine new practices, and form new habits and new international norms.

Sea cable security is key to the stable operation of global communications infrastructure. Through technological innovation, policy strengthening and international cooperation, countries can effectively improve the security of sea cables and ensure the smooth development of the future digital economy.

References

1. Dan Swinhoe. DataCenterDynamics (22 Feb 2022). Tonga's international subsea cables repaired after volcanic eruption. https://www.datacenterdynamics.com/en/news/tongas-international-subsea-cable-repaired-after-volcanic-eruption/

2. David Sachs. (6 Jul 2023). Will China's Reliance on Taiwanese Chips Prevent a War, Council on Foreign Relations. https://www.cfr.org/blog/will-chinas-reliance-taiwanese-chips-prevent-war

3. Huizhong Wu, Johnson Lai. Associated Press (18 Apr 2024). Taiwan suspects Chinese ships cut islands' internet cables. https://apnews.com/article/matsu-taiwan-internet-cables-cut-china-65f10f5f73a346fa788436366d7a7c70

4. Jakub Janda and James Corera. (31 Dec 2024). Baltic subsea sabotage: We're letting Russia (and China) undertake target practice. ASPI. From https://www.aspistrategist.org.au/baltic-subsea-sabotage-were-letting-russia-and-china-undertake-target-practice/

5. Jane Rickards (19 Feb 2025). Wary of cable sabotage, Taiwan looks to satellites as back-ups. ASPI Australian Strategic Policy Institute. https://www.aspistrategist.org.au/wary-of-cable-sabotage-taiwan-looks-to-satellites-as-back-ups/

6. Jon Gambrell. Associated Press (4 Mar 2024). 3 Red Sea data cables cut as Houthis launch more attacks in the vital waterway. https://apnews.com/article/red-sea-undersea-cables-yemen-houthi-rebels-attacks-b53051f61a41bd6b357860bbf0b0860a#

7. Josh Dzieza. The Verge (16 Apr 2024). The Cloud Under the Sea. https://www.theverge.com/c/24070570/internet-cables-undersea-deep-repair-ships

8. Kathrin Hille (27 Jan 2025). Taiwan blocklists Chinese-owned shadow-fleet ship. Financial Times. https://www.ft.com/content/bb6b6a16-bbeb-4b04-9445-7f47fc78663b

9. Keoni Everington. Taiwan News (23 Feb 2024). Cut sea cables said to be China's dry run to end Taiwan's internet. https://www.taiwannews.com.tw/news/4819380

10. LAI,YU-CHEN, CNA News (25 Feb 2025). China frequently uses expedient ships to damage submarine cables and even holds patents for cable cutting. The Central News Agency. https://www.cna.com.tw/news/aipl/202502260140.aspx

11. Ministry of Digital Affairs. Enhancing the Resilience of Communications Network. https://moda.gov.tw/en/digital-affairs/communications-cyber-resilience/operations/310#AC

12. Olivia Solon, Mark Bergen. Bloomberg (23 Apr 2023). Fishing Boats Can't Stop Running Over Undersea Internet Cables. https://www.bloomberg.com/news/articles/2023-04-24/fishing-boats-keep-running-over-ocean-internet-cables

13. Sarah Whiteford. (23 Apr 2021). How is subsea cable repaired? https://www.onesteppower.com/post/subsea-cable-repair

14. Su Si Yun (10 Jan 2025). The submarine cable is like Taiwan's "digital lifeline". The Central News Agency. https://www.cna.com.tw/news/aipl/202501100036.aspx

15. Su Si Yun. (16 Feb 2023). Taiwan-Matsu sea cable outage. The Central News Agency. https://www.cna.com.tw/news/aipl/202302160241.aspx

16. TeleGeography. Submarine Cable Frequency Asked Questions. https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions

17. The Guardian (17 Jan 2020). Pacific data cable not safe from China if Hong Kong included, says US. https://www.theguardian.com/technology/2020/jun/18/pacific-data-cable-not-safe-from-china-if-hong-kong-included-says-us

18. TVBS (27 Dec 2006) HenChun Earthquake Statistics. TVBS News. https://news.tvbs.com.tw/life/339845

The Hague Centre
for Strategic Studies

HCSS
Lange Voorhout 1
2514 EA The Hague

Follow us on social media:
@hcssnl

The Hague Centre for Strategic Studies
Email: info@hcss.nl
Website: www.hcss.nl