papers

No. 26|01 (January 2026)

What Lies Beneath: Hybrid Threats to Taiwan's Submarine Cables and the Contest in the Information Domain

by **Aurelio Insisa**

Between 2023 and 2025, multiple disruptions affected Taiwan's submarine cables, a critical yet vulnerable infrastructure essential to the island's connectivity and security. Against the backdrop of China's diplomatic, economic and military pressure targeting Taiwan, these disruptions are generally defined as "grey zone operations". Yet, reframing them as hybrid threats allows for a better understanding of how specific threats to the infrastructure domain can spill over in the information domain. Disruptions to submarine cables may be exploited by threat actors to erode trust in domestic institutions and destabilise society. Uncertainty in the information domain emerging from these disruption presents opportunities for Taiwanese authorities to mobilise public support, international partners and resources to enhance infrastructure resilience. A strategic communications approach drawing on the experience of the EU can strengthen response through enhanced coordination among institutions, coherent messaging, constructive public engagement and improved awareness of information-domain contestation. An effective adoption of this approach may mitigate risks from threat actors while reinforcing the capacity of Taiwanese authorities to safeguard critical infrastructure and maintain societal trust.

Submarine cables constitute a critical infrastructure that serves as the backbone of global connectivity, guaranteeing the uninterrupted flow of data across regions and continents, underpinning international commerce, communications and digital services. Since Sino-American great power competition flared up in the early 2020s, submarine cables, framed as the "new arteries of power" in contemporary international politics,[1] have turned into a terrain of techno-political competition.[2] Major disruptions affecting this infrastructure have proliferated across the globe since 2022, in

Aurelio Insisa *is Senior Research Fellow for Asia within the 'Global actors' programme at the Istituto Affari Internazionali (IAI).*

[1] Kuok, Lynn, "The New Arteries of Power", in *Foreign Affairs*, 2 January 2026, https://www.foreignaffairs.com/new-arteries-power.

[2] McGeachy, Hilary, "The Changing Strategic Significance of Submarine Cables: Old Technology, New Concerns", in *Australian Journal of International Affairs*, Vol. 76, No. 2 (2022), p. 161-177, https://doi.org/10.1080/10357718.2022.2051427; Morel, Camille "The Pacific Caught in the World Wide Web? Geopolitics of the Submarine Cables in Oceania", in *Études de l'Ifri*, September 2022, https://www.ifri.org/en/node/24801; Bintang Timur, Fitriani et al., "The Politics of Subsea Cables in Indonesia: Navigating Great Power Competition", in *PRIO Policy Briefs*, No. 15/2024 (2024), https://www.prio.org/publications/14070.

Major disruptions affecting submarine cables have proliferated across the globe since 2022

particular the Nordic-Baltic region as the Russo-Ukrainian War has unfolded.[3] Similar disruptions, this time allegedly involving Chinese-crewed vessels, also affected Taiwan's submarine cables on separate occasions: twice in January 2023, and again in January 2025 and February 2025.[4]

This double-edged threat of great power competition over infrastructure control and of major disruptions by hostile actors has sparked renewed urgency in securing submarine cables through diplomatic, financial, technological and military means.[5] The Taiwan case has led experts and policymakers alike to focus on designing new regulations to impose "legal deterrence", strengthening infrastructure supervision, improving technical protection capabilities and enhancing international cooperation with an eye on intelligence sharing and disruption reporting.[6] Some of these policy proposals reflect, but have also informed, reflections on marine cables security in Europe. In 2024, the European Commission recommended improved coordination across the EU to enhance governance and ensure the security and resilience of the submarine cables.[7] Eventually, in February 2025, it launched its 1 billion euro Action Plan on Cable Security.[8] The G7 too addressed the issue, signing a Joint Statement on Cable Connectivity, in 2024 under the Italian presidency, and adopting a Declaration on Maritime Security and Prosperity in 2025, under the Canadian presidency.[9]

[3] Donald C. Hellman Task Force Programme (DCHTFP), *Hidden Highways of the Internet: Global Subsea Cable Security*, Henry M. Jackson School of International Studies, University of Washington, March 2025, p. 18-24, https://jsis.washington.edu/nie/wp-content/uploads/2025/03/Task-Force-B-Final-Report.pdf.

[4] Ibid., p. 19, 24. The official name of the polity subject to this study is the "Republic of China" (ROC). Official domestic publications use the moniker "Republic of China (Taiwan)". This study uses the common term "Taiwan" to refer to the polity.

[5] Koshino, Yuka, "The Changing Submarine Cables Landscape", in *EUISS Briefs*, No. 19 (October 2024), https://www.iss.europa.eu/node/3270; Besch, Sophie and Erik Brown, *Securing Europe's Subsea Data Cables*, Washington, Carnegie Endowment, 2024, https://carnegieendowment.org/research/2024/12/securing-europes-subsea-data-cables; Khanna, Monty, "A Roadmap for Securing India's Undersea Cables", in *ORF Special Reports*, No. 266 (June 2025), https://www.orfonline.org/research/a-roadmap-for-securing-india-s-undersea-cables; Swanström, Niklas, "China, Russia and Undersea Cable Vulnerability: Shoring Up Protection", in *ISDP Policy Briefs*, 29 January 2025, https://www.isdp.eu/?p=40279.

[6] au, Hon-min, "Undersea Cybersecurity: Countering Gray Zone Operations and Strengthening the Digital Resilience of Subsea Cables for Taiwan", in *The Journal of East Asian Affairs*, Vol. 38, No. 1 (Spring/Summer 2025), p. 7-37, https://www.inss.re.kr/common/download.do?atchFileId=F20251107104407610&fileSn=4; Huang, Kenny, "Strengthening Taiwan's Sea Cable Security", in *HCSS Papers*, March 2025, https://hcss.nl/?p=72710.

[7] European Commission, *Recommendation (EU) 2024/779 of 26 February 2024 on Secure and Resilient Submarine Cable Infrastructures*, C/2024/1181, http://data.europa.eu/eli/reco/2024/779/oj.

[8] European Commission, *EU Action Plan on Cable Security*, JOIN/2025/9, 21 February 2025, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:52025JC0009.

[9] G7, *Joint Statement on Cable Connectivity for Secure and Resilient Digital Communications Networks*, Annex to the *G7 Industry, Technology and Digital Ministerial Meeting Ministerial Declaration*, Verona and Trento, 15 March 2024, https://www.

Disruptions to Taiwan's submarine cables should be understood as hybrid threats, not "grey zone operations"

In analyses concerning Taiwan's security, disruptions to submarine cables are usually understood as "grey zone operations", namely offensive operations conducted below the threshold of direct kinetic confrontation. Yet, the broader meaning and implications of these disruptions for Taiwan, especially within the information domain, can better appreciated via the "hybrid threats" paradigm. Grey zone operations and hybrid threats have been deemed as ultimately interchangeable terms.[10] However, the concept of grey zone operations emphasises the "construction" of a geographically defined area of low-intensity contestation.[11] Instead, the hybrid threats paradigm highlights how hostile activities may widen the range of options available to achieve a strategic objective without precluding the escalation to kinetic conflict, even if they can prepare the terrain for it.[12] In doing so, it emphasises the blending of different activities across multiple security domains within the DIMEFIL categorisation (diplomacy, intelligence, military, economy, finance, infrastructure and law),[13] and the production of spill-over effects from one domain to another.[14]

Disruptions to submarine cables may be corrosive, expanding from the infrastructure to the information domain, thus undermining trust in the Taiwanese authorities among both domestic and international audiences while raising doubts about their competence. The issue of attribution – central to hybrid threats – poses multiple dilemmas in the information domain for the bureaucratic actors tasked with guaranteeing Taiwan's security. How should they respond

g7.utoronto.ca/ict/2024-declaration.html#fnt1; G7, *G7 Foreign Ministries' Declaration on Maritime Security and Prosperity*, Charlevoix, Quebec, 14 March 2025, https://www.g7.utoronto.ca/foreign/250314-declaration.html.

10 Cordesman, Anthony H. and Grace Hwang, "Chronology of Possible Chinese Gray Area and Hybrid Warfare Operations", in *CSIS Reports*, updated 28 September 2020, https://www.csis.org/node/56684; Kouretsos, Peter, "Annex A: Contextualising Chinese Hybrid Warfare", in Ross Babbage (ed.), *Stealing a March. Chinese Hybrid Warfare in the Indo-Pacific: Issue and Options for Allied Defense Planners. Volume II: Case Studies*, Washington, Center for Strategic and Budget Assessment, 2019, p. 1-6, https://csbaonline.org/research/publications/stealing-a-march-chinese-hybrid-warfare-in-the-indo-pacific-issues-and-options-for-allied-defense-planners.

11 Baqués-Quesada, Josep, "Is Morocco Operating a Grey Zone in Ceuta and Melilla?", in *Defence Studies*, Vol. 23, No. 2 (2023), p. 198-214, https://doi.org/10.1080/14702436.2022.2159815; Kardon, Isaac B., *Combating the Gray Zone: Examining Chinese Threats to the Maritime Domain*, Testimony before the House Committee on Homeland Security, Subcommittee on Transportation and Maritime Security, 4 June 2024, https://carnegieendowment.org/posts/2024/06/combating-the-gray-zone-examining-chinese-threats-to-the-maritime-domain.

12 Insisa, Aurelio, "Hybrid After All: The 'Grey Zone', the 'Hybrid Warfare' Debate, and the PLA's Science of Military Strategy", in *Defence Strategic Communications*, Vol. 12 (Spring 2023), p. 165-186, https://doi.org/10.30966/2018.RIGA.12.1.

13 Oskarsson, Katerina, "The Effectiveness of DIMEFIL Instruments of Power in the Gray Zone", in *OPEN Publications*, Vol. 1, No. 2 (Winter 2017), p. 1-16, https://issuu.com/spp_plp/docs/the_effectiveness_of_dimefil_instruments_of_power_.

14 Giannopoulos, Georgios et al. (eds), *The Landscape of Hybrid Threats: A Conceptual Model*, Luxembourg, Publications Office of the European Union, 2021, https://doi.org/10.2760/44985.

when attribution of foul play is probable but not certain? How can bureaucratic actors avoid contradictory messaging in scenarios of uncertain attribution? And how can they communicate reassurance to the public and project deterrence to hostile actors in both cases where attribution is certain and when it remains uncertain? These are critical questions experts and policymakers – in Taiwan as well as elsewhere – should engage with in order to appreciate the full extent of the damage that submarine cables disruptions may cause.

This study proceeds as follows. Section 1 maps Taiwan's submarine cables, covering existing and upcoming projects by listing cables systems' landing points, owning companies and supplying companies. Section 2 frames threats to submarine cables as a form of hybrid threat to explain the rationale behind such operations. Section 3 examines in detail the major incidents that occurred to Taiwan's submarine cables in recent years and assesses the current threat landscape, while Section 4 sketches how a strategic communications approach can be implemented to counter such threats. The conclusion sums up the findings and discusses their wider significance for the Euro-Atlantic theatre in the context of non-diplomatic relations between the EU and Taiwan.

1 Mapping Taiwan's Submarine Cables

Taiwan's connection with its territories, as well as the outside world, relies on thirteen optic fibre submarine data cable systems

Taiwan's connection with its territories,[15] as well as the outside world, relies on thirteen optic fibre submarine data cable systems. These cables can be broadly divided in three groups. The first group consists of cable systems connecting Taiwan to its outlying islands and Mainland China. The second group includes cable systems connecting Taiwan to countries in Northeast Asia and Southeast Asia. The third group consists of cable systems connecting Taiwan to the US West Coast as well as selected East Asian landing points.

[15] Article 2 of the 1992 Act Governing Relations between the People of the Taiwan Area and the Mainland Area defines the territory under the effective control of authorities in Taipei as the "Taiwan Area" (*Taiwan diqu*). This area includes "Taiwan, Penghu, Kinmen, Matsu, and any other area under the effective control of the Government". See Taiwan Mainland Affairs Council, *Act Governing Relations between the People of the Taiwan Area and the Mainland Area*, 1992, https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=Q0010001. In detail, the area includes: Taiwan; the Penghu Islands (known also as the Pescadores Islands), located 50 km west of the main island in the Taiwan Strait; the Kinmen Islands, located in proximity to the bay of Xiamen in the Fujian Province, Mainland China; the Matsu Islands, located in front of the bay of Luoyuan – also in Fujian; the Wuqiu Islands, administratively part of the Kinmen County, facing the city of Putian (also in Fujian); the island of Tungsha (also known as Pratas), located in the South China Sea at around 450 km from the southern shores of Taiwan; and the two Nansha Islands – Taiping (also known as Itu Aba) and Zhongzhou – in the South China Sea, distant 1,500 km from Taiwan's southern shores.

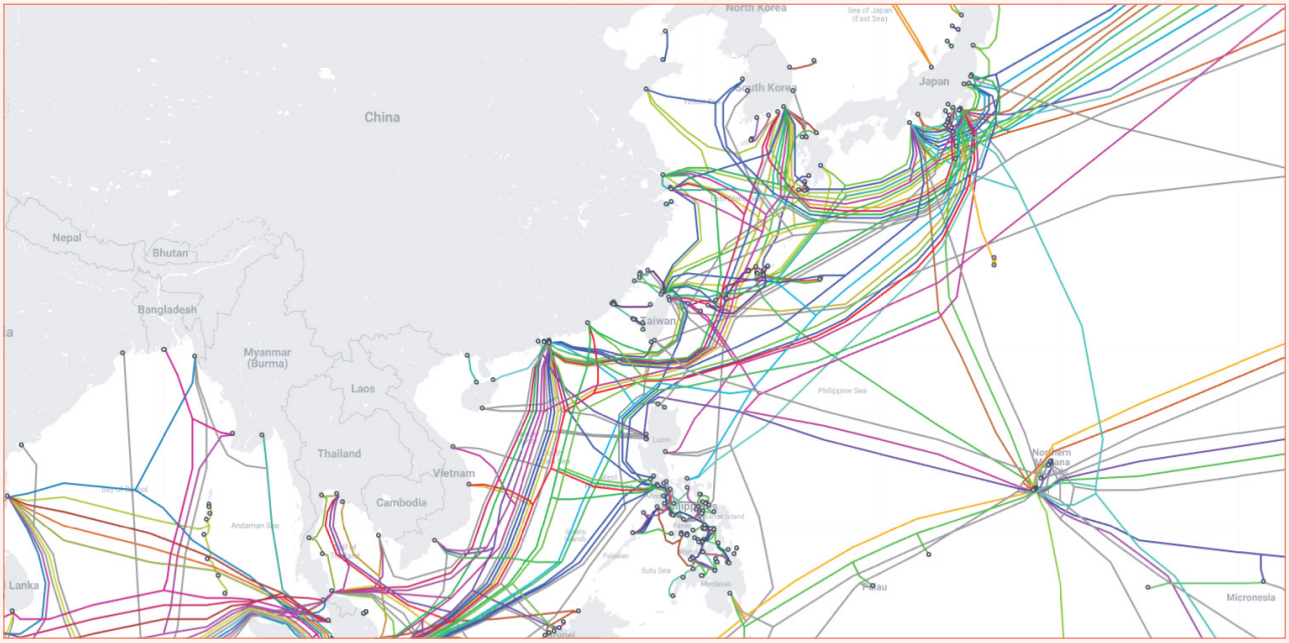


Figure 1 Taiwan and submarine cables in Asia

Source: TeleGeography, "Taiwan", in *Submarine Cable Map*, last updated 15 January 2026, https://www.submarinecablemap.com/country/taiwan.

Within the first group is the Taiwan Penghu Kinmen Matsu No.2 (TPKM2) and Taiwan Penghu Kinmen Matsu No.3 (TPKM3), both connecting Taiwan island with smaller islands and archipelagos part of its territory. In service since 2000 and 467 km long, TPKM2 connects Budai and Yuanli on Taiwan's western coast to Huxi (Penghu Islands) and Jinhu (Kinmen), respectively; and Tanshui on the northern coast to Dongyin (Matsu). The Yuanli-Jinhu section stretches across almost the entirety of the Taiwan Strait, given the Kinmen Islands' proximity to the Chinese Mainland.[16]

The sister project TPKM3 connects Tainan on the western coast of Taiwan to multiple landing points in the Penghu Islands (Huxi, Magong and Xiyu), stretching then to Jincheng, in the Kinmen Islands. A second section of TPKM3 bridges the Taiwanese city Taoyuan, in the north of the island, to multiple landing points on the Matsu Islands (Xiju, Nangan, Beigan, Dongyin). In total, TPKM3 covers 510 km and has been in service since 2013. Both TPKM2 and TPKM3 are owned by the Taiwanese telecommunication company Chunghwa Telecom and are supplied by the Japanese company NEC.[17]

Two other cable systems, connecting Taiwan to the People's Republic of China (PRC) can be included in this first group. The 21 km-long Cross-Straits Cable Network (CSCN), in service since 2012,

[16] TeleGeography, "Taiwan Penghu Kinmen Matsu No.2", in *Submarine Cable Map*, last updated 15 January 2026, https://www.submarinecablemap.com/submarine-cable/taiwan-penghu-kinmen-matsu-no-2-tpkm2.

[17] TeleGeography, "Taiwan Penghu Kinmen Matsu No.3", in *Submarine Cable Map*, last updated 15 January 2026, https://www.submarinecablemap.com/submarine-cable/taiwan-penghu-kinmen-matsu-no-3-tpkm3.

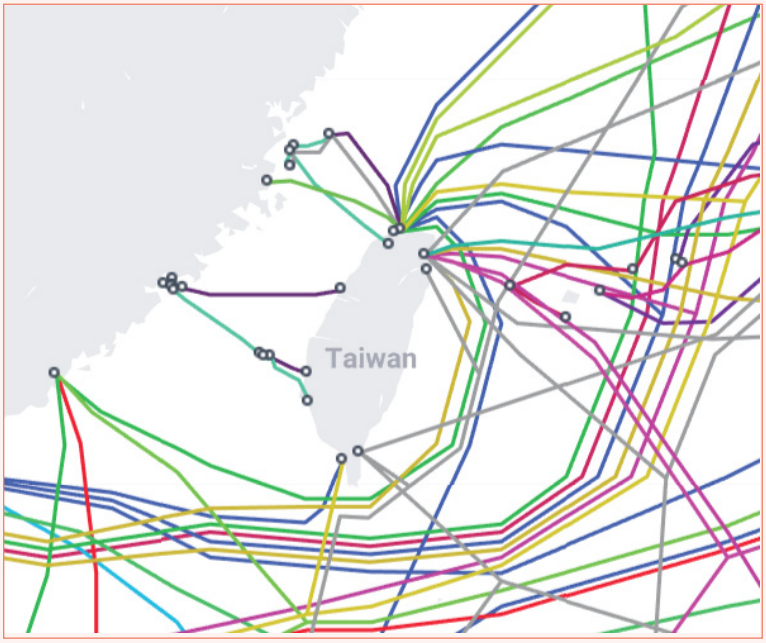


Figure 2 Taiwan's submarine cables landing points

Source: TeleGeography, "Taiwan", in *Submarine Cable Map*, cit.

connects two landing points in the Kinmen Islands to Dadeng Island and Guanyin, in the PRC's Fujian Province. CSCN's ownership is shared between the Taiwanese company Chunghwa Telecom and multiple Chinese companies – China Mobile, China Telecom and China Unicom.[18] The Taiwan Strait Express-1 (TSE-1) cable system, in service since 2013, connects the Tanshui landing point in northern Taiwan to Fuzhou, also in the Fujian Province, on Mainland China. Owned by a consortium of two Chinese (China Mobile and China Unicom) and four Taiwanese companies (Chunghwa, FET, TIGC and Taiwan Mobile), and supplied by the Chinese HMN Tech, this cable system stretches for 260 km.[19]

The second group includes cable systems, connecting Taiwan to Northeast and Southeast Asian countries. The FLAG North Asia Loop/REACH North Asia Loop, in service since 2001, extends for 9,504 km and links Taiwan to the Hong Kong Special Administrative Region (HKSAR), Busan (South Korea) and Wada (Japan). It is owned by Hong Kong's PCCW, Australia's Telstra and the British company FLAG, and supplied by France's ASN and Japan's Fujitsu.[20] EAC-C2C, a merger between the EAC with the C2C and one of the major

[18] TeleGeography, "Cross-Strait Cable Network", in *Submarine Cable Map*, last updated 15 January 2026, https://www.submarinecablemap.com/submarine-cable/cross-straits-cable-network-cscn.
[19] TeleGeography, "Taiwan Strait Express-1 (TSE-1)", in *Submarine Cable Map*, last updated 15 January 2026, https://www.submarinecablemap.com/submarine-cable/taiwan-strait-express-1-tse-1.
[20] TeleGeography, "FLAG North Asia Loop/REACH North Asia Loop", in *Submarine Cable Map*, last updated 15 January 2026, https://www.submarinecablemap.com/submarine-cable/flag-north-asia-loopreach-north-asia-loop.

submarine cable systems in the world, is 36,500 km long. It connects three landing points in Taiwan to the HKSAR, Mainland China (respectively in Nanhui, within the Shanghai municipality, and in Qingdao, in Shandong Province), as well as South Korea, Japan and the Philippines. The system is owned by Telstra and supplied by the American company SubCom, the Japanese company KDD-SCS and ASN.[21]

Other cable systems that can be included in the second group are the Southeast Asia-Japan Cable 2 (SJC2), the Asia Pacific Gateway, the APCN-2 and Apricot. The SJC2 system, launched in 2025 and 10,500 km long, links landing points in Fangshan and Tanshui to the HKSAR (Chung Hom Kok) and Shanghai, as well as to other landing points in Japan, South Korea, Vietnam, Thailand and Singapore. Multiple companies from these countries, including Taiwan's Chunghwa Telecom and Donghwa Telecom, own the cable system, which is supplied by NEC.[22]

The Asia Pacific Gateway cable system is 10,400 km long, has been in service since 2016, is owned by a wide consortium including both Chunghwa Telecom and a number of Chinese telecommunication companies, and supplied by NEC. From the landing point of Toucheng, it connects Taiwan to the Shanghai municipality in the PRC, the HKSAR, Japan, South Korea, as well as Vietnam, Thailand, Malaysia and Singapore.[23]

The APCN-2 cable system is 19,000 km long, has been in service since 2001, is owned by an even larger consortium including Chunghwa Telecom together with companies from more than ten countries, and it is also supplied by NEC. It connects Taiwan to landing points in Mainland China and Japan.[24]

Finally, the Apricot cable system has connected the Taiwanese landing point of Toucheng to the US territory of Guam and to Minamibōsō in Japan since late 2025. Apricot is owned by a consortium including Meta, Google and Chunghwa Telecom, among others, and is supplied by SubCom. A further extension to the Philippines, Indonesia and Singapore is scheduled to be operative by 2027, eventually reaching a length of 11,972 km.[25]

[21] TeleGeography, "EAC-C2C", in *Submarine Cable Map*, last updated 15 January 2026, https://www.submarinecablemap.com/submarine-cable/eac-c2c.
[22] TeleGeography, "Southeast Asia-Japan Cable 2", in *Submarine Cable Map*, last updated 15 January 2026, https://www.submarinecablemap.com/submarine-cable/southeast-asia-japan-cable-2-sjc2.
[23] TeleGeography, "Asia Pacific Gateway (APG)", in *Submarine Cable Map*, last updated 15 January 2026, https://www.submarinecablemap.com/submarine-cable/asia-pacific-gateway-apg.
[24] TeleGeography, "APCN-2", in *Submarine Cable Map*, last updated 15 January 2026, https://www.submarinecablemap.com/submarine-cable/apcn-2.
[25] TeleGeography, "Apricot", in *Submarine Cable Map*, last updated 15 January 2026, https://www.submarinecablemap.com/submarine-cable/apricot; Jose, Ashley Erika O., "PLDT Eyes to Finish Apricot Submarine Cable Project by 2027", in *BusinessWorld Online*,

Within the third group is the Trans-Pacific Express (TPE) cable system, which extends for 17,968 km, connecting Tanshui to the US West Coast as well as to Mainland China once again, South Korea and Japan. The cable system is owned by a consortium including Chunghwa Telecom together with Chinese and American companies, such as China Telecom, China Unicom, AT&T and Verizon, and it is supplied by SubCom.[26]

The 11,629 km-long cable system FASTER connects the landing point of Tanshui to the US West Coast, as well as to Japan. This cable system is owned by a consortium including Chinese companies such as China Mobile and China Telecom, as well as Google, and it is supplied by NEC.[27]

The New Cross Pacific (NCP) cable system, in service since 2018, has a layout similar to the TPE, connecting another northern landing point, Toucheng, to US West Coast in Oregon. NCP also links to Mainland China (two locations in the Shanghai municipality), South Korea and Japan. Long 13,618 km, NCP is owned by a consortium including Chunghwa Telecom together with companies such as Microsoft and Softbank, as well as China Telecom and China Unicom, and it is supplied by SubCom.[28]

The most recent cable system within this group is the Pacific Light Cable Network. In service since 2022 and jointly owned by Google and Meta, it links once again Toucheng to the Philippines and finally to US West Coast. Long 11,806 km, it is also supplied by SubCom.[29]

Adding to the fourteen described above, there are six other cable systems scheduled within the next decade. Starting from 2026, the Taiwan-Philippines-US (TPU) cable system, owned by Google, will connect the Dawu landing point in southern Taiwan to Claveria in the Philippines and to the US West Coast, via Guam and Tinian (in the Northern Mariana Islands), extending for 13,600 km across most of the Pacific Ocean.[30] Scheduled for 2027 and with a planned length of 12,482 km, the ORCA cable system will link Toucheng to two separate landing points in California. The cable system will be owned by Meta

2 April 2025, https://www.bworldonline.com/?p=663254.

[26] TeleGeography, "Trans-Pacific Express (TPE)", in *Submarine Cable Map*, last updated 15 January 2026, https://www.submarinecablemap.com/submarine-cable/trans-pacific-express-tpe-cable-system.

[27] TeleGeography, "FASTER", in *Submarine Cable Map*, last updated 15 January 2026, https://www.submarinecablemap.com/submarine-cable/faster.

[28] TeleGeography, "New Cross Pacific (NCP) Cable System", in *Submarine Cable Map*, last updated 15 January 2026, https://www.submarinecablemap.com/submarine-cable/new-cross-pacific-ncp-cable-system.

[29] TeleGeography, "Pacific Light Cable Network", in *Submarine Cable Map*, last updated 15 January 2026, https://www.submarinecablemap.com/submarine-cable/pacific-light-cable-network-plcn.

[30] TeleGeography, "TPU", in *Submarine Cable Map*, last updated 15 January 2026, https://www.submarinecablemap.com/submarine-cable/tpu.

and supplied by ASN.[31] The Asia United Gateway East (AUG East) will link Taiwan to Japan, South Korea, the Philippines, Malaysia, Singapore, Brunei and Indonesia from 2029. AUG East will stretch for a total of 8,900 km and be supplied by NEC. Ownership will be divided among multiple companies, including Amazon, but without any Taiwanese participation.[32]

Another cable system slated to start in 2029, Candle, owned by a consortium including Meta and Softbank, aims instead to connect Toucheng to landing points in Japan, the Philippines, Singapore, Malaysia and Indonesia.[33] Also scheduled for 2029 is E2A, which will connect Toucheng to the US West Coat, South Korea and Japan. Supplied by ASN, the cable system will be owned by a consortium including Chunghwa Telecom, South Korea's SK Broadband, Japan's Softbank and Verizon.[34] Finally, the Taiwan-Matsu No. 4 cable system, scheduled to be in service at the end of 2026, will connect Tanshui to three landing points in the Matsu Islands. Owned and supplied by Chunghwa Telecom thanks to subsidies by Taiwan's Ministry of Digital Affairs, it will be 300 km long.[35]

Table 1 provides a list of the operating submarine cable networks connecting Taiwan. It includes the landing points on the island of Taiwan; other landing points either on Taiwan's outlying islands or on other polities; the total length in kilometres of each cable network; the date each cable network entered service; Taiwanese companies and/or foreign companies from relevant countries that own or are members of consortia owning the cable networks; and the cable network suppliers.

Table 2 provides a list of submarine cable networks connecting Taiwan that are scheduled to come into service.

[31] TeleGeography, "ORCA", in *Submarine Cable Map*, last updated 15 January 2026, https://www.submarinecablemap.com/submarine-cable/orca.

[32] TeleGeography, "Asia United Gateway East", in *Submarine Cable Map*, last updated 15 January 2026, https://www.submarinecablemap.com/submarine-cable/asia-united-gateway-east-aug-east.

[33] TeleGeography, "Candle", in *Submarine Cable Map*, last updated 15 January 2026, https://www.submarinecablemap.com/submarine-cable/candle.

[34] TeleGeography, "E2A", in *Submarine Cable Map*, last updated 15 January 2026, https://www.submarinecablemap.com/submarine-cable/e2a.

[35] Chiu, Charlotte, "Taiwan's Submarine Cable Network Strategic Value and Future Outlook", in *Ketagalan Media*, 23 February 2025, https://wp.me/p4ka8Y-8qn.

Table 1 Operating submarine cables connecting Taiwan

Cable system name	Landing points on Taiwan island	Other relevant landing point	Total length in km	In service since	Relevant owning companies	Suppliers
Taiwan Penghu Kinmen Matsu No.2 (TPKM2)	Budai, Yuanli, Tanshui	Huxi [Penghu, ROC], Jinhu [Kinmen, ROC], Dongyin [Matsu, ROC]	467	2000	Chunghwa Telecom [ROC]	NEC [JAP]
Taiwan Penghu Kinmen Matsu No.3 (TPKM3)	Tainan, Taoyuan	Huxi, Magong, Xiyu [Penghu, ROC], Jincheng [Kinmen, ROC], Xiju, Nangan, Beigan, Dongyin [Matsu, ROC]	510	2013	Chunghwa Telecom	NEC [JAP]
Cross-Straits Cable Network (CSCN)	Guningtou, Jinning	Fujian [PRC]	21	2012	Chunghwa Telecom China Mobile, China Telecom. China Unicom [PRC]	information not publicly available
Taiwan Strait Express-1 (TSE-1)	Tanshui	Fuzhou [PRC]	260	2013	Chunghwa, FET, TIGC, Taiwan Mobile [ROC] China Mobile, China Unicom [PRC]	HMN Tech [PRC]
FLAG North Asia Loop / REACH North Asia Loop	Toucheng	Tong Fuk [HKSAR], Busan [ROK], Wada [JAP]	9,504	2001	PCCW [HKSAR]; Telstra [AUS]; FLAG [UK]	ASN, Fujitsu [JAP]
EAC-C2C	Pa Li, Tanshui, Fangshan	Chung Hom Kok, Tseung Kwan O [HKSAR]; Shanghai, Qingdao [PRC], Shima, Chikura, Ajigaura [JAP], Shindu-Ri, Busan [ROK], Cavite [PHI]	36,500		Telstra	ASN, KDD-SCS [JAP], SubCom [US]
Southeast Asia-Japan Cable 2	Fangshan, Tanshui	Chung Hom Kok [HKSAR]; Shanghai [PRC]; Shima, Chikura [JAP], Busan [ROK], Quy Nhom [VNM], Songkhla [THA]; Changi South [SGP]	10,500	2025	Chunghwa Telecom, Donghwa Telecom [ROC] China Mobile [PRC]; KDDI [JAP], Meta [US], SK Broadband [ROK]	NEC
Asia Pacific Gateway	Toucheng	Shanghai, Chongming [PRC]; Tseung Kwan O [HKSAR]; Shima Maruyama [JAP]; Busan [ROK]; Danang [VNM]; Songkhla [THA]; Cherating [MLY]; Changi South [SGP]	10,400	2016	Chunghwa Telecom China Mobile, China Telecom, China Unicom [PRC]; KT, LG Uplus [ROK]; Meta [US], NTT [JAP]	NEC
APCN-2	Toucheng	Shantou [PRC]; Chikura [JAP]	19,000	2001	Chunghwa Telecom China Telecom, China Unicom [PRC]; HKBN, PCCW [HKSAR]; KT, LG Uplus [ROK]; KDDI, NTT, Softbank [JAP]; AT&T, Verizon [US]; BT, Vodafone [UK]; Orange [FRA]; Telstra [AUS]	NEC

Table 1 Operating submarine cables connecting Taiwan (continued)

Apricot	Toucheng	Minamibōsō [JAP]; Guam [US]	11,972 [planned]	2025, extension scheduled in 2027	Chunghwa Telecom Meta, Google [US]; NTT [JAP]	SubCom
Trans-Pacific Express (TPE)	Tanshui	Nedonna Beach [US], Shanghai, Qingdao [PRC], Geoje [ROK]; Maruyama [JAP]	17,968	2008	Chunghwa Telecom China Telecom, China Unicom [PRC], AT&T, Verizon [US]; KT [ROK]; NTT [JAP]	SubCom
FASTER	Tanshui	Bandon [US]; Shima, Chikura [JAP]	11,629	2016	China Mobile, China Telecom [PRC]; Google [US]; KDDI [JAP]	NEC
New Cross Pacific (NCP)	Toucheng	Pacific City (US), Shanghai [PRC], South Korea, Japan	13,618	2018	Chunghwa Telecom Microsoft [US]; Softbank [JAP]; China Telecom, China Unicom [PRC]	SubCom
Pacific Light Cable Network	Toucheng	El Segundo [US], Baler [PHI]	11,806	2022	Google, Meta [US]	SubCom

Table 2 Scheduled submarine cables connecting Taiwan

Cable system name	Landing points on Taiwan island	Other relevant landing point	Total length in km	In service since	Relevant owning companies	Suppliers
Taiwan-Philippines-US (TPU)	Dawu	Tinian, Guam, Eureka [US], Claveria [PHI]	13,600	2026	Google	
ORCA	Toucheng	Manchester, Hermosa Beach [US]	12,482	2027	Meta	ASN
Asia United Gateway East (AUG East)	Dawu, Wujie	Wada [JAP]; Gunsan [ROK]; Luna [PHI]; Mumong [BRU]; Sedili [MLY]; Changi [SGP]; Batam [IDN]	8,900	2029	Chunghwa Telecom Amazon Web Services, Microsoft, [US]; Arteria [JAP]; Dreamline [ROK]	NEC
Candle	Toucheng	Maruyama [JAP]; Nasugbu, Baler [PHI]; Changi [SGP]; Sedili [MLY]; Batam [IDN]	8,000	2029	Meta [US], IPS, Softbank [JAP]	NEC
E2A	Toucheng	Morro Bay [US]; Maruyama [JAP]; Busan [ROK]	12,500	2029	Chunghwa Telecom SK Broadband [ROK]; Softbank [JAP]; Verizon [US]	ASN
Taiwan-Matsu No.4	Tanshui	Dongyin, Nangang, Xiju [Matsu, ROC)	300	2026	Chunghwa Telecom	Chunghwa Telecom

Hybrid threats create ambiguity and hide real intent, manipulate thresholds concerning detection and response, exploit political cleavages, and favour dispersion of response forces

2 HYBRID THREATS – THE RATIONALE FOR TARGETING SUBMARINE CABLES

The concept of "hybrid *threats*" is arguably the most effective tool to understand why actors target submarine cables. Yet the enduring popularity of the contiguous term "hybrid *war/warfare*" continues to create confusion. As a matter of fact, Russia's targeting of European countries' infrastructures against the backdrop of the War in Ukraine has led to a further entrenchment of the term "hybrid war/warfare" in the public discourse due to its use by generalist media.[36] Originally, throughout the second half of the 2000s, the term hybrid warfare referred to military innovations on the battlefield, describing a "range of different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder".[37] Following Russia's operations in Ukraine since 2014, the ensuing politicisation of the term among Western practitioners and academics, and the increasing Western attention towards Chinese sovereignty-affirming operations in its near seas, eventually led to a more expansive understanding of hybrid warfare.[38] Hybrid warfare migrated from the battlefield to the full spectrum of great power competition. The result was an unresolved "tension between the idea of hybrid warfare as a form or mode of warfare versus its understanding as part of a strategy".[39]

The adoption of the term "hybrid threats" by institutions such as the EU and NATO reflects the need to move beyond "war/warfare" to achieve conceptual clarity.[40] However, there is still a lack of consensus over the purpose of hybrid threats are designed to serve. Are hybrid threats used to influence, interfere or coerce?[41] The issue

[36] Butler, Katherine, "Drone Dilemma: How Russia's 'Hybrid War' Is Using Fear to Destabilise Europe", in *The Guardian*, 8 October 2025, https://www.theguardian.com/p/x3cqdf.

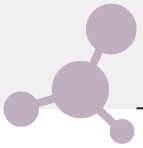
[37] Hoffman, Frank G., *Conflict in the 21st Century: The Rise of Hybrid Warfare*, Arlington, Potomac Institute for Policy Studies, 2007, p. 8, https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.

[38] Fridman, Ofer, *Russian 'Hybrid Warfare'. Resurgence and Politicisation*, New York, Oxford University Press, 2018, p. 158-159; Libiseller, Chiara, "'Hybrid Warfare' as an Academic Fashion", in *Journal of Strategic Studies*, Vo. 46, No. 4 (2023), p. 858-880, https://doi.org/10.1080/01402390.2023.2177987.

[39] Aoi, Chiyuki et al., "Introduction 'Hybrid Warfare in Asia: Its Meaning and Shape'", in *The Pacific Review*, Vol. 31, No. 6 (2019), p. 693-716 at p. 701, https://doi.org/10.1080/09512748.2018.1513548.

[40] Council of the EU website: *Hybrid Threats*, updated 15 December 2025, https://www.consilium.europa.eu/en/policies/hybrid-threats; NATO website: *Countering Hybrid Threats*, updated 7 May 2024, https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats.

[41] Wigell, Mikael, "Hybrid Interference as a Wedge Strategy: A Theory of External Interference in Liberal Democracy", in *International Affairs*, Vol. 95, No. 2 (2019), p. 255-275, https://doi.org/10.1093/ia/iiz018; Giannopoulos, Georgios et al. (eds), *The Landscape of Hybrid Threats*, cit., p. 36-37; West, Michael J. and Aurelio Insisa, "Reunifying Taiwan with



is particularly relevant in the case of China's Taiwan policy. While Beijing has incontrovertibly stated its intention to achieve unification with Taiwan as a milestone of its process of "national rejuvenation",[42] it remains debatable whether China's projection of hybrid threats is (1) geared towards the preparation of a coercive military takeover of the island within a short-term timeline, (2) aimed at influencing the electoral choices of the Taiwanese public in favour of forces open to the possibility of peaceful unification, or (3) an open-ended endeavour in itself, allowing Beijing to pursue multiple courses of action – the option this author considers most likely.[43]

The opacity surrounding the desired outcome of the PRC's hybrid threat projection against Taiwan is most likely deliberate

The opacity surrounding the desired outcome of the PRC's hybrid threat projection against Taiwan is most likely deliberate. Hybrid threats create ambiguity and hide real intent, manipulate existing thresholds concerning detection and response, exploit cleavages within liberal democratic societies and between different jurisdictions, generate unanticipated effects and favour dispersion of forces instead of concentration and attrition with the aim to overstretch opponents' capabilities.[44] Ultimately, actors engaged in hybrid threat projection aim at leading opponents "into a state of cognitive impasse regarding its political, strategic, and tactical intentions".[45]

From this perspective, it is possible to appreciate why Taiwan's submarine cables constitute an ideal target. The severing of submarine cables poses a dilemma concerning the scope of such operations. Is it the prelude to a major kinetic operation after having isolated and blinded the opponent? Or is it an operation mainly aimed at testing the logistical and economic resilience of the target? Is it a way to gradually mollify trust in the targeted actor's capacity to respond to attacks, aiming at producing a sense of vulnerability and impotence vis-à-vis the threat actor, thus allowing the threat actor itself to "win without fighting"? Or is it, simply by virtue of its execution, a way of

China through Lawfare", in *The China Quarterly*, No. 257 (2024), p. 186-201, https://doi.org/10.1017/S0305741023000735.

[42] Chinese Communist Party, *Resolution of the Chinese Communist Party Central Committee on the Major Achievements and Historical Experiences of the Party's One-Hundred-Year Struggle*, 16 November 2021, https://english.www.gov.cn/policies/latestreleases/202111/16/content_WS6193a935c6d0df57f98e50b0.html; Chinese State Council Information Office, *The Taiwan Question and China's Reunification in the New Era*, 10 August 2022, https://english.news.cn/20220810/df9d3b8702154b34bbf1d451b99bf64a/c.html.

[43] On the issue of potential timelines for unification between Taiwan and China, see: Pugliese, Giulio and Aurelio Insisa, "How to Use the Maximum of Potential for the EU-Taiwan Cooperation: What Can the EU Learn from the US and Other Actors?", in *European Parliament Studies*, September 2025, p. 33-34, https://doi.org/10.2861/6301949.

[44] Giannopoulos, Georgios et al. (eds), *The Landscape of Hybrid Threats*, cit., p. 11; Mumford, Andrew and Pascal Carlucci, "Hybrid Warfare: The Continuation of Ambiguity by Other Means", in *European Journal of International Security*, Vol. 8, No. 2 (May 2023), p. 192-206, https://doi.org/10.1017/eis.2022.19.

[45] Mumford, Andrew and Pascal Carlucci, "Hybrid Warfare", cit., p. 199.

Submarine cables are an inherently fragile infrastructure, and damages to them are common events

opening multiple paths to all the options described above?

Submarine cables are an inherently fragile infrastructure, and damages to them are common events. According to one estimate, there are about 150-200 incidents a year, mostly due to fishing or anchoring, while natural hazards, abrasion and equipment failure, albeit less common, can also cause harm.[46] This fragility is exploited by hostile actors who have an interest in portraying deliberate disruptions as accidental damages (or even the other way round, in the most brazen cases) in order to undermine the military, constabulary, technological and diplomatic responses to threats against submarine cables. Hybrid threats in the infrastructure domain inevitably reverberate in the information domain, creating opportunities for both foreign and domestic actors to manipulate information surrounding incidents in order to reshape public perceptions of a polity's security and institutional effectiveness, extending beyond the immediate damage to infrastructure.

3 Disruptions to Taiwan's Submarine Cables

Between 2018 and 2022, submarine cables enabling internet connectivity between Taiwan and the Matsu Islands were disrupted 27 times by anchors dragging and trawling nets from Chinese fishing vessels.[47] Matsu residents, however, experienced their first major disruption – a six-week internet outage – following the severing of the TPKM2 and TPKM3 cables respectively on 2 February and 8 February 2023.[48] Following speculation of Chinese foul play by Taiwanese legislators, the National Communications Commission stopped short of accusing Beijing, stating that a Chinese fishing vessel and an unidentified cargo ship had accidentally severed the cables.[49] The disruption, while considered accidental, had global resonance given Beijing's intense pressure against Taipei, highlighting the vulnerability of these Taiwanese infrastructures.

Concerns about Taiwan's submarine cables re-emerged in January 2025, when open intelligence sources revealed that a Russian vessel

[46] Clare, Mike, *Submarine Cable Protection and the Environment: Keeping Subsea Cables Safe from Volcanic Eruptions*, International Cable Protection Committee, November 2025, p. 14, https://www.iscpc.org/publications/submarine-cable-protection-and-the-environment.

[47] Tobin, Meaghan and Vic Chiang, "Internet Outage Has Taiwan Worried about Threat from Chinese Sabotage", in *The Washington Post*, 9 March 2023, https://www.washingtonpost.com/world/2023/03/09/taiwan-matsu-internet-access-china-fishing.

[48] Ibid.

[49] "NCC Confirms Undersea Cables Linking Taiwan, Matsu Cut by Vessels", in *Focus Taiwan*, 16 February 2023, https://focustaiwan.tw/society/202302160022; "Taiwan-Matsu Submarine Cable Severed by Chinese Vessell – Backup Communications Will Be Brought Up to Normal Operational Levels by Year-End" [in Chinese], in *CNA*, 16 February 2023, https://www.cna.com.tw/news/aipl/202302160263.aspx.

Concerns about Taiwan's submarine cables re-emerged in January 2025

flying a Belizean flag of convenience, the *Vasily Shukshin*, travelled for about three weeks between December 2024 and January 2025 in a suspicious criss-cross pattern in proximity to the Fangshan landing point – on the southern shores of Taiwan, where the cable systems EAC C2C and SJC2 reach Taiwan.[50] The presence of the *Vasily Shukshin* near Taiwan's southern shores reminded observers of an incident that occurred in the Baltic Sea some weeks prior.

On 17-18 November 2024, the Chinese-flagged bulk carrier *Yi Peng 3* severed, with its anchor and within Sweden's exclusive economic zone, the BCS East–West Interlink cable connecting Sweden and Lithuania and the C-Lion 1 cable connecting Finland and Germany, causing disruptions to data transfers and internet capacity in the Nordic–Baltic region.[51] Information concerning the *Yi Peng 3* incident continues to be uncertain. Beyond contradicting information about the presence of a Russian captain on the vessel, the results of a Swedish investigation conducted on board of the ship have not been disclosed.[52] According to Swedish authorities, Chinese authorities obstructed their efforts.[53] Taken together, the cases of the *Vasily Shukshin* in the waters near Taiwan and of the *Yi Peng 3* in the Baltic Sea leave the door open for speculations, albeit unsubstantiated, of cooperation, if not coordination in the projection of hybrid threats between Russian and Chinese actors across the Asia-Pacific and the Euro-Atlantic theatres.[54]

A third incident also happened in January 2025. On 3 January, the Hong Kong-registered, Cameroon-flagged, Chinese-crewed ship *Shunxin 39* damaged the TPE cable system, connecting Taiwan to the United States, off the coast of the Taiwanese city of Keelung. The vessel travelled in a criss-cross pattern while dragging its anchor, pointing to intentional action. The damage did not cause a disruption in the data flow, however.[55] Hours after the incident, Taiwan's coast

[50] Ray Powell (@GordianKnotRay), "IT'S LEAVING! ...", X post, 14 January 2025, https://x.com/GordianKnotRay/status/1878953699617468488.
[51] Andersson, Patrik et al., "What the Yi Peng 3 Cable-Cutting Incident Reveals about China-Russia Relations", in *SNCC Commentaries*, No. 3/2025, https://kinacentrum.se/en/?p=7792.
[52] Jönsson, Oskar, "Aboard the Chinese Vessel: Significant Observations" [in Swedish], in *SVT Nyheter*, 20 December 2024, https://www.svt.se/nyheter/utrikes/var-ombord-pa-kinesiska-fartyget-betydelsefulla-iakttagelser.
[53] Milne, Richard, "Sweden Criticises China for Refusing Full Access to Vessel Suspected of Baltic Sea Cable Sabotage", in *Financial Times*, 22 December 2024, https://www.ft.com/content/9094dcc4-b0f8-4191-b6f6-d1196a5f2822.
[54] On the potential implications emerging from different configurations of Sino-Russian coordination, see Andersson, Patrik et al., "What the Yi Peng 3 Cable-Cutting Incident Reveals", cit., p. 3-4.
[55] DCHTFP, *Hidden Highways of the Internet*, cit., p. 22; Hioe, Brian, "Is China's Latest Form of Grey Zone Activity Cutting Submarine Cables?", in *New Bloom Magazine*, 7 January 2025, https://newbloommag.net/?p=38695. The *Shunxin 39* was also registered under two additional flag state identities, both using the name *Xingshun 39*: one flying the Tanzanian flag and the other flying the Cameroonian flag. See: Lloyd's List Intelligence, "Taiwan Is Hunting One Cable Cutting Vessel Disguised with Three

guard (the ROC Coast Guard) dispatched a ship and found *Shunxin 39* in waters north of Taiwan but failed to board it or force its return and docking for inspections in Keelung due to rough weather conditions. With *Shunxin 39* sailing towards Busan, Taiwanese authorities sought assistance from their South Korean counterparts.[56] Yet, no law enforcement developments have been made public. It is also worth noting that a few days after the TPE cable's disruption, a Mongolian-flagged vessel with a Chinese moniker, the *Baoshun*, was spotted navigating in an erratic criss-cross pattern similar to that of the *Shunxin 39* around the coast of Shimen in northern Taiwan, in an area with a high concentration of submarine cables, before being escorted away by Taiwan's constabulary forces, reinforcing the suspicions of a concerted offensive against the island's data infrastructure.[57]

On 25 February 2025, the Chinese-registered ship Hong Tai 58 damaged the Taiwan-Penghu segment of the TPKM3 undersea cable system

Finally, on 25 February 2025, the Chinese-registered, Togolese-flagged, Chinese-crewed ship *Hong Tai 58* damaged the Taiwan-Penghu segment of the TPKM3 undersea cable system, without however causing any data disruption because of the activation of a redundant backup cable.[58] The ROC Coast Guard identified the vessel and escorted it to the port of Anping on the same day of the incident, yet it eventually released seven of the eight members of the crew (all PRC-passport holders) to Mainland China, the captain being the exception. The Tainan Prosecutor Office indicted and eventually sentenced him to three years of imprisonment for the damaging of submarine cable infrastructure "by means of theft, destruction, or other illegal means" – but not, notably, for threatening national security due to insufficient evidence.[59]

After the *Hong Tai 58* incident, no other major disruptions to Taiwan's submarine cables were publicly detected or announced by Taiwanese authorities throughout 2025.[60] According to Ma Cheng-kun,

Separate Digital Identities", in *Lloyd's List Intelligence Blog*, 8 January 2025, https://www.lloydslistintelligence.com/thought-leadership/blogs/taiwan-is-hunting-one-cable-cutting-vessel-disguised-with-three-separate-digital-identities.

[56] Yang, William, "Chinese Vessel Suspected of Damaging Undersea Cable Near Taiwan", in *VOA News*, 7 January 2025, https://www.voanews.com/a/7926977.html.

[57] "Suspected Chinese Vessel with Flag of Convenience Manoeuvring Erratically Once Again, Targeting the Northern Submarine Cable Zone" [in Chinese], in *The Liberty Times*, 6 January 2025, https://news.ltn.com.tw/news/politics/breakingnews/4914711.

[58] DCHTFP, *Hidden Highways of the Internet*, cit., p. 24.

[59] Chiang, Huang-Chih and Po-Hsiang Liao, "The 'Hong Tai 58' Case and Criminal Jurisdiction Over Submarine Cable Sabotage in 'New' Internal Waters", in *Prospects & Perspectives*, No. 65 (25 November 2025), https://www.pf.org.tw/en/pfen/33-11657.html; Taiwan National Communications Commission, *Telecommunications Management Act*, 2 July 2025, https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=K0060111.

[60] The absence of disruptions to submarine cables since February 2025 did not mean, however, a decrease in the amount of hybrid threats targeting the island. According to the National Security Bureau of Taiwan, Taiwan's critical infrastructure (namely, government administration and agencies, energy, communications and transmission, transportation, emergency rescue and hospitals, water resources, finance, science parks and industrial parks, and food) suffered from 2.6 million intrusion attempts per day from China in 2025, a 6 per cent increase compared to 2024. See: Taiwan National

Figure 3 TPKM2 cable system

Source: TeleGeography, "Taiwan Penghu Kinmen Matsu No.2", cit.

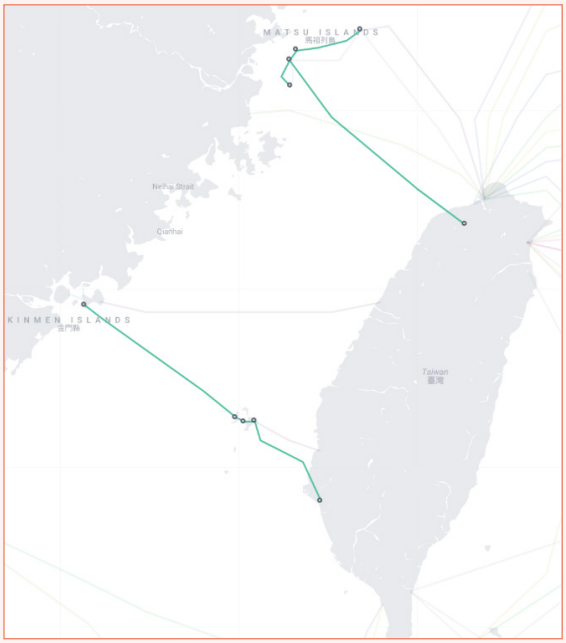


Figure 4 TPKM3 cable system

Source: TeleGeography, "Taiwan Penghu Kinmen Matsu No.3", cit.

a leading Taiwanese academic expert in Chinese military affairs, this state of affairs may be the result of the continuing purges affecting senior military officers of the People's Liberation Army (PLA) under Xi Jinping. In particular, Ma points to the purge of He Weidong, former second-ranking Vice Chairman of the Central Military Commission of the Chinese Communist Party (CCP), in October, described as a key figure in favour of imposing pressure on Taiwan, and the consequently increasing influence of the first-ranking Vice Chairman Zhang Youxia, who allegedly opposes escalation via hybrid threats.[61]

This explanation ignores the wider implications of the Sino-American détente that emerged throughout 2025 under the second Trump Administration. Tellingly, no major military exercise in the mould of those launched in 2022 after the pathbreaking visit to Taiwan by the then Speaker of the US House of Representatives Nancy Pelosi was carried out between April and 29-30 December 2025 – only eleven days after the US announced a record 11 billion

Security Bureau, *Analysis on China's Cyber Threats to Taiwan's Critical Infrastructure in 2025*, 4 January 2025, https://www.nsb.gov.tw/en/assets/documents/%E6%96%B0%E8%81%9E%E7%A8%BF/9976f2e1-3a8a-4fa2-9a73-b0c80fca1f04.pdf.

[61] Hope, Arran, "Beijing's New Approach towards Taiwan", in *China Brief*, Vol. 25, No. 20 (31 October 2025), p. 2-7 at p. 4-5, https://jamestown.org/?p=822336. The first major round of purges within the PLA under Xi Jinping occurred between 2014 and 2016. The second round has been ongoing since 2023. See Wuthnow, Joel, "Can Xi Jinping Control the PLA?", in *China Leadership Monitor*, No. 83 (1 March 2025), https://www.prcleader.org/post/can-xi-jinping-control-the-pla; Tang, K. Tristan, "Cronyism and Failed Promotion: Xi's PLA Purge", in *China Brief*, Vol. 25, No. 19 (18 October 2025), p. 30-33, https://jamestown.org/?p=822549.

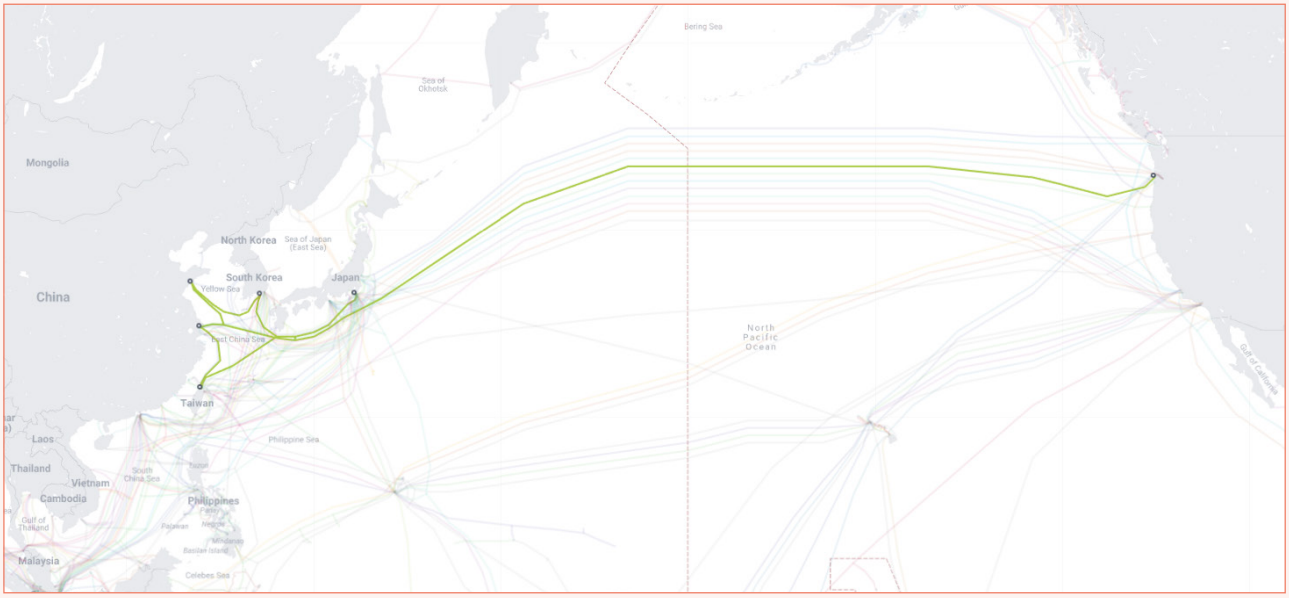


Figure 5 Trans-Pacific Express cable system

Source: TeleGeography, "Trans-Pacific Express (TPE)", cit.

US dollars arms package to Taiwan.[62] Whether a slowdown in the Beijing-Washington détente would coincide with new disruptions to Taiwan's submarine cables remains a critical question for regional security as of early 2026.

Against this backdrop, it is possible to provide a broader assessment of the disruptions that occurred between 2023 and 2025. A first feature to examine is which cable systems were affected. The disruptions on 2 February 2023, 8 February 2023 and 25 February 2025 concerned the two cable systems connecting Taiwan to the Matsu Islands and Penghu Islands – TPKM2 and TPKM3. The exception was the disruption occurred on 3 January 2025, which affected the TPE cable system connecting Taiwan to the US West Coast. Assuming that these incidents were all planned and executed by Chinese actors, they highlight the vulnerability of Taiwan's outlying islands facing the Chinese Mainland vis-à-vis Beijing. Yet, as always in the case of hybrid threats, attribution remains the most crucial issue. Only in the case of the *Hong Tai 58* could Taiwanese authorities apprehend, indict and sentence culprits. In fact, even in this case, Taiwanese authorities failed to build a case based on the "intent to endanger national security or social stability"[63] – the very same objective of hybrid threats. The *Hong Tai 58* incident highlights the major monitoring, constabulary and jurisprudential challenges in imposing a cost on

[62] Lee, Yimou et al., "China Encircles Taiwan in Massive Military Display", in *Reuters*, 30 December 2025, https://www.reuters.com/world/china/china-launches-live-firing-drills-around-taiwan-its-biggest-war-games-date-2025-12-30.

[63] Art. 72, Taiwan National Communications Commission, *Telecommunications Management Act*, cit. See Chiang, Huang-Chih and Po-Hsiang Liao, "The 'Hong Tai 58' Case", cit.

The vessels involved in the January and February 2025 incidents were Chinese-crewed and owned by Chinese or Hong Kong companies

threat actors and exercising deterrence.[64]

A final point to discuss is the type of vessels used to provoke these disruptions – assuming the responsibility of Chinese bureaucratic actors. The vessels involved in the January and February 2025 incidents, *Shunxin 39* and *Hong Tai 58*, as well as the one suspected of planning a disruption in January 2025, *Baoshun*, were Chinese-crewed and owned by Chinese or Hong Kong companies, although they flew flags of convenience. This suggests the deployment of the Chinese Maritime Militia (CMM), the PRC's third maritime force, institutionally separated from the PLA Navy and the China Coast Guard yet ultimately "tethered" to the PLA via its Provincial Military Districts.[65] This force comprises civilian-economy mariners who have received training and can be mobilised to support the defence and advancement of China's maritime territorial claims and to safeguard its "maritime rights and interests.[66] Furthermore, while CMM mostly use "fishing vessels that are specially designed, constructed or renovated, and operated using funds dedicated to maritime militia affairs", analyses of Chinese sovereignty-affirming operations across the Spratly Islands have highlighted the existence of other vessels lacking such designation to provide a "greater degree of deniability".[67]

4 Hybrid threats and the ensuing contest in the information

Recent disruptions to submarine cables across the globe like the ones occurred around Taiwan have led policy incubators to provide comprehensive responses to secure this infrastructure. As explained in a US-focused study, securing submarine cables rests on three pillars: providing infrastructure redundancy (that is,

[64] As Kuok writes: "Countries often struggle to hold perpetrators to account for deliberate damage to subsea cables given jurisdictional limits in UNCLOS, weak flag state enforcement, and difficulties attributing incidents to actors. If incidents occur beyond the territorial waters of a coastal state, then only the country in which a suspected ship is registered—the flag state—has jurisdiction to investigate and prosecute any actors suspected of causing damage to cables. But many commercial vessels are registered in regimes that lack the will or the capacity to act. [...] Even when the will and the capacity to prosecute exist, successful prosecution remains elusive. Attribution—linking damage to a particular vessel or crew—is often difficult, and holding the sponsoring state accountable is harder still since it requires proof that the act was carried out under the state's instructions or that the state had control of the ship or crew." Kuok, Lynn, "The New Arteries of Power", cit.

[65] Henley, Lonnie D., "Civilian Shipping and Maritime Militia: The Logistics Backbone of a Taiwan Invasion", in *CMSI China Maritime Reports*, No. 21 (May 2022), p. 10, https://digital-commons.usnwc.edu/cmsi-maritime-reports/21. See also: Kennedy, Conor M. and Andrew S. Erikson, "China's Third Sea Force, The People's Armed Forces Maritime Militia: Tethered to the PLA", in *CMSI China Maritime Reports*, No. 1 (March 2017), https://digital-commons.usnwc.edu/cmsi-maritime-reports/1.

[66] Kennedy, Conor M. and Andrew S. Erikson, "China's Third Sea Force", cit. p. 2.

[67] Poling, Gregory B. et al., "Pulling Back the Curtain on China's Maritime Militia", in *CSIS Reports*, November 2021, p. 12-13, https://www.csis.org/node/63079.

Taiwan authorities have compiled a blacklist of 52 Chinese-owned ships operating under flags of convenience to monitor Beijing's shadow fleet

building more infrastructure than strictly needed); making existing infrastructure more resistant, and improving the capability to repair this infrastructure. Such efforts entail streamlining bureaucratic processes and regulatory frameworks to establish new submarine cables, improving monitoring tools and enhance information-sharing and best practices among like-minded countries facing the same threats, and aligning security and financial priorities and thus also providing strategic financing even when there are no strong business and profitability cases.[68]

Some early measures have already been implemented in Taiwan. Authorities have compiled a blacklist of 52 Chinese-owned ships operating under flags of convenience to monitor Beijing's shadow fleet.[69] The Ministry of Digital Affairs (MODA) has launched the International Sea Cable Landing Station Resilience Construction Subsidy Program in 2024, to provide subsidies for the establishment of new cable systems, and for covering the protection and repair of existing infrastructure. The TM4, scheduled for 2026 and connecting the southern Taiwanese landing point of Tanshui with the landing points of Dongyin, Nangang and Xiju in the Matsu Islands, is the first project emerging from this programme, specifically designed to create redundancy in data flow between Taiwan and Matsu following the incidents in 2023 and 2025.[70] A similar drive towards improving redundancy can be seen in the plethora of projects aiming at linking Taiwan to the US West Coast, South East Asia and North East Asia scheduled to be operative before the end of the current decade: TPU, ORCA, AUG East, E2A and Candle. At the same time, Taiwanese authorities are also exploring how to establish a technological ecosystem capable of switching to satellite communications.[71] At a legislative level, Taiwanese lawmakers passed amendments to four laws: the Law of Ships (to facilitate identification and monitoring of vessels), the Meteorological Act (introducing penalties for negligently damaging or illegally endangering the normal functioning of meteorological facilities and equipment), the Telecommunications Management Act (authorising the "confiscation of tools, vessels and machinery used to steal, damage or otherwise illegally endanger equipment relating to undersea cables") and the Commercial Port Law (allowing confiscation for "discrepancies in vessel registration,

[68] Murphy, Erin L., "Redundancy, Resiliency, and Repair. Securing Subsea Cable Infrastructure", in *CSIS Reports*, November 2025, https://www.csis.org/node/119556.
[69] Hille, Kathrin and Haohsiang Ko, "Taiwan Blacklists Chinese-Owned Shadow-Fleet Ship", in *Financial Times*, 27 January 2025, https://www.ft.com/content/bb6b6a16-bbeb-4b04-9445-7f47fc78663b.
[70] Huang, Kenny, "Strengthening Taiwan's Sea Cable Security", cit., p. 5-6.
[71] Rickards, Jane, "Wary of Cable Sabotage, Taiwan Looks to Satellites as Back-Ups", in *The Strategist*, 19 February 2025, https://www.aspistrategist.org.au/?p=91779.

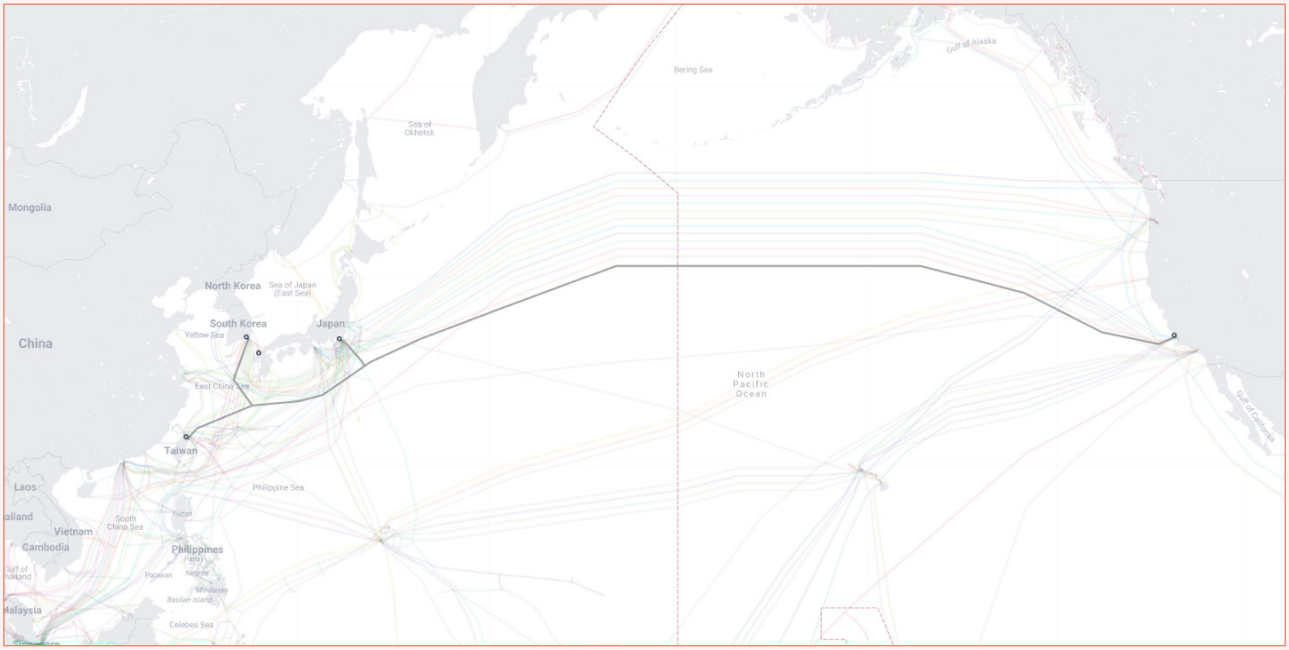


Figure 6 ORCA cable system, scheduled for 2029

Source: TeleGeography, "Orca", cit.

vessel certificates or other identification information").[72]

Even though a roadmap to improve resilience against hybrid threats targeting Taiwan's submarine cables is being sketched, the spillover effect of such hybrid threats from the infrastructure domain to the information domain and then to the design of policy responses is still underappreciated. Like in the case of other types of hybrid threats targeting infrastructure, the key to understanding this dynamic is to focus on the *possibility* of submarine cable disruption, and what it means for state actors to operate in a cognitive environment haunted by this possibility. Yet, the implications are not straightforward. China has deployed an ever-expanding toolkit of diplomatic, intelligence, military, economic, financial and legal instruments deployed against Taiwanese authorities since the collapse of cross-Strait relations in 2016.[73]

This approach has, in turn, shaped a cognitive environment in which every disruption to submarine cables is immediately perceived as a hybrid threat, obscuring the fact that this infrastructure is inherently fragile and routinely affected by maritime traffic and normal wear and tear. The realistic possibility that China could target Taiwan's submarine cables creates a shared terrain for confrontation that could be exploited by both sides. This predicament allows

[72] Taiwan Overseas Community Affairs Council, *Legislature Passes Amendments Strengthening Undersea Cable Protections*, 17 December 2025, https://www.ocac.gov.tw/OCAC/Eng/Pages/Detail.aspx?nodeid=329&pid=82223900.

[73] Insisa, Aurelio, "No Consensus across the Strait: Chinese and Taiwanese Strategic Communications in a Contested Regional Order", in *Asian Perspective*, Vol. 45, No. 3 (Summer 2021), p. 503-531, https://doi.org/10.1353/apr.2021.0033.

Figure 7 Taiwan-Matsu No. 4, scheduled for 2026

Source: TeleGeography, "Taiwan-Matsu No.4", in ***Submarine Cable Map***, last updated 15 January 2026, https://www.submarinecablemap.com/submarine-cable/taiwan-matsu-no-4.

Beijing to exploit objective difficulties in attribution and consequent deniability to delegitimise Taiwanese authorities.

This can be seen in the (albeit delayed) reaction to the *Hong Tai 58* incident. On 24 December 2025, the local public security authorities of the city of Weihai issued a "fugitive warrant notice" for two ROC passport-holders: Jian Wensheng and Chen Shunjin. According to Chinese authorities, the two led a gang responsible for smuggling frozen goods from Taiwan to Mainland China with multiple vessels – including the *Hong Tai 58*. Central to the indictment of the Chinese authorities was the confession of a Chinese crew member of the vessel. The sailor testified that on 25 February 2025, after repairs conducted in Kaohsiung, the vessel encountered adverse weather conditions and sought anchorage off the Jiangjun Fishing Harbour near Tainan. The ROC Coast Guard, however, ordered the *Hong Tai 58* to relocate, escorting it to a safe port. Upon berthing, the crew were informed that the vessel had allegedly severed the TPKM3 submarine cable linking Taiwan to Penghu. Crew members denied knowledge of any incident during anchoring operations and maintained they would have detected such an occurrence.[74]

Chinese state media predictably provided ample coverage to local authorities' reconstruction of the *Hong Tai 58* incident. But, crucially, the Chinese version of the incident also provided ammunition

[74] "The Truth about the Hong Tai 58 Incident. The Vessel Had Sustained a Hull Leak and Sought Anchorage Outside Kaohsiung Port for Repairs" [in Chinese], in *CCTV.com*, 25 December 2025, https://tv.cctv.com/2025/12/25/VIDESI6qoSm7qdCKnsl4DaAe251225.shtml.

The Chinese version of the Hong Tai 58 incident provided ammunition to Taiwanese opponents of the Lai Ching-te administration

to Taiwanese media who oppose the Lai Ching-te administration and the Democratic Progressive Party (DPP) and endorse policies and positions more attuned to Beijing.[75] Once disseminated in the Taiwan information environment, the Chinese version of the *Hong Tai 58* incident worked on multiple fronts. First, it cast doubts about the sentencing of the vessel's captain. Second, it aligned with the narrative espoused by opposition parties and critics of the DPP that DPP-led administrations amplify the "China threat" for domestic political advantage.[76] Third, in a subtler but still effective way, Chinese authorities signalled to both Chinese and Taiwanese audiences that, under DPP governments, the island had turned into a source of insecurity, a base for criminals smuggling frozen goods into Mainland China. Tellingly, this accusation echoes arguments to justify the ban of supposedly unsafe Taiwanese exports for "biohazard risks".[77]

The width of the range of options for operations in the information domain revealed by the *possibility* of hybrid threats targeting cables can be better appreciated looking to China's reactions to Taiwanese constabulary activities and jurisprudential decisions. In March 2025, the China Ship Scientific Research Centre, a research unit of the state-owned enterprise China State Shipbuilding Corporation, announced the development of a deep-sea cable-cutting device capable of operating at a depth of 4,000 metres, designed to be integrated with the *Fendouzhe* bathyscaphe and with the *Haidou* unmanned underwater vehicles, both operated by the Chinese Academy of Sciences.[78] Officially created as a tool for civilian salvage and seabed mining, the new tool presented explicit dual-use capabilities.

By unveiling this capability through a coordinated media strategy, Beijing may be aiming to signal deterrence and project maritime power without resorting to conflict.[79] The announcement of the new cable-cutter device was indeed delivered less than a month after the *Hong Tai 58* incident. If the incident was the result of a deliberate operations by Chinese actors, possibly the CMM, it shows

[75] Ching, Chang, "Expert Analysis: The Legal Controversy and Political Manoeuvring Surrounding the Hong Tai 58 Cable-Cutting Incident" [in Chinese], in *United Daily News*, 27 December 2025, https://udn.com/news/story/7331/9228737.
[76] Chen, Yuyao, "How the Narrative of China as a Threat Evolved into a Populist Attitude in Taiwan during the Administration of the Democratic Progressive Party (2016–24)", in *International Relations of the Asia-Pacific*, Vol. 25, No. 2 (2025), Article lcaf003, https://doi.org/10.1093/irap/lcaf003.
[77] Insisa, Aurelio, "Taiwan 2021: Heightened Geo-Economic Relevance amid Rising Cross-Strait Tensions", in *Asia Maior*, No. 32/2021 (2022), p. 125-151 at p. 128, https://doi.org/10.1353/apr.2021.0033.
[78] Chen, Stephen, "China Unveils a Powerful Deep-Sea Cable Cutter that Could Reset the World Order", in *South China Morning Post*, 22 March 2025, https://www.scmp.com/news/china/science/article/3303246/china-unveils-powerful-deep-sea-cable-cutter-could-reset-world-order.
[79] Mehboob, Cynthia, "Cutting Through the Narrative: What China's Deep-Sea Cable-Cutter Really Signals", in *The Interpreter*, 26 March 2025, https://www.lowyinstitute.org/node/39403.

a willingness to augment the threat by exploiting deniability while communicating resolve to attack and expected impunity. Conversely, if there was no Chinese responsibility behind the *Hong Tai 58* incident, it shows a willingness to exploit a cognitive environment haunted by the possibility of Chinese hybrid attacks and paralysed in the search for an effective response.

Counterintuitively, this very same cognitive environment haunted by the possibility of hybrid threats has provided opportunities for Taiwanese authorities. While the 2023 disruptions affecting the cables linking the Matsu Islands were ultimately deemed unintentional incidents rather than targeted attacks, their resonance at both domestic and international levels contributed to mobilising domestic resources and international partners to improve infrastructure resilience against hybrid threats – a key dossier in the current under-the-radar cooperation between Taiwan and the EU.[80] The simultaneous threat convergence in both the Nordic-Baltic theatre and the Taiwan theatre, against the backdrop of closer Russo-Chinese security ties following the full-scale invasion of Ukraine, had a further compounding effect on this dynamic.

Challenges in the information domain caused by disruptions to submarine cables remain pressing for Taiwan

This notwithstanding, it is important to highlight that challenges in the information domain caused by disruptions to submarine cables remain pressing for Taiwan. The main challenge for Taiwanese authorities is the risk of cognitive impasse: uncertainty over both the causes and attribution of submarine cable disruption could lead to institutional paralysis, giving threat actors free rein to shape perceptions of the event within the information domain. A strategic communications approach to the issue could increase the chance of avoiding the "cognitive impasse" in which hybrid threats may result. Strategic communications has been broadly defined as "the use of words, actions, images, or symbols to influence the attitudes and opinions of target audiences to shape their behavior in order to advance interests or policies, or to achieve objectives".[81] However, within the EU, it is understood more specifically as a tool of statecraft playing a twofold role. First, it aims to connect the Union's policies to its member states' citizens, producing a sense of buy-in and avoiding alienation. Second, it aims to deliver a critical line of defence against hybrid threats in the information domain by producing and disseminating timely and coherent messages.[82] Embracing this understanding of strategic communications may be particularly fruitful for Taiwan.

[80] Interviews with EU and Taiwanese officials, July 2025 and November 2025.
[81] Farwell, James P., *Persuasion and Power. The Art of Strategic Communication*, Washington, Georgetown University Press, 2012, p. xviii-xix.
[82] European External Action Service (EEAS), *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy*, Brussels, Publications Office of the EU, 2016, https://data.europa.eu/doi/10.2871/9875.

In concrete terms, a strategic communications approach to the challenge caused by the submarine cable disruption would entail five steps. First, clarifying standards used for attributing hybrid threats against the infrastructure. Second, increasing awareness among the domestic public of both (1) the inherent fragility of submarine cable infrastructure and (2) the recent the recent legal tools empowering constabulary forces and the judiciary in Taiwan to counter threat actors targeting submarine cables. Third, establishing an ad hoc coordination mechanism between all Taiwanese bureaucratic actors involved in the response to submarine cable disruptions: the ROC Coast Guard, the National Communications Commission, the Ministry of Digital Affairs, the Ministry of Justice and the Mainland Affairs Council. The aim here is to guarantee timely, coherent, consistent and clear communication from Taiwanese authorities when disruptions occur. Fourth, empowering this coordination mechanism to deliver timely and effective state-driven communication addressing Chinese operations in the information domain exploiting disruptions to submarine cables. Fifth, using this very same mechanism to pre-emptively address and disarticulate possible Chinese counternarratives about the disruptions.

The measures suggested above easily fit into the roadmap sketched by the Ministry of Foreign Affairs of Taiwan with its RISK Management Initiative on International Undersea Cable, launched in October 2025.[83] Still in its early stages, the initiative may provide a platform for fostering cooperation with international partners against the backdrop of the concrete legal, financial and logistical efforts described at the beginning of this section. In relation to the information domain, RISK's objective number 2 and 4 are particularly relevant. The former "encourage[s] the sharing of relevant, timely, and actionable information regarding potential threats and risks affecting undersea cable infrastructure [...] creating channels for the exchange of threat intelligence, early warnings, and lessons learned from incidents". The latter focuses on "support[ing] the enhancement of technical capabilities and knowledge across all stakeholder groups by facilitating training programs, workshops, and the exchange of best practices". Achieving these objectives may indeed provide the necessary foundation to effectively implement a strategic communications approach facing the challenge of submarine cable disruptions.

[83] Taiwan Ministry of Foreign Affairs, *RISK Management Initiative on International Undersea Cables*, 28 October 2025, https://ws.mofa.gov.tw/Download.ashx?u=LzAwMS9VcGxvYWQvNDAyL3JlbGZpbGUvNzQvMTIwOTcwLzkyNjk5NmU2LTE5NWMtNGEyNy1hY2YxLTg4Y2I5NTUxNDhkNC5wZGY%3D&n=5rW357qc5YCh6K2w5Y6f5paHLnBkZg%3D%3D.

Conclusion

Against the backdrop of diplomatic isolation and exclusion from international organisations, Taiwan's submarine cables are tangible evidence of the island's connection to the outside world – a critical infrastructure tethering the island to the global economy and guaranteeing its survival. Disruptions to this infrastructure pose an existential risk for the island in case of a Chinese-imposed quarantine or an attempt to take over it via military force. At a less immediate level, the ability to impose disruptions to this infrastructure has become part of Beijing's wide array of tools and tactics aiming at destabilising Taiwanese society and eroding trust in domestic institutions, inducing a state of cognitive impasse vis-à-vis the threat to Taiwanese authorities, and gradually chipping away the island's residual sovereignty.

These dynamics, and the domestic and international responses to counter them, must be taken into consideration also in a yet underappreciated dimension: their impact on the information domain at a Taiwanese, cross-Strait and international level. The challenge over submarine cables should therefore be framed in terms of hybrid threats rather than the more common "grey zone operations". While the concepts are contiguous, the hybrid threats paradigm allows for better understanding how threats in the infrastructure domain spill over into the information domain, and consequently into other domains of Taiwan's security.

Still, the *threat* of disruptions to submarine cables – rather than the disruption per se – shapes a contest in the information domain which does not favour China in a straightforward fashion. The threat of disruption to critical infrastructure is in fact a tool that could be exploited to mobilise public opinion, international partners and resources in support of Taiwan's resilience vis-à-vis China. This notwithstanding, Taiwan's challenges in the information domain remain real and to be addressed. A strategic communications approach, adapted from the EU, may constitute a solution to this challenge, emphasising sharply defined standards of attribution, increasing public awareness of the inherent fragility of this infrastructure beyond the realistic threat of sabotage, projecting deterrence through new legal tools and improving coordination about state ministries and other agencies to disseminate timely, coherent, consistent and clear communication capable to assure domestic public and international partners, while disarticulating Chinese counter-narratives.

References

Andersson, Patrik et al., "What the Yi Peng 3 Cable-Cutting Incident Reveals about China-Russia Relations", in *SNCC Commentaries*, No. 3/2025, https://kinacentrum.se/en/?p=7792

Aoi, Chiyuki et al., "Introduction 'Hybrid Warfare in Asia: Its Meaning and Shape'", in *The Pacific Review*, Vol. 31, No. 6 (2019), p. 693-716, https://doi.org/10.1080/09512748.2018.1513548

Baqués-Quesada, Josep, "Is Morocco Operating a Grey Zone in Ceuta and Melilla?", in *Defence Studies*, Vol. 23, No. 2 (2023), p. 198-214, https://doi.org/10.1080/14702436.2022.2159815

Besch, Sophie and Erik Brown, *Securing Europe's Subsea Data Cables*, Washington, Carnegie Endowment, 2024, https://carnegieendowment.org/research/2024/12/securing-europes-subsea-data-cables

Bintang Timur, Fitriani et al., "The Politics of Subsea Cables in Indonesia: Navigating Great Power Competition", in *PRIO Policy Briefs*, No. 15/2024 (2024), https://www.prio.org/publications/14070

Butler, Katherine, "Drone Dilemma: How Russia's 'Hybrid War' Is Using Fear to Destabilise Europe", in *The Guardian*, 8 October 2025, https://www.theguardian.com/p/x3cqdf

Chen, Stephen, "China Unveils a Powerful Deep-Sea Cable Cutter that Could Reset the World Order", in *South China Morning Post*, 22 March 2025, https://www.scmp.com/news/china/science/article/3303246/china-unveils-powerful-deep-sea-cable-cutter-could-reset-world-order

Chen, Yuyao, "How the Narrative of China as a Threat Evolved into a Populist Attitude in Taiwan during the Administration of the Democratic Progressive Party (2016–24)", in *International Relations of the Asia-Pacific*, Vol. 25, No. 2 (2025), Article lcaf003, https://doi.org/10.1093/irap/lcaf003

Chiang, Huang-Chih and Po-Hsiang Liao, "The 'Hong Tai 58' Case and Criminal Jurisdiction Over Submarine Cable Sabotage in 'New' Internal Waters", in *Prospects & Perspectives*, No. 65 (25 November 2025), https://www.pf.org.tw/en/pfen/33-11657.html

Chinese Communist Party, *Resolution of the Chinese Communist Party Central Committee on the Major Achievements and Historical Experiences of the Party's One-Hundred-Year Struggle*, 16 November 2021, https://english.www.gov.cn/policies/latestreleases/202111/16/content_WS6193a935c6d0df57f98e50b0.html

Chinese State Council Information Office, *The Taiwan Question and China's Reunification in the New Era*, 10 August 2022, https://english.news.cn/20220810/df9d3b8702154b34bbf1d451b99bf64a/c.html

Ching, Chang, "Expert Analysis: The Legal Controversy and Political Manoeuvring Surrounding the Hong Tai 58 Cable-Cutting Incident" [in Chinese], in *United Daily News*, 27 December 2025, https://udn.com/news/story/7331/9228737

Chiu, Charlotte, "Taiwan's Submarine Cable Network Strategic Value and Future Outlook", in *Ketagalan Media*, 23 February 2025, https://wp.me/p4ka8Y-8qn

Clare, Mike, *Submarine Cable Protection and the Environment: Keeping Subsea Cables Safe from Volcanic Eruptions*, International Cable Protection Committee, November 2025, https://www.iscpc.org/publications/submarine-cable-protection-and-the-environment

Cordesman, Anthony H. and Grace Hwang, "Chronology of Possible Chinese Gray Area and Hybrid Warfare Operations", in *CSIS Reports*, updated 28 September 2020, https://www.csis.org/node/56684

Donald C. Hellman Task Force Programme (DCHTFP), *Hidden Highways of the Internet: Global Subsea Cable Security*, Henry M. Jackson School of International Studies, University of Washington, March 2025, https://jsis.washington.edu/nie/wp-content/uploads/2025/03/Task-Force-B-Final-Report.pdf

European Commission, *Recommendation (EU) 2024/779 of 26 February 2024 on Secure and Resilient Submarine Cable Infrastructures*, C/2024/1181, http://data.europa.eu/eli/reco/2024/779/oj

European Commission, *EU Action Plan on Cable Security*, JOIN/2025/9, 21 February 2025, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:52025JC0009

European External Action Service (EEAS), *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy*, Brussels, Publications Office of the EU, 2016, https://data.europa.eu/doi/10.2871/9875

Farwell, James P., *Persuasion and Power. The Art of Strategic Communication*, Washington, Georgetown University Press, 2012

Fridman, Ofer, *Russian 'Hybrid Warfare'. Resurgence and Politicisation*, New York, Oxford University Press, 2018

G7, *G7 Foreign Ministries' Declaration on Maritime Security and Prosperity*, Charlevoix, Quebec, 14 March 2025, https://www.g7.utoronto.ca/foreign/250314-declaration.html

G7, *G7 Industry, Technology and Digital Ministerial Meeting Ministerial Declaration*, Verona and Trento, 15 March 2024, https://www.g7.utoronto.ca/ict/2024-declaration.html

Giannopoulos, Georgios et al. (eds), *The Landscape of Hybrid Threats: A Conceptual Model*, Luxembourg, Publications Office of the European Union, 2021, https://doi.org/10.2760/44985

Henley, Lonnie D., "Civilian Shipping and Maritime Militia: The Logistics Backbone of a Taiwan Invasion", in *CMSI China Maritime Reports*, No. 21 (May 2022), https://digital-commons.usnwc.edu/cmsi-maritime-reports/21

Hille, Kathrin and Haohsiang Ko, "Taiwan Blacklists Chinese-Owned Shadow-Fleet Ship", in *Financial Times*, 27 January 2025, https://www.ft.com/content/bb6b6a16-bbeb-4b04-9445-7f47fc78663b

Hioe, Brian, "Is China's Latest Form of Grey Zone Activity Cutting Submarine Cables?", in *New Bloom Magazine*, 7 January 2025, https://newbloommag.net/?p=38695

Hoffman, Frank G., *Conflict in the 21st Century: The Rise of Hybrid Warfare*, Arlington, Potomac Institute for Policy Studies, 2007, https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

Hope, Arran, "Beijing's New Approach towards Taiwan", in *China Brief*, Vol. 25, No. 20 (31 October 2025), p. 2-7, https://jamestown.org/?p=822336

Huang, Kenny, "Strengthening Taiwan's Sea Cable Security", in *HCSS Papers*, March 2025, https://hcss.nl/?p=72710

Insisa, Aurelio, "Hybrid After All: The 'Grey Zone', the 'Hybrid Warfare' Debate, and the PLA's Science of Military Strategy", in *Defence Strategic Communications*, Vol. 12 (Spring 2023), p. 165-186, https://doi.org/10.30966/2018.RIGA.12.1

Insisa, Aurelio, "No Consensus across the Strait: Chinese and Taiwanese Strategic Communications in a Contested Regional Order", in *Asian Perspective*, Vol. 45, No. 3 (Summer 2021), p. 503-531, https://doi.org/10.1353/apr.2021.0033

Insisa, Aurelio, "Taiwan 2021: Heightened Geo-Economic Relevance amid Rising Cross-Strait Tensions", in *Asia Maior*, No. 32/2021 (2022), p. 125-151, https://doi.org/10.1353/apr.2021.0033

Jönsson, Oskar, "Aboard the Chinese Vessel: Significant Observations" [in Swedish], in *SVT Nyheter*, 20 December 2024, https://www.svt.se/nyheter/utrikes/var-ombord-pa-kinesiska-fartyget-betydelsefulla-iakttagelser

Jose, Ashley Erika O., "PLDT Eyes to Finish Apricot Submarine Cable Project by 2027", in *BusinessWorld Online*, 2 April 2025, https://www.bworldonline.com/?p=663254

Kardon, Isaac B., *Combating the Gray Zone: Examining Chinese Threats to the Maritime Domain*, Testimony before the House Committee on Homeland Security, Subcommittee on Transportation and Maritime Security, 4 June 2024, https://carnegieendowment.org/posts/2024/06/combating-the-gray-zone-examining-chinese-threats-to-the-maritime-domain

Kennedy, Conor M. and Andrew S. Erikson, "China's Third Sea Force, The People's Armed Forces Maritime Militia: Tethered to the PLA", in *CMSI China Maritime Reports*, No. 1 (March 2017), https://digital-commons.usnwc.edu/cmsi-maritime-reports/1

Khanna, Monty, "A Roadmap for Securing India's Undersea Cables", in *ORF Special Reports*, No. 266 (June 2025), https://www.orfonline.org/research/a-roadmap-for-securing-india-s-undersea-cables

Koshino, Yuka, "The Changing Submarine Cables Landscape", in *EUISS Briefs*, No. 19 (October 2024), https://www.iss.europa.eu/node/3270

Kouretsos, Peter, "Annex A: Contextualising Chinese Hybrid Warfare", in Ross Babbage (ed.), *Stealing a March. Chinese Hybrid Warfare in the Indo-Pacific: Issue and Options for Allied Defense Planners. Volume II: Case Studies*, Washington, Center for Strategic and Budget Assessment, 2019, p. 1-6, https://csbaonline.org/research/publications/stealing-a-march-chinese-hybrid-warfare-in-the-indo-pacific-issues-and-options-for-allied-defense-planners

Kuok, Lynn, "The New Arteries of Power", in *Foreign Affairs*, 2 January 2026, https://www.foreignaffairs.com/new-arteries-power

Lee, Yimou et al., "China Encircles Taiwan in Massive Military Display", in *Reuters*, 30 December 2025, https://www.reuters.com/world/china/china-launches-live-firing-drills-around-taiwan-its-biggest-war-games-date-2025-12-30

Libiseller, Chiara, "'Hybrid Warfare' as an Academic Fashion", in *Journal of Strategic Studies*, Vo. 46, No. 4 (2023), p. 858-880, https://doi.org/10.1080/01402390.2023.2177987

Lloyd's List Intelligence, "Taiwan Is Hunting One Cable Cutting Vessel Disguised with Three Separate Digital Identities", in *Lloyd's List Intelligence Blog*, 8 January 2025, https://www.lloydslistintelligence.com/thought-leadership/blogs/taiwan-is-hunting-one-cable-cutting-vessel-disguised-with-three-separate-digital-identities

McGeachy, Hilary, "The Changing Strategic Significance of Submarine Cables: Old Technology, New Concerns", in *Australian Journal of International Affairs*, Vol. 76, No. 2 (2022), p. 161-177, https://doi.org

/10.1080/10357718.2022.2051427
Mehboob, Cynthia, "Cutting Through the Narrative: What China's Deep-Sea Cable-Cutter Really Signals", in *The Interpreter*, 26 March 2025, https://www.lowyinstitute.org/node/39403
Milne, Richard, "Sweden Criticises China for Refusing Full Access to Vessel Suspected of Baltic Sea Cable Sabotage", in *Financial Times*, 22 December 2024, https://www.ft.com/content/9094dcc4-b0f8-4191-
Morel, Camille "The Pacific Caught in the World Wide Web? Geopolitics of the Submarine Cables in Oceania", in *Études de l'Ifri*, September 2022, https://www.ifri.org/en/node/24801
Mumford, Andrew and Pascal Carlucci, "Hybrid Warfare: The Continuation of Ambiguity by Other Means", in *European Journal of International Security*, Vol. 8, No. 2 (May 2023), p. 192-206, https://doi.org/10.1017/eis.2022.19
Murphy, Erin L., "Redundancy, Resiliency, and Repair. Securing Subsea Cable Infrastructure", in *CSIS Reports*, November 2025, https://www.csis.org/node/119556
Oskarsson, Katerina, "The Effectiveness of DIMEFIL Instruments of Power in the Gray Zone", in *OPEN Publications*, Vol. 1, No. 2 (Winter 2017), p. 1-16, https://issuu.com/spp_plp/docs/the_effectiveness_of_dimefil_instruments_of_power_
Poling, Gregory B. et al., "Pulling Back the Curtain on China's Maritime Militia", in *CSIS Reports*, November 2021, p. 12-13, https://www.csis.org/node/63079
Pugliese, Giulio and Aurelio Insisa, "How to Use the Maximum of Potential for the EU-Taiwan Cooperation: What Can the EU Learn from the US and Other Actors?", in *European Parliament Studies*, September 2025, https://doi.org/10.2861/6301949
Rickards, Jane, "Wary of Cable Sabotage, Taiwan Looks to Satellites as Back-Ups", in *The Strategist*, 19 February 2025, https://www.aspistrategist.org.au/?p=91779
Swanström, Niklas, "China, Russia and Undersea Cable Vulnerability: Shoring Up Protection", in *ISDP Policy Briefs*, 29 January 2025, https://www.isdp.eu/?p=40279
Taiwan Mainland Affairs Council, *Act Governing Relations between the People of the Taiwan Area and the Mainland Area*, 1992, https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=Q0010001
Taiwan Ministry of Foreign Affairs, *RISK Management Initiative on International Undersea Cables*, 28 October 2025, https://ws.mofa.gov.tw/Download.ashx?u=LzAwMS9VcGxvYWQvNDAyL3JlbGZpbGUvNzQvMTIwOTcwLzkyNjk5NmU2LTE5NWMtNGEy-Ny1hY2YxLTg4Y2I5NTUxNDhkNC5wZGY%3D&n=5r-W357qc5YCh6K2w5Y6f5paHLnBkZg%3D%3D
Taiwan National Communications Commission, *Telecommunications Management Act*, 2 July 2025, https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=K0060111
Taiwan National Security Bureau, *Analysis on China's Cyber Threats to Taiwan's Critical Infrastructure in 2025*, 4 January 2025, https://www.nsb.gov.tw/en/assets/documents/%E6%96%B0%E8%81%9E%E7%A8%BF/9976f2e1-3a8a-4fa2-9a73-b0c80fca1f04.pdf
Taiwan Overseas Community Affairs Council, *Legislature Passes Amendments Strengthening Undersea Cable Protections*, 17 December 2025, https://www.ocac.gov.tw/OCAC/Eng/Pages/Detail.aspx?nodeid=329&pid=82223900
Tang, K. Tristan, "Cronyism and Failed Promotion: Xi's PLA Purge", in *China Brief*, Vol. 25, No. 19 (18 October 2025), p. 30-33, https://jamestown.org/?p=822549
Tobin, Meaghan and Vic Chiang, "Internet Outage Has Taiwan Worried about Threat from Chinese Sabotage", in *The Washington Post*, 9 March 2023, https://www.washingtonpost.com/world/2023/03/09/taiwan-matsu-internet-access-china-fishing
West, Michael J. and Aurelio Insisa, "Reunifying Taiwan with China through Lawfare", in *The China Quarterly*, No. 257 (2024), p. 186-201, https://doi.org/10.1017/S0305741023000735
Wigell, Mikael, "Hybrid Interference as a Wedge Strategy: A Theory of External Interference in Liberal Democracy", in *International Affairs*, Vol. 95, No. 2 (2019), p. 255-275, https://doi.org/10.1093/ia/iiz018
Wuthnow, Joel, "Can Xi Jinping Control the PLA?", in *China Leadership Monitor*, No. 83 (1 March 2025), https://www.prcleader.org/post/can-xi-jinping-control-the-pla
Yang, William, "Chinese Vessel Suspected of Damaging Undersea Cable Near Taiwan", in *VOA News*, 7 January 2025, https://www.voanews.com/a/7926977.html
Yau, Hon-min, "Undersea Cybersecurity: Countering Gray Zone Operations and Strengthening the Digital Resilience of Subsea Cables for Taiwan", in *The Journal of East Asian Affairs*, Vol. 38, No. 1 (Spring/Summer 2025), p. 7-37, https://www.inss.re.kr/common/download.do?atchFileId=F20251107104407610&fileSn=4

IAI Istituto Affari Internazionali

The Istituto Affari Internazionali (IAI) is a private, independent non-profit think tank, founded in 1965 on the initiative of Altiero Spinelli. IAI seeks to promote awareness of international politics and to contribute to the advancement of European integration and multilateral cooperation. Its focus embraces topics of strategic relevance such as European integration, security and defence, international economics and global governance, energy, climate and Italian foreign policy; as well as the dynamics of cooperation and conflict in key geographical regions such as the Mediterranean and Middle East, Asia, Eurasia, Africa and the Americas. IAI publishes an English-language quarterly (*The International Spectator*), an online webzine (*AffarInternazionali*), two book series (*Trends and Perspectives in International Politics* and *IAI Research Studies*) and some papers' series related to IAI research projects (*Documenti IAI*, *IAI Papers*, etc.).

Via dei Montecatini, 17
I-00186 Rome, Italy
T +39 06 6976831
www.iai.it

Latest IAI Papers

Editor: **Riccardo Alcaro** (r.alcaro@iai.it)
ISSN 2610-9603 | ISBN 978-88-9368-395-1