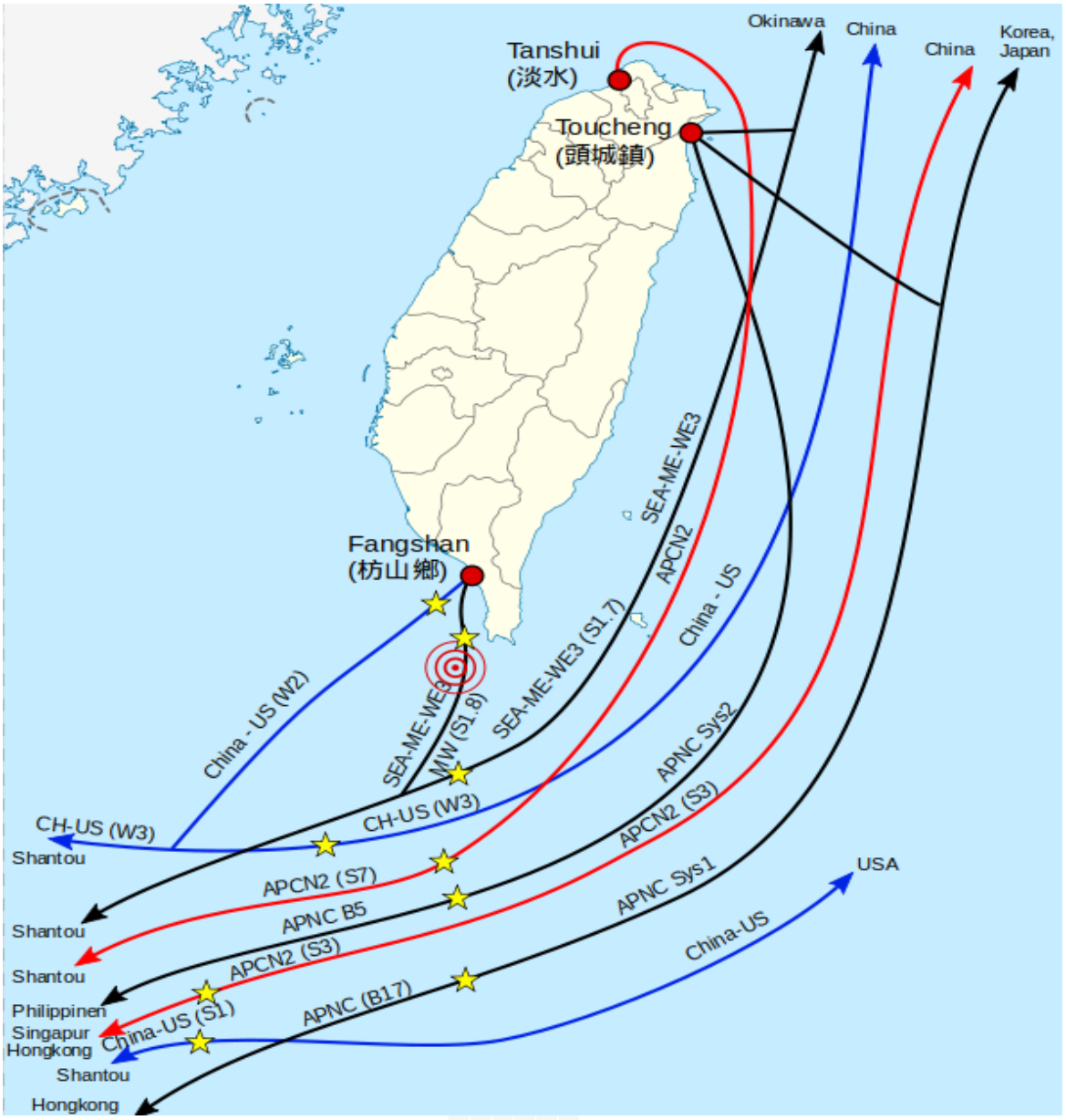


Undersea cables, grey-zone threats and the UK: Lessons from Taiwan

By: Francis Annagu

September 2026

Image by Furfur

In February 2025, a cargo ship with a Chinese crew, registered in Togo, was docked for several days near the southwestern coast of Taiwan, largely ignoring Taiwanese Coast Guard attempts to make contact. After the vessel was ordered to leave on the 25th of February, it finally moved into waters where anchoring is prohibited. Minutes after this move, the state telecom operator of Taiwan, Changhwa Telecom, detected damage to an undersea cable that linked the main island of Taiwan with Penghu.

At first, investigators did not know what had caused the damage to the cable, whether it was the result of an accident or a deliberate act. In dealing with grey-zone incidents, uncertainty is important to consider. The first challenge was the work required to repair the cable, the second to determine what or who was responsible, and from there to determine whether the damage was deliberate or not. Four months later, a court in Tainan convicted the captain of the ship, and found out that he had knowingly ordered the vessel to anchor in a prohibited area, causing the cable to break. Chunghwa Telecom put the costs for repair at NT$17 million (about £418,788), and the captain was sentenced to three years in prison.

The case in hand was revealing insofar as it spoke less about the captain than it did about a growing security problem in the region, and for globally shared communications cables generally.

This was not, by far, the earliest 'accident' with undersea internet cables Taiwanese authorities had experienced. Between 2018 and 2023, internet cables between Matsu and Taiwan were cut, accidentally or otherwise over 27 times:

"We can't rule out that China destroyed these on purpose," said Su Tzu-yun, a defense expert at the government think tank, Institute for National Defense and Security Research, citing a research that only China and Russia had the technical capabilities to do this. "Taiwan needs to invest more resources in repairing and protecting the cables."

The number of recorded accidents of damaged undersea cables around Taiwan should be a warning for Britain, whose economy depends almost entirely on subsea cables but has not yet had to confront a sustained campaign of deliberate cable "accidents".

Critical gaps in UK preparedness

Britain's recent experience of this kind of potential threat gives it common interest with countries facing rising accidental or deliberate disruption of subsea communications cables in the Indo-Pacific. In March this year a subsea cable linking mainland Orkney Island with Westray Island was damaged. It took a month for the damage to be recognised and repaired, affecting about 1,700 people within the North Isles, disrupting broadband and mobile services, card payments, digital phone lines, and internet access at schools and GP surgeries.

Undersea cable reels at the UK's coast port estuary, Blyth. Image by David Martin.

In this case there was insufficient evidence to suggest cable sabotage by hostile actors, but the occurrence exposed commonly known vulnerabilities in the infrastructure security of the UK. Even accidental cable failures can have serious repercussions for infrastructure and communications security when repair capacities are very thin, and the vessels which are designed to repair them are not necessarily owned by Britain, nor are they available on time when needed.

A more serious threat was realised just weeks later when, in April 2026, Defence Secretary John Healey made it known that the UK and Norwegian security forces had spent a month monitoring the activities of a Russian submarine and two other vessels linked with Russia's GUGI deep sea research directorate in the North Atlantic, around the area where Britain and its allies have critical undersea infrastructure. Healey justified public disclosure of this operation on the basis that Moscow had to realise its activity had been detected and was being actively monitored. The naval operation by the two NATO countries reported no damage to undersea cables in the area, but the episode was also a demonstration of Britain's security responsibilities in the event that any hostile state intends to sabotage such infrastructure, upon which the UK's economy is dependent.

Around 99% of the UK's international data traffic is carried by subsea cables, with this network created to minimally withstand the impact of most probable human errors.

What was not calculated at the time was what happens, what legacy systems are in place, if or when several cables are deliberately tampered with at the same time, during heightened diplomatic or military tension and grey zone conflict with another nation, or during an active kinetic war. An inquiry into subsea cable security set up by the UK parliament found that Britain currently does not have its own sovereign cable repair ship, with the most recent cable repair company ship contracted out of Singapore. The inquiry also raised concerns about the legal framework for penalising cable damage being outdated, and pointed to a fragmentation of responsibility for subsea cables lying across dozens of government departments and agencies. One witness to the inquiry testified of uncertainty over who even leads a response during a major incident.

Why governance matters more than geography

This is where the UK can learn from Taiwan since it has experience of dealing with this issue in an active theatre of grey zone maritime activities by a hostile neighbour today, which may well become the UK's experience tomorrow.

Taiwan has strengthened its institutional response mechanisms to give as much protection to all undersea cables as possible, tightened oversight of vessels operating near its cable routes, and further expanded the capacity of local agencies to investigate any suspected interference. Taiwan's approach has increasingly shifted from focussing on supplying and repairing damaged cables to identifying risks early and taking steps to prevent disruption before it happens.

However, these measures have not been enough in bringing the problem to an end. Taiwan continues to face increasing maritime pressures from The People's Republic of China around Matsu, the Taiwan Strait, and the waters off northern Taiwan where it is exposed to potential disruption to all its undersea cables. Whilst most of the cable faults Taiwan experiences are still unintentionally caused by anchor dragging, the experience has forced Taiwanese agencies to develop institutional mechanisms required to respond quickly, especially when an incident is open to different interpretations. There is now a recognition that detecting suspicious vessels, preserving evidence, identifying who is responsible, and pursuing legal consequences where cable sabotage is done on purpose requires a fast, co-ordinated, and structured, operating procedure.

Up to now, the UK has not developed a similar ability to act quickly when responding to accidental cable damage or sabotage. Its network has sufficient backup systems to adapt to multiple separate faults, even so, the evidence from latest parliamentary investigations reveal that it is still unclear who would be responsible for leading a response in the event of a coordinated attack on several cables. The most pertinent question for the UK then is not whether the cables are at risk, it's whether the State has the capacity to clearly detect, identify and respond to intentional damage to cables within a timeframe that reduces the impact on the wider country.

The steps the UK should take

A closer look of the comparison between the two cases points to four important steps that the UK could take to strengthen its preparedness and response:
First, Britain should do more than counting cables and mapping how well its system can cope with disruption. For instance, it needs to plan out which routes, landing stations, and data flows would become critical weak points if several subsea cables failed at once? It needs to game scenarios where a hostile agency is seeking to cause maximum damage or disruption.

Second, the HM Coastguard should form a working partnership with Taiwan's Coast Guard, their digital authorities, and telecommunications operators, so that it can learn from Taiwan's practical experience in cable route monitoring, investigating suspicious incidents, and distinguishing cable damages caused by accidents from possible coercion.

Third, the UK's Undersea Infrastructure Security (UIS) Oversight Board, chaired by the Cabinet Office, should urgently step up measures toward strengthening the UK's independent repair capacity, as parliamentary investigations have recommended, rather than leaving the responsibility entirely on repair vessels owned by foreign nations whose support may not always be available when it is needed.

And fourth, it should modernise the legal framework under all matters governing deliberate cable damage, as this ensures that those responsible for proven interference can and will face serious legal and financial consequences.

In conclusion, none of the measures highlighted in this piece require the UK to change its diplomatic posture regarding Taiwan and China, and neither are these measures being advocated on the basis that Russian submarines and ships are cutting undersea cables or will start imminently.

The measures do say that the tampering of undersea cable infrastructure most likely has become a grey zone tool used by States to pressure and disrupt other States without starting an open kinetic conflict. For Taiwan, the PRC has the opportunity, means, and motivation, and the world has seen how the PRC is flexing its muscles through not only its Coast Guard but also a large maritime militia inside other countries Exclusive Economic Zones.

Where Taiwan has years of experience, the UK is only now recognising it faces similar challenges in its own waters. The lesson for Westminster now is straightforward and easy to understand: the UK cannot continue to wait for a cable to cut before it starts preparing to take action. The steps it needs to take to respond to incidents of damage or sabotage must be planned out now and put in place before the next break is reported.

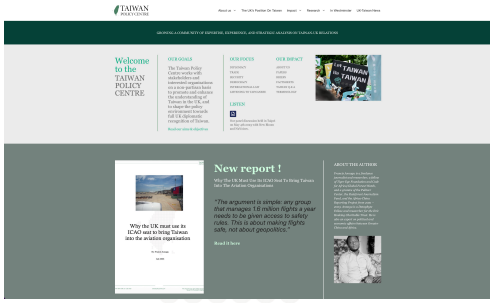
ABOUT US

The Taiwan Policy Centre is a non-partisan organisation dedicated to boosting political, cultural, and trading relations between the UK and Taiwan. We aim to increase the knowledge and understanding that policy-makers, the media, and the British public have about Taiwan though a combination of research, educational events, and outreach.

TAIWAN
POLICY CENTRE

We further aim to highlight the threats and injustices that Taiwan faces at the hands of the Chinese Communist Party and lobby the UK Government to take a stronger and more proactive stand in support of Taiwan on the global stage.

Too often, media coverage and understanding of Taiwan is shaped by the language and claims of the Chinese Communist Party, a governing authority which does not, and never has, governed Taiwan. The Taiwan Policy Centre aims to correct these misconceptions and ensure that the UK's policies towards Taiwan and media coverage of Taiwanese affairs is rooted in research and law.



DONATIONS

The Taiwan Policy Centre is a not-for-profit organisation that relies on supporter donations to fund our work. We welcome all donations large and small and owing to the sensitive nature of our work, we only publish details of our funding in general terms and have a policy publishing a list of donations over £1200 per annum.

If you would like to make a donation to enable the Taiwan Policy Centre to continue its work, please visit our website at www.taiwanpolicycentre.com/donate

Author: *Francis Annagu*

Francis Annagu is a freelance journalist and researcher. He earned his bachelor's degree in political science from Kaduna State University. He has been a fellow of Tiger Eye Foundation and Code for Africa/Global Forest Watch since 2022, and a grantee of the Pulitzer Center, the Rainforest Journalism Fund, and the Africa-China Reporting Project from 2021 - 2023. He has collaborated on research with international teams at the Curatorial Research LAB (South Korea) and curated a botany project with Co-iki (Japan). Annagu is a Dataphyte Fellow and researcher for the UK's Eric Hosking Charitable Trust. He is also an expert on political and economic affairs between Greater China and Africa.

Edited by: Ben Goren & David Spencer
Issued: September 2026