March 2026

Taiwan's Resilience in the Face of China's Cyber Challenge

Dr. Valentin Weber

Senior Associate Fellow, German Council on Foreign Relations (DGAP)
Visiting Fellow, Institute for National Defense and Security Research (INDSR)

Executive summary:

- In the past few years Taiwan has impressively increased the resilience of its connectivity including through a growing number of subsea cables, access to satellite networks, and cyber capabilities.
- To further enhance its resilience, the Taiwanese government should facilitate the deployment of a national mesh network that would enhance Taiwan's domestic internet capabilities.
- In terms of cybersecurity, Taiwan has a systemic advantage in comparison to China, since the latter weakens security for surveillance purposes.
- In terms of resilience Germany can learn a lot from Taiwan and especially when it comes to establishing deterrence by punishment in the context of subsea cable cutting.

The present author uses a slightly altered NATO definition of resilience for the purposes of this article:

[…] Resilience is defined as the continuous ability […] to deter, defend […]. This requires forces that can anticipate, adapt, and prepare for strategic shocks, and when necessary, withstand, respond to, and recover from both short-term disruptions and protracted crises.[1]

March 2026

Taiwan is often hailed as one of the most resilient countries when it comes to the digital realm.[1] Its mis and mal-information debunking infrastructure is renowned across the world.[2] In terms of cybersecurity, few countries have been exposed to the sheer size and depth of Chinese cyber operations. In short, Taiwan's resilience has been often tested by China, but not only. Earthquakes are common and they challenge Taiwan's connectivity too.[3]

And despite the frequent tests of Taiwan's resilience, there is no consensus on how resilient Taiwan really is. Taiwan's strength is a matter of perception. Parts of the international community, for instance, believe that if the Democratic Progressive Party (DPP) wins elections this means that Taiwan is resilient. If the DPP wins elections, Chinese political interference has not been successful, since the DPP is seen as less pro-China than the other major party, the Kuomintang (KMT). But Taiwan's resilience is much more complex and cannot be reduced to which party is winning.[4]

Perceptions of resilience change over time, and they also depend on who is assessing resilience: is it the Taiwanese population, the NGO sector, industry, the Taiwanese government, China, or the international community? The term "resilience" itself, is very broad. It can involve defensive measures, such as keeping information networks running while they are under attack. However, it also involves the development of active defense capabilities, including those in cyberspace. The narrative too is important. A successful country shapes the narrative about its own resilience, it does not just respond to information campaigns.

Another distinguishing factor of resilience is that it requires endurance. Resilience is akin to a marathon. For a marathon you need to keep training. Just because you ran a marathon it does not mean you can run it again. You need to constantly evaluate and train your strength. As you run the first few kilometers, attrition will kick in. Therefore, you need to use your resources well and not get exhausted in the first sections of the race. Cyber operations, for instance, are

aimed at hitting during holiday periods, right before the weekend or later in the evening, when defenders are ready to take a break. In those situations, defending forces spread thin and get exhausted.

Taiwan's resilience needs to be seen also in comparison to China's digital resilience. Eventually, it is about who can hold out longer. And Taiwan and China could not be more different. Taiwan, a democratic country, China an authoritarian one. Taiwan is one that thrives in decentralization, China is geared toward centralization. Beijing's focus on surveillance also has systemic negative implications for Chinese cyber resilience compared to Taiwan's resilience.

This piece of work is divided into three parts. The first gives a short overview of the current state of Taiwan's digital resilience. It primarily looks at connectivity and cybersecurity. The second section compares Taiwan's cybersecurity resilience to China's. The final part proposes recommendations to improve Taiwanese connectivity resilience via the establishment of a national mesh network. The conclusion lays out the major findings of this article and lessons learned for Germany by looking at Taiwan's example.

1. The current state of Taiwan's resilience

Active defense cyber capabilities

Cyber capabilities for active defense are a crucial component of Taiwan's ability to withstand external pressure. Letting China perceive that one is in their networks complicates things further for Beijing. Cyber tools can give Taiwan early warnings of Chinese preparations for conflict or other intended malicious behavior. In line with NATO's definition of resilience, it gives Taiwan the capability of anticipating behavior.

And it appears that Taiwan has capabilities, both self-developed and purchased, as the 2025 ROC National Defense Report lays out.[5]

Chinese cybersecurity companies, for their part, have been tracking Taiwanese cyber activities.[6] They put Taiwan in a category with other nation state actors such as the United States, India, and Vietnam. Taiwan's cyber capabilities are therefore by definition advanced and persistent.

Taiwanese cyber capabilities could be also useful in disrupting or weakening Chinese malicious operations, i.e. go beyond reconnaissance operations, into active defense cyber operations, in case the geopolitical situation turns grimmer. And beyond that, the perception that Taiwan has breached Chinese networks might be yet another factor that shapes Chinese offensive calculations, especially when combined with punitive measures in, e.g., the maritime domain. Recently, Taiwan jailed a Chinese national, who damaged undersea cables, to three years in prison.[7]

Defensive cyber capabilities

China's perception of Taiwan's cyber defenses is almost certainly more complete than its perception of the activities of Taiwanese cyber forces. This is because China knows exactly, which Taiwanese networks it has breached and which it has not been able to get into. On the flipside, Beijing does not know which networks Taiwanese operators have buried themselves inside.

Taiwan has experienced many noteworthy Chinese cyber operations.[8] Among these, two are especially central. The first one targeted public screens during the visit of Nancy Pelosi, then Speaker of the U.S. House of Representative, in 2022. The screens in subway stations and convenience stores displayed threatening messages. On the one hand, defacements of

websites or viewing interfaces of convenience stores are in most cases not remarkable, since they can rely on unsophisticated techniques.[9] Defacing websites, does in most cases, not require as much technical skill as breaching hardened networks. On the other hand, the target in this case is itself critical to Taiwan's food supply and thereby worrying. China managed to breach those low hanging fruits, but it cannot assess this as a major success. After all, 7/11 stores were in this case able to simply turn off the TV. So, many people did not even take notice of the cyber operation.[10]

The second noteworthy Chinese cyber operation was against the Chinese Petroleum Corporation (CPC). Chinese cyber threat actors, breached CPC networks, encrypted data, and left a ransom note. But there was no way to decrypt data via payment channels, so it was likely to be an intentionally destructive cyber operation.[11] The effect on oil and gas supply in Taiwan was marginal, as only CPC payment cards were not working, cash and credit cards were still accepted.[12] Other noteworthy Chinese cyber operations targeting Taiwan had similar marginal effects.[13]

Connectivity

While Taiwan has been building more subsea cables to improve its resilience (the number currently stands at 24), there is also a common understanding that those can be easily cut.[14] And repair ships are rare, making the re-establishment of connectivity slow.[15]

Taiwan is trying to mitigate this vulnerability by improving its satellite connectivity. This is done with Eutelsat, which, in cooperation with Taiwan's Ministry of Digital Affairs helped reestablish connectivity during the 2024 emergency communication in areas affected by a heavy earthquake.[16] A key part of this effort was to deploy First Emergency Network Mobile Vehicles,

which can be sent to affected areas at short notice and provide vital internet access regarding emergency communications for rescue personnel and affected victims.[17] Taiwan's National Science and Technology Council, on the other hand, is seeking closer collaboration with Amazon's Kuiper project.[18]

Satellites are crucial due to their resilience. Low Earth Orbit constellations keep connectivity even in Ukraine, where war and heavy interference have raged for years.[19] And Medium Earth Orbit constellations are resilient too.[20]

2. (Mis)perceptions of Taiwan's resilience

Perception plays a key role in resilience. If China does not believe that Taiwan is resilient it may consider to invade, create a blockage or quarantine. Beijing's perceptions are shaped by daily testing of Taiwan's defenses. And Taiwan's relative resilience compared to China is also an important factor, which this piece now turns to.

Democracy versus autocracy

Taiwan's resilience is not only about recovering quickly from something unpleasant.[21] In that case Taiwan would be a mountain that experiences strong winds (Typhoons) and perhaps changes its appearance slightly (some stones are being loosened), but the mountain remains strong. As the president of Taiwan Lai said in 2025: "[…] that like a mountain, the Republic of China (Taiwan) will stay strong and endure."

But Typhoons, just like mountains do not think. They do not adjust their strategy based on how the aggressor or defender acts. So, equating Taiwanese resilience to a mountain is perhaps not the most adequate. China/Taiwan constantly adjust their strategy based on how Taiwan or China (re)acts and it does matter what either country thinks about the other's resilience. It

matters what China and Taiwan think about China's resilience and how they think Taipei's resilience compares to Beijing's.

The key factor that distinguishes the two countries is that one is a democracy and the other an autocracy. The type of government has a far-reaching impact on cybersecurity resilience. While autocracies have certain advantages in terms of controlling the information environment, they also display systemic weaknesses, which could play to Taiwan's advantage.

China's cybersecurity landscape is highly vulnerable.[22] Because of the Chinese Communist Party's (CCP) yearning for complete control of the online environment Beijing has introduced a deeply invasive surveillance infrastructure. This means that end-to-end encryption is not common in China.[23] HTTPS adoption of websites in China has been lagging, which translates into yet another weak point in China's cybersecurity. While at least on governmental websites, HTTPS adoption has increased recently, regular leaks containing confidential information are common.[24] Backdoors in company equipment are found too, for instance in software that is used to pay local taxes, which in turn makes government surveillance easier.[25] Many Chinese apps, too, are built with weak security.[26]

This means that there is systemic (cyber)insecurity in China, potentially for a combination of reasons, such as a weak security engineering culture and CCP paranoia. As a result, the CCP can read highly sensitive messages of its population and companies. But so can other foreign intelligence services, including Taiwan's Communication Development Office, which oversees signals intelligence collection.[27]

Since the CCP is paranoid about its regime security, these weaknesses are unlikely to vanish. Quite to the contrary, the more insecure the CCP feels, the more surveillance, the more backdoors there will be in the Chinese internet infrastructure. This is also visible in the People's

Liberation Army (PLA) communications infrastructure. Soldiers' phones are constantly monitored. Specialized software detects if soldiers reach out to acquaintances outside China, what their most visited websites are, what products they buy online, what their speech behavior and psychological state of mind is.[28]

Contrast this with Taiwan, where end-to-end encryption is common and HTTPS websites are ubiquitous. While Taiwan has been breached on multiple occasions by Chinese actors, it does not have these systemic weaknesses that China has.[29]

3. Recommendation to improve Taiwan's resilience

Taiwan currently relies on subsea cables, satellites, as well as fiber optic cables to remain connected. However, in times of conflict, none of these suffices to ensure that Taiwan's government can communicate with its citizens, or that citizens could communicate with each other. A mesh network, on the other hand, ensures sovereignty and autonomy. Hence the Taiwanese government should initiate a discussion about constructing the world's first national mesh network in Taiwan.

The section below lays out how a national mesh network could ensure Taiwan's connectivity when everything else fails. It would be a measure of last resort.[30] Mesh networks have been used by protesters in Hong Kong and elsewhere to keep communication going even when the traditional internet is shut down. They often consist of small personal devices such as smartphone or Meshtastic LoRa nodes that relay messages through wireless signal or Bluetooth to each other, instead of going through a centralized server.

Taiwan currently relies on subsea cables, and satellites, as well as fiber optic cables to maintain connectivity, but none of these suffices to ensure that Taiwan's government can communicate

with its citizens in times of conflict. This article hence suggests the construction of the world's first nationwide mesh network globally in Taiwan.

Taiwan's current connectivity strategy is prone to fail. In times of conflict an adversary would cut subsea cables. Internet exchange points could be hit by missiles, thereby further diminishing domestic connectivity. Cell towers, which are connected to the internet backbone would be impacted too.[31] Satellites could provide a backup connectivity to allow emergency services to provide internet to citizens. Cars with satellite dishes are in these cases deployed to crisis regions. But with a limited amount of those, they can be targeted by sabotage or missiles too.

This article hence suggests the Taiwanese government build yet another layer of defense for its resilience that focuses on strengthening the domestic intranet. Germany is doing so too, via the establishment of 33,000 km additional fiber optic network connections alongside its railway network. Germany suggested that this was done due to the harshening geopolitical environment and due to its military utility.[32]

Taiwan should work on strengthening its domestic intranet. There are a variety of ways it could do so, for instance, by establishing a nationwide mesh network. To create a reliable network that connects the west coast urban areas from Keelung to Kaohsiung one would need large amounts of handheld devices, probably in the hundreds of thousands. For maintaining connectivity on Taiwan's east coast, mesh networks could still play a role, but it would have to rely on more nodes that are more long range than the handheld devices and ideally deployed on roofs.

Why do all this? When the government has no other way of communicating with its population, mesh devices would be the primary channel to relay the most essential government

information via text. While the government could not send video or audio messages, text should be sufficient for the most important updates. Handheld devices also have a long battery life that would further expand resilience. As there are so many devices, a foreign adversary would be unable to destroy a significant number.

Nevertheless, there are a few things to keep in mind. In the case of the Meshtastic network, around 80-90 percent of the devices would be on client mute mode, which functions as receive only nodes, and the rest of the 10 percent of devices would be relays that actively extend the network. This method prevents the network from becoming over congested.

What is more, wireless signals that a mesh network relies on to relay messages could be jammed. However, this can be mitigated through frequency hopping techniques. Another weak point might be that a foreign adversary could hijack these networks to spread disinformation, but with proper cryptography to authenticate message origins in place, such as the Reticulum network, this risk could be strongly mitigated.

This brings us to the next hurdle in deploying a national mesh network. Many of the current producers of mesh devices hail from the People's Republic of China. However, Taiwan could easily manufacture these LoRa mesh devices with its advanced chip producing capability. Mesh devices only consist of a microcontroller (chip), another radio chip, an antenna and a battery.

If Taiwan's government were to initiative a broader discussion on the pros and cons of a national mesh network and if it decided to adopt the mesh network strategy it could easily set up and scale production. With collaboration from other mesh network leading countries, such as Germany, a potentially even more resilient network could be established.[33] And when the project is deployed successfully, Taiwan could export its solution to other countries, who face similar adversarial challenges to connectivity.

Conclusion

The above article consists of three parts. The first part covers known knowns of Taiwan's resilience, the second part, the known unknowns, which primarily concern the (mis)perception of Taiwanese resilience. The final part looks at how Taiwan could create unknown unknowns for its adversaries, by establishing novel resilience initiatives that few would have expected. The above knowledge matrix of known knowns, known unknowns and unknown unknowns is already a few decades old.

In 2022, Donald Rumsfeld, a former US defense secretary of state said:

"…we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns — the ones we don't know we don't know. And if one looks throughout the history of our country and other free countries, it is the latter category that tends to be the difficult ones."[34]

The known knowns of Taiwan's resilience

The known knowns of Taiwanese resilience are its subsea cables and satellite networks, as well as reconnaissance cyber capabilities (Taiwanese network operators know exactly which Chinese networks they have breached). It is common knowledge that subsea cables are incredibly vulnerable and that satellite networks are great for improving redundancy but are not intended to supply millions of users in cities communications concurrently.[35] Satellite connectivity is also vulnerable to geopolitical and business calculations by foreign companies that provide these services.

The known unknowns

The known unknowns of Taiwan's digital resilience are mostly about Taiwan being a democracy and how resilient that makes Taiwan in comparison to adversaries that are autocratic. Who can hold through longer? Who weathers attrition better? How efficient is crisis decision-making in democracies? This article has demonstrated that at least in cybersecurity defense terms, Taiwan might have an edge compared to China's surveillance state, since Taiwan's systems are designed to be secure rather than monitored. But perceptions are not always shared and they keep shifting. Therefore, Taiwan needs to actively shape them in its favor.

The unknown unknowns

The unknown unknowns of Taiwanese resilience are potential resilience measures that have not yet been thought about broadly. One such unknown unknown has been the nationwide deployment of mesh networks. Once this idea has been proposed it will be moving to the known unknowns category and if fully deployed it will go further onward to the known knowns section, as the vulnerabilities and strengths of a nationally deployed mesh network will become clearer.

Now that this paper has analyzed some aspects of Taiwanese digital resilience and suggested recommendations, the final paragraphs will illustrate what aspects of the Taiwanese approach Germany could emulate, to strengthen its own resilience.

What Germany can learn from Taiwan

Germany can learn a lot from Taiwan in terms of how to combat grey zone activities. In 2025, Taiwan detained the Hong Tai 58 vessel, which damaged submarine cables between Penghu islands and Taiwan. The eight Chinese nationals were shortly detained and one of them was

sentenced to three years in prison.[36] At the same time Taiwan has doubled down on penalties related to subsea cable protection. Ships that do not relocate or depart from sensitive areas may be confiscated. And negligence that leads to the damaging of cables can be punished by being sent to prison or may involve a substantial fine.[37]

These new measures should bring about better chances for deterrence by punishment. Malicious actors should think twice before damaging critical infrastructure. Taiwan is akin to a porcupine, which imposes costs on its adversary. Its porcupine quills signal to malicious actors, that in the future too, there will be punishment. The quills in this case are the laws of Taiwan as well as the Taiwanese Coast Guard, which can intercept an adversary's ships quickly.

Germany should engage in close collaboration with Taiwanese authorities to exchange lessons learned related to grey zone activities on the seas that impact a country's connectivity. Berlin would benefit in terms of how to deal with Russian and other malicious vessels in its neighborhood.

Acknowledgements

I am very grateful to Taiwan's Ministry of Foreign Affairs, whose financial support made this publication possible, as well as to the Institute for National Defense and Security Research (INDSR) for providing me with a workspace and intellectual home during my time as a visiting fellow. A huge thank you to Chen-Yi Tu (杜貞儀) and Yisuo Tzeng (曾怡碩) for providing feedback on earlier versions of the article. The section on mesh networks received crucial input from Myf Ma, a human rights researcher.

Notes

[1] Duncan Barron, June 28, 2025. Taiwan's Model for Digital Defense of Democracy Goes Global, https://thediplomat.com/2025/06/taiwans-model-for-digital-defense-of-democracy-goes-global/; Kuang-Cheng Hsu and Calvin Chu, 29 April 2025. Taiwan Bolsters Whole-of-Society Defense Resilience, https://jamestown.org/chinese-military-drill-escalates-tensions-underscoring-taiwans-commitment-to-whole-of-society-defense-resilience/.

[2] Elaine Chan, June 5, 2024. From Beef Noodles to Bots: Taiwan's Factcheckers on Fighting Chinese Disinformation and 'Unstoppable' AI, https://www.theguardian.com/world/article/2024/jun/05/from-beef-noodles-to-bots-taiwans-factcheckers-on-fighting-chinese-disinformation-and-unstoppable-ai.

[3] Telecom Review, November 5, 2025. When the Waves Hit: Protecting Submarine Cables from Natural Disasters, https://www.subseacables.net/reports-and-coverage/when-the-waves-hit-protecting-submarine-cables-from-natural-disasters.

[4] Tim Niven, June 2024. How Taiwan Should Combat China's Information War, https://www.journalofdemocracy.org/online-exclusive/how-taiwan-should-combat-chinas-information-war/.

[5] Taiwanese Ministry of National Defense, 2025. ROC National Defense Report 2025, https://www.mnd.gov.tw/newupload/ndr/114/114ndreng.pdf.

[6] Ibid.

[7] Koh Ewe and I-ting Chiang, June 12, 2025. Taiwan Jails China Captain for Undersea Cable Sabotage in Landmark Case, https://www.bbc.com/news/articles/cwy3zy9jvd4o.

[8] Valentin Weber, June 2023. Cyberprotection for Critical Infrastructure Resilience: The Case of Taiwan, https://dgap.org/system/files/article_pdfs/Report_EnhancingResilienceinaChaoticWorld_June23.pdf.

[9] Industrial Defender Staff, May 7, 2025. CISA Observes Unsophisticated Cyber Activity Against U.S. Oil & Natural Gas Infrastructure, https://www.industrialdefender.com/blog/cisa-observes-unsophisticated-cyber-activity-against-u-s-oil-natural-gas-infrastructure.

[10] Interview with Taiwanese civil society representative.

[11] Weber, June 2023. Cyberprotection for Critical Infrastructure Resilience.

[12] Ibid.

[13] Ibid.

[14] Taiwan News, March 4, 2026. Former KMT Legislator Urges Taiwan to Pass Defense Budget to Strengthen Deterrence, https://www.taiwannews.com.tw/news/6313722; Margo Anderson, December 5, 2024. Protecting Undersea Internet Cables Is a Tech Nightmare, https://spectrum.ieee.org/undersea-internet-cables-protection-tech.

[15] Jordan McGillis and Pieter van Wingerden, July 1, 2024. Why Taiwan Needs to Secure Its Undersea Cables, https://thediplomat.com/2024/07/why-taiwan-needs-to-secure-its-undersea-cables/.

[16] Industrial Technology Research Institute (ITRI) Industry Service Center Research Team, February 25, 2026. Global Low Earth Orbit (LEO) Satellite Deployment and the Transformation of Taiwan's Supply Chain, https://investtaiwan.nat.gov.tw/intelInfoPageCht202602250001jpn?lang=eng&search=202602250001.

[17] Ministry of Digital Affairs of Taiwan, April 3, 2024. Ministry of Digital Affairs Supported the Establishment of the First Emergency Network Mobile Vehicle, Which Has Already Arrived in Hualien for Disaster Relief Dispatch, https://moda.gov.tw/en/press/press-releases/11992.

[18] Focus Taiwan, May 17, 2025. NSTC in Talks on Communications Satellite Network With Amazon Kuiper, https://focustaiwan.tw/sci-tech/202505170008.

[19] John T Psaropoulos, February 6, 2026. Ukraine Pulls Plug on Russian Starlink, Beefs up Drone Defence, https://www.aljazeera.com/features/2026/2/6/ukraine-pulls-plug-on-russian-starlink-beefs-up-drone-defence.

[20] THALES, March 10, 2026. Thales and SES Demonstrate Compatibility of Secure Anti-Jamming Waveforms With MEO Satellites, https://www.thalesgroup.com/en/news-centre/press-releases/thales-and-ses-demonstrate-compatibility-secure-anti-jamming-waveforms.

[21] Oxford University Press, n.d.. resilience, https://www.oxfordlearnersdictionaries.com/definition/english/resilience.

[22] Valentin Weber, November 12, 2020. How China's Control of Information is a Cyber Weakness, https://www.lawfaremedia.org/article/how-chinas-control-information-cyber-weakness.

[23] Ibid.

[24] Alexander Martin, February 10, 2026. Leaked Technical Documents Show China Rehearsing Cyberattacks on Neighbors' Critical Infrastructure, https://therecord.media/leaked-china-documents-show-testing-cyber-neighbors; Digital Watch, February 4, 2026. Major Chinese Data Leak Exposes Billions of Records, https://dig.watch/updates/major-chinese-data-leak-exposes-billions-of-records.

[25] Weber, November 12, 2020. How China's Control of Information is a Cyber Weakness.

[26] Mona Wang, May 12, 2025. WireWatch, https://citizenlab.ca/research/wirewatch-measuring-the-security-of-proprietary-network-encryption-in-the-global-android-ecosystem/.

[27] Matthew Strong, January 3, 2026. Taiwan Taps Former Submarine Chief to Head Intelligence Agency, https://www.taiwannews.com.tw/news/6275796.

[28] Valentin Weber, January 7, 2026. Inside the PLA's Instant Messaging Ecosystem, https://chinatechnosphere.substack.com/p/pla-instant-messengers-security-vs.

[29] Weber, June 2023. Cyberprotection for Critical Infrastructure Resilience.

[30] Valentin Weber and Myf Ma, March 20, 2026. National Mesh Network an Option, https://www.taipeitimes.com/News/editorials/archives/2026/03/20/2003854127; Wikipedia, PACE (communication methodology), https://en.wikipedia.org/wiki/PACE_(communication_methodology).

[31] The Fiber Optic Association, n.d.. Fiber Optics for Wireless, https://www.thefoa.org/tech/ref/appln/wireless.html.

[32] DerStandard, February 5, 2026. Deutschland Verlegt 33.000 Kilometer Glasfasernetz Entlang Bahnschienen, https://www.derstandard.de/story/3000000307017/deutschland-verlegt-33000-kilometer-glasfasernetz-entlang-bahnschienen.

[33] Ken Research, 2024. Global Wireless Mesh Networking Market, https://www.kenresearch.com/global-wireless-mesh-networking-market.

[34] U.S. Department of Defense, February 12, 2002. DoD News Briefing - Secretary Rumsfeld and Gen. Myers, https://web.archive.org/web/20160406235718/http://archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=2636.

[35] News Y Combinator, October 3, 2024. Starlink Offering Free Internet Access for 30 Days for Hurricane Helene Victims, https://news.ycombinator.com/item?id=41733672.

[36] Ewe and Chiang, June 12, 2025. Taiwan Jails China Captain for Undersea Cable Sabotage in Landmark Case.

[37] Lin Ching-yin and James Thompson, 16 December, 2025. Legislature Passes Amendments Strengthening Undersea Cable Protections, https://focustaiwan.tw/society/202512160012.