LONDON POLITICA

The Geopolitics of Undersea Cables

Underappreciated and Under Threat

19.12.22

Research Analyst
Sarah Kuszynski

Research Director
Ginny Hamilton Barns

Table of Contents

Executive Summary

This report assesses the range of threats facing undersea cables, which are central to the internet's infrastructure, the world's communication system and thus the global economy. The paper draws particular attention to the nation-state threats, and espionage tactics, namely, cyber-attacks and cable tapping used for surveillance purposes by intelligence agencies and adversarial states to collect sensitive data as well as monitor crime and terror activities. In terms of physical damage to cables Russia presents a persistent threat due to the advanced capabilities of Russian spy vessels. This has led many experts to characterise the threat as existential. Similarly, Chinese telecommunications companies are increasing their global influence, which is of growing importance as US-China technology tensions intensify; illustrating that undersea cable sabotage would have dangerous geopolitical consequences if China were ever to invade Taiwan. Lastly, the report foregrounds how the lack of clarity in regulation represents a critical global infrastructure vulnerability.

1

Introduction

"It is not satellites in the sky, but pipes on the ocean floor that form the backbone of the world's economy" as stated by Admiral James Stavridis, US Navy (Ret). Despite the lexicon surrounding the internet being full of intangibles — "the cloud," "cyberspace" and "the Metaverse"—the Internet is dependent on physical entities, such as servers and cables to run[1]. The security and resilience of undersea cables and the data that moves across them are an understudied and often underappreciated element of modern internet geopolitics.

Undersea cables have been in use worldwide for around two centuries, with submarine cables being used in the 1820s by an attaché to the Russian Embassy in Munich to send telegraphs [2]. Now undersea cables are described as the "world's information super- highways," and carry over 95% of international data [3]. There are over 400 active cables worldwide covering half a million miles (see figure 1).

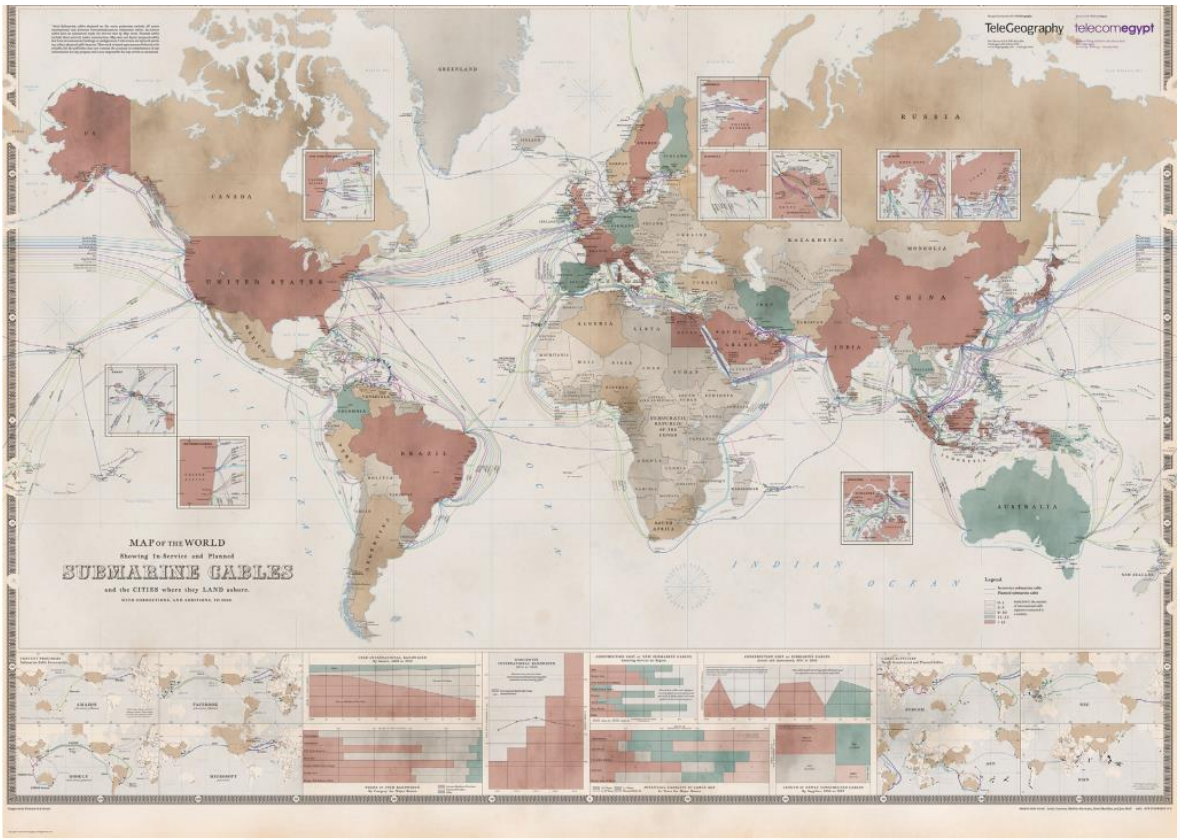


Figure 1 *map showing the global distribution of undersea cable connections* ***Source****:* https://blog.telegeography.com/2020-submarine-cable-map.

Fibre optic cables are faster and cheaper than satellite communications, undersea cables can transfer data at speeds of 25 terabytes per second — twice the amount of data generated by the Hubble Space Telescope each year [4]. The fibre cables themselves, as shown in figure 2, are surprisingly light containing only eight fibre-optic strands. Reliance on these cost-

effective submarine cables will continue to increase as demand for data grows due to developments in cloud computing and the spread of 5G [5]. The rise of cloud services has also increased the sensitivity of data traversing undersea cables, with cabling carrying everything from streaming videos to ATM transactions [6]. Submarine cables are thus at the core of global internet infrastructure.

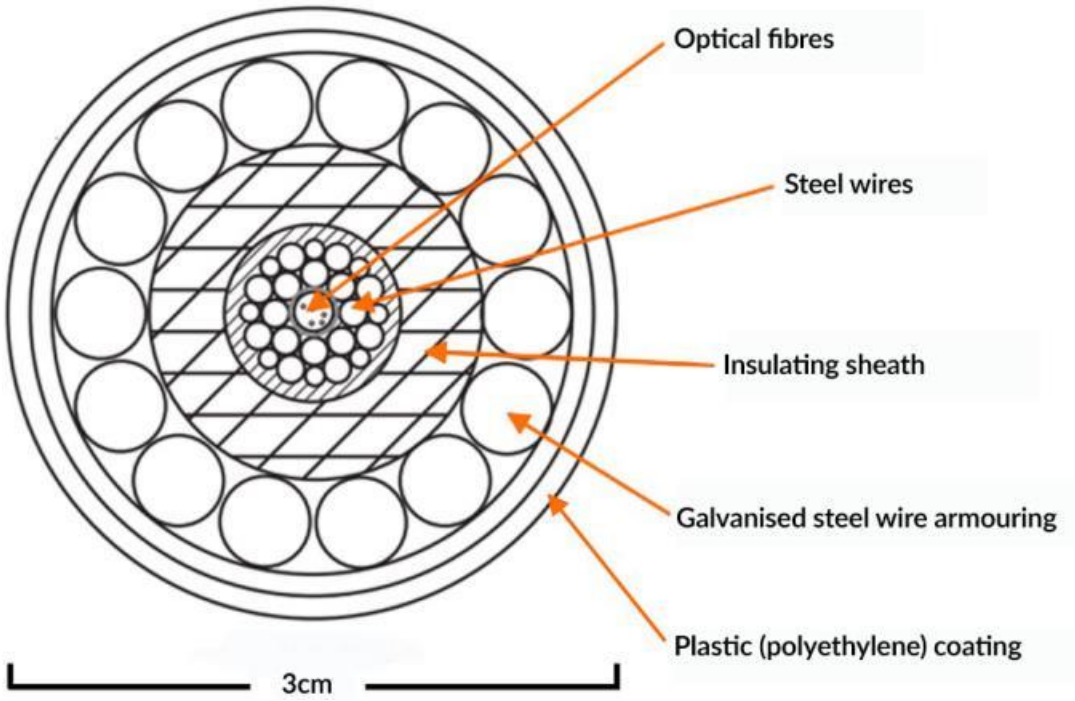


Figure 2 *cross section of a submarine fibre-optic cable* ***Source:*** https://policyexchange.org.uk/publication/undersea-cables-indispensable-insecure/

Geopolitical Risks and Resilience

Ensuring the resilience of undersea cables is vital. Undersea cabling must be able to route data around failures and be easily reparable to minimise disruption to global Internet traffic[7]. The global undersea network suffers more than 100 yearly cable outages, some more severe than others [8]. In 2015, the Basslink cable between mainland Australia and Tasmania failed, and took over six months to repair [9]. In order to avoid this and achieve resilience, it is important understand threats facing submarine cabling. Cables are vulnerable to physical and digital attacks from sea, on land, and in cyberspace. The relative risk of each of threats to specific sections of undersea cabling is visualised in the table below.

Table 1 *Upper-level conceptual threat matrix for submarine cable segment, on "Threats to Undersea Cable Communications, September 28, 2017".*

Threat impact level depicted in colours: Green = Low; Yellow = Medium; Red = High

Submarine Cable Segment Threat	Land and Beach Area (Seg.1)	Near Shore Area ~50 m (Seg.2)	Off Shore Area ~ 50 – 100 m (Seg.3)	Continental Shelf ~ 100 – 200 m (Seg.4)	Deep Sea ~ 200 m + (Seg.5)
Natural Threats					
Sharks					
Earthquake					
Landslide					
Volcano					
Tsunami					
Iceberg					
Ocean currents					
Accidental Threats					
Fishing					
Anchor dragging					
Dredging					
Malicious and undersea warfare					
Cyber Attacks					
Vandalism					
Activists					
Theft					
Terrorist					
State-actors					
Undersea warfare					

Source: Hummelholm, A. (2019). Undersea optical cable network and cyber threats. In Proceedings of the European conference on information warfare and security. Academic Conferences International.

The most frequent cause of damage to submarine cabling (causing 150 to 200 faults every year), remains physical damage from commercial shipping, undersea cables are also uniquely vulnerable to hostile threat actors compared with other internet infrastructure [10]. The

locations of most undersea cables are publicly available and submarine cables must travel through narrow bodies of water, like in the Strait of Malacca [11]. At these flashpoints there is both a greater risk of damage from commercial shipping and geopolitical disputes, since multiple countries have competing interests at these shipping chokepoints[12]. Similarly, the UK is vulnerable, given the large quantities of data transferred across transatlantic cables to be stored in US data centres [13]. This opens up transatlantic cabling to being destroyed or tapped—by non-state actors, including pirates , terror groups or more often a state adversary.

Hypothetically, if every transatlantic cable were to be cut, it would become extremely difficult to communicate overseas [14]. Thus, highlighting the strategic significance of undersea cabling.

However, it is worth noting that although undersea cables are vulnerable, European nations, the United States and many Asian countries, rely on far more than one cable to link them to the rest of the world. Therefore, attacking one internet cable is akin to blocking a single lane on a four-lane motorway. One lane may be closed, yet traffic still passes through as the other lanes (cables) can still function. This demonstrates that internet traffic routed through cables is somewhat resilient to accidental damage and cyber-attacks. Although large scale, targeted military operations remain a significant threat to even the most connected states' internet access.

There are several goals that state and non-state actors may achieve from targeting undersea cabling. Firstly, cutting off communications during or prior to conflict could enable one state to gain a direct military advantage over the other; secondly, cable attacks could sabotage a competitor economically and cutting an adversary's undersea communications can also serve as a form of geopolitical one-upmanship [15]. Moreover, by hacking into network management systems that manage data passing through cables, adversaries could insert malicious code and significantly disrupt data flows. Theoretically a hacker can gain control, or administrative rights, of a cable's network management system, exploit physical vulnerabilities, disrupt data traffic, and execute a "kill click" effectively deleting the transmitted data [16]. A "cyber pearl harbour" attack on the internet's backbone is something that the West's adversaries could enact to induce socio-economic disaster and potentially escalate into direct conflict [17]. In January 2022, the head of the UK armed forces warned that cutting transatlantic cables would be an "act of war", the Minister of Defence echoed this sentiment stating sabotage to undersea cables presents an "existential threat".

Undersea Espionage

Although internet geopolitics seems very 21st century, undersea cabling has long been targeted for espionage. In the late nineteenth century, British intelligence used its access to an international hub of telegram cables in Porthcurno to gain eavesdropping advantage [18]. Additionally, at the outbreak of World War I, Britain severed all but one of Germany's undersea telegraph lines. The British tapped the remaining cable, which allowed them to intercept communications, such as the Zimmerman telegram which shaped the outcome of the war[19].

Undersea espionage was also extensively utilised during the cold war; a joint NSA, Navy and CIA mission, called 'Operation Ivy Bells' tapped Soviet deep sea communication cables in the Sea of Okhotsk using a modified submarine [20] [21]. Operation Ivy Bells only failed in 1981, when NSA employee Ronald Pelton sold information about the programme to the KGB [22].

In the present, espionage appears to be achieved through three main methods: inserting backdoors during the cable manufacturing process, targeting onshore landing stations linking cables to networks on land, or tapping the cables at sea[23]. Tapping fibre-optic cables underwater requires opening up armoured sheaths, avoiding shocks from the cable and then splicing open highly sensitive glass fibre. Ships such as the USS Jimmy Carter are believed to have such capabilities. Tapping this way still requires highly specialised equipment and high-risk operations.

A strategic weak spot which may be exploited is where cable signals are amplified and the fibre optics are no longer bundled together but are laid out individually, this occurs when the cables come to shore at Cable Landing Stations (CLS)[24]. These points are also vulnerable to physical attack as typified by a foiled Al-Qaeda plot to destroy a vital internet exchange in 2007. Relatedly, the UK is geographically in an ideal position to access cables as they emerge from the Atlantic, enabling intelligence cooperation between UK-USA signal intelligence agencies – the NSA and GCHQ. Past tapping programmes revealed in the Snowden files included: "Global Telecoms Exploitation" and "Tempora" which were able to collect around 21 million gigabytes of cable data per day [25] [26].

Undersea espionage is a vital intelligence function for enabling intelligence agencies to sift for evidence of serious crime and ensure that as much as possible is known in advance of strategic and/or military actions. It is, however, important to limit excesses in data collection, and mitigate privacy concerns. This necessitates appropriate legal checks and balances in tandem with credible deterrence.

Nation State Threats to Undersea Cabling

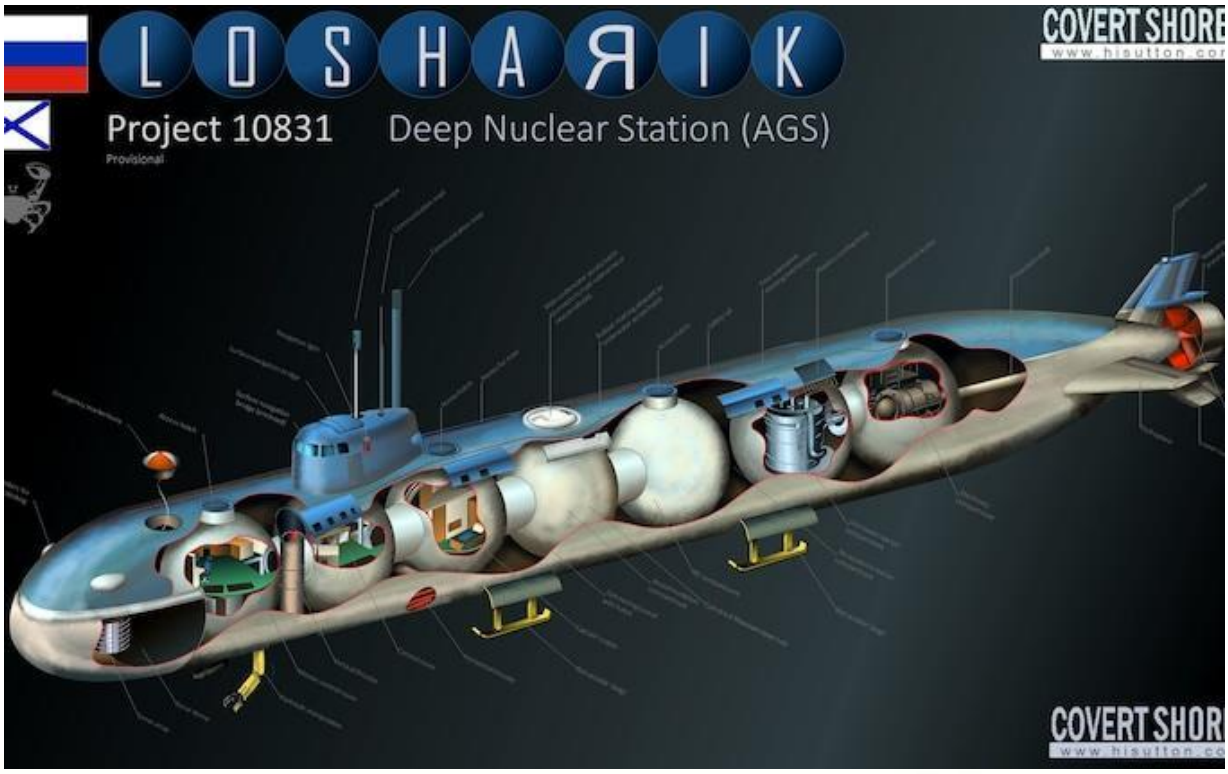
Russian Undersea Aggression

The primary nation-state threats to undersea cabling come from Russia and China. Russia directly threatens the cables via submarines and surface vessels that are operated by Russia's

Main Directorate of Deep-Sea Research (GUGI). Such vessels include the Losharik and the Russian spy ship Belogorod – the mother ship of the Losharik (see figure 3)[27].

Figure 3 *Russian spy vessel the Losharik* ***Source*****:** https://www.telegraph.co.uk/news/2021/03/21/royal-navy-deploy-spy-ship-stop-russian-submarines-

sabotaging/



Losharik sits on the sea bed and has a robotic arm to cut internet cables. The hull is designed to withstand extreme pressures and the submersible is operatable at depths of up to a kilometre [28]. The Yantar submarine is of equal intelligence gathering and sabotage capabilities as it also possesses devices that can tap undersea cables [29]. These spy vessels could cause considerable damage to swathes of undersea cabling and obtain data of strategic value flowing through them.

The UK's response to Russia's submarine capabilities has been to deploy a new Multi Role Ocean Surveillance ship (MROSS) to match Russia's routine operations near undersea cables in Scandinavia, especially in the Artic and the Atlantic. This 'submarine' competition was foregrounded by a collision in 2020 between the Royal Navy's HMS Northumberland and a Russian submarine vessel, sparking further speculation about cable-mapping and sabotage activity.

In the US, the 2021 Office of the Director of National Intelligence's threat assessment found that Russia "continues to target critical infrastructure, including underwater cables". The

assessment also highlighted that the Kremlin has expanded its control over domestic technology firms to serve its foreign policy agenda. For example, Russian state-owned telecommunication firm Rostelecom has been linked with hijacks of the Border Gateway Protocol (BGP), the Internet's "GPS". Rostelecom deliberately rerouted global Internet traffic through Russian borders, with the primary objective of acquiring sensitive Internet data.

Significantly, the threat from Russian undersea aggression has remained despite the ongoing war in Ukraine. Russia has also sort submarine operations within and around the Artic Circle to further its aims of becoming the dominate power in the region and thus establish primacy over the Arctic's resources[30] [31]. A recent example of submarine aggression may have occurred in October this year, when the Shetland Islands lost internet connection after the cable linking islands to the mainland was cut. Significantly, the Boris Petrov, a Russian 'research vessel' was in the area. Such an act would typify Russian grey-zone warfare, and conform to the Gerasimov doctrine[32]. The doctrine was developed by General Valery Gerasimov—Russia's chief of the General Staff. In 2013 he wrote: "The very 'rules of war' have changed. The role of non-military means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness. ... All this is supplemented by military means of a concealed character"[33]. This quote, summaries Russia's core motivations for attacking undersea cables. Attacks on cabling from Russian submarines and tapping from Russia's state-owned enterprises are likely to continue to threaten the security of submarine communication infrastructure.

China – Underhanded Undersea Competition

The second threat actor to analyse is China. The ocean floor is another arena where US-China grand power competition is unfolding [34]. Xi Jinping stated that he intends to extend China's global influence through a "Digital Silk Road"[35], undersea cabling forms part of the marine road. Notably in the "Made in China 2025" plan, the Chinese government set out a road map to acquire 60% of the global fibre optic market, to bolster both Chinese hard and soft power. This strategic objective was backed up by CCP officials explaining that "although undersea cable laying is a business, it is also a battlefield where information can be obtained."

China is typically not viewed as a marine power, yet it has gained influence over cable companies, the cables themselves and the cable building process [36]. The Chinese company HMN Tech, formerly Huawei Marine Networks, has become a major player in undersea cable provision[37]. The company alone has built or repaired almost a quarter of the world's submarine cables. Hence, just as there were concerns about espionage and the installation of 'back doors' in Huawei's 5G technology, intelligence analysts also oppose the company's undersea equivalent.

Several other Chinese companies — such as ZTE, China Telecom, China Mobile and China Unicom — have invested in the construction and maintenance of submarine cables or have

acquired ownership of cables through a consortium from state-owned telecommunications companies. Some of these companies are inextricably tied to the Chinese Communist Party (CCP), including China's largest producer of advanced submarine-cabling whose founder, Cui Genliang, has sat on the National People's Congress.

China also leverages its economic power to attempt to lay cables on behalf of small nation-states such as Pacific Island countries to bring the Indo-Pacific into its sphere of influence [38]. Chinese companies are set to lead several other cable laying projects. Notably, China Telecom Global will lead a new consortium to build a $300m submarine cable system that will connect Hong Kong and Singapore with the Philippines, Brunei, and Hainan. Moreover, China frequently lays cables between Chinese outposts in the disputed Paracel Islands to bolster territorial claims in the South China Sea. There is push back on Chinese lead undersea cable projects: last year a World Bank-led project declined to award a contract to lay sensitive undersea communications cables after Pacific Island governments registered the seriousness of the security threat that Chinese cable laying companies posed.

In relation to the CCP's ambition to reunify with Taiwan. There are potential disruptions to undersea internet cables in the Taiwan Strait. A disruption in a conflict with China could result in Taiwan getting cut off with global geopolitical implications[39]. Current actions against cabling around Taiwan strait have included sand dredging, where sand dredgers frequently encroach on Taiwanese controlled waters. The CCP is employing this as both an intimidation tactic and a potential method to damage undersea communications in the event of an invasion. The Mercatus Centre found that disruptions to submarine internet cables – crucial for Taipei's semiconductor industry – would also severely affect the global economy. For instance, the Pacific Light Cable Network, owned by Meta, has its key landing points in Toucheng, Taiwan and El Segundo, California – it is thus vital for communications between big tech companies. In response, the Taiwanese government it set to spend US$17.11 million on bolstering mobile infrastructure, including submarine cables and to accelerate the deployment of 5G mobile network by 2024.

To summarise, China's threat to global network of submarine cabling, stems from its desire to reshape the Internet's physical layout through companies that control Internet infrastructure[40], to route data more favourably, gain better control of internet chokepoints for espionage advantages and to realise its ambition of reunification with Taiwan[41].

An Overview of Undersea Cable Ownership

Ownership structures play into the vulnerabilities facing undersea cabling. Ownership structures enable assessments of state influence. Data routing patterns shift through which countries' borders sensitive information flows, and shifting private ownership alters profit levels for companies[42]. This can enable the development of technological reliance between states. On top of this, depending on the company/state owner - especially those linked with

authoritarian government's security apparatus - will increase the likelihood of backdoors being inserted into and increase the levels of monitoring at landing stations[43]. Cable builders might similarly compromise the security of the physical infrastructure along the ocean floor before and during installation.

Significantly, undersea cabling is developed by an international consortium of companies. One single cable may have several corporate owners. For example, the Europe India Gateway cable, has sixteen different co-owners, ranging from AT&T (the United States) to Djibouti Telecom (Djibouti) to Airtel (India) to Vodafone (the United Kingdom). Yet, 65% of cables have a single corporate owner. The responsibility of cable repairs becomes a commercial responsibility, rather than a national security concern, despite diplomatic cables and military communication also largely passing through privately-owned cables. Hence, governments looking to spy on the data traveling across submarine cables often turn to private sector companies given their heavy involvement in cable ownership and maintenance[44]. Evidently, ownership structures can be exploited by nation state adversaries[45].

The Legal Environment Surrounding Submarine Cables

In terms of legal protections, enforcement and ramifications, undersea cable regulations are comprised of a patchwork of international conventions and customary laws that seem ill-equipped to govern such an indispensable part of the world's communication infrastructure[46].

The earliest international law agreement on the topic is the Convention on the Protection of Submarine Cables, signed in Paris in 1884, much of which forms the basis of the current legal framework. Secondly, the 1958 Geneva Conference on the Law of the Sea addressed submarine cables in two treaties, the Convention on the High Seas[47] and the Convention on the Continental Shelf. The High Seas Convention included the submarine cable protections of the 1884 Convention and highlighted the "freedom to lay submarine cables," as a fundamental freedom of the high seas in international law[48].

Yet, of particular relevance is the United Nations Convention on the Law of the Sea (UNCLOS). Under UNCLOS all states have a right to lay cables and pipelines on the seabed and continental shelf up to a 12 nautical mile limit. To run a cable to shore through another state's territorial sea, a state needs the permission of the respective coastal state. But beyond that, the power of the coastal state to impose conditions on where a cable is laid is quite limited. Additional gaps remain: current regulation does not explicitly prohibit, for instance, states from treating undersea cables as legitimate military - the Tallinn Manual on submarine communications leaves cables carrying both military and civilian traffic as a legitimate target under the law of armed conflict as Rule 39 of the Tallinn Manual details that objects used for military and civilian purposes are legitimate military objectives.

International law does however make the crucial distinction between attacks on cables and espionage[49]. As spying operations on cables consist of passively tapping the information coming through the pipes at landing sites rather than forceful attacks that impede the cables' functioning. However, international law lacks sufficient protections of civilian uses of

undersea cabling[50].

Conclusions and Implications

This report has highlighted that the threat landscape facing undersea cabling is complex covering multiple attack domains. It is vital to fully unpack these as undersea cabling is and will remain central to the internet's infrastructure. Threats come from state and non-state actors from land, sea and cyberspace. Undersea cabling and communication have a history of being exploited for military and political advantages, this has intensified as dependence on submarine cabling has risen. The most notable state actors analysed were Russia and China. China primarily looks to gain ownership of cables, and acquire data flows with a military

interest in cabling around the Taiwan strait. Russia seeks intimidation through submarine activity and grey-zone operations to damage and cut cables, as the recent Shetlands outage displays.

In order to effectively counter the aforementioned threats improving monitoring and attribution of hostile action is key. Governments can scrutinise projects to avoid security breaches, ensuring that cable routes guarantee their overall resilience. This would involve intelligence sharing among allies through assessments of the risk of each cable project and be aided by a modernised legal framework, thereby developing a public-private model for cable projects and the maintenance of current cabling[51]. It is evident that good maintenance is a step toward reducing the disruption from accidental damage or a premeditated attack. In short, it is crucial that undersea cables do not remain an underappreciated aspect of geopolitics.

References

1. Aid, M. M. (2001). The National Security Agency and the Cold War. Intelligence & National Security, 16(1), 27-66.
2. Alleslev, L. (2019). NATO Anti-submarine warfare: rebuilding capability, preparing for the future. Science and Technology Committee (STC).
3. BBC News (2017) *Russia a 'risk' to undersea cables, Defence chief warns*, *BBC News*. BBC. Available at: https://www.bbc.co.uk/news/uk-42362500.
4. BBC News (2021) *New Royal Navy ship to protect 'critical' undersea cables*, *BBC News*. BBC. Available at: https://www.bbc.co.uk/news/uk-56472655.
5. Bishop Jr, W. W. (1962). The 1958 Geneva Convention on fishing and conservation of the living resources of the high seas. Colum. L.

Rev., 62, 1206.

6. British Royal Navy warship hits Russian Nuclear Submarine in Atlantic clash (2022) YouTube. YouTube. Available at: https://www.youtube.com/watch?v=kNcktDNQY1U

7. Brown, G. (2015). Spying and Fighting in Cyberspace: What Is Which. J. Nat'l Sec. L. & Pol'y, 8, 621.

8. Brown, I. (2013). Expert witness statement for big brother watch and others re: Large-scale internet surveillance by the UK.

9. Buchanan, B., 2020. *The hacker and the state: Cyber attacks and the new normal of geopolitics*. Harvard University Press.

10. Burdette, L. (2021). Leveraging Submarine Cables for Political Gain: US Responses to Chinese Strategy. Journal of Public & International Affairs.

11. Burnett, D., Davenport, T., & Beckman, R. (2014). Overview of the international legal regime governing submarine cables. In Submarine Cables (pp. 61-90). Brill Nijhoff.

12. Carrell, S. (2022) Shetland loses telephone and internet services after Subsea Cable Cut, The Guardian. Guardian News and Media. Available at: https://www.theguardian.com/uk-news/2022/oct/20/shetland-loses-telephone- internet-services-subsea-cable-damaged.

13. Chapman, B. (2021). Undersea Cables: The Ultimate Geopolitical Chokepoint.

14. Clark, B. (2016). Undersea cables and the future of submarine competition. *Bulletin of the Atomic Scientists*, *72*(4), 234-237.

15. Communications, O.D.N.I.O.of S. (no date) Odni Home, Home. Available at: https://www.dni.gov/index.php/newsroom/reports-publications/reports- publications-2021/item/2204-2021-annual-threat-assessment-of-the-u-s- intelligence-community.

16. Crain, J. K. (2012). *Assessing resilience in the global undersea cable infrastructure*. NAVAL POSTGRADUATE SCHOOL MONTEREY CA.

17. Curtis, L., & Rasser, M. (2021). A techno-diplomacy strategy for telecommunications in the Indo-Pacific. *Center for New American Security*.

18. Davenport, T. (2012). Submarine communications cables and law of the sea: Problems in law and practice. Ocean Development & International Law, 43(3), 201- 242.

19. Davenport, T. (2015). Submarine cables, cybersecurity and international law: An intersectional analysis. Cath. UJL & Tech, 24, 57.

20. Doffman, Z. (2020) Russia and China 'hijack' your internet traffic: Here's what you do, Forbes. Forbes Magazine. Available at: https://www.forbes.com/sites/zakdoffman/2020/04/18/russia-and-china-behind-internet-hijack-risk-heres-how-to-check-youre-now-secure/.

21. Downer, A. (2022) The threat to Britain's undersea cables, The Spectator. Available at: https://www.spectator.co.uk/article/the-threat-to-britains-undersea-cables/.

22. Eddy, N. (2015) Microsoft undersea cables are really about the cloud, InformationWeek. Available at: https://www.informationweek.com/enterprise- applications/microsoft-undersea-cables-are-really-about-the-cloud.

23. Elsa B. Kania for The Diplomat (2019) Made in China 2025, explained, – The Diplomat. for The Diplomat. Available at: https://thediplomat.com/2019/02/made- in-china-2025-explained/

24. Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball (2013) GCHQ taps fibre-optic cables for secret access to World's communications, The Guardian. Guardian News and Media. Available at: https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world- communications-nsa.

25. Goldman, E.O. and Warner, M. (2017) *Why a digital Pearl Harbor makes sense . . . and is possible - understanding cyber conflict: 14 analogies*, *Carnegie Endowment for International Peace*. Available at: https://carnegieendowment.org/2017/10/16/why- digital-pearl-harbor-makes-sense-.-.-.-and-is-possible-pub-73405.

26. Guilfoyle, D., Paige, T. P., & McLaughlin, R. (2022). The final frontier of cyberspace: The seabed beyond national jurisdiction and the protection of submarine cables. International & Comparative Law Quarterly, 71(3), 657-696.

27. Hannam, P. (2018) Hopes for Tasmania's 'Battery of the nation' dangle by a cable, or two, The Sydney Morning Herald. The Sydney Morning Herald. Available at: https://www.smh.com.au/environment/hopes-for-tasmanias-battery-of-the-nation- dangle-by-a-cable-or-two-20180117-h0jm5j.html.

28. Hicks, K. (2019) *Russia in the Gray Zone*, *The Aspen Institute*. Available at: https://www.aspeninstitute.org/blog-posts/russia-in-the-gray-zone/.

29. Hillman, J.E. (2022) The Digital Silk Road: China's quest to wire the world and win the future. London: Profile Books.

30. Hinck, G. (2019) *Cutting the cord: The legal regime protecting undersea cables*, *Lawfare*. Available at: https://www.lawfareblog.com/cutting-cord-legal-regime- protecting-undersea-cables.

31. Hinck, G. (2019) *Evaluating the Russian threat to undersea cables*, *Lawfare*. Available at: https://www.lawfareblog.com/evaluating-russian-threat-undersea-cables.

32. In Focus: Subsea cables in China's crosshairs (2022) Taipei Times. 台北時報. Available at: https://www.taipeitimes.com/News/taiwan/archives/2022/10/31/2003788016.

33. Kamiński, T., & Szewczyk, R. (2022). The coastal state obligation not to impede the laying or maintenance of submarine pipelines on the continental shelf according to United Nations convention on the law of the sea. Marine Policy, 143, 105086.

34. Khazan, O. (2013) The creepy, long-standing practice of undersea cable tapping, The Atlantic. Atlantic Media Company. Available at: https://www.theatlantic.com/international/archive/2013/07/the-creepy-long- standing-practice-of-undersea-cable-tapping/277855.

35. Kirchner, S. (2020). Interference with Subsea Cables: An Arctic Perspective. In Cybersecurity and Resilience in the Arctic (pp. 190-199). IOS Press.

36. Lee, S. (2019) The cybersecurity implications of Chinese Undersea Cable Investment, The Henry M. Jackson School of International Studies. Available at: https://jsis.washington.edu/news/cybersecurity-implications-chinese-undersea-cable-investment/.

37. Lee, Y. (2021) China's latest weapon against Taiwan: The Sand Dredger, Reuters. Thomson Reuters. Available at: https://www.reuters.com/article/us-taiwan-china- security-idUSKBN2A51EJ.

38. Lele, A., & Roy, K. (2019). Analysing China's Digital and Space Belt and Road Initiative. Institute for Defence Studies and Analysis.

39. Leppard, D. (2007) *Al Qaeda plot to bring down UK internet*, *The Sunday Times*. The Sunday Times. Available at: https://www.thetimes.co.uk/article/al-qaeda-plot-to- bring-down-uk-internet-b8vb32twcwt.

40. Loughran, J. (2018) Huawei's undersea internet cable banned by Australia over spying fears, RSS. Available at: https://eandt.theiet.org/content/articles/2018/01/huawei-s-undersea-internet- cable-banned-by-australia-over-spying-fears/.

41. Luke Coffey Senior Fellow Luke Coffey Oct 20 *et al.* (2022) *Protecting undersea cables must be made a national security priority*, *Hudson*. Available at: https://www.hudson.org/national-security-defense/protecting-undersea-cables- must-be-made-a-national-security-priority.

42. Magnier , M. (2022) 'highly likely' Taiwan attack may cut internet cables, causing global costs, South China Morning Post. Available at: https://www.scmp.com/news/china/military/article/3190898/report-about- potential-attack-taiwan-focuses-vulnerability.

43. Matis, M. S. (2012). *The protection of undersea cables: A global security threat*. ARMY WAR COLL CARLISLE BARRACKS PA.

44. Mauldin, A. (2017) A complete list of content providers' Submarine Cable Holdings, TeleGeography. TeleGeography. Available at: https://blog.telegeography.com/telegeographys-content-providers-submarine- cable-holdings-list.

45. Mauldin, A. (2019) Cable breakage: When and how cables go down, TeleGeography. TeleGeography. Available at: https://blog.telegeography.com/what-happens-when- submarine-cables-break.

46. McDaniel, C. A., & Zhong, W. (2022). Submarine Cables and Container Shipments: Two Immediate Risks to the US Economy If China Invades Taiwan. Mercatus Policy Brief Series.

47. McGeachy, H. (2022). The changing strategic significance of submarine cables: old technology, new concerns. Australian Journal of International Affairs, 76(2), 161-177.

48. Mckew, M.K. *et al.* (2017) *The gerasimov doctrine*, *POLITICO Magazine*. Available at: https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia- foreign-policy-215538/.

49. Minister of Defence (2021) New Royal Navy surveillance ship to protect the UK's critical underwater infrastructure, GOV.UK. GOV.UK. Available at: https://www.gov.uk/government/news/new-royal-navy-surveillance-ship-to- protect-the-uks-critical-underwater-infrastructure.

50. Mori, S. (2019). US technological competition with China: The military, industrial and digital network dimensions. Asia-Pacific Review, 26(1), 77-120.

51. Morris, C. (2012). Operation IVY BELLS: Lessons learned from an'intelligence success'. *Journal of the Australian Institute of Professional Intelligence Officers*, *20*(3), 17-29.

52. Nixon, D. W. (1999). Blind Man's Bluff--The Untold Story of AmericanSubmarine Espionage. *Marine Technology Society. Marine Technology Society Journal*, *33*(4), 86.

53. O'Halloran, J. (2021) More than $8bn forecast for Cable Investments over next three years, ComputerWeekly.com. ComputerWeekly.com. Available at: https://www.computerweekly.com/news/252502398/More-than-8bn-forecast-for-cable-investments-over-next-three-years.

54. Oxford Analytica. (2021). US-China tensions loom over undersea internet cables. Emerald Expert Briefings, (oxan-db).

55. PA Media (2022) *UK military chief warns of Russian threat to vital undersea cables*, *The Guardian*. Guardian News and Media. Available at: https://www.theguardian.com/uk-news/2022/jan/08/uk-military-chief-warns-of- russian-threat-to-vital-undersea-cables.

56. Person and Jonathan Barrett, Y.L.T. (2021) Exclusive Pacific Undersea Cable Project Sinks after U.S. warns against Chinese bid, Reuters. Thomson Reuters. Available at: https://www.reuters.com/world/asia-pacific/exclusive-pacific-undersea-cable- project-sinks-after-us-warns-against-chinese-2021-06-18/.

57. Pincus, R. (2020). Towards a new Arctic: changing strategic geography in the GIUK Gap. the RUSI Journal, 165(3), 50-58.

58. Raspotnik, A. (2022) *Underneath the ice: Undersea Cables, the Arctic Circle, and international security*, *The Arctic Institute - Center for Circumpolar Security Studies*. Available at: https://www.thearcticinstitute.org/underneath-ice-undersea-cables- arctic-circle-international-security/.

59. Ratiu, A. (2022) *Cyber defense across the ocean floor: The geopolitics of submarine cable security*, *Atlantic Council*. Available at: https://www.atlanticcouncil.org/in- depth-research-reports/report/cyber-defense-across-the-ocean-floor-the- geopolitics-of-submarine-cable-security/.

60. Robb, J. (2014) The 'intelligence special relationship' between Britain and the United States, E. Available at: https://www.e-ir.info/2014/06/15/the-intelligence-special- relationship-between-britain-and-the-united-states/.

61. Ross, M. (2014). Understanding interconnectivity of the global undersea cable communications infrastructure and its implications for international cyber security. *The SAIS Review of International Affairs*, *34*(1), 141-155.

62. Schadlow, N. and Helwig, B. (2022) *Protecting undersea cables must be made a national security priority*, *Defense News*. Defense News. Available at: https://www.defensenews.com/opinion/commentary/2020/07/01/protecting- undersea-cables-must-be-made-a-national-security-priority/.

63. Sechrist, M. (2010). Cyberspace in deep water: Protecting the arteries of the Internet. Kennedy School Review, 10, 40-45.

64. *Securing the Subsea Network: A Primer for Policymakers* (2021) *Securing the Subsea Network: A Primer for Policymakers | Center for Strategic and International Studies*. Available at: https://www.csis.org/analysis/securing-subsea-network-primer- policymakers.

65. SEIBT, S. (2022) *Threat looms of Russian attack on undersea cables to shut down West's internet*, *France 24*. France 24. Available at: https://www.france24.com/en/europe/20220323-threat-looms-of-russian-attack-on-undersea-cables-to-shut-down-west-s-internet.

66. Shen, H. (2018). Building a digital silk road? Situating the internet in China's belt and road initiative. International Journal of Communication, 12, 19.

67. Stavridis, J. (2019) China spying: The internet's underwater cables are next, Bloomberg.com. Bloomberg. Available at: https://www.bloomberg.com/opinion/articles/2019-04-09/china-spying-the- internet-s-underwater-cables-are-next.

68. Sunak, R. (2022) *Undersea cables: Indispensable, insecure*, *Policy Exchange*. Available at: https://policyexchange.org.uk/publication/undersea-cables-indispensable-insecure/.

69. TeleGeography (no date) *Submarine Cable Faqs*, *Submarine Cable FAQs*. Available at: https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions.

70. The Tallinn manual. Available at: https://ccdcoe.org/research/tallinn-manual/

71. The Week Staff (2022) *The undersea cables that connect the world*, *The Week UK*. The Week. Available at: https://www.theweek.co.uk/news/technology/955812/undersea-cables-connect- world-subject-concern.

72. Ultramap@angelfysh.com (2020) *The biggest threat to subsea cables.*, *UltramapGlobal*. Available at: https://ultra-map.org/the-biggest-threat-to-subsea- cables/.

73. Underwood, B., & Saiedian, H. (2021). Mass surveillance: A study of past practices and technologies to predict future directions. Security and Privacy, 4(2), e142.

74. United Nations Convention on the law of the sea. International Maritime Organization. Available at: https://www.imo.org/en/OurWork/Legal/Pages/UnitedNationsConventionOnTheLa wOfTheSea.aspx.

75. UNTC. United Nations. Available at: https://treaties.un.org/Pages/showDetails.aspx?objid=08000002800338fb.

76. Walker, J. (2022) *The battle for control of undersea internet cables*, *Verdict*. Available at: https://www.verdict.co.uk/the-battle-for-control-of-undersea-internet-cables/.

77. Wall, C. and Morcos, P. (2021) *Invisible and vital: Undersea cables and transatlantic security*, *Invisible and Vital: Undersea Cables and Transatlantic Security | Center for Strategic and International Studies*. Available at: https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic- security.

78. Winseck, D., (2017). The geopolitical economy of the global internet infrastructure. *Journal of Information Policy*, *7*(1), pp.228-267.

79. Wither, J. K. (2021). An Arctic security dilemma: assessing and mitigating the risk of unintended armed conflict in the High North. European Security, 30(4), 649-666.


London Politica