ROYAL AUSTRALIAN NAVY
SEA POWER
SOUNDINGS

Issue 32, 2021

Securing Australia’s Submarine Communications Infrastructure

A history of Australia's engagement with undersea cables and lessons for understanding the contemporary strategic environment

By Angus Eckstein

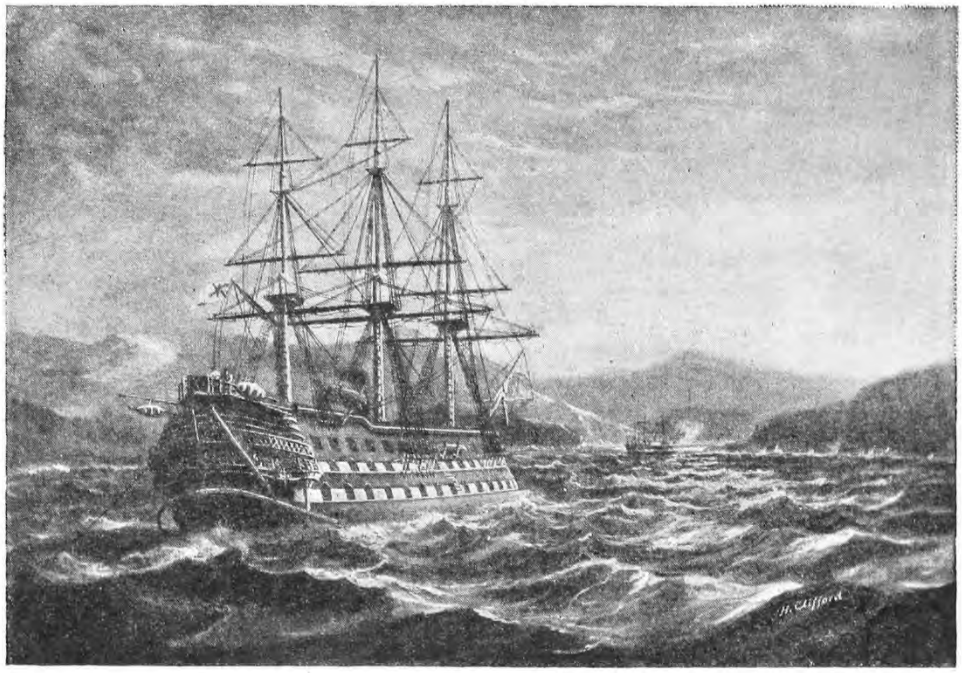
Angus Eckstein attended the Sea Power Centre-Australia as part of the Australian National Internships Program

ROYAL AUSTRALIAN NAVY
SEA POWER
SOUNDINGS

Issue 32, 2021

ROYAL AUSTRALIAN NAVY
SEA POWER
SOUNDINGS

Issue 32, 2021



H.M.S. Agamemnon entering Valentia Bay with first Atlantic Cable.
Frontispiece.

Painting by Henry Clifford, a telegraph engineer. Reprinted in Charles Bright, The Story of the Atlantic Cable *(New York: D. Appleton and Co., 1903).*

Executive summary

The security of submarine communications cables (SCCs) is vital to Australia's strategic and economic interests. Transoceanic information flows for military, government, corporate and private communications rely almost entirely on SCCs. There is no alternative system capable of handling this data as satellite communications have relatively low bandwidth and high latency. As an island state, Australia is dependent on SCCs and especially vulnerable to SCC system interruptions.

This report collates and expands upon primary and secondary historical sources, including important archival material, and makes an essential contribution to the currently scarce literature around the strategic value of Australia's SCCs. Australian-linked SCCs and their terrestrial infrastructure have significant vulnerabilities. While Australia has several legal and regulatory protections for SCC infrastructure, further action by Defence and other government agencies are required to protect these vital links, especially as the country enters an uncertain strategic future.

There is a strong historical basis for recognising the importance of SCCs, especially the need for a diversity of cable routes and landing points to avoid the geographic concentration of infrastructure. German naval action in the Pacific during the First World War indicates the potential for isolated incidents to have significant ramifications for communications when there is an insufficient distribution of infrastructure. Espionage operations conducted by Australian and US forces in the Second World War and the Cold War

demonstrate the importance of submarine cables for defence forces, which rely on fast, secure communications to maintain command.

SCC vulnerabilities expose Australia's globalised economy and its security links with allies to damage occurring from natural disasters and attacks by malicious actors, including terrorist groups, state-sponsored actors and other states. Future cable projects should extend along Australia's coastline to hedge against these geographic vulnerabilities. Lack of demand and high costs have so far prevented this, but government intervention would go some way to rectifying the problem. The importance of SCCs to the ADF's and Defence's secure communications cannot be overstated. Defence Science and Technology Group should undertake research to determine Defence's level of reliance upon SCCs and the potential for alternative technologies to reinforce its communications infrastructure.

The lack of a dedicated inter-agency strategy to respond to hostile action against Australia's SCC infrastructure presents a gap in defence planning, especially with new cable projects underway on Australia's vulnerable northern approaches. Australia's allies have and continue to invest in capabilities to secure their SCC networks. Current maritime security arrangements should be expanded upon: Defence, Home Affairs and the national intelligence community should collaborate on forming a strategy to protect SCC infrastructure and respond to hostile action targeting it. In addition, regular patrols around Australian Communications and Media Authority (ACMA)-designated SCC protection zones should be conducted to ensure compliance and prevent cable damage. Current and precise publicly available data around the locations of submarine cables is limited. ACMA should release this coordinate data on at least a yearly basis to assist further studies of Australia's SCCs.

Issue 32, 2021

Introduction

Submarine communications cables (SCCs) have been essential to Australia's economic and national security since the late nineteenth century. These cables are more important to Australia now than ever before due to the accelerating digitisation of information, trade, culture and society. For an increasingly connected defence force, SCCs will only become more essential to the command, control, communications and computer (C4) systems that enable the effective deployment of Defence capabilities and personnel within the region and around the globe. In 2021, SCCs carry 99 per cent of transoceanic internet traffic and are far more capable than any wireless or satellite technology. To the public and many policy-makers, however, their importance goes unnoticed; after all, they are far less glamorous than the launch of a new satellite constellation or a new generation of mobile technology. SCCs and their terrestrial landing sites are part of an invisible but essential telecommunications infrastructure, the majority of which lies under the seas and oceans of the world, out of sight and out of mind. This report seeks to rectify the invisibility of modern submarine cable networks by detailing the threats SCC networks have been presented with from their inception. It considers how technological and geostrategic change has affected Australian cable systems, and the legislative, regulatory and defence regimes constructed to protect them.

Australia's international cable systems have a storied history. For an island nation initially reliant on months-long voyages to receive information from the other side of the world, the invention of undersea telegraph communications was ground-breaking. The first half of this report is dedicated to a recounting and analysis of Australia's historical engagement with undersea cables. Beginning with an overview of the first steps taken to achieve undersea communications in Europe, the nineteenth-century Australian experience is examined, considering the information security concerns of the British Empire at the time. Following this, German attacks on Pacific cable stations in the First World War are identified as particularly significant events, given they present the only examples of malicious attack in the history of Australia's SCCs. After developments in the interwar period are discussed, the report moves on to a history of Australian action around SCCs in the Second World War, where the midget submarine Operation SABRE provides a valuable example of a clandestine cable-cutting effort. The historical section concludes with an account of the US intelligence-gathering operation Ivy Bells, which presents a further useful example of clandestine operations during the Cold War.

Following a transitional section that examines changes in technology from telegraph lines to fibre-optic cable, the contemporary SCC network in Australia and abroad comes into focus. The details of Australia's current international connections are examined and particular concerns about the lack of landing stations' geographic diversity come to the fore. The implications of this lack of diversity are examined by observing the most significant threats to SCCs. Natural disasters, undersea phenomena, fishing and dredging vessels, and malicious attack are all understood to pose a more significant threat to SCCs when cables land in very few places along a coastline. In a particularly important section of this report, the likelihood of a genuine malicious attack against cables or landing points is considered. Attacks cannot be discounted, particularly in an era of rising strategic tensions.

This part of the report continues by asking why the geographic distribution of cables has not occurred in Australia and finds that it is largely due to high costs and lack of demand. After observing some nascent geostrategic concerns from an international perspective, the importance of SCCs to uninterrupted and secure military communications is considered. The final parts of the section discuss Australia's legislative and regulatory protections for SCCs, finding them potentially wanting in their clarity and effectiveness.

The report concludes with five recommendations seeking to aid the ongoing protection of Australia's vital SCC links. Factors that will contribute to the ongoing security of SCCs in Australia include in-depth studies of SCCs' importance for secure Defence communications, diversifying future Australian cable landing sites, creating an inter-agency response plan to combat hostile action against SCC infrastructure, making additional resources available for protection zone enforcement, and providing current and accurate data about the locations of SCCs in Australian waters.

Australia's historical engagement with submarine cables

The nineteenth century

In 1837, Samuel Morse's invention of a point-to-point communication technique using pulses of electrical current ushered in a telecommunications revolution. A near-instantaneous method of long-distance communication meant that vital information could be sent to and from far-flung concessions and territories in minutes or hours, rather than days, weeks or months. By the mid-nineteenth century, terrestrial telegraph systems were commonplace in Europe and the United States and were growing quickly.[1] While communications between New York and San Francisco or Moscow and Vladivostok could now take place without waiting for a horse- or train-carried message, telegraph systems stopped at coastlines, and so had to be supplemented with ships where necessary. Communications from Europe to Oceania were markedly improved by terrestrial transmission from Europe to South Asia, but not to the extent made possible by the complete internal terrestrial networks in Europe or America.

In efforts to further the speed and convenience of telegraphy, it became evident that laying cables along the seabed could offer a solution. Experiments that insulated iron or copper wires with the recently discovered (by Europeans) latex sap from the gutta-percha tree in Southeast Asia proved successful. Carl Siemens and Christopher Nickels of the Royal Society were instrumental in setting up the Gutta Percha Company, which would merge with other telecommunications infrastructure interests to dominate submarine cable production for decades.[2]

In 1851, the first consistently working telegraph link under the English Channel was completed between Dover and Calais. Work quickly began on other short links between England and Ireland, and within North America, but Britain, Canada and the US were not connected until 1858. Even then, soon after President James Buchanan and Queen Victoria exchanged messages, the first transatlantic cable failed due to the high currents being pumped through it.[3] By 1866, reliable telegraph communication was achieved between North America and Europe.[4]

Until 1872, Australia had to rely on international communications that travelled at the speed of sail or steam. This meant a months-long lag for news from Britain. Indeed, in the mid-nineteenth century, out-of-date information fostered paranoia about Russian attacks on Australian ports and cities.[5]

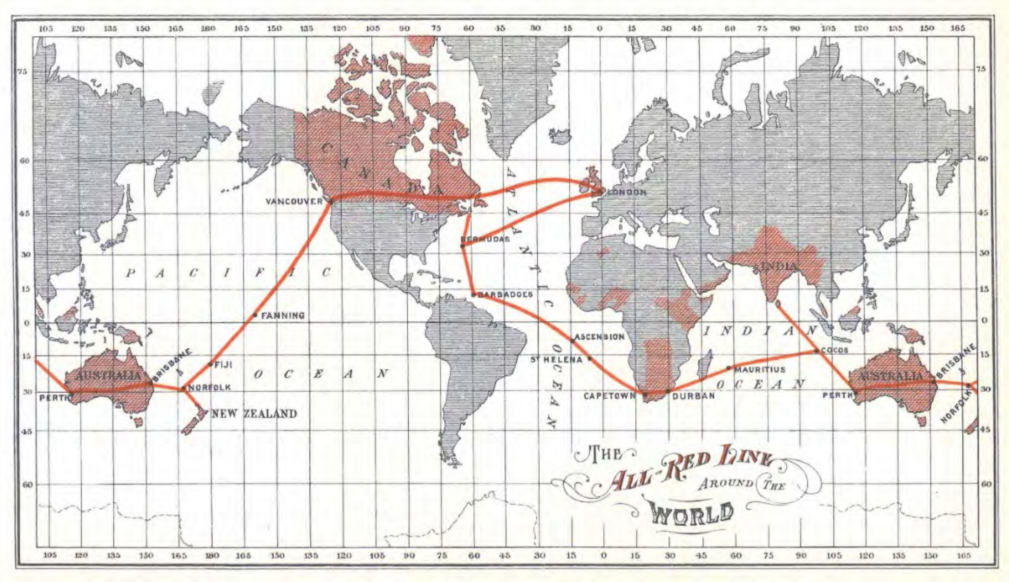
After the successful laying and operation of the Atlantic cable, it was obvious that Britain could use the same technology to communicate with its even further-flung dominions in the antipodes. With the completion of the Overland Telegraph Line from Darwin to Adelaide, and a submarine cable laid between Port Darwin and Banjoewangie in Java, Dutch East Indies, complete telegraphic communications between Australia and the United Kingdom were finally possible in 1872. Additional cable was laid between Broome (Cable Beach) and Java in 1889.[6]

Even in the infancy of the global submarine cable network, the strategic value of SCCs was not lost on the colonial powers. Despite telegraphic communication with Australia being achieved, the path of cables on terrestrial sections, through South Asia, the Middle East and Europe, did not inspire confidence in the security of the network – the potential for cable-cutting, interference and tapping was obvious to the British government.[7]

Reprinted on request of a Canadian senator in 1880, the Ottawa *Daily Citizen* published two articles espousing the importance of sovereign control over the SCCs that connected England to Canada:[8]

> Already it is impossible to communicate telegraphically between the various provinces of the Dominion, or between the Imperial Government of Great Britain and her North American possessions, without every dispatch passing under the censorship of citizens and consequently of the Government of the United States.

While some terrestrial networks followed the French example and were created as public utilities, and others had been nationalised (Britain's private networks were placed under the control of the Post Office in 1868), submarine cable networks were largely owned and managed by private interests. This did nothing to assuage concerns about "purely United States enterprises . . telegraphically [ruling] the whole continent of America, under United States management".[9]



The pan-Britannic cable system described by George Johnson in The All Red Line: The Annals and Aims of the Pacific Cable Project *(Ottawa: James Hope & Sons, 1903). Note the Fanning and Cocos Islands connection points.*

The solution proposed was an "all-red line" of communications that passed exclusively through British territory, akin to Cecil Rhodes' red line of concessions from Egypt to South Africa. The all-red line cable route would run from the UK to Newfoundland, across Canada, and then south-west through the Pacific to Fanning Island, then onto Fiji, Norfolk Island and Australia proper. George Johnson noted the importance of such a project to maintain centralised control over the empire:[10]

> *The wonderful power of electricity applied to telegraphy has suggested its employment on an extended scale, to bring all the parts of the outer Empire within speaking distance of each other, and within instant touch of the Mother Country, the great centre of British power, and the source of influence and national cohesion.*

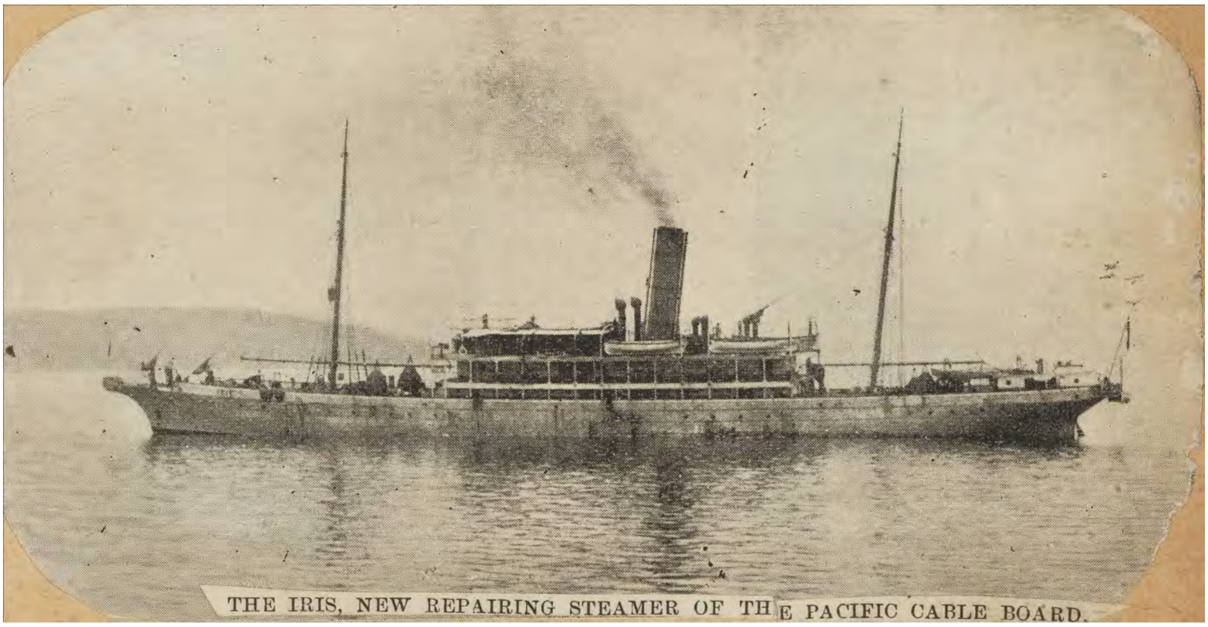
The first transpacific cable was completed in October 1902, and along with existing British cable infrastructure in the Indian and Atlantic Oceans, it formed the first telecommunications girdle around the Earth. Messages could be sent between London and Sydney in just ten hours.[11]

Pacific cable systems in the First World War

Concerns about the vulnerabilities of cables passing through the territory of third parties remained well into the twentieth century. In 1914, three years before the US declared war on Germany, there was great consternation among American telegraph companies, which claimed that UK government censors were suppressing messages that should have been passed through to other "neutral" countries, and that telegram senders were not even notified of non-delivery.[12] The British government was aware of the potential economic value of commercial telegrams, and refused to transmit cables "facilitating commercial transactions with enemy countries".[13]

Even in 1911, the British government was cognisant of the "considerable advantages which would…. accrue to an enemy from the interruption of British telegraphic communications …. at the outbreak of war". While British connections to Canada and South Africa had appropriate redundancies (fifteen and five cables respectively) to continue operations in case of accidental or malicious damage, much of the Commonwealth was only connected by a few cables: the 'all-British connection to Australia relied solely upon the Cocos Island–Darwin and Brisbane–Norfolk Island cable sections.[14] The strategic value of Britain's "all-red line" was obvious to German naval forces operating in the Pacific in 1914, particularly to Karl von Müller, Captain of SMS *Emden*, a Dresden-class German cruiser. Buoyed by his great success raiding shore stations and disrupting allied shipping routes in the Indian Ocean in the first months of the war, von Müller decided to disrupt communications between Britain and Australia by cutting the eastern cable line at the relay station on Direction Island, in the Cocos (Keeling) Islands. Surprisingly, given the essential infrastructure there, Direction Island station did not have a guard complement and was essentially defenceless. Had it been a German installation, Edwin P. Hoyt argues that a company-sized contingent would have been stationed there – the landing party from *Emden* expected fierce resistance. The defenceless cable station staff gladly provided the German party with the location of vital equipment, however, and the station manager even congratulated the commanding German Lieutenant on his award of the Iron Cross, information that had been received via the wireless station.[15] The landing party set about destroying essential wireless and cable communication equipment, blowing up the radio antenna and fishing the submarine cables from the shore before cutting them, though they failed to cut all three cables.

Unfortunately, for *Emden*, the telegraph station was able to send a wireless message to HMAS *Sydney*, which steamed towards Direction Island and on 9 November, *Sydney* engaged in a successful battle that resulted in the grounding of *Emden* and the RAN's first victory.[16] While von Müller, if not German High Command, had been keenly aware of the strategic value of one of the only communications links between Australia and Britain, their efforts had been foiled by a warning sent not over submarine cable but a wireless transmission to the *Sydney*.



The cable ship Iris. *State Library of Western Australia: call Z43b.*

The eastern cable route through the Indian Ocean was not the only piece of SCC infrastructure of interest to German commanders; the Pacific cable was also targeted to disrupt allied communications. The all-red line's existence was hardly a secret given the project had been widely publicised. In September of 1914, the Fanning Island relay station was attacked by another German cruiser, SMS *Nurnberg*, flying a French ensign to deceive the cable station workers until it was too late. The German landing party dynamited the cable and destroyed essential equipment for telegraph operations.[17] A final telegram received by the Vancouver station on 7 September reported that armed soldiers had entered the superintendent's office, and the connection was severed.[18] Concerns about the whereabouts of German cruisers in the area meant that the cable ship HMCS *Iris* waited weeks in Fiji before it could continue to Fanning Island and repair the fault, and did not arrive until 26 October.[19] Every British–Australian telegram had to be rerouted via the Caribbean, South Africa and Direction Island until the cable was finally repaired on 6 November, just three days before *Emden*'s raid on the Direction Island station.[20]

Had the Fanning Island raid happened mere days later or had von Müller managed to attack any earlier, Australia would have been without a direct cable connection to Britain within the first months of the war. The Governor of New Zealand cabled the Australian Prime Minister's office in the days after the raid on Fanning Island, asking whether there was "any information [as to whether] Cocos Island Station is secure".

The reply from the Prime Minister's secretary, Malcolm Shepherd, stated there was "available no reason to suppose any interference with Cocos Island Station".[21]

Archival material also indicates that the Minister for Defence at the time, Senator Edward Millen, had been forewarned about the potential for an attack on a Pacific cable station at least three weeks before German action, but had not set any defensive plans in motion, such as having a British cruiser provide additional security.[22] The stations had no dedicated military defence and were only staffed by telegraph company employees, who had little motivation to prevent the destruction of the communication facilities.[23] There were varying levels of appreciation for the importance of cables and cable stations. While the British had been forward-thinking enough to sever Germany's cables in the North Sea in 1914, they had neglected their own in the Pacific, which perhaps was too far away to consider adequately protecting.

Interwar period

In the years between the world wars, there was minimal change in the structure of the cable system that linked Australia with the rest of the world. British military intelligence documents report that the all-British cable links – vital for the flow of information in the First World War, but as evidenced, vulnerable to attack – remained the same, except for some instances of duplication for redundancy. The lines between Direction Island and Cottesloe in Perth, and Fanning Island and Suva (Fiji) were duplicated in 1926, but no cable routes were added, for example, between Australia and the United States.[24]

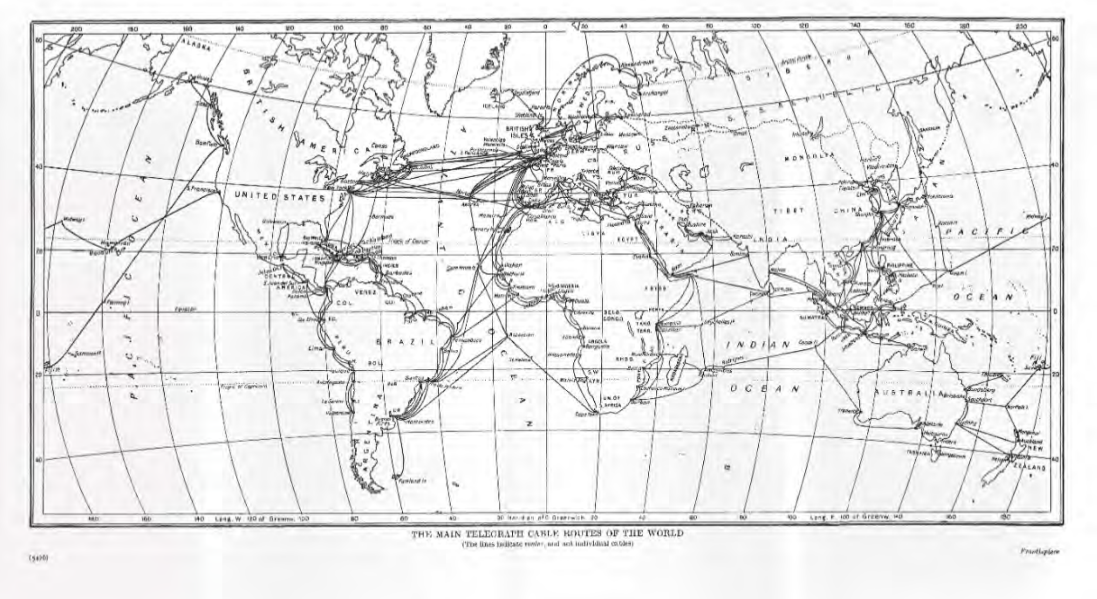
Wireless telegraphy made great advances in the early twentieth century – the first two-way transatlantic radio telegrams were sent and received in 1906 by Reginald Fessenden. By 1919, European radio telephony transmissions were powerful enough to reach North America, and a year later Dame Nellie Melba performed at a radio station in Chelmsford, England, and was heard in Newfoundland.[25] After the First World War, a chain of wireless stations was built throughout the empire, resulting in a British all-red line of wireless operations that stretched from the UK to Canada, India, South Africa, East Asia and Australasia, where the Belconnen station in Canberra received high-frequency transmissions from Britain.[26]

The Belconnen wireless station in Canberra. AWM: P11039.001.

While wireless communication was essential for any advanced, early twentieth-century military – especially for those which, like the British, had to communicate with a massive navy and between far-flung territories – it was not without disadvantages over wired submarine communication. For a time, the relevance of SCCs declined relative to wireless communication, which could reach the other side of the world when transmitted on short wave with a high-frequency broadcast.[27] Wireless communication, however, was and remains insecure, given that anyone with a receiver was able to pick up transmissions, which had to be coded when secret information was transmitted. When Britain severed German cables in the English Channel in 1914 and 1939, Germany was forced to rely on wireless communication, which British code breakers monitored and made operational use of.[28]

SCCs were remarkably secure in comparison – copper cables were only able to be tapped by placing a listening device directly on the cable. Despite cables being fairly easy to grapple and cut, even out of sight of land, the British Overseas Defence Committee noted that cutting them would require an adversary to have "possession of sufficiently accurate information as to the route of the cable". Provided a station was not defended properly, it would be far easier to land and destroy or make useless the telegraph equipment. "No technical knowledge would be required."[29] British Colonial Office documents considering the protection of Fanning Island in 1904 claimed that the remoteness of the landing station was its primary defence: "The cable lies visible in shallow water, and could be grappled and cut without difficulty near the shore".

Rifles and ammunition were provided to the cable station workers, but they were not used when attacked; government documents indicate later plans for a larger gun emplacement on the island that "would probably be quite capable to drive off a raiding merchant vessel".[30]


THE MAIN TELEGRAPH CABLE ROUTES OF THE WORLD
(The lines indicate routes, and not individual cables)
UNITED STATES
BRAZIL
INDIAN OCEAN
PACIFIC OCEAN
AUSTRALIA
NEW ZEALAND
Frontispiece

International cable routes in 1930. F. J. Brown, The Cable and Wireless Communications of the World (London: Sir Isaac Pitman and Sons, Ltd., 1930).

Australian action in the Second World War

With the knowledge that cable communications were secured from interception, cable-cutting operations also occurred in the Pacific theatre during the Second World War. Nearing the end of the war, sensitive Japanese military communications relied on cables between Singapore, Saigon, Hong Kong and Tokyo, and any landing to reoccupy Singapore would necessitate the cutting of these cables. While it might have been possible to use a heavily escorted cable repair ship for this task, the threat posed by Japanese airfields nearby could not be discounted. In May 1945, planning began for a joint RAN/RN operation: SABRE. Two British midget submarines would slip by Japanese defences and sever the cables. Lt Cdr Max Shean, RAN, commanded the submarine XE-4, which was well equipped for the mission. The exact cable locations were already known to the allied force, as the navigator of HMS *Bonaventure,* the midget submarine mother ship, had possession of accurate and current hydrographic charts of the area. Additionally, a Cable and Wireless engineer was able to provide advice on how the submarines could best grapple the cables, which could then be cut by a diver.[31] After two months of training in Hervey Bay, practising on a disused undersea cable that ran from Queensland to New Guinea, and just weeks before the bombing of Hiroshima and Nagasaki, XE-4 was towed to the Mekong Delta by the S-class submarine HMS *Spearhead.* Shean and his crew quickly located and cut both the Saigon–Singapore and Saigon–Hong Kong cables on the afternoon of 31 July 1945 and returned to *Bonaventure.*[32]

Crippling an adversary's cable infrastructure without attacking landing points required (a) diving personnel trained to operate in a hostile marine environment, and with additional training to find and sever cables quickly, and (b) hydrographic information about the seabed and intelligence about the specific location of cables.

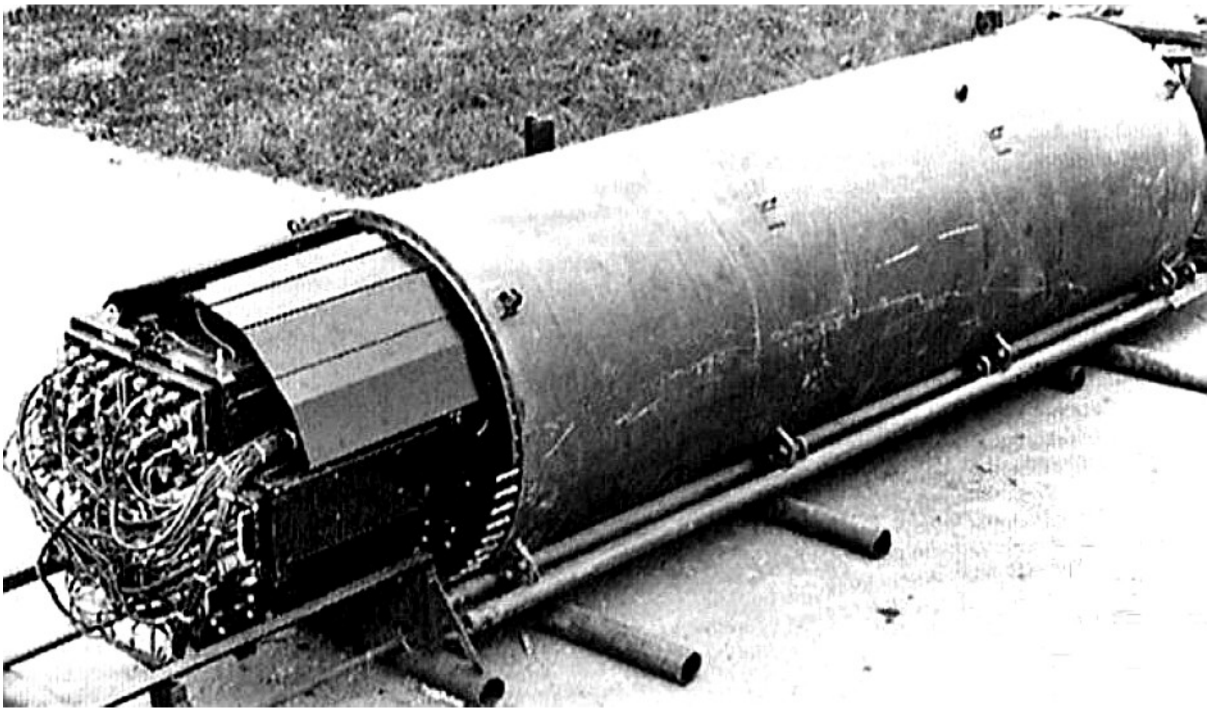
Advents in submersible technology now allow for the repair or cutting of cables using remotely operated underwater vehicles. Of course, this still requires a crew of remote operators, but it is safer and more effective than past methods of cable repair. Additionally, almost every high-capacity undersea fibre cable's precise location can be garnered from companies specialising in selling location data to commercial shipping ventures, which need to avoid costly accidental damage to cables for which they are liable to pay repair costs.[33]

SCC espionage in the Cold War: Operation Ivy Bells

So far, this paper has primarily considered the strategic value of severing communications cables to deny an adversary the ability to quickly and securely transmit information. The tapping of communications cables to *retrieve* this information, however, rather than destroy it – especially without the knowledge of the cable operator – would be an intelligence coup.

In the early 1970s, a cable linking Moscow, Soviet Pacific fleet headquarters in Vladivostok, and the Soviet submarine base at Petropavlovsk in the Sea of Okhotsk was eyed as a prime target by the US Office of Naval Intelligence for a tapping operation: Operation Ivy Bells. While there was no solid evidence that a cable even existed, it was reckoned that Soviet commanders would have wanted to avoid the significant financial and time costs of having to encrypt and decrypt wireless communications, and so would have preferred a hardwired telephone cable for communications.

USS *Halibut*, a nuclear-powered and armed submarine converted to a special operations platform for USN, CIA and National Reconnaissance Office operations, was modified to allow divers to enter and exit a special compartment for operations on the seafloor.[34] Locating the cable only required the crew of *Halibut* to find a Russian "submarine cable here" sign that had been placed to avert damage from fishing vessels. Diving in the near-freezing water, frogmen placed a three-foot-long device that contained reels of tape to record the signals transmitted along the cable, which was not cut or spliced but had a conductor wrapped around it.

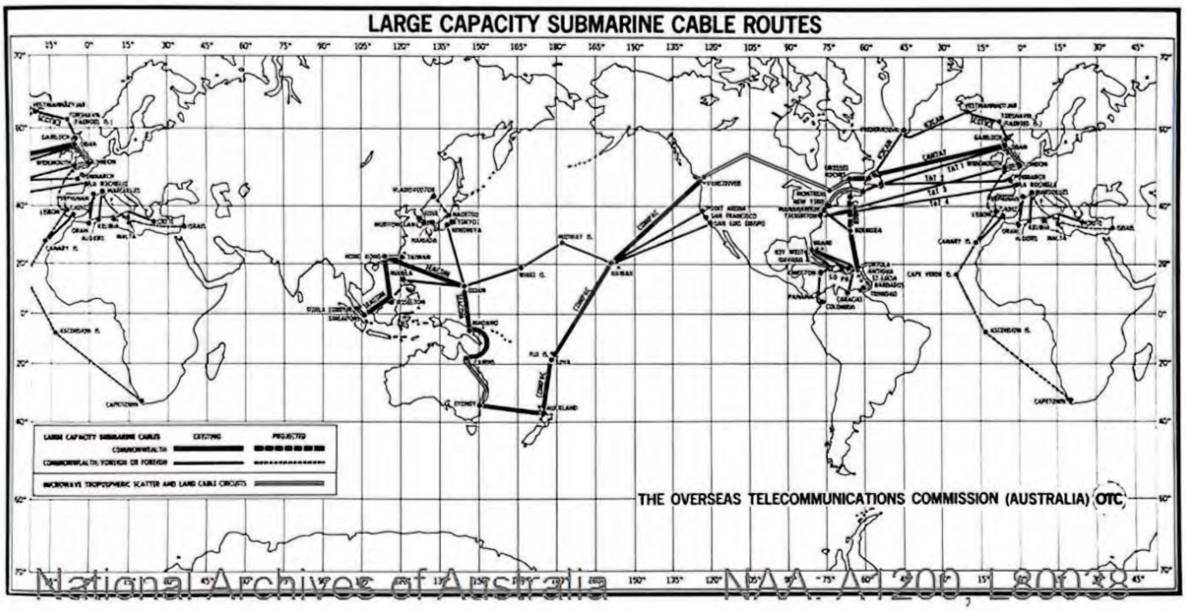


One of the "bugs" placed by US divers on a Russian cable as part of Operation Ivy Bells, later discovered by the Soviets. Courtesy http://www.hisutton.com.

Ivy Bells was a success level above anything US intelligence agencies had previously achieved during the Cold War, and in 1972, a far larger tap with greater storage capacity was installed by *Halibut*. The cable carried dozens of telephone signals simultaneously, on which conversations about sensitive naval operations, maintenance and defect issues with Soviet ships, and plans for submarine reconnaissance in US waters could be listened to. The tapes from the cable tap were retrieved and replaced frequently and sent to National Security Agency (NSA) headquarters, where they could be decrypted and translated – though the Soviet military brass thought the line was secure, given that many communications were sent unencrypted or only used basic cryptography. Only in the early 1980s were the Soviets alerted to the presence of the tap after Ronald Pelton, an NSA communications specialist, met with KGB agents and told them of the operation.[35]

From Morse code to high-speed broadband

After the introduction of submarine telegraph lines in the nineteenth century, the first major innovation in undersea communications was the use of a coaxial cable to facilitate telephone communications. While early trials took place in the 1930s, serious uptake of transoceanic telephone cables only came about in the 1960s and 70s. At this point, significant capacity increases had been achieved and “round-the-world” systems were installed.[36] Despite significant improvements in cable technology and increasing demand, Australia remained connected to the world via only two routes in 1969. The previous telegraph line heading west from Perth was replaced with a coaxial cable from Cairns to Guam, which provided a second link to Hawaii and the continental United States, and onward connections to Japan, China and Southeast Asia. Australia’s major routes of international connection were all located on the east coast.


LARGE CAPACITY SUBMARINE CABLE ROUTES
THE OVERSEAS TELECOMMUNICATIONS COMMISSION (AUSTRALIA) OTC
National Archives of Australia
NAA: A1200, L80038

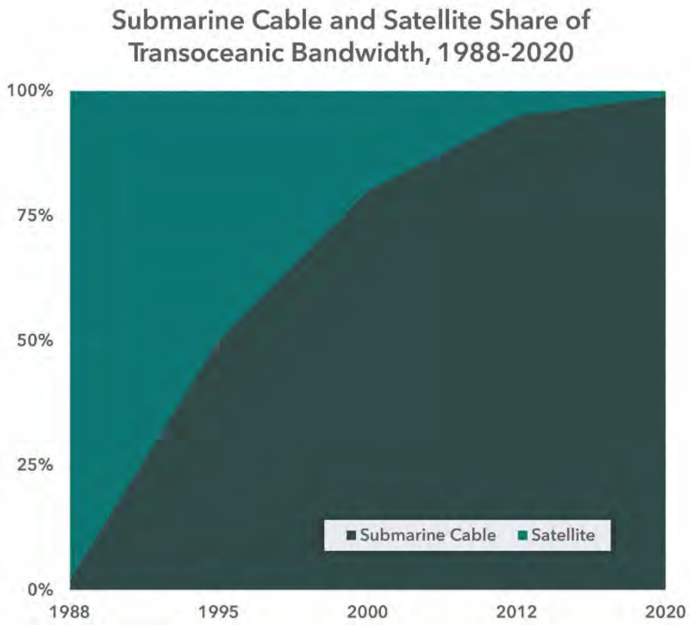
Australia’s major international cable connections in 1969. Note the concentration of connections from the east coast. NAA: A1200, L80038.

During the mid-to-late twentieth century, significant advances were also made in satellite technology. While coaxial SCCs had superior telephone service over short runs, satellites provided better quality transoceanic communication and could even transmit video and broadcast TV, which coaxial cables could not.[37] Satellite communication was the future: like the advent of radio and wireless communication between the world wars, new technology again appeared to be overtaking submarine cables in capability.

Any prospects for a satellite-dominated future, however, were dashed with the invention of fibre-optic cables. Innovations in semiconductor, laser and optical technologies meant that information could be transmitted at the speed of light along glass fibres. Compared to copper cables, fibre-optic lines could carry complex data far more efficiently. By the late 1980s, low latency, high bandwidth transmissions were possible on undersea fibre cables.[38] A similar leap forward for satellite technology never occurred, with those networks relying on comparatively iterative improvements in capacity and latency.

Submarine cables leapfrogged satellites to regain their place as the backbone of global communications: while they provided just two per cent of transoceanic bandwidth in 1988, they account for more than 99 per cent of it in 2021. Commercial interest in satellite communications has grown in recent years, as modern networks operate closer to the Earth and are "meshed", decreasing latency and increasing bandwidth.[39] Nonetheless, cables still provide significantly cheaper and more reliable communications than satellites, which have difficulty providing uninterrupted service in the event of breakdowns.

Submarine cable networks can hand off connections to more reliable lines markedly quicker when there is a cable fault, and the capacity of the global cable infrastructure still far exceeds that of satellite networks.[40]



This data is from several sources and should be taken as only indicative of the growth in cable relevance. Sources: Mandell, 2000; APEC, 2012; Bueger and Liebetrau, 2021.

Submarine cables in Australia today

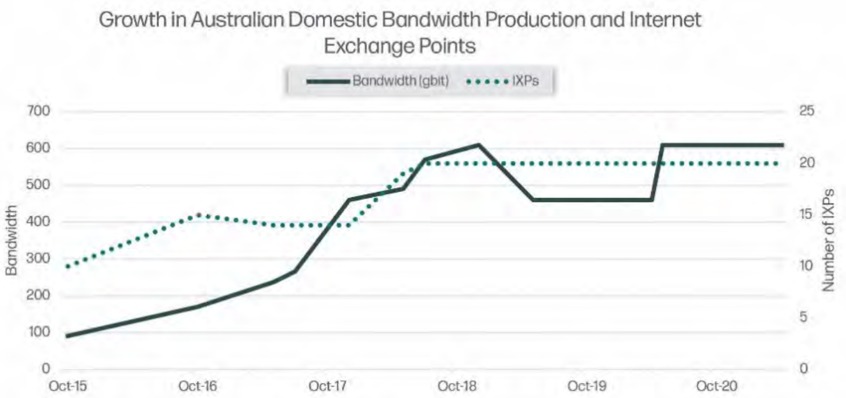
Australia's undersea fibre network

The importance of SCCs to Australia cannot be overstated. When a mobile phone in Sydney communicates with a cell tower, it does so wirelessly, but the remainder of the path data takes to reach a server in New York hosting a news story, online store or cloud computing platform is entirely physical, and mostly along the submarine cable. The connectivity SCCs provide enables Australia's participation in the global economy, which is continuing to rapidly digitise. A massive increase in the viability and uptake of mobile technologies, and the increasing potential of networked artificial intelligence, cloud computing and connected devices (the "internet of things") all rely on international connectivity.[41]

The last decade has seen unprecedented growth in Australia's domestic bandwidth production, which sextupled between 2015 and 2021. In the same period, the number of Australian internet exchange points (IXPs), where various domestic networks interconnect and often link to international cable networks, has doubled.

The desire of individuals, businesses and government for higher bandwidth and lower latency connections will only increase. APEC modelling in 2012 estimated that a 100 per cent loss in cable capacity would cost the Australian economy over three billion dollars a month, a figure that would be far higher today.[42]

Australia is currently connected to the world via thirteen international cables (see Appendix B). In a return to the telegraph age, Sydney and Perth serve as the only points where cables land.[43] While precise locations of interconnection differ within these cities, the presence of highly concentrated landing places presents a situation like that experienced during and between the world wars. This is not a case unique to Australia: Singapore, Taiwan and the UK have concentrated cable landing sites by their size and geography. Australia, however, does not have the same excuse for having a highly concentrated set of landing sites. As a point of comparison, the United States has highly distributed landing points on its east coast connecting to Asia, while most cables connecting it to Europe land in tight groups in New Jersey or New York. Attempts have been made in the US, however, to prevent the over-convergence of cable landings and links to data centres or IXPs.[44]



The chart indicates growth in bandwidth capacity supplied by IXPs. Source: Packet Clearing House, https://www.pch.net/ixp/summary_growth_by_country, last accessed 11 May 2021; includes data from archived versions accessed via archive.org.

The importance of geographically distributed landing stations

For a country with a coastline as significant as Australia's, a wider distribution of cable landing points has distinct advantages. The concentration of international connection points allows for a single event to cause catastrophic damage to various cable systems simultaneously, rather than only affecting a single or few cables that have been spread broadly along the coastline. Australian Communications and Media Authority (ACMA) maps indicate that four cables landing in Sydney's north arrive within a 2.5-kilometre stretch of Narrabeen Beach. Similarly, four cables in southern Sydney land in the 3 kilometres between Bondi and Clovelly beaches. Just a few kilometres offshore, these sets of cables converge even further, to within one nautical mile, before diverging (see Appendix A for reproductions of these maps).[45]

It should be noted that ACMA data regarding current undersea infrastructure is very limited, and the maps it supplies are at least ten years out of date. Additional cables have since been installed and are not indicated, making it difficult for up-to-date analysis to be made.

Threats to SCCs

Natural disasters and undersea phenomena

Earthquakes, tsunamis and storms can cause significant damage to undersea cables, and though Australia does not experience frequent serious earthquakes, there remains a cause for concern. It would only take one major disaster occurring close to Sydney to decimate Australia's international connectivity. The 1929 Grand Banks earthquake off Newfoundland broke twelve transatlantic cables and significantly affected telegraph communications.[46] Improved technology has not made subsea networks any more immune to acts of nature. A series of earthquakes in the Luzon Strait near Taiwan in 2006 broke seven cable systems in nineteen places. It took eleven cable repair ships 49 days to rectify all faults, and network disruptions remained for two months. Banking and booking systems, financial markets and general trade were all severely affected.[47] These events caused significant damage to the entirety of Canada's and Taiwan's connectivity because of the proximity of cables to one another. If they had been significantly distributed, damage resulting from earthquakes would have been minimised. Other important and more regular causes of cable breaks include underwater landslides, currents forcing cables against rough surfaces, and even shark bites, though these have less potential to affect multiple systems.[48]

Damage resulting from human activity

Many international cable faults are the result of misplaced anchors or fishing activity from trawlers and fixed nets. Estimates of human impact on cable infrastructure range from 40 to 70 per cent of total damage.[49] In 2008, a five-ton anchor abandoned in the Persian Gulf resulted in major outages in the Middle East and Asia after it severed FLAG Telecom's FALCON cable.[50] Where cables are bunched together close to shore at a concentrated landing point, the potential for a single vessel to cause significant damage to multiple systems, even accidentally, is amplified.

Malicious attack

In addition to the potential for natural disasters, undersea phenomena, fishing and dredging to damaged cables, concentrated landing sites make the entire network more vulnerable to a malicious attack. An adversary has fewer targets to consider, and even if only one is targeted the damage will still be significant if an attack is successful, given multiple systems will be affected. This is especially true of physical attacks on terrestrial cable infrastructure, such as locations where several cables come ashore in the same place or terminate at one data centre or IXP. The redundant capacity of having many cable connections is again undermined by their proximity to one another. Isolated attacks like the First World War raids on Direction and Fanning Islands have the potential to knock out a massive portion of Australia's international bandwidth.

The physical domain is also no longer the only route of attack for networked infrastructure. Weak security protocols and network management systems that are not up to date provide fertile ground for cyberattacks.[51] Contemporary adversaries can coordinate multiple operations across domains to far greater effect than German cruisers in the First World War. Even non-state actors are highly capable: the 1998 attacks on US embassies in Nairobi and Dar es Salaam occurred within ten minutes of one another.[52] As landing site diversity decreases, the potential for one attack to have a significant effect on the entirety of a country's cable system increases.

Is a malicious attack a realistic threat to SCCs?

While there was a lull in concern for submarine cable infrastructure after the Cold War, likely due to the overwhelming US naval and military presence globally, increasingly sophisticated terrorist threats and renewed perceptions of Russian and Chinese naval hostility have given rise to renewed interest in the security of SCCs.[53] In one instance, writing in *Foreign Affairs* in 2015, Robert Martinage argued that the proliferation of remotely operated underwater vehicles meant that it would be possible for a terrorist group to interfere with cables at will.[54] Importantly, Bueger and Liebetrau find that "no intentional hostile disruptions to the [modern] submarine cable infrastructure have been reported publicly". They argue that hypothetical scenarios about interference or attack are based on "overall assessments of the geopolitical landscape", rather than a solid base of historical evidence, indicating the potential for "threat inflation".[55] Rishi Sunak's 2017 Policy Exchange paper on "Indispensable, insecure" SCCs dedicates an entire chapter to "The Risk from Russia", despite a lack of any evidence that Russia had interfered with undersea cables; rather, the policy document focuses on Russian naval investment and "aggressive" operations happening close to cable routes.[56]

Russian Navy oceanographic ship Yantar reported operating near SCC routes. Yoruk Isik, 2016.

Why has landing site diversification not happened?

Developing the large telecommunications estates required for international connectivity from the ground up is an expensive affair. New data centre construction and equipment purchases present significant costs and barriers to entry for the sector, given these facilities should be highly secure and protected against natural disasters. Ongoing costs include massive power consumption and finding qualified technical staff.

Lack of demand for international connection points outside of major cities means that telecommunications companies are not interested in investing in cable links from regional areas of the coastline. In Australia, this has resulted in a problematic externality: the concentration of landing points in Sydney and Perth.

Potential for broader distribution of landing sites

There are plans for new Australian-linked cables to be distributed away from Perth and Sydney. The Northern Territory government has announced its intention to aid in the construction of significant data centre and telecommunications infrastructure around Darwin. Fibre-optic links to Dili, Singapore and Kupang in Indonesia are planned.[57] Additionally, Project Koete is a private initiative that will lay cable in the Timor Sea from Darwin to Jakarta, Singapore and Kuantan in Malaysia, via Broome, Port Hedland, Dampier and Exmouth, providing new direct links to archipelagic and mainland Asia.[58] These projects mark an important departure from Sydney and Perth as Australia's only significant points of international connection. Darwin's location on Australia's northern approaches, however, presents new issues given this region's consistent identification as the most likely vector for a military threat to Australia.[59] Australia would benefit from additional cable projects that are situated in the north of Western Australia or Queensland, where telegraph and coaxial cables were connected in the nineteenth and twentieth centuries.

Geopolitical concerns for new projects

The private sector and states sponsoring cable projects are increasingly concerned with the safety of their cable routes. Areas like the South China Sea and the maritime approaches to Hong Kong are now considered to pose a higher risk for transiting cables. New systems traversing the Arctic Sea have been enabled by diminishing ice caps: these cables will avoid existing chokepoints and make the journey from Asia to Europe without having to cross the Americas (this is also a far shorter route). The Arctic Connect cable will potentially link Scandinavia, Russia, China and Japan in the coming years.[60] In 2013, following revelations of US global surveillance programs, the BRICS countries (Brazil, Russia, India, China and South Africa) began planning for a global cable system that would avoid US access and influence. Funding issues and a lack of cohesion among the states involved, however, meant that the project was never completed.[61]

Military reliance upon SCCs

SCCs are essential for secure military communications. While highly secure military satellites do supply some degree of connectivity, C4 systems often rely heavily on bandwidth leased from SCCs or provided by private military cables. Even accidental damage can severely curtail military operations: in 2008, a cable break in the Mediterranean forced the number of drone sorties flying from the US airbase in Balad, Iraq, to decrease from hundreds to tens per day.[62] SCCs' cheap bandwidth and light-speed latency provide the only means of operating large amounts of remote equipment across continents.

Between 2012 and 2014, USNS *Zeus*, the only operating US military cable ship, was tasked with laying a $40-million fibre cable between Miami and the US military base in Guantanamo Bay, Cuba, to provide a more reliable link with the continental US.[63]

USNS Zeus. *National Steel and Shipbuilding, 1983*

Other states are considering the procurement of specialised navy vessels built to protect submarine infrastructure, along with investing in alternative defence communications systems. The UK's March 2021 Defence Command Paper commits to building a "Multi-Role Ocean Surveillance" ship which would use a variety of sensors and submarine drones to detect activity directed at submarine cables. Additionally, the UK military plans to develop a sovereign satellite Intelligence, Surveillance and Reconnaissance (ISR) capability and a "digital backbone" in space.[64] The continued digitisation of the Australian Defence Force's (ADF) C4 systems has meant Australia's military has often enjoyed decision superiority alongside allied military forces during recent conflicts.[65] SCCs sits at the nexus between the physical and intangible infrastructure essential for this digitisation and will remain essential for a highly connected defence force.

Protections in place at the private sector level

The businesses that own undersea cables are responsible for planning, building and maintaining their systems, and these services are almost always contracted out to a company specialising in them under a marine maintenance contract. Cable companies operate constant surveillance of their cables from Network Operations Centres. In the event of a fault, modern systems make it far easier to diagnose the type and location of damage than in the past. Engineers use Network Management Systems to detect and locate faults by observing an interruption to service or monitoring the actual cable characteristics, such as information from signal repeaters. Data is quickly rerouted to other working cables that the operator has a mutual restoration agreement with, or on which they have purchased additional capacity for maintenance scenarios.[66] Once the approximate location of a fault is determined, a nearby cable repair ship (not all cable vessels can perform repairs) will be dispatched. Depending on whether the fault is in a lightweight or heavily armoured section of cable, different repair techniques are employed.[67]

With few exceptions, the submarine cables connecting Australia to the world are all privately owned and operated. Operators range from dedicated SCC businesses that rent capacity to other businesses, to consortiums of telecommunications companies and big tech firms, which are increasingly building their infrastructure to lower costs.[68] The global undersea network has become far more diverse in its ownership when compared to the situation a century ago when the British government and Cable and Wireless dominated global communications. Motivated by profit, SCC operators have minimal incentive to dedicate resources to the security and stability of the entire cable system, and their willingness to pay for mitigation efforts is restricted by their expected losses from network disruption.[69] Because of this, governments have been required to step up, providing regulatory guidance and introducing legislation to protect SCC infrastructure critical to the economy and national security.

Legislative and regulatory protections in Australia

Responding to attacks on marine infrastructure

The Guide to Australian Maritime Security Arrangements (GAMSA) indicates the relative responsibilities among government agencies to uphold maritime security in Australia. Under the GAMSA, Maritime Border Command (MBC) is responsible for protecting and responding to attacks on fixed maritime infrastructure, which includes SCCs, drilling platforms, pipelines and ports. MBC is an interagency task force composed of Australian Border Force (ABF) and ADF personnel. The GAMSA does not provide provisions to secure cable landing sites or manholes on land. MBC is commanded by an ADF officer who is also a sworn ABF officer, enabling the use of assets from both organisations.[70]

The GAMSA is concerned with maritime terrorism as the major threat to critical infrastructure, in addition to other illegal activities like piracy and robbery at sea. Attacks on critical infrastructure, however, may come from actors other than unaffiliated terrorist organisations. State-sponsored actors engaging in "grey-zone" activity use actions short of war to pressure that state's adversaries. Due consideration must be given to formulating a response to the malicious attack that considers the type and motive of the actor, and which is based on intelligence about their potential state-backing.

Cable protection zones

The *Telecommunications Act 1997* designates undersea cables and landing sites as critical communications infrastructure, affording their security special consideration by national security and defence agencies. Within Australian waters, the Australian Communications and Media Authority is authorised to designate cable protection zones that limit certain activities recognised as presenting a threat to the integrity of cable systems. The scheme is primarily orientated towards protecting cables from accidental damage by fishing or dredging vessels. Under the GAMSA, state and territory governments are designated as the lead agencies responding to illegal activity in protected areas within Australia's territorial seas, with additional support to be provided by their police forces, the Australian Federal Police (AFP), MBC, ABF and Department of Defence as required.[71]

In a 2010 submission to ACMA, the AFP reported that it was "not equipped with the resources to monitor the protection of [Australian] cables" and relies on other Commonwealth authorities like fisheries management and maritime safety authorities for surveillance and monitoring functions.[72] While cable protection zones have likely prevented damage to some extent, they are unlikely to prevent the majority of faults, given they rely on ships to be aware of them rather than presenting a physical barrier or constant surveillance of potential threats.

Recommendations

1. **A study should be undertaken by the Defence, Science and Technology Group, and/or other relevant communications sections of Defence, to determine the reliance of Defence's APS and ADF capabilities on SCCs.** SCCs are essential to Defence's operations and secure communications within the region and globally. Depending on the outcomes of this study, investigations into alternative or redundant technologies should be undertaken to ascertain the viability and costs of additional wireless and satellite communication capabilities.

2. **Government should take advantage of new private cable projects to encourage the further distribution of cable landing sites**. For cables initially proposed to land only in Sydney or Perth, the potential for additional or alternative landing sites should be considered – for a cable landing in Sydney, potential extensions to Melbourne, Newcastle, Brisbane or Cairns could provide significantly increased geographic diversity for the SCC network. Additional landing site proposals should consider local demand for international connectivity to avoid overbuilding while keeping in mind that broadening infrastructure along the coast is the primary objective. For extensions that may be less profitable, subsidies might be considered. Care should be taken to ensure that cables diverge towards different landing points at a significant distance from the shore, preventing damage to more than one connection due to an adverse natural or man-made event.

3. **Defence, the Department of Home Affairs (including MBC), the AFP and Australia's national intelligence community should collaborate on forming a response plan to any hostile action against critical undersea infrastructure and cable landing sites.** While malicious attacks on Australia's submarine cable network have not occurred since the First World War, the importance of this critical infrastructure to Australia as an island state is not lost on its adversaries. A response plan should include various protective measures to respond to varying threat levels. These measures would range from actionable intelligence regarding a potential terrorist or grey-zone actor seeking to damage cables, to the threat posed by enemy states to SCCs during a war.

4. **Regular patrols around SCC protection zones should be conducted by agencies with adequate capabilities to ensure compliance and prevent cable damage**. Australia's cable protection zones play a necessary but insufficient role in protecting SCCs.

Their passive ability to protect SCCs from fishing and dredging vessels can only be achieved when ships are aware of their responsibilities in protection zones. This could be achieved by coordinating MBC, ABF and potentially Defence assets through state and territory governments in line with the GAMSA.

5. **ACMA should increase the availability of current data for precise submarine cable routes around Australia.** Given this has been done previously there is precedent for it to continue, preferably yearly. The significant costs of obtaining accurate coordinate data from private firms that have a monopoly on its supply, and charge thousands of dollars to obtain it, present barriers to further academic study of Australia's SCCs. The fact that private businesses have precise cable route data obviates any potential security concerns preventing ACMA or other government agencies from supplying it to the public free of charge.

Conclusion

The first telegraph cable laid across the English Channel in 1851 heralded a revolution in human communication, the ramifications of which the world is still dealing with today. SCC infrastructure has seen significant technological changes since the rapid spread of telegraph routes girdled the Earth in the late 1800s, preceding the even faster growth of telephone and fibre systems into the twenty-first century. The objective of this report was to provide an account of Australia's historical engagement with submarine cables and seek to understand the contemporary issues around their security both in an increasingly digitised world and within a region facing an uncertain strategic future. The implications of SCCs' increasing importance for Australia's security and the Department of Defence are significant.

Beginning with a brief account of the invention and early adoption of SCCs in the nineteenth century, the ramifications of near-instantaneous communication on a previously disparate British Empire were observed. SCCs quickly became essential to the British for maintaining a firm grasp on their territories around the world, and contemporaneous reporting from government and media was considered to support this thesis. The report then moved to an examination of evidence around German action towards Pacific and Indian Ocean cable stations in the First World War, coming to the important conclusion that Australia's highly limited points of an international connection made the country vulnerable to being entirely cut off from communications with the UK and the rest of the world. Considering the lack of growth in the geographic distribution of cables in the interwar period, the Second World War and the mid-twentieth century, similar conclusions were reached. Two clandestine cable-cutting and tapping operations were examined, and their effects demonstrated the importance of SCCs in the military domain. While early wireless communication techniques were compared to SCCs and found to be severely lacking, satellite capabilities greatly improved wireless communications from the mid-twentieth century and briefly overtook SCCs as the primary means of communication across oceans. Innovation in computing technology in the 1980s, however, provided new momentum for SCCs and renewed their importance for global communications, as fibre-optic cables were able to transmit far more data than satellites, and at a much faster rate.

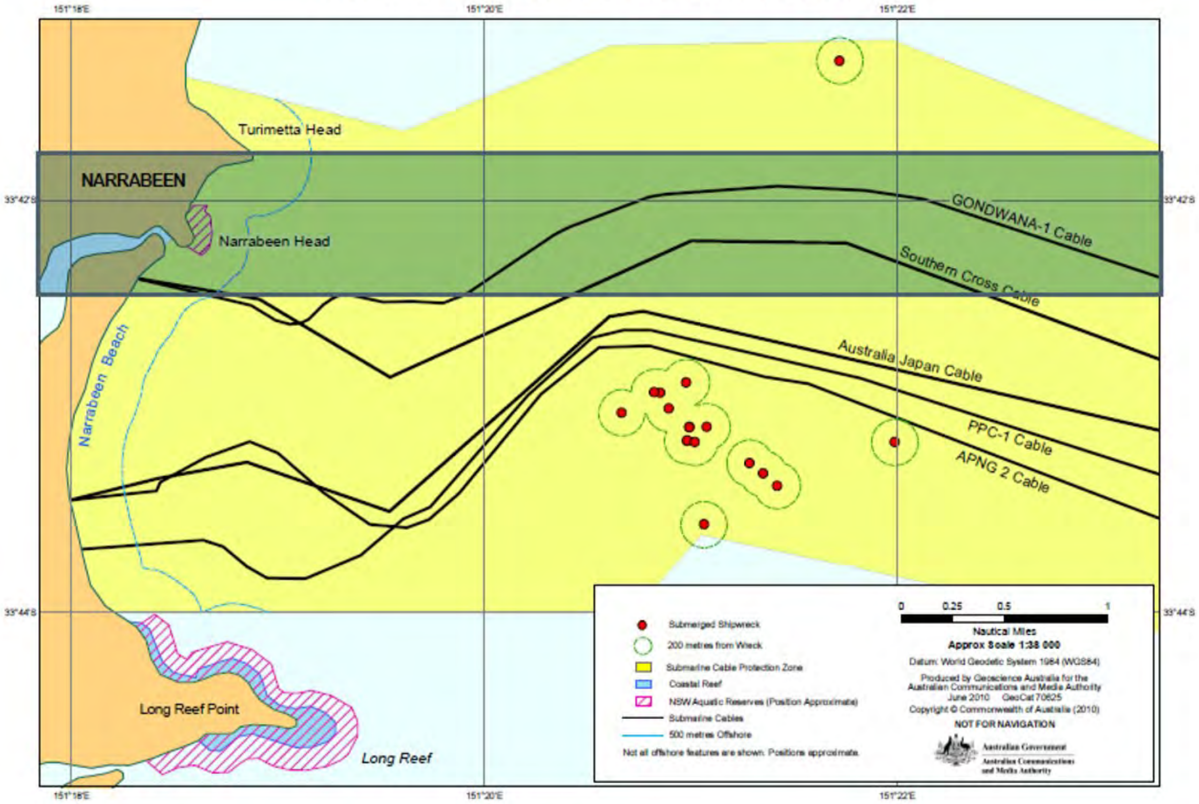
Turning to the contemporary situation, Australia's current international SCC network was described, and the continued lack of geographic distribution of landing points was evidenced. Considering this primary concern, various threats to SCC system integrity were examined. Evidence of the potential for natural disasters to wreak havoc on several cable systems simultaneously was considered, and despite the low likelihood of earthquake and tsunami events in Australia, this was found to be concerning nonetheless, given the country's lack of landing station diversity. Accidental damage caused by fishing and dredging activity and malicious attack by terrorist groups and grey-zone actors to SCC infrastructure were identified as having the potential to affect multiple systems given the concentration of landing points in Australia. While the potential for threat inflation was identified, this report still considered malicious damage to SCCs a concern for Australia. The lack of geographic diversity in SCC landing points was deemed to have resulted from a lack of demand and the high costs associated with building large telecommunications estates. The potential for further growth away from Sydney and Perth, however, was examined and found to be promising, with the caveat that new systems installed on Australia's northern approaches would be more vulnerable to any that were established further south. Subsequently, the protections put in place by the private sector to protect cables were examined, and the increasingly diverse ownership of cable systems was considered. Finally, the legislative and regulatory protections put in place by the Australian government to protect the undersea communications infrastructure were observed and found to be somewhat wanting.

The security of SCCs is essential to protect ADF capabilities and sensitive information. Despite decreasing anxiety about SCC security after the Cold War, increased terrorist activity and growing interstate tensions have resulted in a renewal of concerns about the potential for SCC interference. The ADF and allied defence forces continue to increase their reliance upon SCC infrastructure as their capabilities become increasingly digitised and networked, demanding far greater amounts of data to be transmitted far more quickly.

Appendices

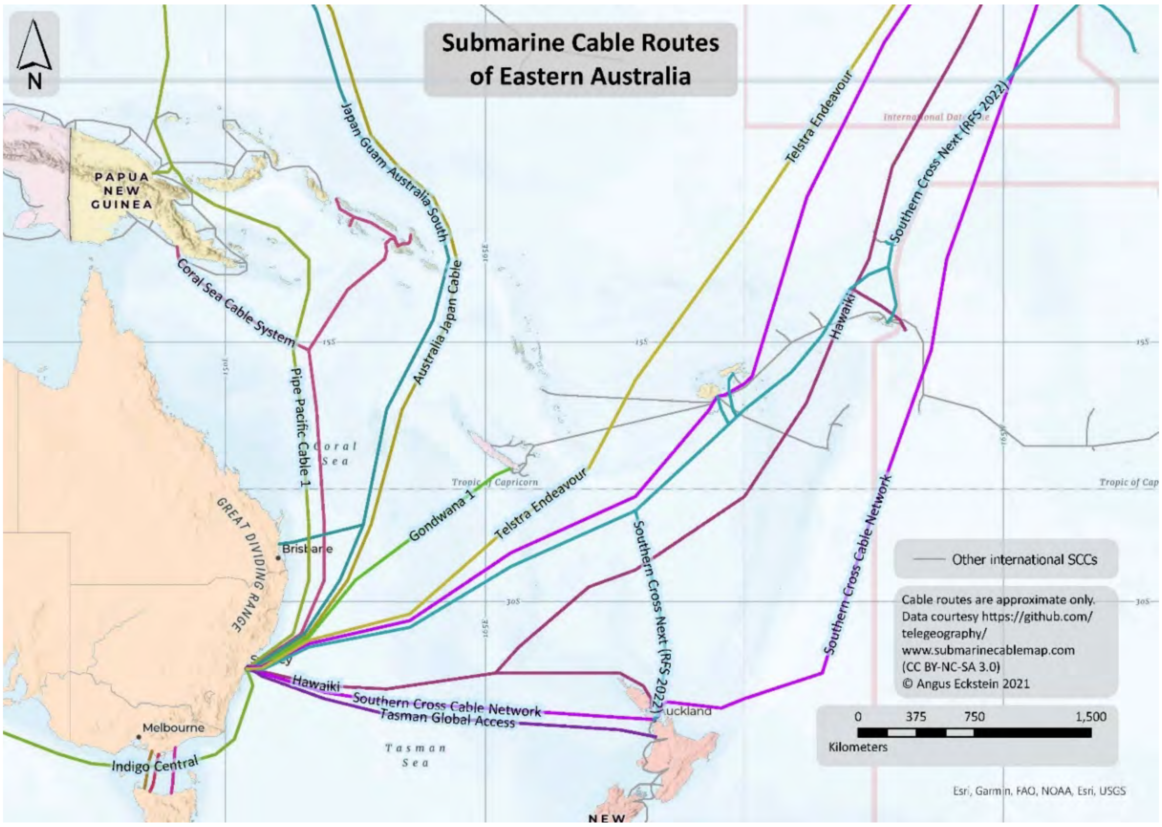
Appendix A: ACMA-designated cable protection zones

Northern Protection Zone - Inshore Detail



ROYAL AUSTRALIAN NAVY
SEA POWER
SOUNDINGS

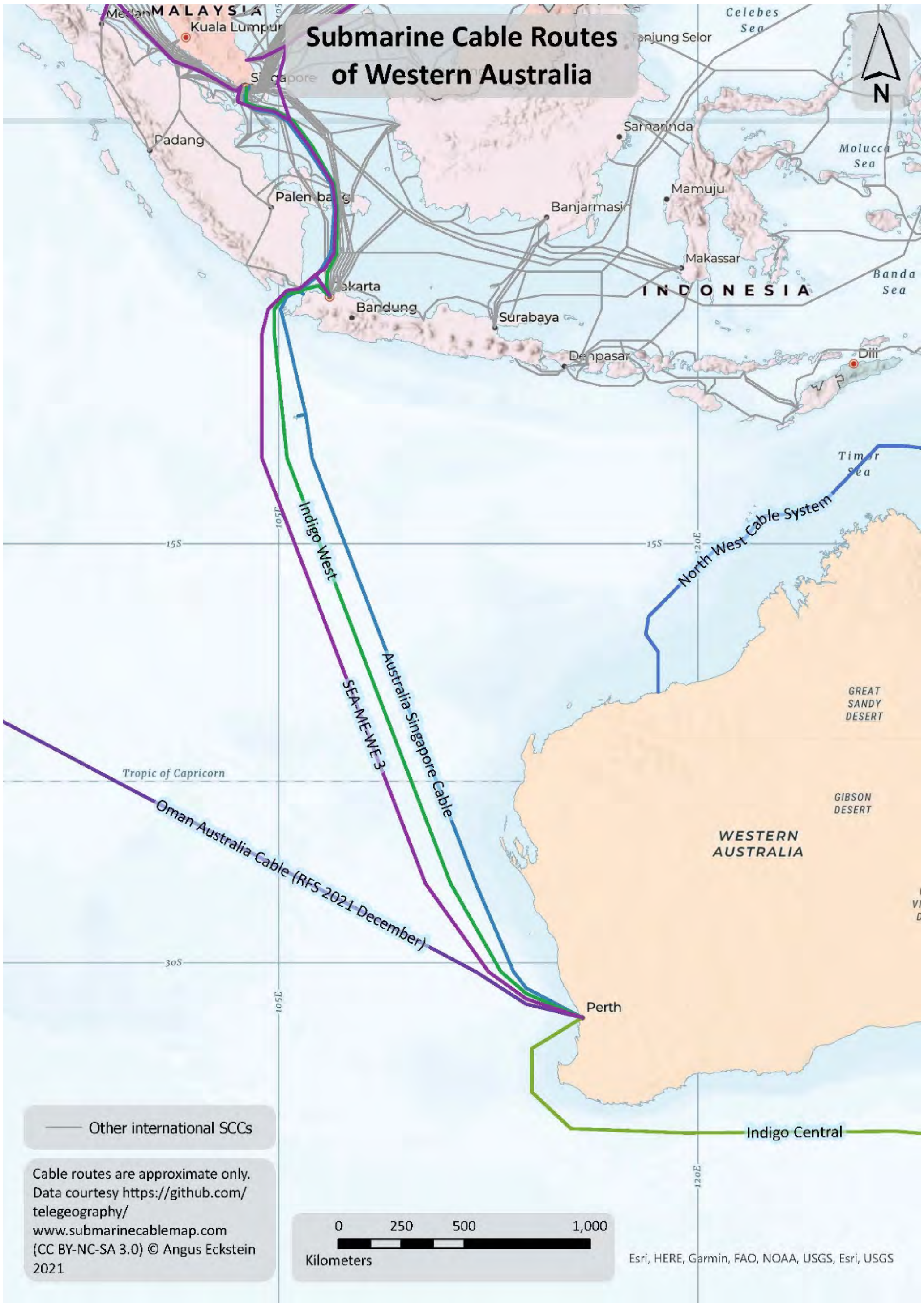
Appendix B: Australia’s SCC connections as of May 2021



Cable routes are approximate only. Data courtesy https://github.com/telegeography/www.submarinecablemap.com (CC BY-NC-SA 3.0)
© Angus Eckstein 2021

Esri, Garmin, FAO, NOAA, Esri, USGS

Appendix C: Australia's SCC connections as of May 2021



Cable routes are approximate only. Data courtesy https://github.com/telegeography/www.submarinecablemap.com (CC BY-NC-SA 3.0) © Angus Eckstein 2021

Esri, HERE, Garmin, FAO, NOAA, USGS, Esri, USGS

Endnotes

[1] Gérard Fourchard, “Historical Overview of Submarine Communication Systems”, in *Undersea Fiber Communication Systems*, ed. Jose Chesnoy (San Diego: Elsevier, 2015), 23, https://doi.org/10.1016/C2015–0-00778-X.

[2] Helen Godfrey, *Submarine Telegraphy and the Hunt for Gutta Percha* (Leiden: Brill, 2018), 18–19.

[3] Charles Bright, *The Story of the Atlantic Cable* (New York: D. Appleton and Co., 1903), 146–51.

[4] Ibid., 204–7.

[5] Frank Clune, *Overland Telegraph: An Epic Feat of Endurance and Courage* (Sydney: Angus and Robertson, 1955), 11; Simon Moorhead, “Alice Springs Telecommunications Facilities”, *Australian Journal of Telecommunications and the Digital Economy* 5, no. 4 (December 2017), 63, https://doi.org/10.18080/AJTDE.V5N4.132.

[6] Owen Peake, *Broome to Java Submarine Telegraph Cable* (Barton: Engineers Australia, 2006), https://web.archive.org/web/20210323073004/https://portal.engineersaustralia.org.au/system/files/engineering-heritage-australia/nomination-title/Broome_Java_Nomination_Ceremony_Report.pdf.

[7] P. M. Kennedy, “Imperial Cable Communications and Strategy, 1870–1914”, *The English Historical Review* 86, no. 341 (October 1971), 731, https://www.jstor.org/stable/563928; Daniel R. Headrick and Pascal Griset, “Submarine Telegraph Cables: Business and Politics, 1838–1939”, *Business History Review* 75, no. 3 (Autumn 2001), 547, https://www.jstor.org/stable/3116386.

[8] “The Telegraph Submarine Cable Question”, *Daily Citizen*, Ottawa, 12/21 April 1880, 2–3, https://www.canadiana.ca/view/oocihm.25129/.

[9] Ibid., 7–8.

[10] George Johnson, *The All Red Line: The Annals and Aims of the Pacific Cable Project* (Ottawa: James Hope & Sons, 1903), 9.

[11] George Johnson, “Addendum: Interview with Sir Sandford Fleming on the Completion of the Trans-Pacific Cable”, in Johnson, *The All Red Line*, 442–43.

[12] Telegram from Acting Secretary of State to Ambassador (to the UK) W. H. Pope, 26 September 1914. “Censorship of Telegrams Transmitted by Cable and Wireless”, *The American Journal of International Law* 9, no. 3 (June 1915), 276, https://doi.org/10.2307/2212253.

[13] Ibid, 307. Memorandum from the British Foreign Office telegraphed by Ambassador W. H. Page to the Secretary of State, 10 March 1915.

[14] The National Archive (UK): Committee of Imperial Defence; CAB 38/19/56, Photographic Copies of Minutes and Memoranda, “Report of the Standing Sub-Committee. Submarine Cable Communications in Time of War”, 11 December 1911, https://discovery.nationalarchives.gov.uk/details/r/C6172902.

[15] Edwin P. Hoyt, *The Last Cruise of the Emden* (London: Andre Deutsch, 1967), 144–46.

[16] State Library of NSW: Eastern Extension Telegraph Company Ltd., MLMSS 9772, telegram sent by superintendent Darcy Farrant to the Sydney office of the Eastern Extension Telegraph Company, 11 November 1914, http://archival.sl.nsw.gov.au/Details/archive/110575670.

[17] National Archives of Australia: Pacific Cable Board, A2911, General correspondence files, two and three number system with year suffix, 1909–16, 1583/1914, “Copy of cablegram received from the manager in the Pacific”, 23 September 1914.

[18] Paul G. Halpern, *A Naval History of World War I* (London: UCL Press, 1994), 88; “German Tars Seize British Cable Station: Land on Fanning Island in the Pacific and Cut Line to Australia”, *The New York Times*,

15 September 1914, 1; Lynne McDonald, “Cable stations”, *Griffith Review* 43 (2014), https://www.griffithreview.com/articles/cable-stations/.

[19] National Archives of Australia: Pacific Cable Board, A2911, General correspondence files, two and three number systemwith year suffix, 1909–16; 1583/1914, “Copies of cablegrams received from the manager in the Pacific”, 29 October 1914.

[20] National Archives of Australia: Pacific Cable Board, A2911, General correspondence files, two and three number systemwith year suffix, 1909–16; 1583/1914, “Pacific Cable”, September 10, 1914; “British Cable Repaired: Fanning Island Station, Destroyed by Germans, Again in Order”, *The New York Times*, 6 November 1914, 4.

[21] National Archives of Australia: Government House, A2, Correspondence files, annual single number series, 1895–1926; 1915/3948, documents relating to Pacific Islands Cable Stations, “De-cypher of cablegram from Governor New Zealand, dated Wellington, 8th September, 1914, 11.50. a.m.”; and cablegram sent by Malcom Lindsay Shepherd, secretary of the Prime Minister’s Department, to the Governor of New Zealand, 9 September 1914.

[22] National Archives of Australia: Prime Minister’s Department, A2, Correspondence files, annual single number series 1895–1926; 1915/3948, documents relating to Pacific Islands Cable Stations, letter or cable sent from Niel Nielson to William Holman, Premier of NSW, and forwarded to the Prime Minister’s office, 27 October 1914.

[23] Australian War Memorial: Defence of Bases Committee, AWM 54, Written records, 1939–45 War, 1926–92; 243/1/4, [Defence Schemes – General:] Defence Plan for South Africa, The Gulf of Aden, Faroe Island and Fanning Island, Oct 1943, “Fanning Island”, 8 April 1945; Australian War Memorial: Oversea[s] Defence Committee, AWM 124, Naval historical collection, 1788–1987; 1/34, CID. Overseas Defence Committee, “Protection of Cable Landing Places at St. Helena, Rodrigues and Direction Island”, 11 November 1912.

[24] Australian War Memorial: Department of Defence, AWM 54, Written records, 1939–45 War, 1926–92; 425/12/7, [Inter-Communication – Cables:] Department of Defence, Military Board, CGS Branch, Military Intelligence: Foreign Communications News, “The British Cable System”, 12 July 1940.

[25] Russell W. Burns, *Communications: An International History of the Formative Years* (Stevenage: The Institution of Engineering and Technology, 2004), 324, 430–31.

[26] Barrie Kent, *Signal! A History of Signalling in the Royal Navy* (Clanfield, UK: Hyden House, 1993), 73.

[27] Motohiro Tsuchiya, “Submarine Cables and International Relations”, Japan Institute of International Affairs, 20 October 2020, https://www.jiia.or.jp/en/column/2020/10/research-reports-economy-security-linkages02.html.

[28] Nigel West, *GCHQ: The Secret Wireless War* (London: Weidenfeld and Nicholson, 1986), 6, 143–44.

[29] Australian War Memorial, AWM 124 1/34. “Protection of Cable Landing Places at St. Helena, Rodrigues and Direction Island”, 11 November 1912.

[30] National Archives of Australia: Department of Defence, A5954, “The Shedden Collection” [Records collected by Sir Frederick Shedden during his career with the Department of Defence and in researching the history of Australian Defence Policy], two number series, 1901–71; 1713/25, Cable Landing Places at Fanning Island – western Pacific – Protection of, report by J. E. Clauson, “Protection of Cable Landing Place at Fanning Island”, 5 August 1904; National Archives of Australia: Prime Minister’s Office, A2, Correspondence files, annual single number series, 1895–1926; 1915/3948, documents relating to Pacific Islands Cable Stations, “Copy of telegram from Admiralty to Navy Office”, 15 July 1915.

[31] Max Shean, *Corvette and Submarine* (Claremont, WA: published by the author, 1992), 236–37. XE-4 was of the updated XE-class of midget submarines that superseded the X-class, which had already showed great value during their participation in the sinking of the massive German battleship *Tirpitz* in 1944.

[32] Ibid., 245–47; “Operation ‘SABRE’”, Naval Historical Papers, produced 195W9–60, AWM 124 2/1; “H. M. S. Bonaventure”, Royal Navy Research Archive, last modified 16 June 2020, http://www.royalnavyresearcharchive.org.uk/BPF-EIF/Ships/BONAVENTURE.htm.

[33] *United Nations Convention on the Law of the Sea*, Montego Bay, Jamaica, 10 December 1982, United Nations Treaty Series, § 113; in addition to UNCLOS, which applies on the high seas, domestic regimes like the *Submarine Cables and Pipelines Protection Act 1963* and the *Telecommunications Act 1997* apply.

[34] Sherry Sontag and Christopher Drew, *Blind Man's Bluff* (London: Arrow, 2000), 158–59, 167.

[35] Steven Aftergood, "Soviet Spy Ronald W. Pelton to Be Released from Prison", Federation of American Scientists, 23 November 2015, https://fas.org/blogs/secrecy/2015/11/pelton-release/.

[36] Gérard Fourchard, "Historical Overview of Submarine Communication Systems", in *Undersea Fiber Communication Systems*, ed. Jose Chesnoy (San Diego: Elsevier, 2015), 34–37.

[37] Ibid., 39–40.

[38] *Economic Impact of Submarine Cable Disruptions* (Singapore: APEC Policy Support Unit, 2012), 6, https://www.apec.org/Publications/2013/02/Economic-Impact-of-Submarine-Cable-Disruptions.

[39] Mattias Fridström, "The Carrier Guide to 2021: Traffic, Technology and Unsung Heroes", *Submarine Telecoms Magazine* 116 (January 2021): 17, https://subtelforum.com/subtel-forum-magazine-116-global-outlook-out-now/.

[40] *Economic Impact of Submarine Cable Disruptions*, 6–7.

[41] Rowena Barrett and Sara Bennett, *Digital Economy: Our Perspective*, working paper (Brisbane: Centre for the Digital Economy, 2015), 7, https://research.qut.edu.au/cde/wp-content/uploads/sites/279/2021/03/Digital-Economy-our-perspective-by-Rowena-Barrett-Sara-Bennett.pdf.

[42] *Economic Impact of Submarine Cable Disruptions*, 42.

[43] The one exception being the Japan–Guam–Australia cable's extra connection point in Maroochydore. Submarine Telecoms Forum, "Japan–Guam–Australia South", *Submarine Cable Almanac* 37 (February 2021), 244, https://subtelforum.com/products/submarine-cable-almanac/.

[44] Patrick Faidherbe, Laurent Campagne, Georges Krebs and Jean DeVos, "Submarine Cable Hubs around the World", *Submarine Telecoms Forum Magazine* 116 (January 2021): 59–61.

[45] Australian Communications and Media Authority, "Zone to Protect Sydney Submarine Cables", 7 October 2020, https://www.acma.gov.au/zone-protect-sydney-submarine-cables.

[46] I. V. Fine et al., "The Grand Banks Landslide-Generated Tsunami of November 18, 1929: Preliminary Analysis And Numerical Modelling", *Marine Geology* 215 (2005): 46, https://doi.org/10.1016/j.margeo.2004.11.007.

[47] *Economic Impact of Submarine Cable Disruptions*, 18, 27.

[48] UltraMap, "The Biggest Threat to Subsea Cables", 3 September 2020, https://ultra-map.org/the-biggest-threat-to-subsea-cables/.

[49] Ibid.; Christian Bueger and Tobias Liebetrau, "Protecting Hidden Infrastructure: The Security Politics of the Global Submarine Data Cable Network", *Contemporary Security Policy* (March 2021): 6, http://doi.org/10.1080/13523260.2021.1907129.

[50] Katarina Kratovac, "Ship's Anchor Caused Cut in Internet Cable", *NBC News*, 9 February 2008, https://www.nbcnews.com/id/wbna23068571.

[51] Garret Hinck, "Cutting the Cord: The Legal Regime Protecting Undersea Cables", *Lawfare*, 21 November 2017, https://www.lawfareblog.com/cutting-cord-legal-regime-protecting-undersea-cables.

[52] US State Department, "U.S. Embassy Bombings", 16 November 2006, archived at archive.org, https://web.archive.org/web/20070805035833/http://usinfo.state.gov/is/international_security/terrorism/embassy_bombings.html.

[53] Bueger and Liebetrau, "Protecting Hidden Infrastructure", 5.

[54] Robert Martinage, "Under the Sea: The Vulnerability of the Commons", *Foreign Affairs* 94, no. 1 (January/February 2015): 121, https://www.jstor.org/stable/24483224.

[55] Bueger and Liebetrau, "Protecting Hidden Infrastructure", 5–6.

[56] Rishi Sunak, "Undersea Cables: Indispensable, Insecure" (London: Policy Exchange, 2017), 28–33, https://policyexchange.org.uk/publication/undersea-cables-indispensable-insecure/.

[57] Gill Savage, "Northern Territory's Digital Infrastructure Plans Face Big Challenges", *The Strategist*, 15 March 2021, https://www.aspistrategist.org.au/northern-territorys-digital-infrastructure-plans-face-big-challenges; Department of the Chief Minister and Cabinet, "Terabit Territory", 18 May 2020, https://cmc.nt.gov.au/advancing-industry/terabit-territory.

[58] Submarine Telecoms Forum, "Project Koete", *Submarine Cable Almanac* 37 (February 2021): 43; Fibre Expressway, "Project Koete", last accessed 14 May 2021, https://www.fibreexpressway.com/index.html#map.

[59] *2016 Defence White Paper* (Canberra: Department of Defence, 2016), 33, http://www.defence.gov.au/whitepaper/docs/2016-defence-white-paper.pdf.

[60] *Economic Impact of Submarine Cable Disruptions*, 16; Submarine Cable Networks, "Arctic Connect", last accessed 17 May 2021, https://www.submarinenetworks.com/en/systems/asia-europe-africa/arctic-connect.

[61] Stacia Lee, "International Reactions to U.S. Cybersecurity Policy: The BRICS Undersea Cable", Henry M. Jackson School of International Studies, 8 January 2016, https://jsis.washington.edu/news/reactions-u-s-cybersecurity-policy-bric-undersea-cable/.

[62] Michael Sechrist, *Cyberspace in Deep Water* (Cambridge, MA: Harvard Kennedy School, 2010), 10, https://www.belfercenter.org/publication/cyberspace-deep-water-protecting-undersea-communications-cables-creating-international.

[63] Carol Rosenberg, "Navy Plans $40 Million Fiber-Optic Link to Guantánamo Base", *Miami Herald*, updated 20 August 2014, https://www.miamiherald.com/news/nation-world/world/americas/guantanamo/article1941012.html.

[64] Ministry of Defence, *Defence in a Competitive Age* (London: Ministry of Defence, 2021), 46–47, https://www.gov.uk/government/publications/defence-in-a-competitive-age.

[65] Christopher Wardrop, "Bridging the Gap Between Cyber Strategy and Operations: A Missing Layer of Policy", *Australian Defence Force Journal* 204 (March 2018), 63, https://www.defence.gov.au/ADC/ADFJ/Documents/issue_204/ADFJournal204_Bridging_the_gap.pdf.

[66] Discussion with industry stakeholders; Keith Ford-Ramsden and Douglas Burnett, "Submarine Cable Repair and Maintenance", in *Submarine Cables: The Handbook of Law and Policy*, ed. Douglas R. Burnett, et al. (Leiden: Brill, 2014), 158.

[67] Ibid., 161–67.

[68] Doug Brake, *Submarine Cables: Critical Infrastructure for Global Communications*, brief (Washington: Information Technology & Innovation Foundation, 2019), 2, http://www2.itif.org/2019-submarine-cables.pdf.

[69] *Economic Impact of Submarine Cable Disruptions*, 48.

[70] *Guide to Australian Maritime Security Arrangements* (Canberra: Maritime Border Command, 2020), 93, https://www.abf.gov.au/what-we-do-subsite/files/gamsa-2020.pdf; Australian Border Force, "Maritime Border Command", 21 April 2020, https://www.abf.gov.au/about-us/what-we-do/border-protection/maritime.

[71] *Guide to Australian Maritime Security Arrangements,* 41–49.

[72] ACMA, *Report on the Operation of the Submarine Cable Protection Regime* (Canberra: ACMA, 2010), 15, archived by archive.org, 20 September 2015, https://web.archive.org/web/20150920233243/http://www.acma.gov.au/webwr/_assets/main/lib311258/acma_submarine_cables_report.pdf.