Postdigital war beneath the sea?

The Stack's underwater cable insecurity

Richard J. Aldrich & Athina Karatzogianni

Abstract

This article addresses the problem of undersea cable security, arguing that for almost a century undersea cables have been the playground of major states that have enjoyed the practice of cable interference as part of international conflict. Over the last two decades, it has been a major source of intelligence for organisations like NSA and GCHQ, and so there has been a reluctance to advance international legalisation in this area. Nonetheless, the effect of this has been a failure to protect the digital global commons, and as a consequence, the level of risk to critical infrastructure is growing. The use of cables for intelligence gathering has resulted in a legal regime that is patchy and piecemeal, reflecting a general conspiracy of silence amongst major states about intelligence and its interplay with international law, very much raising questions about the interplay of hardware and software sovereignty with the declining sovereignty of states in modern geopolitics defined by the additional problem of the emergency of the looming ecological disaster. Ultimately, we argue that the end of the digital, through its dependency and risk to the Earth layer, poses critical questions regarding emergent postdigital battlefields, right at the heart of the deep materiality of computation.

Introduction: when will the Stack fall?

In 2015, Benjamin Bratton published an influential book entitled The Stack. Its central proposition was that computing has become a global leviathan. He argued that current computing systems are best conceptualised as a global megastructure—the Stack. This structure is layered by six tiers: Earth, Cloud, City, Address, Interface, and User. Bratton's most important claim is that The Stack is rendering other forms of human governance and sovereignty obsolete. Bratton's assertions are by equal turns beguiling and bewildering, since they often involve convoluted rhetoric and abstraction. Nevertheless, Bratton's idea of a computational megastructure is of critical importance. It underlines the assertion that the internet is a physical thing that is built one layer upon another—and as such is vulnerable. Precisely because it consists of 'machines and material', he suggests that it could be 'a causality of its own potentially disastrous impacts'. To evidence this, he refers to a typhoon that broke at least nine communications cables 4000 m down in the ocean that disrupted the internet and telecommunications between Taiwan, China and Hong Kong, pointing to a report that 'over 95% of global communications traffic is handled by just 1 million km of undersea fiber-optic cable.' (Bratton 2015, 96 cites Foster, 18 August 2011). In other words, if the Stack is a layered physical-virtual construct, then one of the questions it begs most urgently is: When will this contingent megastructure fail and how?

Bratton is not the first to assert the physical nature of the internet and its connectivity with real-world geography. In 2005, Vincent Mosco laid down a challenge to what he called the myth of cyberspace. In The Digital Sublime, he argued that the false prophets of the digital era had promised nothing less than the transformation of society. The cyber utopians assured us that with the computer, we could escape the constraints of the physical world, transcending time and space, and

overturn traditional economic, social and political relationships. Mosco examined the myths constructed around the new digital technology and explored why they were so compelling. The myths of cyberspace looked curiously like the similar mythic pronouncements prompted by past technological advances—the telephone, the radio, and television, which in fact offered only incremental change not revolution or liberations. His proposition was cyberspace was not a different place and offered no fundamental escape from our present reality (Mosco 2005). The internet consists of computers, servers and above all cables—much of it remarkably unprotected.

This article addresses precisely this problem of undersea cable security from the conceptual premise of the Stack. In a post-Stuxnet decade when digital war is the hot topic of the day, the widespread assumption is that attacks must take the form of code and consist of viruses or worms. Instead, this article suggests that the most vulnerable elements of the internet are actually within its Earth Layer of the Stack, the 'geological substrate of computational hardware and of the geopolitics of mineral and resource flows of extraction, consumption, and discarding' (Bratton 2015, 70).

Nicole Starosielski is an archaeologist who specialises in the materiality of the internet. She observes that the terms used to describe important elements of the internet, such as 'wireless and 'cloud', seem almost deliberately designed to disguise the underlying need for physical infrastructure, and as a result, this is only dimly appreciated. 'Our seemingly wireless lives are predicated on a mess of tangled wires' (Starosielski 2015). The cloud is an example of the use of utopian language deployed to market less than romantic products and this, in turn, conjures up visions of 'other worlds' (Amoore 2018). Bratton talks of the Cloud layer of the Stack as 'vast server archipelagos behind the scenes and behind the surface that provide ubiquitous computational services as well as the geopolitical intrigue that involves them' (Bratton 2015, 70). He includes within this 'the entire infrastructural complex of server farms, massive databases, energy sources, optical cables, wireless transmission media, and distributed applications' (ibid). His account focuses on the conflicts arising from 'the juxtaposition and superimposition of state geography and cloud platforms' and on how the 'evolution of states into cloud platforms extends and complicates the locations of infrastructural and legal sovereignty' (ibid).

In this article, we argue that for almost a century undersea cables have been the playground of major states that have enjoyed the practice of cable interference as part of international conflict. Over the last two decades, it has been a major source of intelligence for organisations like NSA and GCHQ, and so there has been a reluctance to advance international legalisation in this area. Nonetheless, the effect of this has been a failure to protect the digital global commons, and as a consequence, the level of risk to critical infrastructure is growing. The use of cables for intelligence gathering has not in itself often resulted in damage to cables, either above or below the sea. However, it has resulted in a legal regime that is patchy and piecemeal, reflecting a general conspiracy of silence amongst major states about intelligence and its interplay with international law, very much raising questions about the interplay of hardware and software sovereignty with the declining sovereignty of states in modern geopolitics defined by the additional problem of the emergency of the looming ecological disaster.

This article argues that the end of the digital, through its dependency and risk to the Earth layer, poses critical questions regarding emergent postdigital battlefields, right at the heart of the deep materiality of computation. To support this argumentation, the article first explains the operational value of undersea cables, proceeds to situates their use in wars historically, and then discusses the legal and regulation problems that arise, in order to conclude with what can be done, in relation to the problems identified.

The Stack is dependent on undersea cables

Worries about the cloud have been voiced before. This debate has mostly focused on the security of the data itself, with less attention given to the sustainability of access to that data. Today, the world's oceans are criss-crossed by over a million kilometres of undersea fibre-optic cable, carrying over 95% of the world's communications traffic. This data consists of a mixture of voice, text, pictures, video and commercial data. The biggest concentration of data exchange is transatlantic. The world's major financial and military systems are increasingly dependent on this data. Without it, the banks cannot trade and the killer drones cannot fly. How vulnerable is this infrastructural landscape and why is it so poorly protected?

Perhaps the most material manifestation of the internet is its global undersea cable network. This physical system of fibre-optic cables joins the major countries of the world and carries over 95 per cent of international voice and data traffic. As late as 1988, microwave and satellites were the main data carriers, sending their information through air and space. In the same year, the first Atlantic fibre-optic cable was laid with the capacity for 50,000 simultaneous phone calls, more than ten times that of equivalent copper cables. The undersea communications revolution had begun. Owing to their vast capacity, lower cost and extended lifespan, submarine cables have now completely overtaken satellites as the principal means of delivering international communications (ICPC).

Once upon a time, these undersea cables only carried Victorian telegraph messages. Now they carry many kinds of data—telephone calls, emails, bank account transfers, above all video around the world. Accessing your data from the cloud is highly convenient. Multinational companies rely on these cables more and more to access their files as the cloud grows, and therefore the potential economic impact of an interruption to these cables becomes more serious. Arguably, the growth in cloud storage has increased the importance of undersea cables, because our ability to access our essential files is crucially dependent on them. Moreover, the matter of who would be responsible for the economic loss associated with such a disruption is highly ambiguous (Hantover 2013, 1–9). Certain users have already identified this problem and have decided upon a solution. Some have decided to do away with the requirement for undersea cables altogether when it comes to data storage in the cloud. Google, one of the key providers, has allowed customers to pay extra costs to specify where their data is stored. The City of Los Angeles has a contract with Google, and it has guaranteed that the city's data will remain within the 'contiguous forty-eight states' making it immune to ocean cable interference (ibid. 18).

What do these undersea cables look like?

Trevor Paglen learned scuba diving and underwater navigation, venturing to the ocean floor to photograph undersea cables, which top-secret documents show are tapped by the NSA (see Paglen, n.d.): 'The photographs of coastlines point to the places where undersea cables connecting the European and American continents meet the mainland and are tapped by the NSA for the purpose of surveillance. Maritime maps visualise the locations of fibre-optic cables to prevent ships from colliding with them. The works are supplemented by NSA documents from the archives of Edward Snowden, corporate documents and photography of the sites (Fig. 1).

To a remarkable degree, they resemble a garden hosepipe. Although given a protective coating of woven steel, they are only about four centimetres in diameter and so are relatively vulnerable. While they are normally buried in trenches up to a metre deep when running close to the surface, below 300 metres they simply run along the surface of the seabed. Burying the cables close to shore is achieved by subsea ploughing and more recently by water-jetting (Muneez et al. 2018). They have proved remarkably vulnerable to accidents—normally fishing by trawlers and ship anchors, together with natural disaster, such as seismic activity. Vulnerability is increased by concentration, since all except one of the transatlantic cables achieve landfall in the USA with the same 50-km area on the East Coast. It is much the same story in other parts of the world.

The biggest peacetime threat is probably to the global financial sector. International banks probably process over $10 trillion each day using undersea cables almost exclusively. Serious disruption of these cables would halt this activity. While there are now hundreds of cables crossing the global seabed, for particular states, banks and markets, often dependant on a few cables, there are serious points of vulnerability. Moreover, because of the growth in internet traffic generated primarily by video for entertainment, supply is barely keeping pace with demand. Accordingly, there is not enough undersea communication network redundancy available to support global banking transactions in a crisis, nor could satellites provide enough back-up. Manufacturing supply chains are also vulnerable. Connectivity is responsible for an increasing portion of advanced industrial output. The more sophisticated commercial products now involve commodities and components sourced from many different countries, constituting a bewilderingly complex chain of subcontractors, designers and retailers. These disparate players are able to seamlessly integrate their efforts using the internet, enabling greater specialisation and impressive economies of scale with each stage of the process of assembly. This is beneficial since it has advanced economic growth in places that are unable to build an entire product domestically. In short, today's global manufacturing chains and financial services are only made possible by transoceanic cables (Clark 2016).

Major military operations are increasingly dependent on these cables. A significant portion of US Department of Defence data travelling on undersea cables is unmanned aerial vehicle (UAV) video. In 2010, UAVs flew 190,000 h, and the Air Force estimates that it will need more than one million UAV hours annually to be prepared for future wars. The best way to bring down the US drone fleet, or indeed to undermine the Five Eyes intelligence system, which is hugely dependant on internet surveillance, would be to attack submarine cables (Hamilton and Kreuzer 2018). The physical destruction of a number of cables would slow the internet down rather than stop it. But what if this physical attack were combined with a Stuxnet type attack against network management systems used to control the cable infrastructure? Would a combination of digital hacks and the use of hack-saws combined have the potential to kill military connectivity across entire regions for days even weeks?

The historic lineage of cable interference

Historic examples suggest that cable cutting is possible and that the effects are serious. Cable cutting has an honourable lineage. The beginning of the First World War was marked by a British effort to send out specialist cable ships determined with to disrupt German undersea telegraph cables. Early on 5 August 1914, only a few hours after war was declared, Britain carried out an operation that seemed to be minor, but was actually vital. A British cable ship severed five German overseas underwater cables, which passed from Emden through the English Channel to Vigo, Tenerife, the Azores and the USA. Germany was left with access to only one cable and any message sent through

this could be read by Britain. In revenge, Germany sought to destroy British telegraph cables in the Pacific and Indian Oceans, attacking stations at Fanning Island and the Cocos Islands in late 1914. On 3 September 1939, shortly after the outbreak of the Second World War, the Allies once more cut the German cables from Emden to New York via the Azores and from Emden to Lisbon. Similar cable cutting operations marked the start to the Korean War and even the Gulf War in 1991. These early 'cable wars' underlined the strategic importance of the global telegraph network (Rankin 2008; Aid 2009).

The Cold War was more about cable interference than cutting. During the 1970s, the US Navy converted the nuclear-powered submarine USS Halibut into a dedicated espionage platform that intruded into Soviet waters with a team of highly trained saturation deep divers. Their task was to introduce recording devices onto Soviet submarine cables in Shelikhova Bay, at the northern point of the Sea of Okhotsk, which could listen in without physically violating or disturbing the cable. The programme was given the codename "Operation Ivy Bells," and allowed the USA to listen to the Soviet Pacific Fleet base near Vladivostok. This was not an isolated case and 10 years later, the NSA was fighting the US press to prevent it being written about, because although the Soviets had blown this particular operation, it was being used against other countries (Bradlee 1996).

It is likely that this process of intelligence exploitation explains why major states have fought shy of protecting cables under international law. In June 2013, the Snowden revelations illuminated the way in which submarine cables have become even more important in cyber-espionage and intelligence gathering. The initial advance of fibre-optic cables seemed to offer some protection against eavesdropping, since they were technically hard to tap into. But once this problem was overcome, they provided an intelligence bonanza. Both the main intelligence techniques used by the NSA and GCHQ codenamed "Tempora" and "Prism" ultimately depend on cable tapping. Tempora was a cable access technique and Prism was system of backdoor access to servers—but also dependent on tapping into cables between data centres (Davenport 2015).

However, serious problems can be caused by events much less dramatic than war. Currently, the majority of cable faults arise from trawl fishing and anchoring, but because these tend to be local events, they represent a routine nuisance rather than a strategic hazard to major countries. Some small countries are dependent in some cases on one cable and can be cut off by one person wielding a hoe or a shovel. In 2011, a peasant farmer in Georgia halted most of the internet traffic in Armenia when she unearthed two of its three fibre-optic lines while searching for scrap metal (Starosielski 2015). Natural disasters, primarily related to seismic activity are much less frequently but can cause widespread disruption with significant economic effects. In 2006, an earthquake off the southern coast of Taiwan resulted in undersea landslides that severed nine undersea cables. As a result, communications with China, Hong Kong, Japan, Korea, Singapore, and Vietnam were badly affected for a period of 3 months, since satellites were unable to carry more than a percentage of the traffic. This halted trading on the Hong Kong stock exchange and also stopped currency trading in South Korea. For a period of days much of the internet communication in this region was dependent on one remaining cable. A complex operation using a fleet of eleven ships was required to carry out the repair work (Sechrist 2010).

The matter of deliberate disruption remains mysterious. During 2008, multiple undersea cables that connected Egypt and Dubai were severed. Two cable breaks were at opposite ends of the Mediterranean, one close to Alexandria, and the other not far from Marseille. The third incident was off the coast of Dubai and the fourth was on a cable connecting the United Arab Emirates to Qatar. About 70% of the international communications between Europe, North Africa, the Middle East, and Indian subcontinent were carried by these cables and so about 80% of India's international

connectivity was lost. The Maldives lost practically all its communications capability. The debate continues as to whether this was a series of storms or sabotage, but divers were arrested off the coast of Egypt. In 2013, three divers with hand tools cut the main cable connecting Egypt with Europe, reducing Egypt's internet bandwidth by 60% (Timmons 2008).

Cable cutting and the law of the sea

Given the importance of undersea cables, they are poorly protected by international law. They represent perhaps the most extreme example of states privatising critical infrastructure but failing to extend protection. At present international law, mostly consisting of the 1982 United Nations Convention on the Law of the Sea, does little to secure undersea cables or indeed cables where they emerge from the sea onto land. States have much less power to address miscreants than say in the realm of piracy and even have uncertain rights when boarding suspect vessels. One suspects this reflects the fact that historically, major powers have seen it as an advantage to attack the cables of minor powers in war (Sunak 2017).

The United Nations Convention on the Law of the Sea, to which most states are signatories, is perhaps the most important sea treaty of the last 100 years. This law does not prevent states from regarding undersea cables as military targets during wartime. Although it requires states to implement national laws that criminalise the breaking of undersea cables by vessels bearing their flag, this has been ignored by the convention's signatories or gestured to with only a low fine. Typically, the US federal law for submarine cable protection offers a maximum penalty of just $5000 for wilful injury to cables. Predictably, perhaps, in the light of what we have learned about the activities of organisations like NSA, the USA helped draft and signed the treaty, but has not ratified it, and so is not bound by it. There is no attempt to create an international crime, in which all states have jurisdiction over the offender, indeed warships do not appear to have the right to board a vessel suspected of interfering with undersea cables in international waters (Sunak 2017).

The present system delegates too much activity to nation-states. Enforcement at a local level is simply too patchy and a better mechanism would be to regard attacks on cables as akin to terrorism or piracy which would allow universal jurisdiction. This would have the advantage of avoiding any jurisdictional entanglements and would allow any country to take action, even those not directly affected by the incident. This change would not be straightforward, since the laws of piracy focus on private gain by seizing 'vessels'. However, the recent history of states stretching terrorist legislation to cover other criminal actions suggests that this would not be too difficult to achieve, if states genuinely wished to do this (Wrathall 2010, 246–248; Matis 2012).

British and American defence chiefs have warned loudly about the danger of Russia interfering with cables, reflecting recent anxiety over Moscow's campaign of unconventional or hybrid means of warfare. Certainly, in the Crimea, Russia quickly severed all digital communications from the peninsula, and it has been reconnoitring undersea cables in the Atlantic using submarines (Sunak 2017). Fear of Russian cable cutting has a long history. The UK government recently declassified a 1959 report about British intelligence fears about a Soviet attack on Allied communications by cutting cables across the Atlantic that carried much of the traffic between GCHQ and NSA. Most of the data used by the world's Signals Intelligence Leviathan is still carried by these cables (Goodman and Dylan 2016).

Other commentaries are less anxious about Moscow. They argue that because faults occur quite frequently, cable repair ships would deal with minor incidents quite quickly. Some argue that Russia enjoys integral continental communications, and so would enjoy seeing global communications disrupted, but others suggest that much Russian content, and money, is actually stored abroad. While the most important cable traffic is transatlantic, there is also more redundancy here and ultimately some of this traffic could be routed across the Pacific.

The biggest dangers are for smaller countries. The highest risk is for those places with limited infrastructures, such as Africa, and some parts of Southeast Asia. An attack here could mean real internet disruption, partly because of the way in which services have developed in these countries. They are often more dependent on the internet for certain services, including banking, than western countries. Other countries simply represent key nodal points in the network. For example, if Egypt's undersea cables were destroyed, at least one-third of the global internet could be impacted (Starosielski 2015). Fortaleza, a city in northern Brazil that few have heard of, is one of the undersea cable capitals of the world connecting much of North and South America. If this was attacked it would interrupt much of the data flowing across the Western hemisphere (Matsakis 2018).

One suspects that cables are poorly protected by law because major states have historically wished to preserve the privilege of cable cutting for themselves. Like strategic airpower or nuclear submarines, there has been a high-cost entry barrier to deep ocean activity. Only major navies or advanced research organisations have possessed the technology to operate in such an environment. However, this is changing because of the emergence of undersea drones. Many enemies, either state or non-state could employ a modified commercial robot vehicle combined with explosives to attack undersea infrastructure. The biggest threat comes from Unmanned Undersea Vehicles or UUVs. Just as drones are posing a puzzling security problem on land, so their undersea equivalent is likely to present challenges (Wrathall 2010, 237).

Mending an undersea cable at sea is time-consuming and difficult. Most new cables have integral monitoring systems that give some indication as to the sector where the break has occurred. Thereafter, maintenance vessels trace to that location and haul up the cable until they reach the affected point. Fresh cable then has to be introduced and this is something that can take several days. Onshore arrival points are also vulnerable, and are rather isolated and unprotected. Often a small building on cliff top or beach, these are frequently the arrival point of several cables. While repair would be simple on land, these sites offer the possibility of cutting several cables at once.

Conclusion: what can be done

'Going forward, there is no Earth layer without the Cloud layer, and vice versa' (Bratton 2015, 140).

Despite the Cloud layer's governance of the Earth layer, through the fluid boundaries of cloud jurisdiction, single states or binaries can still do quite a lot. Some have suggested information storage legislation that would require corporations and local governments to maintain separate and redundant information in a way that ensures restore regular functionality. Certified data storage providers would charge more but would offer highly redundant systems to access their data with more local storage. This would mirror ideas of a splinternet already emerging in other contexts. It would also make sense to construct hidden additional cables to build resilience, but admittedly this would be expensive. The Southern Cross Cable, for instance, which connects Australia, New Zealand, Hawaii, and the continental USA, costs more than $1.5 billion (Sunak 2017, 16).

However, as Robert Martinage has suggested, fundamentally this is a problem of global governance, since it is about the vulnerability of the commons (2015). Many of the remedies advanced by commentators focus on national resilience and local infrastructure. Certainly, countries should follow the Australian example and designate a single national point of contact for undersea cable protection, rather than having it spread across many ministries, as is often the case at present. Alliances like NATO and regional organisations like the Organisation of American States need to work with the major companies to develop better cable-protection strategies, typically involving smart sensors. Commander Michael Matis of the US Navy recommends creating a new international cable construction monitoring regime that would copy current maritime tariff trading technology to promote greater international cooperation and information sharing (Matis 2012). Ultimately, this problem is international, since a cable break off the coast of Egypt could impact India significantly. In the long term, any viable security strategy must be global in scope. There are a range of international associations in this area including International Cable Protection Committee, and regional bodies like the North American Submarine Cable Association (NASCA), but there is a lack of a central monitoring authority that works with appropriate ministries around the world (Hantover 2013, 18).

Global telecom companies would like to see the USA ratify the 1982 Law of the Sea, since within that jurisdiction, they are currently reliant on customary international law and statues dating back to 1884. Telecom and energy companies desire greater government support in enforcing property rights and undersea infrastructure security outside of territorial seas. This might take the form of a proclamation that declares the sovereignty of all undersea infrastructure, which is US owned or services US consumers, and provides for a retaliatory response if it is besieged. President Truman's proclamation on the Continental Shelf represents a viable precedent (Wrathall 2010, 249). The most sensible option would be to extend international legislation dealing with pirates or terrorism, two areas where we have seen effective international action. Because critical infrastructure under the sea is often well beyond national jurisdiction, falling it within the law of the Sea that protects other ocean platforms against piracy would make sense (ibid. 256). International law has also made advances in areas like action against terrorism financing and this might also offer a model (Brennan 2018).

Perhaps it is worth pondering why the structural vulnerability of undersea cables remains unaddressed, despite a decade of panic about the resilience of critical infrastructure. Equally puzzling, states worry about digital cyberattacks on electrical grids, but do not devote attention to protecting the Internet from physical attacks. Why is this? Perhaps it is because for a 100 years states that have had an attack mentality must now take action to protect the physical structure of the internet. Yet for organisations like the NSA, focusing on defence, rather than attack, is not in their nature. In that regard, as Bratton (2015, 140) observes, things are likely to change because of the emergent threat of ecological disaster: He argues: 'as the geopolitics of climate change—related energy production and consumption effects loom larger, the questions of energy provision, dissemination, transparency, monitoring, alliance, and allegiance will […] drive realignments of jurisdictional loyalties around common predicaments, whether we prefer them to do so or not'.

References

Aid, Matthew. 2009. The Secret Sentry. New York: Bloomsbury.

Amoore, Louise. 2018. Cloud geographies: Computing, data, sovereignty. Progress in Human Geography 42 (1): 4–24.

Bratton, B. 2015. The Stack: On Software and Sovereignty. Cambridge, MA: MIT Press.

Bradlee, Ben. 1996. A Good Life: Newspapering and Other Adventures. NY: Simon and Schuster.

Brennan, Anna Marie. 2018. Transnational Terrorist Groups and International Criminal Law. London: Routledge.

Clark, Bryan. 2016. Undersea cables and the future of submarine competition. Bulletin of the Atomic Scientists 72 (4): 234–237.

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

Foster, Peter. 2011. Cloud Computing—A Green Opportunity or Climate Change Risk? The Guardian. 18 August. https://www.theguardian.com/sustainable-business/cloud-computing-climate-change. Accessed 18 May 2020.

Goodman, Michael, and Huw Dylan. 2016. British intelligence and the fear of a Soviet attack on allied communications. Cryptologia 40 (1): 15–32.

Hamilton, Col Shane P., and Usaf Lt Col Michael P. Kreuzer. 2018. The big data imperative. Air and Space Power Journal 32 (1): 4–20.

Hantover, Lixian Loong. 2013. The cloud and the deep sea: How cloud storage raises the stakes for undersea cable security and liability. Ocean and Coastal Law Journal 19: 1.

Martinage, Robert. 2015. Under the sea: The vulnerability of the commons. Foreign Affairs 94: 117.

Matis, Michael S. 2012. The protection of undersea cables: A global security threat. Dissertation, Army War College, Carlisle Barracks Pa.

Matsakis, Louise. 2018. What would really happen if Russia Attacked Undersea Internet Cables. Wired, 5 January. https://www.wired.com/story/russia-undersea-internet-cables/. Accessed 18 May 2020.

Mosco, Vincent. 2005. The Digital Sublime: Myth, Power, and Cyberspace. Boston: MIT Press.

Muneez, Mohamed, Ir Vinesh Thiruchelvam, and Nai Shyan Lai. 2018. On pervasive trenching technologies to bury optical fibre networks at sea. Journal of Marine Environmental Engineering 10 (2): 85–96.

Paglen, Trevor. (n.d.) 'Project Trevor Paglen' TBA21 Journals. https://www.tba21.org/journals/article/trevorpaglen. Accessed 18 May 2020.

Rankin, Nicholas. 2008. Churchill's Wizards: The British Genius for Deception 1914–1945. London: Faber & Faber.

Sechrist, Michael. 2010. Cyberspace in Deep Water: Protecting Undersea Communication Cables by Creating an International Public-Private Partnership. Harvard Kennedy School of Government. https://www.belfercenter.org/sites/default/files/files/publication/PAE_final_draft_-_043010.pdf. Accessed 18 May 2020.

Starosielski, Nicole. 2015. The Undersea Network. Durham: Duke University Press.

Sunak, Rishi. 2017. Undersea Cables: Indispensible, Insecure. London, Policy Exchange. https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf. Accessed 18 May 2020.

Timmons, Heather. 2008. Ruptures call safety of Internet cables into question. The New York Times. 4 February. https://www.nytimes.com/2008/02/04/technology/04iht-cables.4.9732641.html.

Wrathall, Laurence Reza. 2010. The vulnerability of subsea infrastructure to underwater attack: Legal shortcomings and the way forward. San Diego International Law Journal 12 (1): 223–262.