NATIONAL SECURITY, TECHNOLOGY, AND LAW

Securing the Undersea Cable Network

John Arquilla

INTRODUCTION

With regard to what strategists call the "sea lines of communication," the month of July in the year 1866 still resonates, in life and art. That was when the first durable transatlantic undersea cable began operating (an earlier effort in 1858 quickly failed), thereby reducing communications time across the ocean from "two weeks to two minutes," per the slogan of that era.[1] July 1866 is also the date that Jules Verne chose to mark the appearance of Captain Nemo's submarine, the *Nautilus*, in *Twenty Thousand Leagues under the Sea*. Verne soon had Nemo attacking the world's sea-lanes, threatening commerce by being able to hold at risk any route upon what A. T. Mahan later described as the "wide common, over which men may pass in all directions."[2] Nemo waged a kind of war against the world, seeking to bring down the great powers who exploited others—and who had taken his land, killing many of his people and enslaving the survivors, as we learn in Verne's later novel, *The Mysterious Island: Abandoned*. Nemo sought "mass disruption." His motive, Ray Bradbury speculated, was a self-perceived need "to spread a more personal and therefore more constructive terror in the world."[3]

Thus, in life, 1866 was a time of great promise. In art, Verne showed, it could also be a time of peril. Today, amid the many unfolding wonders of the Information Age, the world is connected in a way that reduces communication time, to modify the nineteenth-century slogan, "from two minutes to two seconds (if that)." To be sure, there are multiple ways to send and receive messages, including via satellites. But the bandwidth of orbital platforms is limited, so much so that over 95 percent of international communications still travel by undersea cable.[4] Now information moves by pulses of light via fiber optics, rather than along the old copper wires—protected by hemp, tar, rubberlike gutta-percha, and wire rope—of the previous era. But a cable is still a cable, as vulnerable as ever.

Late in *Twenty Thousand Leagues*, Verne put the *Nautilus* on a submerged course that took it along the transatlantic cable, but Nemo had no interest in severing it.[5] Perhaps he reasoned

A Hoover Institution Essay

Aegis Series Paper No. 2302

that the economic disruption caused by attacking ships would be greater than by keeping information from moving across the sea bottom. And after all, Nemo *wanted* the world to know of and fear the *Nautilus*. If Verne had reasons for keeping fictional Nemo from attacking the undersea cable, in real life, even back then, its security was already a concern taken very seriously. The British, who were cable pioneers, came up with the idea of using their globe-spanning colonies as landing points for their cable networks to reduce their exposure to attack.

Because cables ran then (as now) from landing point to landing point, these vulnerable spots—and the land telegraphs to which they linked—were thought to be more secure if all were located on Imperial territory. This notion of keeping land links on the homeland and in colonies was the origin of the "All Red Line" (British holdings were colored red on maps) that started up in 1902. It was an earlier era of great-power competition and, as Paul Kennedy has noted of the importance of cables in that previous period, "in an age of imperial disputes, early knowledge of developments on the other side of the globe was of prime importance, particularly if rival nations did not possess this information or only acquired it later."[6]

Although radio communication was improving at the same time—Marconi's first transatlantic transmission took place in December of 1901—the British had a good sense of how vulnerable radio waves were to jamming or listening in. Other countries clearly felt the same, and a number of nations began to build their own undersea cable networks. However, when the Great War erupted in 1914, Britain used its naval mastery to cut the cable of the Germans, severing this link to their colonies in Africa and the Far East, as well as to neutrals in the Americas. Indeed, the British attack on the German cable system forced the latter to depend upon the Swedes for international cable-communication purposes.

Yet the Swedes themselves were using a British-administered cable network (now expanded beyond and separate from the All Red Line). And so the Germans, aware that their message traffic would likely be monitored, had to rely on encryption. But the British, foreshadowing the code-breaking enterprise that arose at Bletchley Park during World War II, regularly intercepted and decoded the German message traffic. At a key point, they hacked and decrypted the January 1917 "Zimmermann Telegram" that sought to lure Mexico into going to war with the United States. When the message was shared with leaders in Washington, it sparked an angry American reaction that brought the United States a big step closer to entering the war against Germany—which it did three months later.[7]

Today, satellite bandwidth limits aside, undersea cable communications are still much preferred for sensitive communications because they offer better security than any form of wireless transmission. This is so not only in national security—i.e., governmental and military—matters, but in terms of the day-to-day business and financial communications that are so essential to the health and functioning of the global economy.[8] Yet, for all of the remarkable technological advances of our time, the same types of vulnerabilities that caused concern a century ago persist: cables can be cut, landing points attacked, messages intercepted.

PHYSICAL VULNERABILITY OF CABLE COMMUNICATIONS NETWORKS

An existence proof regarding undersea cables' vulnerability to physical breaks is the fact that they are generally cut between 150 and 200 times annually. Half the breaks result from fishing activity and one-fifth from trailing anchors, with almost all of the remainder due to dredging, drilling, and natural phenomena like earthquakes and sedimentary shifts. One study even notes that fish bites account for 2 percent of the breaks.[9] There are only a handful of intentional or suspicious incidents to date having to do with the severing of undersea cables, a few by pirates operating in shallower waters who cut segments, salvage, and try to sell the fiber optics. One of the best-known incidents had to do with Vietnamese fishermen who, having been granted official permission to salvage copper from old, no-longer-used cables, mistakenly—or with theft in mind, as some early reports alleged—pulled up several miles of fiber-optic links, sharply reducing Vietnam's connections to the world for at least a month, the key point being that these cables are physically quite vulnerable.[10] Nicole Starosielski has summed up the situation concisely, noting that the global undersea network is "precarious rather than resilient."[11]

Attendees of the first major summit on undersea cable security, an event known as ROGUCCI (Reliability of Global Undersea Communications Cable Infrastructure), came from senior leaders in telecommunications, finance, and various agencies of government, and all concurred that the security of the undersea cable network was "absolutely essential" for the world to thrive, both socially and economically. So it is curious that little has been achieved in the years since that 2009 meeting to improve the network's resilience. As one recent study commented about the open discourse on securing undersea cables at a major meeting of NATO defense ministers in October 2020, "despite the proliferation of public statements underlining the importance of protecting them, collective action to enhance their security has so far been lacking."[12]

Why this lack of action? Perhaps the simplest answer is that there has not been a sense of urgency about improving the security of the undersea network due to the absence of a major attack upon it. This complacency is complemented by the inherent impediments to collective action arising from the widely diverse range of owners of the world's nearly five hundred (as of 2023) undersea cables. Roughly 60 percent of them are completely privately held, either by lone companies or consortia, with the owners coming from many nations. Government-private partnerships own approximately another 20 percent, with pure state-owned cables accounting for almost all the remaining 20 percent.[13]

But even in the absence of significant attacks on the undersea network, there are signs of interest by some hostile powers in *having the ability* to strike at the cables. The Russian navy in particular has shown a considerable degree of interest in undersea cables, its submarines often patrolling near them.[14] There is also the Russian "research ship" *Yantar*, capable of deploying minisub drones able to dive and operate robot arms nearly four miles beneath the surface of the sea. For years, the *Yantar* has often been spotted cruising right above undersea cables.[15] These ways to attack the cables may be technologically advanced, but the results they could achieve are no different from what the British were doing to enemy cables during World War I. For that matter, the United States prefigured this form of attack on undersea cable networks even earlier, in its 1898 war with Spain, severing Madrid's links with its colonies in the Caribbean and as far off as the Philippines.[16] Yet, despite the current evidence of serious Russian interest in and capabilities for disrupting undersea cable networks, and the historical precedents for mounting attacks of this sort set by both the United States and Britain, there is still a strong sense that this threat is "an over-hyped scenario" and that "snipping a handful of cables . . . would disturb the global Internet very little."[17]

The view that small-scale attacks on the undersea network would have little disruptive effect is, at first glance, supported by the record of breaks from a variety of natural or accidental causes, which suggests that the current fleet of repair ships—there are sixty, worldwide—has the capacity to cope with anything less than a major assault on the network.[18] Beyond repair ship capacity, those who believe in the robustness of the cable system rely on the complexity and alternative routing possibilities inherent in the network design. For example, there are over three dozen alternate routes for sending information out from the continental United States. While this is far above the average, even small nations have a number of alternate routes—Vietnam, for example, has three, a common number for countries of its size. The problem with this "network complexity defense" construct is that, as in any network, not all connective nodes are created equal. There are some nodes at critical junctures that act as choke points in the global network. Hawaii provides an example of one such point. As Starosielski has noted, at and near Electric Beach on Oahu, "cable systems extend directly to California, Oregon, Fiji, and Guam and reach onward to Australia, Japan, and much of East Asia . . . establish[ing] Hawai'i as a critical node in our global t elecommunications networks."[19]

Starosielski goes on to describe the mindset of the cable industry in recent decades as reflecting faith in the security of deep-sea cables, keeping their numbers limited—often to just a single line—over long distances. But concerns about the vulnerability of landing points, where the cables come ashore, has led to the idea of having many branch points near landfall. Thus, a system arose that "entailed using one cable with multiple endpoints."[20] This improved the security "at the level of the individual [i.e., local] network, without necessarily taking into consideration the stability of the system as a whole."[21]

Concern about the vulnerability of landing points is well founded, and there are some dramatic examples of operations that have exploited for intelligence or, in time of war, knocked out landing points. Perhaps the best-known example of the former was the US Navy's "Ivy Bells" operation during the 1970s, launched in the wake of a submarine skipper locating a Russian landing point. His discovery led to deployment by navy divers of a tap wrapped around the nearby cable. They returned to the tap monthly to retrieve information. Eventually, a traitor, John A. Walker Jr., apprised the Russians of the tap. The navy also struck at landing points and the cables running from them during the conflict with Spain in 1898—taking advantage of a "wartime exemption" in the 1884 Convention for the Protection of Submarine Telegraph Cables.[22]

This concern forms part of the virtual problem set that is increasingly important to the security of the global undersea cable network, an issue considered in the following section. But before doing so, it is worth mentioning that there are undersea cables that do more than just transmit data; they can move electricity, oil, and natural gas as well. And they, too, are vulnerable to physical attack and cyberattack.

The most salient example of undersea network vulnerability to sabotage arose in September of 2022, when both Nord Stream pipelines—which move gas from Russia to Germany—were hit by explosions that resulted in significant leaks into the Baltic Sea. Nord Stream was not in operation at the time, but there was still natural gas in the line. Though the perpetrator remains publicly unknown, the European Union and NATO, in a joint declaration, called these attacks the "gravest threat to Euro-Atlantic security in decades."[23] And while it has not been hit by any kind of sabotage to date, the undersea cable between Norway and Britain that provides electricity back and forth, based on the needs of each—much of it "green," with hydropower from Norway and wind power from Britain—is also vulnerable, to both physical sabotage and virtual "cybotage" of its system controls when hacked.[24]

VIRTUAL VULNERABILITY OF THE UNDERSEA CABLE NETWORK

Whereas physical attacks on deep-sea cables require sophisticated technical abilities—purpose-built minisubs, robot arms, and more—and striking at landing points entails higher risks of detection, the very fact that the cables are connected to the internet means they can be accessed virtually by skillful hackers—anonymously, from anywhere in the world, spying on, disrupting flows of, or ransoming data.

Due to the high percentage of cable lines owned by commercial firms, and the number co-owned by such firms and governments, there are many telecommunications companies involved with undersea cables. This means (1) cybersecurity varies significantly across the different owner and operator syndicates, and (2) those firms that are linked to or owned outright by governments may allow intrusions into the undersea network (e.g., China Mobile, a major player, is state owned). As to the first point, in addition to inherent differences in security systems across the many companies involved, they all have the need, in the capital-intensive and high-labor-cost undersea cable industry, to reduce operating expenses. This common need has led to the persistence of less-effective cybersecurity systems and the rise of more economical, but still vulnerable, automated controls. With regard to the second point, both the amount and value of the data flowing via undersea cables create attractive targets for nation-states' cyber teams and nonstate hacker groups. Justin Sherman has summed up the situation concisely as one in which "owners are deploying remote network management systems for cable infrastructure, and these systems are often poorly secured, thus increasing cybersecurity risks. And the growing volume and sensitivity of data flowing over cables increase the incentives states and other actors have to spy on or disrupt traffic."[25]

Indeed, cyberattacks, particularly against increasingly automated systems, could even go beyond attempts at, say, the theft of particular information of a commercial or military nature, or the disruption of communications with one or more nations. It is theoretically possible that whole cable-management systems could be frozen up, held for ransom on a scale hitherto unseen. This potential for "mass disruption" could have even more dire effects in an international crisis or armed conflict, undermining the military capability of one side and giving great advantage to the other. In the case where war is breaking out, one should expect that, in addition to crippling the undersea links that carry military information and commands, the orbital links upon which armed forces increasingly depend would be simultaneously blinded. During the Cold War, the Soviets routinely began their *Zapad* (West) war exercises with a simulated high-altitude electromagnetic pulse (EMP) weapon designed to disrupt NATO command-and-control systems. This is a risk that persists today, at a time when escalation of the Russo-Ukrainian conflict to a wider war remains a live possibility because, according to a recent strategic assessment, Russia "probably remains the world's leader in Non-Nuclear EMP (NNEMP) weapons."[26] Needless to say, the Russians can use nuclear EMP, too.

Simulated combined-arms attacks and other scenarios aside, there have been actual attempts to hack into the undersea network. The best known was reported openly in April 2022, taking place in Hawaii—the node in the network that Nicole Starosielski identified as "critical" to connectivity across a large swath of the world.[27] In this case, what can be reported openly is that access was gained via credential theft, but that the action of the hacker was detected and thwarted before disruption to connectivity could be achieved. Underlining the criticality of Hawaii to the network, John Tobon, the special agent of Homeland Security Investigations (HSI) in charge, said at the time, "[t]his is only one of the many examples of cyber incidents that HSI has responded to in Hawaii and the Pacific region."[28]

Aside from the vulnerability to malware insertion at the supply-chain level, due to the fact that many components are manufactured in countries where security practices may not be of the highest standards, there is yet another major target area for skilled hackers: the cloud. In recent years, there have been sharp increases in the amount of information being stored outside an organization's own systems and instead in the cloud—which consists of outside organizations' computers. This practice has increased rapidly, so much so that, by the fall of 2021, as one report at the time observed, "cloud adoption is steadily rising across industries, with 90% of organizations using cloud computing."[29] Even more organizations have begun cloud computing since then. Where this intersects with undersea cables is in the matter of realizing that, as Starosielski has put it, "the cloud is actually under the ocean."[30] The point is that, since almost all organizations are using cloud computing today, a hack of the companies providing undersea cable service could result in gaining major access to information going to and coming from the cloud. Though Starosielski made this important point in early 2019, at this writing (four years later) there is little recognition that seemingly secure cloud-stored data moved via the undersea network is vulnerable to hacks of cable companies.[31]

Overall, the threat to the undersea cable network from cyberspace-based attacks is at least as great as the network's vulnerability to the range of forms of physical attack. In some ways, the virtual threat is more serious, because the sheer number of actors who may have the hacking skills to target the undersea network is much larger than the ranks of those with the ability to go after deep-sea cables with minisubs and their robot arms. Who can surmount the technological barriers to entry and pose deep-sea physical threats to the United States and its friends and allies? There are only two today: China and Russia. In the case of China, there may be a kind of self-deterrence in play, because of the deep intertwining of the Chinese and the global economies. Mass disruption of the undersea network would have catastrophic effects for the world, but would be just as grievous for China.

The problem for Beijing is similar to what Britain faced in August of 1914, at the outset of World War I, when it sought, as Nicholas Lambert put it, to "exploit her position at the center of the world communications network."[32] The plan to cut off cable-enabled German trade had grave effects but, just months into the war, the British realized their own economy was hurt just as badly as Germany's, and the damage to neutral countries' commerce was severe, too. So, the effort was called off. Perhaps the Chinese are aware of this example. One can only hope.

The key to seeing how the plan to cause economic mass disruption damaged Britain, its allies, the enemy, and neutrals equally was the fact that, per Lambert, "[b]y the turn of the twentieth century, instantaneous communications had transformed the day-to-day conduct of international trade [and] most international (and much domestic) commerce became reliant upon access to cable communications."[33] Moreover, "[t]he economic well-being of whole societies, not merely governments, depended upon a highly optimized economic system, itself dependent upon access to the infrastructure of global trade, reliant upon access to real-time communications."[34]

The situation in the twenty-first century is quite similar. Although cable communications now move via pulses of light rather than copper wires, economic well-being is just as reliant upon cables today as it was a century ago. The strategy of pursuing mass disruption in that earlier era backfired, swiftly and spectacularly. No doubt similar results would arise today if, say, China decided to strike at the various key nodes in the undersea network that keep global commerce humming. Having the world's second-largest economy, the Chinese are far too integrated into the global system to hope that they could escape the effects of their own offensive launched against the infrastructure upon which the prosperity of all is so dependent. This is as true today as it was for Britain in 1914, when it cut off the German and Austrian shares of world manufacturing—together they produced nearly one-fifth of the total—and denied itself and many others German steel production, which was almost *triple* that of Britain.[35]

If the Chinese are contemplative enough—or can be persuaded—to see the folly in attacking the undersea cable infrastructure upon which they and almost all the world depend, then they may be self-deterred from launching such an assault. Can the same be said of the Russians, who are the other major power able to mount an offensive against key points in the global undersea network? It is not clear that deterrence would hold in their case if, say, the war in Ukraine were to escalate into a larger conflict. Russia's gross domestic product is under two trillion US dollars, just about the size of Spain's, and its interconnections with the global economy—particularly that of the United States—are relatively low compared to others'. In the case of its oil exports, even disruption of the global market could be weathered fairly easily, given that China has a huge, growing appetite for that commodity. The point is that Russia is far better poised than China to mount a campaign against the undersea cable network aimed at disrupting the global economy. *In extremis*, for example during a protracted armed conflict like the one in Ukraine that may escalate, even the prospect of causing economic damage to China might not prove strong enough to deter Russia. And in addition to motives for mounting such an attack, and a degree of insulation from its effects, Russia has a long-standing submarine doctrine of "raider warfare" against commerce that easily encompasses the idea of striking at undersea cables.[36]

WHAT IS TO BE DONE?

The body of evidence introduced thus far suggests that the undersea cable network is indeed, as Nicole Starosielski has argued, "precarious rather than resilient."[37] With this fragility in mind, the question now is about how to improve defenses against physical attacks and cyber hacks. Efforts have been undertaken to improve landing-point security through concealment and hardening—including, in the latter case, the shielding with armor of the cable segments in shallower waters near landing points. In terms of protecting deep cables, one can only note (openly) that public mentions of Russian submarines patrolling near these lines imply some ability to detect and then track their movements. This means, in times of crisis and conflict, a Russian submarine offensive targeting the cable network may prove difficult to mount. The once-classified Sound Surveillance System (SOSUS) that tracked Russian subs during the Cold War was based on passive (i.e., listening) sonars. Augmented later by the Surveillance Towed Array Sensor System (SURTASS), the system today includes a suite of new sensors that operate under the rubric of "integrated undersea surveillance." Advances are coming so rapidly that, as one recent study puts it: "Emerging technologies and substantial improvements in existing technologies may . . . enable advanced militaries to locate and track submarines . . . with increasing reliability."[38] Daunting as this should be, a Russian submarine surge right before a war broke out might still achieve disruption of the network—though likely at the cost of serious sub losses.

In terms of defending against cyberspace-based attacks, clearly much fresh attention must be paid to the companies and consortia that provide the undersea network cables. The two main areas of concern have to do with (1) the automated system controls increasingly being used to monitor the cable network for breaks or other disruptions, and (2) the information systems of the cable-provider companies themselves. The automated systems may prove vulnerable to malware inserted at some point in the supply chain, which may lie in wait to be activated. And hacks of the provider companies' home systems—via any of the usual means, from social engineering to password cracking—could also allow placement, in "sleeper mode" or at the time of attack, of worms, viruses, and other disruptive tools that could be employed to disable whole sections of the undersea network, or steal and hold for ransom vast amounts of data in transit.

Because hacks are likely to continue, via credential theft, password cracks, or social engineering—among other techniques—the key to cyber defense is swift detection. And nothing moves faster than automated systems guided by artificial intelligence (AI). AI “sentinels,” ever improving via machine learning, offer hope of rapid detection and response to cyber intrusions. At the same time, though, the offensive use of AI has to be guarded against, especially the insertion of malware into global cable component supply chains during the manufacturing process.[39]

Given that emerging technical capabilities are also increasing the vulnerability of deep-sea communication cables to physical attack, it may prove useful to reassess some aspects of the designs that were favored for undersea cable networks over a century ago, “in which multiple deep-sea cables were laid to the same endpoint.”[40] Adding more deep-sea cables, with varied routes to the same point-to-point destinations, though costly, would greatly enhance overall resilience. As to the physical security of the links between deep-sea cables and connections with the shore, it is no doubt more prudent today to strive to establish and maintain multiple landing points. This approach could also enhance security of the cable network against physical attack, provided the landing points benefit from both concealment and “point defenses.” But having more landing points may also create increased access opportunities for those seeking to intrude upon the network via cyberspace. There would simply be more portals for hackers to ping, perhaps to penetrate.

Despite a threat matrix that continues to grow in sophistication and potential severity, a major reason why the undersea network remains so vulnerable, and why fixes and risk-mitigation measures are slow to be made, is that the cable owners have not faced market pressures to move swiftly to improve cable security. Indeed, the lack of malicious incidents, from crime to sabotage, has reinforced complacency and led to a classic case of “market failure.” Prevalence of private ownership of cables has limited the roles of governments in providing security standards. Given the risk to global prosperity entailed in disruption of the undersea network, it is well past time for governments to become more active in cable security.

An example of governmental steps that might be taken has been provided by Kevin Frazier, who, looking through the lens of the US government, has suggested several measures. One would require “that all undersea cables that cross through federal seabed be ‘dark cables.’”[41] That is, their locations would be known only by private providers and key government actors. Such a step might lead malefactors to focus on locating landing points, so another recommendation would require the hardening of landing points, with both surveillance technologies and increased on-site security. Last, Frazier notes the mix of several government agencies that have some type of oversight of undersea cables and suggests naming or creating just one with the authority to gather and assess data, and to act swiftly when needed.[42]

On this last point, if a “cable czar” position were created, this person might also do well to engage the broad scientific community to generate fresh ideas about how to cope with rising threats to the undersea network. For example, regarding the matter of a malefactor tapping the cable to siphon information (recall the above-mentioned Navy Ivy Bells operation), coherent optical time-domain reflectometry, today used for a range of tasks including detection of seismic activity, is possibly sensitive enough to detect a tap being put in place.[43] There are surely other ideas.

In addition to exploring the range of scientific options and insights, it will be important to reconsider the design path that has unfolded, when efficiencies have driven choices more than security concerns. This is especially important at a time when adversaries' ability to locate and approach deep-sea cables has improved radically. So, as a design principle, the old philosophy of Britain's All Red Line should perhaps be revisited, as its emphasis on multiple deep-sea cables on select routes could be a hedge against the current threat posed by minisubs and robot arms. Another design idea would be to reconsider the network's topology and focus on creating alternative routes or additional nodes to those so critical to its functioning. Right now, there is great vulnerability to concentrated strikes at a few key points in the network (which is why I mention only Hawaii as a key example). Undersea cable projects are hugely expensive endeavors, so serious concern about overall network design should form an essential part of the discourse in planning stages. For example, the current Far North Fiber project, aimed at linking Europe to Japan through Arctic waters, is estimated to cost a billion dollars and will traverse some areas in which Russian submarines have an exceptional aptitude for maneuver. It would cost much more if alternate deep-sea cable lines were added to the plan, but the security gain against mass disruptive threats would be enormous.[44]

CONCLUSION: A ROLE FOR DIPLOMACY?

Aside from the approaches to improving the security of the cable network already mentioned—which may make it less precarious—the possibility of employing a diplomatic approach should also be considered. International agreement on cable security might arise in the form of a treaty, or even by some new aspect of sea law. But this takes time, to be measured in years before taking effect. In the meantime, something less formal might be pursued, an understanding of sorts. What might this look like? Given that the subject of the agreement is the matter of maintaining the flow of information globally—and might apply to undersea electricity transmission and gas pipelines, too—it could prove useful to explore and expand upon some of the efforts to establish a behavior-based regime in the realm of cyberwarfare. A signal event in this area of concern was a meeting between Barack Obama and Xi Jinping in September 2015, when they agreed "that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets."[45] The idea of such an agreement is based on the notion that the many technical *means* for stealing intellectual property cannot be controlled, but *behavior* can. This may be possible even in wartime when it comes to the undersea network, as evidenced by the highly cautionary example of the terrible experience the British had in 1914 when disrupting cable communications. To date, it is clear that China continues to steal trade secrets, but it has refrained from mounting disruptive attacks on infrastructure—a ray of hope for behavior-based cyber restraint.

Perhaps this hypothetical international agreement on undersea cable security might go beyond the matter of dealing with virtual threats to include putting some mutually agreed limitations on the use of submarines to locate and loiter around the network's lines. But even if diplomacy could only mitigate the cyber threat to the world's cable infrastructure, it would be an enormous boon to global security, as there are already robust measures being taken to detect and track the movements of submarines (as noted above) that can pose threats to the undersea network.

Another argument in favor of bringing the cables under the rubric of cyber arms control is that Bejing can join a larger movement already under way to reach agreements aimed at improving the security of land-based infrastructures against cyber threats.[46] As for the basic problem that cyber weaponry cannot be controlled or accurately counted like missiles or fissile materials in traditional arms control, Joseph Nye of Harvard has pointed out that the harms done by mass disruption would be broad, but the ultimate costs of being caught cheating on the agreement would be higher. In an influential article on this subject, written soon after the Obama-Xi meeting, Nye asked, "What is to prevent cheating?" then replied: "The answer is self-restraint."[47] I would add only that self-interest will tamp down cheating, too.

Nye's notion of building international norms to protect the information infrastructures upon which our world depends hearkens to the enthusiasm with which many countries greeted the possibility of becoming connected via undersea cables. S. A. Garnham—who served on cable ships a century ago—and Robert Hadfield enthused, "[f]rom the moment that the land telegraph had become a commercial proposition, inventive genius turned to the idea of passing cables beneath the sea."[48] The first transatlantic cable was also seen as an important step in global community building. As John Gordon noted, "[t]he laying of the Atlantic cable was one of the great international undertakings of the mid-nineteenth century."[49] Even that nautical terrorist conjured by Jules Verne, Captain Nemo, viewed the first functional transatlantic cable with respect, as did his passenger-prisoner Professor Aronnax, who was highly impressed when he observed it—so much so that he concluded, "[t]his cable will probably last indefinitely."[50] Over time, British-owned and -controlled cables did endure, but the Royal Navy severed the undersea links of its enemies in 1914—much as the US Navy did to Spain's cables in 1898. Will today's undersea network "last indefinitely"? It can, if the powers of the world today view it as a common good rather than a strategic target.

NOTES

[1] David Tristan, *July 27, 1866—The Transatlantic Cable That Worked*, ABC27 (Jul. 27, 2022, 2:02 PM), https://www.abc27.com/digital-originals/july-27-1866-the-transatlantic-cable-that-worked/ [https://perma.cc/J9NA-EQTF]. *See also* Anton A. Huurdeman, The Worldwide History of Telecommunications 602 (2003).

[2] Alfred Thayer Mahan, The Influence of Sea Power upon History, 1660–1783, at 25 (5th ed. 1894).

[3] *See* Ray Bradbury, *The Ardent Blasphemers*, introduction to Jules Verne, Twenty Thousand Leagues under the Sea 1, 7 (Anthony Bonner trans., 1962) [hereinafter Verne, Twenty Thousand Leagues]. Nemo's full backstory is revealed in Jules Verne, The Mysterious Island: Abandoned (W. H. G. Kingston trans., 1875).

[4] Lori W. Gordon & Karen L. Jones, The Aerospace Corp., Global Communications Infrastructure: Undersea and Beyond 2 (2022).

[5] Verne, Twenty Thousand Leagues, *supra* note 3, at 352–53.

[6] P. M. Kennedy, *Imperial Cable Communications and Strategy, 1870–1914*, 86 Eng. Hist. Rev. 728, 728 (1971).

[7] See generally Barbara W. Tuchman's classic account, The Zimmermann Telegram (1958), and Thomas Boghardt's recent The Zimmermann Telegram: Intelligence, Diplomacy, and America's Entry into World War I (2012).

[8] *See generally* Gordon & Jones, *supra* note 4, at 1–2.

[9] These causes of disruption are discussed in detail throughout Thomas Worzyk, Submarine Power Cables: Design, Installation, Repair, Environmental Aspects (2009). *See also* Karl Frederick Rauscher, Proceedings of the ROGUCCI Study & Global Summit Report 79 (2010) ("ROGUCCI" refers to the Reliability of Global Undersea Communications Cable Infrastructure Summit held in Dubai, UAE, in 2009).

[10] Reuters Staff, *Vietnamese Fishermen "Salvage" Internet Lines*, Reuters (June 6, 2007, 12:24 AM), https://www.reuters.com/article/us-vietnam-cable/vietnamese-fishermen-salvage-internet-lines-idUSHAN1727620070607 [https://perma.cc/9HZJ-6T9U]; and Gregg Keizer, *Fishermen Pull the Plug on Vietnam's Web, Steal Cable for Scrap; It Could Take a Month for Repairs to Be Made*, Computerworld (June 7, 2007, 12:00 AM), https://www.computerworld.com/article/2541664/fishermen-pull-the-plug-on-vietnam-s-web--steal-cable-for-scrap.html [https://perma.cc/R6VM-Y8ZR].

[11] Nicole Starosielski, The Undersea Network 10 (2015).

[12] Colin Wall & Pierre Morcos, *Invisible and Vital: Undersea Cables and Transatlantic Security*, Ctr. for Strategic & Int'l Studs. (June 11, 2021), https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security [https://perma.cc/33RY-8W5A].

[13] Justin Sherman, Atl. Council, Cyber Defense across the Ocean Floor: The Geopolitics of Submarine Cable Security 9 (2021), https://www.atlanticcouncil.org/wp-content/uploads/2021/09/Cyber-defense-across-the-ocean-floor-The-geopolitics-of-submarine-cable-security.pdf [https://perma.cc/U6AJ-32X5].

[14] *See* P. A. Media, *UK Military Chief Warns of Russian Threat to Vital Undersea Cables*, Guardian (Jan. 8, 2022, 4:59 AM), https://www.theguardian.com/uk-news/2022/jan/08/uk-military-chief-warns-of-russian-threat-to-vital-undersea-cables [https://perma.cc/978S-QCF7].

[15] *See* David E. Sanger & Eric Schmitt, *Russian Ships Near Data Cables Are Too Close for U.S. Comfort*, N.Y. Times, Oct. 26, 2015, at A1. For more on Russian submarine and sub-based drones, see John Arquilla, *From U-boats to "U-bots,"* Comms. of the Ass'n. for Computing Machinery (Apr. 26, 2021), https://cacm.acm.org/blogs/blog-cacm/252157-from-u-boats-to-u-bots/fulltext [https://perma.cc/FRH6-ZDYJ]; and H. I. Sutton, *Russian Spy Ship Yantar Loitering Near Trans-Atlantic Internet Cables*, Naval News (Aug. 9, 2021), https://www.navalnews.com/naval-news/2021/08/russian-spy-ship-yantar-loitering-near-trans-atlantic-internet-cables [https://perma.cc/XJ6S-UPAG].

[16] *See* Cameron McR. Winslow, *Cable-Cutting at Cienfuegos*, 57 Century 708, 708 (1898).

[17] The first quote is from Sebastien Roblin, *Russian Spy Submarines Are Tampering with Undersea Cables That Make the Internet Work. Should We Be Worried?*, Nat'l Interest (Aug. 19, 2018), https://nationalinterest.org/blog/buzz/russian-spy-submarines-are-tampering-undersea-cables-make-internet-work-should-we-be [https://perma.cc/CPH4-25E2]. The second quote is from Louise Matsakis, *What Would Really Happen If Russia Attacked Undersea Internet Cables*, Wired (Jan. 5, 2018, 7:00 AM), https://www.wired.com/story/russia-undersea-internet-cables [https://perma.cc/5MPD-MZ7M].

[18] *See Cableships of the World*, Int'l Cable Prot. Comm. (Feb. 11, 2022), https://www.iscpc.org/information/cableships-of-the-world/ [https://perma.cc/TN9R-UMHY].

[19] Starosielski, *supra* note 11, at ix.

[20] *Id.* at 49.

[21] *Id*.

[22] *See* Sherry Sontag & Christopher Drew, Blind Man's Bluff: The Untold Story of American Submarine Espionage 199–201, 216, 227–28 (2000). A great firsthand account of the navy attack on Spanish cables in 1898 can be found in Winslow, *supra* note 16, at 708.

[23] *After Nord Stream Blasts, NATO, EU Vow to Protect Infrastructure*, Al Jazeera (Jan. 11, 2023), https://www.aljazeera.com/news/2023/1/11/nato-eu-move-to-boost-protection-of-criticial-infrastructure [https://perma.cc/PRC2-LHX8].

[24] *See* Stanley Reed, *Undersea Cables Connecting Britain to Europe Are Key to a Renewable Future*, N.Y. Times (Jan. 4, 2022), at B1.

[25] Justin Sherman, *The U.S. Should Get Serious about Submarine Cable Security*, Council on Foreign Rels. (Sept. 13, 2021, 6:12 PM), https://www.cfr.org/blog/us-should-get-serious-about-submarine-cable-security [https://perma.cc/J62Q-6JKN].

[26] Peter V. Pry, EMP Task Force on Nat'l & Homeland Sec., Russia: EMP Threat—The Russian Federation's Military Doctrine, Plans, and Capabilities for Electromagnetic Pulse (EMP) Attack 1 (2021), https://apps.dtic.mil/sti/pdfs/AD1124730.pdf [https://perma.cc/QU5D-DBXG].

[27] *See supra* note 19.

[28] Jamie Tarabay, *An Underwater Hack and the Digital Ripple Effects*, Bloomberg News (Apr. 20, 2022, 6:45 AM), https://www.bloomberg.com/news/newsletters/2022-04-20/an-underwater-hack-and-the-digital-ripple-effects [https://perma.cc/7CTM-S63E].

[29] VB Staff, *Report: Cloud Adoption by Orgs Increases to 90%,* VentureBeat (Nov. 8, 2021, 6:00 AM), https://venturebeat.com/data-infrastructure/report-cloud-adoption-by-orgs-increases-to-90 [https://perma.cc/BGB4-4CXL].

[30] Nicole Starosielski, *'The Reality Is That the Cloud Is Actually under the Ocean'*, Silicon Republic (Feb. 13, 2019), https://www.siliconrepublic.com/comms/internet-undersea-cables-damage-tonga [https://perma.cc/V4BA-37VH].

[31] *See, e.g.*, Gui Alvarenga, *Top 6 Cloud Vulnerabilities*, CrowdStrike (June 28, 2022), https://www.crowdstrike.com/cybersecurity-101/cloud-security/cloud-vulnerabilities [https://perma.cc/Y8UT-VQD4] (making no mention of the cloud-cable security concern).

[32] *See* Nicholas A. Lambert, Planning Armageddon: British Economic Warfare and the First World War 157 (2012).

[33] Nicholas A. Lambert, *The Strategy of Economic Warfare: A Historical Case Study and Possible Analogy to Contemporary Cyber Warfare*, *in* Cyber Analogies 76, 78 (Emily O. Goldman & John Arquilla eds., 2014).

[34] *Id.* at 80.

[35] *See* Paul Kennedy, The Rise and Fall of the Great Powers: Economic Change and Military Conflict from 1500 to 2000, at 258 (1987).

36. On this point about Russian submarine "raider warfare," see Rear Admiral Edward Wegener's classic The Soviet Naval Offensive 69–70 (Henning Wegener trans., 1975).

37. *See* Starosielski, *supra* note 11, at 10.

38. Ari Kattan, *Emerging Submarine Detection Technologies and Implications for Strategic Stability*, *in* On the Horizon: A Collection of Papers from the Next Generation 62, 63 (2019). Little can or should be said in more detail about undersea surveillance systems in operation today. As to the heyday of SOSUS, see generally Edward C. Whitman, *SOSUS: The "Secret Weapon" of Undersea Surveillance*, Undersea Warfare (Winter 2005); and Gary E. Weir, *The American Sound Surveillance System: Using the Ocean to Hunt Soviet Submarines, 1950–1961*, Int'l J. Naval Hist. (Aug. 2006).

39. On this last point, see Nadia Schadlow & Brayden Helwig, Commentary, *Protecting Undersea Cables Must Be Made a National Security Priority*, Def. News (July 1, 2020), https://www.defensenews.com/opinion/commentary/2020/07/01/protecting-undersea-cables-must-be-made-a-national-security-priority [https://perma.cc/RRP4-DNVN].

40. Starosielski, *supra* note 11, at 49.

41. Kevin Frazier, *On Protecting the Undersea Cable System*, Lawfare (Jan. 12, 2023, 8:16 AM), https://www.lawfareblog.com/protecting-undersea-cable-system [https://perma.cc/3BV2-FWFE].

42. *Id*.

43. *See generally* Lidong Lu, Yuejiang Song, Fan Zhu & Xuping Zhang, *Coherent optical time domain Reflectometry using three frequency multiplexing probe*, 50 Optics & Lasers in Eng'g 1735 (2012) (discussing optical detection techniques).

44. *See* E&T Editorial Staff, *Arctic Fibre-Optic Cable Secures First Investment*, Eng'g & Tech. (Dec. 2, 2022), https://eandt.theiet.org/content/articles/2022/12/arctic-fibre-optic-cable-secures-first-investment/ [https://perma.cc/6RSA-8GLS].

45. *See* Office of the Press Sec'y, *Fact Sheet: President Xi Jinping's State Visit to the United States*, White House (Sept. 25, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-State-visit-united-States [https://perma.cc/ZK2J-FTP4].

46. *See, e.g.,* Martin Giles, *We Need a Cyber Arms Control Treaty to Keep Hospitals and Power Grids Safe from Hackers*, MIT Tech. Rev. (Oct.1, 2018), https://www.technologyreview.com/2018/10/01/139955/we-need-a-cyber-arms-control-treaty-to-keep-hospitals-and-power-grids-safe-from-hackers [https://perma.cc/WG4F-DXLE].

47. Joseph S. Nye Jr., Opinion, *The World Needs New Norms on Cyberwarfare*, Wash. Post. (Oct. 1, 2015), https://www.washingtonpost.com/opinions/the-world-needs-an-arms-control-treaty-for-cybersecurity/2015/10/01/20c3e970-66dd-11e5-9223-70cb36460919_story.html [https://perma.cc/RKT7-J2G3].

48. S. A. Garnham & Robert L. Hadfield, The Submarine Cable 1 (1934).

49. John Steele Gordon, A Thread across the Ocean: The Heroic Story of the Transatlantic Cable xi (2002).

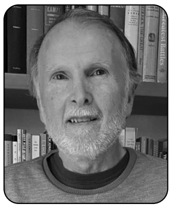
50. Verne, Twenty Thousand Leagues, *supra* note 3, at 353.

The views expressed in this essay are entirely those of the author and do not necessarily reflect the views of the staff, officers, or Board of Overseers of the Hoover Institution.

28 27 26 25 24 23 7 6 5 4 3 2 1

The preferred citation for this publication is John Arquilla, *Securing the Undersea Cable Network*, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 2302 (March 23, 2023), available at https://www.lawfareblog.com/securing-undersea-cable-network.

ABOUT THE AUTHOR



JOHN ARQUILLA

John Arquilla is distinguished professor emeritus of defense analysis at the US Naval Postgraduate School. He is the author of over a dozen books and many articles on a wide range of issues in military and security affairs. His latest book, published by Polity in 2021, is *Bitskrieg: The New Challenge of Cyberwarfare*.

The Jean Perkins Foundation Working Group on National Security, Technology, and Law

The Jean Perkins Foundation Working Group on National Security, Technology, and Law brings together national and international specialists with broad interdisciplinary expertise to analyze how technology affects national security and national security law and how governments can use that technology to defend themselves, consistent with constitutional values and the rule of law.

The group focuses on a broad range of interests, from surveillance to counterterrorism to the dramatic impact that rapid technological change—digitalization, computerization, miniaturization, and automaticity—are having on national security and national security law. Topics include cybersecurity, the rise of drones and autonomous weapons systems, and the need for—and dangers of—state surveillance. The group's output will also be published on the Lawfare blog, which covers the merits of the underlying legal and policy debates of actions taken or contemplated to protect the nation and the nation's laws and legal institutions.

Jack Goldsmith is the chair of the National Security, Technology, and Law Working Group.

For more information about this Hoover Institution Working Group, visit us online at hoover.org/research-teams/national-security-technology-law-working-group.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200

HOOVER INSTITUTION