Bulletin of the Atomic Scientists

ISSN: 0096-3402 (Print) 1938-3282 (Online) Journal homepage: https://www.tandfonline.com/loi/rbul20

Undersea cables and the future of submarine competition

Bryan Clark

To cite this article: Bryan Clark (2016) Undersea cables and the future of submarine competition, Bulletin of the Atomic Scientists, 72:4, 234-237, DOI: 10.1080/00963402.2016.1195636

To link to this article: https://doi.org/10.1080/00963402.2016.1195636

Published online: 15 Jun 2016.

BULLETIN OF THE ATOMIC SCIENTISTS, 2016
VOL. 72, NO. 4, 234–237
http://dx.doi.org/10.1080/00963402.2016.1195636

Routledge
Taylor & Francis Group

Undersea cables and the future of submarine competition

Bryan Clark

ABSTRACT
Today, nearly all voice and Internet traffic, including essential military and financial transmissions, travels through undersea fiber-optic cables. Even temporary damage to these lines of communications can have serious consequences, which is why their future security depends on how well nations understand and exploit the next wave of submarine technology.

KEYWORDS
Cyber security; undersea cables

The two-thirds of the Earth covered by water has traditionally only figured into security strategies as a conduit for commerce and military forces, or as a barrier to potential invasion. This is beginning to change. No longer just a buffer or maritime highway, the seas have begun to represent a territory holding some of the world's most valuable natural and military resources. New technologies enable better tracking and exploitation of these resources in deeper waters. The resulting competition has led countries to pursue territorial claims, or create new territories, to gain control over neighboring seas: In the Mediterranean south of Cyprus, for example, Israel, Turkey, Greece, and Egypt are all vying for ownership of recently discovered oil fields, while in the South China Sea, China is building islands on partially submerged reefs and populating them with military forces and surveillance systems to establish conditions that could enable them to control oil and gas in nearby seabeds, which are also claimed by the Philippines, Vietnam, Taiwan, and Malaysia. The ocean floor also hosts an even more valuable resource than oil and gas: At least 95% of voice and Internet traffic travels through about 300 transoceanic fiber-optic cables along the seabed, including military transmissions and more than $4 trillion per year in financial transactions, all of which could be vulnerable to disruption if nations do not take the right precautions.

Cables, cables, everywhere

Undersea cables date back to the mid-nineteenth century, when the Atlantic Telegraph Company established the first telegraph communications across the Atlantic Ocean in 1858. That initial effort lasted three weeks before failing due to seawater intrusion and corrosion. Despite that early demise, the concept worked and more cables followed, with the first transatlantic telephone cable being completed in 1956. Cables transitioned from copper wire to fiber optic cable in 1988, dramatically increasing their capacity, and helping make possible the bandwidth needed to support the World Wide Web and later the Internet. Today, about 300 submarine cables cross the world's oceans carry everything from phone calls to social media posts to classified diplomatic messages.[1]

National economies now rely on undersea connectivity for a growing portion of their overall output. Today, essentially every consumer or commercial product contains commodities and parts drawn from dozens of separate countries in a "manufacturing chain" of subcomponent builders, product assemblers, suppliers, wholesalers, and retailers. These disparate players are able to seamlessly integrate their efforts using the Internet, enabling greater specialization and economies of scale within each step of the manufacturing process. This, in turn, promotes economic growth in countries that no longer have to either build an entire product domestically with great inefficiency or import it at high cost.

Global manufacturing chains and financial services are made possible by transoceanic cables, and more cable is being laid each year to meet the growing demand for bandwidth. The Asia Pacific Gateway cable, installed in 2014, transmits 55 terabytes of data per second (Tbps) – the equivalent of 100 computer hard drives – between East Asian countries from Malaysia to South Korea, funded in part by Facebook. Similarly, Google helped fund the installation of the FASTER cable between the United States and Japan,

CONTACT Bryan Clark clark@csbaonline.org

which will carry 60 Tbps, and is bankrolling a new 64 Tbps submarine cable between the United States and Brazil. Both content companies are hoping the new networks will increase their user rolls and reduce costs in underserved areas such as Southeast Asia, Latin America, and Africa. Data transmission to these regions with older cables can cost up to 10 times more than to Europe or Japan.

Countries also depend on undersea cables for national security. Aside from their contribution to a country's economic health, nations rely on undersea cables to coordinate military operations, conduct diplomatic missions, and collect intelligence. Radiofrequency circuits used by communications satellites have too little bandwidth to accommodate the terabytes of sensor data recorded by various devices, or to fill operational orders needed to support global military operations. For this reason, classified military communications use the same network of submarine cables as civilian and unclassified data, making them susceptible to eavesdropping taps, the likes of which the United States is reported to have conducted on older copper communication cables during the Cold War.

Tapping today's fiber-optic cables is theoretically possible, but it is easier to cut or damage them and significantly impact the cables' users. And while the exact location of cables is not publicly available, improvements to "bottom survey" equipment and unmanned undersea vehicles are making finding cables easier and faster. In time-sensitive military or diplomatic operations, the loss of communications for a few minutes or hours can be catastrophic. With financial transactions, the loss of even fractions of a second can cost millions of dollars as high-speed trades miss their targets and other transactions fail to go through or are lost entirely. The dozens of cable outages that occur each year do not cause a complete loss of service, but they do slow data-transfer speeds as information is re-routed through fewer intact cables. Most of these cable breaks happen in relatively shallow water, when rough weather moves cables around until they break or fishing trawlers catch a cable in a net. Some outages, however, have more nefarious origins. In 2013, three divers with hand tools cut the main cable connecting Egypt with Europe, reducing Egypt's Internet bandwidth by 60%.

Repairing a submarine cable at sea is difficult and time consuming. First the break has to be located using built-in monitoring systems that can indicate the cable segment in which the break is likely to have occurred. Cable repair ships then must go to that location and pull up the cable until they get to the damaged spot. A new section of cable can then be spliced in, which can take several days to complete.

In addition to the cables themselves, their onshore termination points are particularly vulnerable – and easier to find than a submerged cable. Sometimes consisting of a non-descript building on a beach or marshland, these locations are often the junction of several cables that are then connected with terrestrial phone and cellular networks. An accident or attack on one of them could have the same effect, in the short-term, of cutting multiple cables at once. Because they are easier to monitor, a break at the termination point could be diagnosed more quickly; but it may be harder to repair because more damage could be caused to an exposed cable than one hundreds of feet underwater.

As more cables are installed on the ocean floor, redundancy will increase the resilience of communication networks. But as the case of Egypt shows, the reduction of bandwidth from cutting one or more cables can still be significant. Although communications are not completely lost, lowered bandwidth may have a similar effect on time-critical transmissions as a complete loss of connectivity. For example, stock exchanges must be tightly synchronized for buyers and sellers to work off the same prices. Similarly, military cryptology systems tie codes to time standards; if bandwidth goes down, networks can "drop synch" and be unable to properly decode messages.

Given the likely economic and military impacts of cable breaks, the ability to threaten or protect submarine cables and their shore landings will be increasingly important in future conflicts. In a crisis, an aggressor could use multiple coordinated attacks on cables to compel an opponent to back down or employ them as part of an opening offensive to cut off the defender's military forces from national commanders, intelligence data, and sensor information. Cable attacks could also be highly destabilizing, since they could prevent a nuclear-armed opponent from controlling and monitoring its strategic weapons and early-warning systems. In response, the country targeted could choose to place its nuclear weapons in a higher alert condition – or initiate a preemptive attack.

Exploiting the unmanned revolution

New technologies are increasing the threat to submarine cables, but they could also be leveraged by nations to defend their undersea infrastructure.

Power and control improvements are increasing the endurance and reliability of unmanned undersea vehicles (UUVs), which should be able to operate unrefueled for months at a time within the next decade. The

autonomy of these vehicles will remain constrained, however, by the quality of their sensors. For example, while one may have the computer algorithms and control systems to avoid safety hazards or security threats, it still may only have a fuzzy picture of its surroundings. In the face of uncertain data, a human operator can make choices and be accountable for the results. Commanders may not want to place the same responsibility in the hands of an unmanned control system – or its programmer.

As sensors and processing improve, UUVs will progressively gain more autonomy in operating safely and securely while accomplishing their missions. In the meantime, navies can have unmanned vehicles take on missions where the consequences of an incorrect decision are limited to the damage or loss of the vehicle, rather than the loss of life or an unplanned military escalation. These missions could include surveying undersea cables for damage or tampering, attacking enemy undersea cables and infrastructure, conducting surveillance for threats near friendly ballistic-missile subs (known as SSBNs), or deploying payloads on the sea floor such as sonar arrays and inactive mines. For missions where a human decision maker is required, unmanned systems will need to operate in concert with nearby submarines or use longer-range communications to "check-in" with commanders.

Communications, however, are a longstanding vulnerability of undersea platforms. New or improved undersea communication methods will likely enable submarines and UUVs to communicate with each other, with systems on the ocean floor, and with commanders back home without having to expose a mast. Acoustic communications are increasingly able to function over operationally relevant distances with low bandwidth, while at shorter ranges light-emitting diodes and lasers can achieve nearly the same data rates as wired systems. And new floating or towed radio transceivers enable submerged platforms to communicate with forces above the surface without risking detection.

The limitations of undersea communications and UUV endurance can also be mitigated by a new generation of seabed systems in development. The US Navy's Forward Deployed Energy and Communications Outpost is a shipping container-sized system that can be placed on the ocean floor to act as a rest stop where unmanned vehicles can download data and upload orders while recharging their batteries. The outpost would enable UUVs to conduct sustained operations such as cable- and oil-infrastructure monitoring and surveys, or listening for adversary submarines in SSBN patrol areas. And, in turn, the outpost would communicate with shore using "data mule" UUVs that carry information between it and fiber-optic cable networks that connect to commanders and intelligence analysts ashore. To conduct sustained undersea surveillance in areas where permanent sonar arrays cannot be installed due to time or operational constraints, portable seabed sensors such as the Shallow Water Surveillance System and the Persistent Littoral Surveillance system can be placed in areas such as chokepoints where enemy submarines or UUVs are likely to travel.

The next chapter in undersea competition

The wide availability of new processing and sensor technology and the increased exploitation of ocean resources are making undersea expertise more broadly available around the world. The competition to monitor and control the undersea world will increase over the next one to two decades, defined by some significant changes in how undersea warfare is conducted:

- *A new predominant sensing technology*. The effectiveness of traditional passive sonar will decline as submarines become quieter, their stealth is enhanced with countermeasures, and countries deploy more UUVs that radiate little noise. While anti-submarine warfare relied primarily on passive sonar for the last 50 years, the dominant detection method by the 2020s may be low-frequency active sonar, non-acoustic detection, or some other previously unexploited technique made possible by ongoing technological advances.
- *Undersea families of systems*. Undersea warfare will increasingly shift from submarines to unmanned systems such as UUVs. Large unmanned vehicles and other deployed systems that are smaller and less detectable could be used to a greater degree instead of manned submarines for tactical missions close to enemy shores including searching for adversary SSBNs or attacking the opponent's undersea infrastructure. On defense, UUVs and seabed sensors will be needed for sustained surveillance of friendly submarine cables and energy pipelines and systems.
- *Undersea "battle networks."* New longer-range sensors and emerging undersea communication capabilities will enable undersea fire control network operations analogous to those that use radio signals above the surface of the water. Undersea networks could also enable coordinated surveillance or attack operations by swarms of UUVs operating autonomously or controlled from a manned submarine or other platform.

- *Seabed warfare*. Deployed and fixed sensors and UUVs supported by outpost systems could augment submarine capacity and be managed by them during a conflict. Increased reliance on these capabilities will create a competition in the ability to place or eliminate systems on the coastal seabed, including capabilities for rapidly surveying and assessing the sea floor. Countries with the better capabilities to use undersea terrain are likely to have the upper hand in a conflict, in particular during early phases when a catastrophic attack on submarine cables or ballistic-missile subs could be highly destabilizing.

Stability in international relations depends in part on predictability, and the ability of targets to detect attacks and respond appropriately. Emerging changes in undersea warfare threaten to undermine today's relative stability – including essential underwater infrastructure like submarine cables – through the loss of surveillance information and command-and-control capabilities, or risks to "second strike" nuclear capabilities of ballistic-missile submarines. To sustain their national security and preserve stability, large economies and nuclear powers will need to improve their ability to monitor and control the waters off their shores, just as they do the skies above their lands.

Note

1. For a comprehensive map of these cables, see: http://www.submarinecablemap.com/.

Disclosure statement

No potential conflict of interest was reported by the author.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Notes on contributor

Bryan Clark is a senior fellow with the Center for Strategic and Budgetary Assessments, in Washington.