


CABLE VISION

By Captain Douglas R. Burnett,
U.S. Navy (Retired)

Note to Navy: It's time to pay attention to security for undersea cables—crucial to global communications and commerce, and vital to our national interests.





Underwater (submarine) cables have been part of international communications since 1850, but the strategic importance of the vital infrastructure crossing our oceans has never been more critical than it is today. Given the marine environment in which the extensive and growing networks are laid and maintained, navies are singularly qualified to safeguard them. Any modern understanding of sea power must take into account both the cables and the security challenge they present, especially when it comes to protecting the communications grid from the hostile actions of pirates and terrorists.

Submarine Cable or Satellite? No Contest

The importance of modern fiber-optic cables to the global economy and the Internet cannot be overstated. In the case of the United States, about 36 submarine cables, each the diameter of a garden hose, carry more than 95 percent of the nation's international voice, data, and video communications.

Every day the Society for Worldwide Interbank Financial Telecommunications transmits 15 million messages over cables to more than 8,300 banking organizations, securities institutions, and corporate customers in 195 countries. The Continuous Linked Settlement Bank located in the United Kingdom is just one of the critical market infrastructures that rely on those transmissions, providing global settlement of 17 currencies having an average daily equivalent of approximately \$3.9 trillion. Similarly, the U.S. Clearing House Interbank Payment System processes in excess of \$1 trillion a day to more than 22 countries for investment companies, securities and commodities exchange organizations, banks, and other financial institutions.

The popular belief that international communications are carried largely by satellite is false. The tremendous volume of data carried on less expensive, modern fiber-optic submarine cables dwarfs the limited capacity of the higher-cost satellites. Additionally, the technical transmission delays and other quality limitations inherent in satellites make them marginal for continuous transmission of high-speed voice, video, and data traffic. If the cables connecting the United States to the world were cut, it is estimated that every single satellite in the sky combined could carry only 7 percent of the current total traffic volume.

Referring to the submarine cable networks, the Federal Reserve's staff director for management, Stephen Malphrus, observed that "when the communica-

tion networks go down, the financial sector does not grind to a halt, it snaps to a halt." The same can be said for most sectors enmeshed in the global economy through the Internet, including shipping, airlines, and manufacturing.

The United States is by no means unique. With the laying of cables along the east coast of Africa in 2009–10, the last major group of nations now has access to the world's submarine network. It is the physical tie that binds the world together, allowing torrents of digital data, video, and telecommunications to course throughout the world uninterrupted on a 24/7 basis.

'Cable Maintenance 101' for Naval Officers

Naval forces need to be aware of how cables and cable ships operate internationally. There is no central worldwide cable network any more than there is a central world airline or shipping network. The world's cable network is composed of numerous independent systems that cumulatively allow the Internet and other forms of international communications to flourish. That network—parts of it 160 years old—is the result of the close cooperation and entrepreneurial work of about 124 companies in roughly 62 nations.

On average there are 200 submarine fiber-optic cable faults worldwide each year. Most of these (up to 77 percent) are caused by anchors and fishing gear. Disturbingly, an unprecedented number of hostile actions by terrorists and pirates have been recorded recently.

Such acts raise vulnerabilities, for each cable system effectively functions as a backup—available for rerouting the traffic from a damaged system. Thus anytime a cable is damaged, there is one less restoration path; the risk of more widely spread communications disruptions increases.

Cable repair is an expensive and complex marine operation requiring specially designed ships carrying highly trained crews and skilled engineers. Cable repairs are not directed by national governments, but by contracts. For efficiency and economy, the contracts are pool agreements among cable owners, who charter one or more ships dedicated to the repair of cable systems in a particular region. The ships are strategically based at regional ports and maintained in a high state of readiness. Contractually, they are obligated to sail—with a trained crew and spares for repair—within 24 hours of a cable-fault notification.

Currently there are ten such agreements spanning the globe. Five are "zone" agreements, contracts between consortiums of cable owners and cable-ship owners: The Atlantic Cable Maintenance Agreement (ACMA); the Mediterranean Cable Maintenance Agreement (MECMA); the North American Zone (NAZ); the Yokohama Zone Agreement (YOKO-

NATIONAL STEEL AND SHIPBUILDING

The Navy's only cable ship, the USNS Zeus (T-ARC-7) sports a distinctive bow designed for cable work. The Navy is one of the largest submarine cable owners in the world, but its system is used for acoustic monitoring and sensors, not telecommunications. The author believes there is a significant role for international navies in keeping the world's undersea communications networks secure from terrorism and other acts of deliberate destruction.



Above, the areas covered by the five “zone” agreements for submarine cable systems as well as the base ports for many of the “private” agreements. At any given time roughly half of the world’s more than 40 cable ships are laying new lines while the other half are either contractually performing maintenance/repair or are on standby.

HAMA); and the South East Asia Indian Ocean Cable Maintenance Agreement (SEAIOCSMA).

The five “private” agreements—arrangements between individual cable owners and ship owners—are the Atlantic Private Maintenance Agreement; North Pacific Marine Maintenance Service Agreement; EMarine Agreement (Indian Ocean and Arabian Gulf); South Pacific Agreement (former Fiji Zone area); and the South African Maintenance Agreement.

In aggregate, the ten agreements involve 21 cable ships, about half of the world’s total. The agreements have proved reliable over time for the routine maintenance of cables.

The Gap in Maritime Security

Routine maintenance, however, does not include security. As scholar Robert Beckman of Singapore’s Centre for International Law noted, when it comes to security, submarine cables are international orphans. While the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation addresses the security of vessels, navigational aids, and offshore facilities with regard to terrorism, protection of submarine cables is overlooked.¹

Currently, terrorist and pirate attacks on cables lying outside territorial seas are unlikely to be considered crimes under international law and most national laws. Even if considered a crime, there is no forum, political will, or

any effective means to bring the perpetrators to justice. In that sense, such acts are reminiscent of the piracy debacle off Somalia, in which pirates caught by navies are more likely to be provided humanitarian assistance and freed to attack again, under a notorious “catch-and-release” policy, rather than being tried and punished before the national court of the warship effecting their capture.

International treaties require states to enact laws providing for criminal sanctions against wrongdoers and vessels that injure international cables willfully or by culpable negligence.² But compliance is poor.

Australia and New Zealand have modern and extremely effective deterrent laws that generally comply with the U.N. Convention on the Law of the Sea (UNCLOS). In both nations proactive monitoring of cables and effective enforcement of domestic laws has essentially reduced cable faults to zero. But other countries, such as the United States and the United Kingdom, have telegraph-era statutes dating to the 1880s that are historical relics having virtually no practical utility.

In the United States, for example, the intentional destruction of an international submarine cable is subject to a ridiculously lenient maximum fine of \$5,000 and a prison term of six months.³ The only known attempt to use the archaic law came in 1997, when the U.S. Coast Guard recommended to the U.S. attorney in Florida that

the skipper of a fishing vessel be prosecuted for willfully damaging the U.S.-Cuba cable. The attorney declined to prosecute, deeming the pursuit of a conviction carrying such a paltry penalty to be an inefficient use of his resources. Additionally, that sort of handicap for U.S. telecommunications companies is significantly compounded because the United States has not joined the 162 nations that are parties to UNCLOS. Thus there is no UNCLOS protection for their cables outside U.S. territorial seas.

While the United States justifiably can be criticized for allowing its domestic law protecting cables to sink into obsolescence, many nations have no laws whatsoever addressing damage to international cables—even though their economies depend on the critical global infrastructure.

A Cause for International Concern

That security gap should be of international concern for a number of reasons. The first successful hostile actions by pirates and terrorists against active international cables already have occurred. In March 2007 Vietnamese pirates in multiple vessels carried out high-seas depredations on two active submarine cable systems, including the theft of optical amplifiers that rendered the systems inoperative for 79 days until replacements could be manufactured.⁴ At the time, cable owners urgently pleaded with at least four nations for help in preventing additional attacks, only to learn that none of those governments had contingency plans for such action. Similar damage was inflicted on a newly laid cable in Indonesian archipelagic waters in 2010.

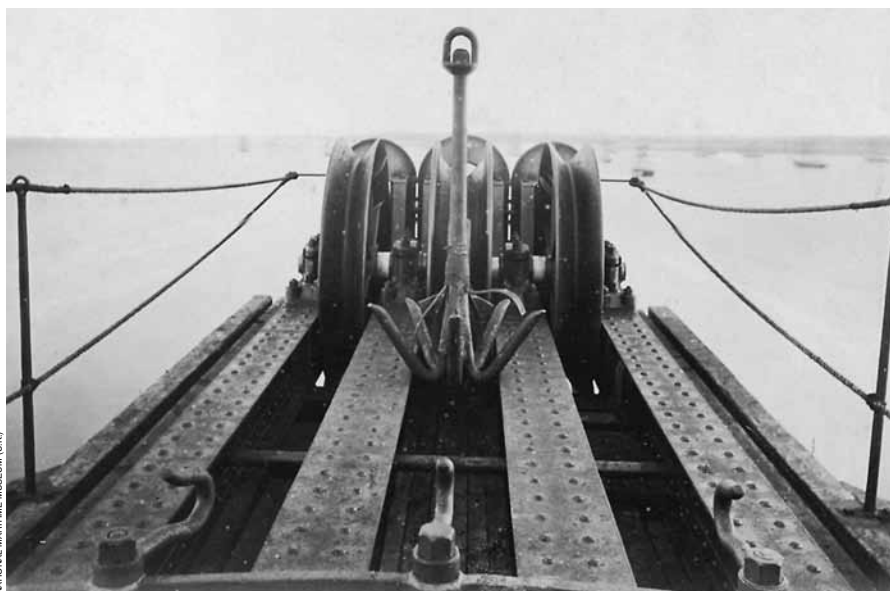
Submarine cables are legitimate targets of belligerents in war.⁵ The United States cut cables linking Spain to its colonies during the Spanish-American War.⁶ The first offensive action of Britain's Royal Navy in World War I was cutting Germany's international links to the rest of the world by severing its cables.⁷

But attacks on cables by terrorists are new. On 11 June 2010, terrorists in the Philippines successfully struck an international cable.⁸ It is naïve to assume that submarine-cable landing stations, cables, the cable ships, and the marine depots that maintain the systems will escape asymmetric terrorist acts.

Contrary to the belief of many, the location of international submarine cables is public information. Cables must be shown on nautical charts so mariners can avoid them. And it is not just seabed cable locations that are readily known—so are the locations of cable landing stations and their connection paths to the cables.

In a case well known within the industry, an anarchist website in New York City in 2006 published the locations (and photographs) of all of the cable stations, beach man-holes, and cable routes in the United States, including security safeguards and access points. Communications companies appealed unsuccessfully to the FBI to intervene, but the agency responded that all the information had come from public sources such as zoning applications, easements, environmental studies, local and federal permit applications, and nautical charts. All the anarchist had done was collect and publish the information on the Internet.

No international organization is responsible for cables in even a general sense, let alone for security, and the purpose here is not to advocate the creation of such a body. There is no need for a new international entity to micro-manage one of the most successful international uses of the world's oceans. The more effective alternative is for nations to meaningfully meet UNCLOS obligations—enacting and enforcing modern cable-protection domestic laws and partnering with the submarine-cable industry on security.



The grappling hook and part of the cable-laying mechanism of the SS *Great Eastern* circa 1865. Designed and launched as an oceanliner with a capacity for 4,000 passengers, she was sold and converted to a cable ship just four and a half years after her maiden voyage. She laid the first lasting transatlantic telegraph cable in 1866.

The cable industry is asking for help with the threats that piracy and terrorism pose. Companies can and do take measures to maximize security for their cable systems in the nations where they land and on board cable ships. Armed crews and guards on those ships and escort vessels are standard in pirate waters. But assistance is needed on an international basis, especially in getting timely, rapid, and effective help in areas outside of territorial seas.

Why Naval Partnerships Make Sense

The cable industry repeatedly has gone on record asking to partner with governments to reduce the risk of hostile actions by terrorists and pirates on submarine cables and

cable-repair ships and to facilitate prompt repair of international cables. The request is threefold.

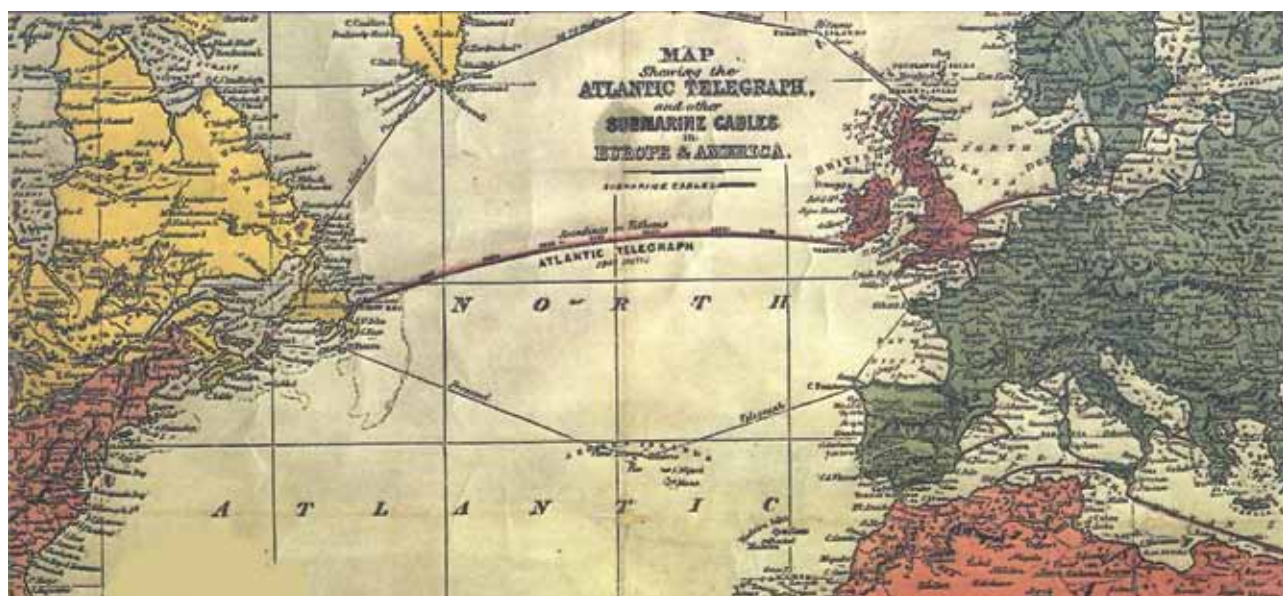
First, governments should have a single point of contact for cable-system owners and cable ships to report suspicious or hostile actions. The single point of contact would be authorized to coordinate with other government agencies and initiate fast action. To date, only Australia and Singapore have designated such single points of contact. That solution sounds simple and obvious, but the reality is much more complicated.

In most nations many agencies have some involvement with submarine cables. In the United States, for example, the following agencies have some link with international cables: Department of State, Department of Defense, Department of the Navy, U.S. Army Corps of Engineers, National Oceanic and Atmospheric Administration, Department of Commerce, Federal Communications Commission, National Security Agency, Central Intelligence Agency, and the Department of Homeland Security. And that's not to mention various state coastal-zone-management agencies. Each of those agencies owns a piece of the submarine cable governance role. But no single agency

sonnel from a U.S. Navy destroyer boarded a Russian trawler that had cut several transatlantic cables linking the United States and Canada with Europe.¹⁰ Besides operating its own cable ship, the Navy also employs well-regarded experts in submarine cable-laying and repair in the Naval Seafloor Cable Protection Office. Those experts work in close contact with the cable industry worldwide on a daily basis. Finally, the Navy has strong existing working relationships with other navies worldwide. Taken together, the U.S. Navy and its partner navies could markedly enhance submarine-cable security.

Second, international cables by nature involve two or more nations. Making one country's cable infrastructure impregnable is meaningless if security is lax in the country where the cable lands. The problem is more acute on the high seas, where no nation enjoys the sovereignty it has for security in its own territorial waters. The unresolved issue is getting international naval cooperation and action in a timely, dependable, and effective manner.

The cable industry has requested that international war games involving both navies and industry be conducted to develop procedures and to practice tactics to reduce



Submarine cables have been in use for more than 150 years. A cable was successfully laid connecting Newfoundland to Ireland in 1858, just 14 years after the invention of the telegraph. That cable was not well constructed and lasted little more than a month. A permanent cable connection was made in 1866.

is in charge. As a result, notification to any agency is likely to be ineffective. Decisive follow-through action is even less likely, because each agency operates in its own limited realm. No coordination mechanism is in place to make timely national decisions, let alone to liaison with foreign governments in an emergency.

Navies have an important role to play. Under international law, the commanding officer of a warship has authority on the high seas to board vessels suspected of damaging an international cable, to carry out a full investigation, and to obtain evidence for use in national courts.⁹ That authority was successfully used in 1959 when per-

the risk from pirates and terrorists against international cable-repair ships and cables.

Australia on a domestic scale conducted a very innovative and successful "Submarine Communications Cable Desktop Exercise" in March 2009 that brought together government agencies, defense forces, and submarine cable, banking, and other vital industries to test the protection, repair, and restoration of submarine cables. The next logical step is to expand that into similar exercises carried out on a bilateral or multilateral basis.

The U.S. Naval War College should reach out to traditional naval allies such as the United Kingdom, Canada, Australia,



LONNIE HAGADORN

Roughly 550,000 miles of undersea telecommunications cables—enough to circle the planet more than 22 times—keep the world connected. Much of it, as seen in this display, is no larger in diameter than a U.S. quarter, or about the size of an ordinary garden hose.

will form partnerships of common interest to counter these emerging threats.

Protection of international submarine cables from terrorists and pirates is an ideal candidate for government and private-sector partnerships. Recognizing that need, in 2010 the International Cable Protection

lia, France, New Zealand, Singapore, and to cable industry representatives in those nations to develop and test cable-protection strategies and protocols that would enable navies to move quickly to suppress and deter pirates or terrorists who threaten cables or interfere with cable repair vessels.

The use of the Automatic Identification System (AIS) in partnership with the cable industry in particular should be an essential feature of such war-gaming. In that regard, the model relationship that exists between the U.K. coast guard and British Telecom merits emulation. Singapore, Malaysia, and Indonesia also have taken bold steps to partner with the regional cable industry on AIS-sharing and in working with the International Maritime Organization to control shipping threats to cables in regional waters.

Such exercises also can work out protocols on assisting cable-repair ships that suffer interference from fishing or other types of vessels. Notwithstanding the requirement under international law for all vessels to maintain a distance of one nautical mile from a cable ship displaying the required day shapes and lights for cable laying or repairs, such interference unfortunately is commonplace in some regions. International naval exercises involving the cable industry could lead to improvements in navigation safety for cable-repair ships as well as enhanced communication security.

Finally, having the various government agencies coordinated and responsible to a single point of contact with the cable industry is something that can be developed only with practice. War games provide a practical mechanism to iron out problems and communications so response is rapid and effective in an actual emergency. As protocols are developed and tested, the number of nations involved can be expanded.

A Cooperative Strategy for 21st Century Seapower states that

Increasingly, governments, non-governmental organizations, international organizations and the private sector

Committee, the key international organization of cable-system owners and cable-ship operators, opened its membership to national governments.

The challenge of security for the world's undersea cable network is real. Governments and their navies can act with foresight to implement an effective international partnership with the cable industry. Or they can muddle through security challenges and react belatedly and ineffectively. But when pirates and terrorists strike, let it not be said that no one in the cable industry ever asked for help. ❄

1. Convention for the Suppression of Unlawful Acts of Violence Against the Safety of Maritime Navigation (10 March 1988) and 2005 Protocol for Suppression of Unlawful acts of Violence Against the Safety of Fixed Platforms on the Continental Shelf ("SUA Convention").
2. See the International Convention for Protection of Submarine Cables (14 March 1884), T.S. 380. ("Cable Convention"), art. 2; the Geneva Convention on the High Seas (29 April 1958), 13 U.S.T. 2312, T.I.A.S. 5200, 450 .N.T.S. 82, art. 27 and the United Nations Law of the Sea (1982) ("UNCLOS"), art. 113.
3. 47 United States Code § 21.
4. Green, M. and Burnett, D., "Security of International Submarine Cable Infrastructure: Time to Rethink?" *Legal Challenges in Maritime Security*, Center for Oceans Law and Policy (2008) p. 557.
5. Cable Convention, art. 15; Eastern Extension Australia and China Telegraph Company Limited (Great Britain) v. United States, 6 Rep. J. Int'l Arb. Awards 112 (Arb. 1923)
6. "Right to Cut Cables in War – Admiral Dewey Created a New Precedent Under the Law of Nations in Manila Bay," *The New York Times*, 24 May 1898.
7. Massie, R., *Castles of Steel*, (New York: Random House, 2003) p. 77.
8. "Reds Bomb Cagayan Globe Site, Disarm Cop, Guards," Alfred Dalizon, *People's Journal*, 11 June 2010.
9. Cable Convention, art. 10.
10. *The Novorossiisk*, Department of State Bulletin Vol. XL, No. 1034 p. 555 (20 April 1959).

Captain Burnett is a 1972 graduate of the U.S. Naval Academy and a retired surface warfare officer. He holds a law degree from the University of Denver. As a partner in an international law firm, he specializes in shipping and ocean industry issues and is legal adviser to the International Cable Protection Committee.