Strategy Research Project

The Protection of Undersea Cables: A Global Security Threat

by

Commander Michael Matis
United States Navy

United States Army War College
Class of 2012

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
07-03-2012	Strategy Research Paper	

4. TITLE AND SUBTITLE

The Protection of Undersea Cables: A Global Security Threat

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

CDR Michael S. Matis

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Captain Stephen Krotow, USN
Director, National Strategic Studies
Department of National Security and Strategy

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution A: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Undersea cables are vital infrastructure to the global economy and the world's communication system. Undersea cables account for 95% of the world's international voice and data traffic (Military, Government, Emergency Response, Air Traffic, Subway, Rail, and Port Traffic) while satellites account for less than 5%. The protection of these cables and their vulnerabilities to man-made and natural disruptions are important to the global community and in need of an overarching organization to coordinate information sharing among the various entities tasked to minimize cable disruptions. The lack of any agreed upon international, tiered protection scheme for global undersea cable routes or a global grid restoration plan represents critical global infrastructure vulnerability. My vision recommends a new undersea cable construction regulatory regime potentially modeled after the Maritime Safety and Security Information system (MSSIS). MSSIS was developed by the U.S. Navy Command Sixth Fleet and the U.S. Department of Transportation's Volpe Center as an unclassified, multinational, freely shared, automatic identification system (AIS) network that tracks the location of merchant ships.

15. SUBJECT TERMS

Fiber Optics, Networks, MSSIS, UNCLOS, Infrastructure

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER *(include area code)*
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED	28	

USAWC STRATEGY RESEARCH PROJECT

THE PROTECTION OF UNDERSEA CABLES: A GLOBAL SECURITY THREAT

by

Commander Michael Matis
United States Navy

Captain Stephen Krotow
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Commander Michael Matis

TITLE: The Protection of Undersea Cables: A Global Security Threat

FORMAT: Strategy Research Project

DATE: 07 March 2012 WORD COUNT: 5,265 PAGES: 28

KEY TERMS: Fiber optics, Networks, MSSIS, UNCLOS, Infrastructure

CLASSIFICATION: Unclassified

Undersea cables are vital infrastructure to the global economy and the world's communication system. Undersea cables account for 95% of the world's international voice and data traffic (Military, Government, Emergency Response, Air Traffic, Subway, Rail, and Port Traffic) while satellites account for less than 5%. The protection of these cables and their vulnerabilities to man-made and natural disruptions are important to the global community and in need of an overarching organization to coordinate information sharing among the various entities tasked to minimize cable disruptions. The lack of any agreed upon international, tiered protection scheme for global undersea cable routes or a global grid restoration plan represents critical global infrastructure vulnerability. My vision recommends a new undersea cable construction regulatory regime potentially modeled after the Maritime Safety and Security Information system (MSSIS). MSSIS was developed by the U.S. Navy Command Sixth Fleet and the U.S. Department of Transportation's Volpe Center as an unclassified, multinational, freely shared, automatic identification system (AIS) network that tracks the location of merchant ships.

THE PROTECTION OF UNDERSEA CABLES: A GLOBAL SECURITY THREAT

Many people around the world believe that their emails and phone messages are being sent through satellites. They are mistaken because satellites account for less than 5%.[1] Global telecommunications development began about 150 years ago with the first commercial international submarine cable, laid between Dover, England and Calais, France in 1850. In 1858, the first trans-Atlantic telegraph cable linked London with the new world, via Newfoundland.[2] The 143 words transmitted in 10 hours, replaced a one-way dispatch that would have previously taken about 12 days.[3]

In the last 25 years, there has been a stunning growth in undersea cables because of the communications revolution triggered by the internet. Undersea cables account for 95% of the world's international voice and data traffic (Military, Government, Emergency Response, Air Traffic Control, Subway, Rail, and Port Traffic).[4] Financial markets utilize undersea cables to transfer trillions of dollars every day. In 2004 alone, nine million messages and approximately $7.4 trillion a day was traded on cables transmitting data between 208 countries.[5] As a result, submarine (undersea) cables are vital infrastructure to the global economy and the world's communication system.

Douglas Burnett, a legal expert on undersea cables notes that international banking institutions process over $ 1 trillion dollars per day via undersea cables. Any disruptions of these cables would severely impact global banking. Indeed, Stephen Malphrus, Chief of Staff to Federal Reserve Chairman Ben Bernanke, recently noted, "When communication networks go down, the financial services sector does not grind to a halt, rather it snaps to a halt.[6] Even though there are hundreds of cables crossing the global seabed, there are just not enough undersea communication network

redundancies available to handle the vast amount of bandwidth needed to keep global banking transactions in check.

The locations of cables on the bottom of the ocean are available to various professions such as mariners, commercial bottom fisherman and undersea seabed developers so that they do not damage them by mistake. The location of these cables is “open source” information and anyone can access them via the Internet. Information on cables is routinely reported to the three major hydrographic authorities that issues worldwide charting. The National Oceanographic Data Center (DMA/NOAA) in the United States, the Admiralty hydrographic office in the United Kingdom (UK), and the Marine Hydrographic and Oceanographic Service (EPSHOM) in France. Without knowing their exact locations, Mariners inadvertently damage cables by dropping ship anchors or dredging near their vicinity. Commercial fishing trawlers drag fishing nets along the sea floor to catch large schools of fish, and in order for these vessels to avoid damaging the cables, they have access to the exact locations of the cables. Seabed developers are those entities that explore the ocean bottom for minerals or oil deposits. If the undersea cables were cut at the locations publicized to mariners, fisherman and/or seabed developers around the U.S. coast, the response capability to restore these cables would not be able to quickly and efficiently repair them because there are not enough cable repair vessels in the area.

Destruction of submarine cables can cripple the world economy to include the global financial market and/or Department of Defense (DoD). An example which reflects the importance of this strategic communication capability took place on December 26, 2006, when a powerful earthquake off Southern Taiwan cut 9 cables and

took 11 repair ships 49 days to restore. The earthquake affected Internet links, financial markets, banking, airline bookings and general communications in China, Hong Kong, India, Singapore, Taiwan, Japan and the Philippines.[7] When a cable loses service, it has a definite, but difficult impact to the global financial sector. The International Cable Protection Committee (ICPC) legal advisor estimates that interruptions of underwater fiber optics communications systems have a financial impact excess of $1.5 million per hour.[8] These estimates target operators that utilize cable bandwidth for day-to-day operations and companies or government entities that own bandwidth on the disrupted cable.[9]

In summary, this paper assumes protection plans for the security of undersea cables are an on-going national as well as a global interest. Submarine cables that originate in the U.S. are much safer than their destination end, which in turn, can inadvertently disrupt our economic well being if they are cut outside of our jurisdiction. The issue is that in a globalized environment, the U.S. cannot act alone because we cannot protect all the undersea cables. Current U.S. strategy to ensure cable connectivity outside of our territorial waters allows the cable industry to coordinate information sharing with foreign cable industry entities around the globe. This cable strategy is complex, cumbersome, and confusing because there is no organization in the U.S. tasked to coordinate information among the various entities that encompass global undersea cable security. This paper details potential threats to vitally important undersea cables and identifies several strategic approaches to mitigating those vulnerabilities.

Undersea Cable History

The history of undersea cables started in 1795 when a Spaniard named Salva suggested the idea of underwater telegraphic communication.[10] Samuel Morse demonstrated “Morse Code” in 1844 and patented the design in 1850. The first undersea (telegraph) cable was laid between England and France in 1850, by the Gutta Percha manufacturing company.[11] The cable was wrapped in a natural rubber (Gutta Percha) which was an effective insulator extracted from plant life, but damaged easily. After being inadvertently cut by a French fisherman within 24 hours of operation, heavy armor wrapping was utilized to protect the gutta percha.

The first trans-Atlantic (telegraph) cable was laid between Ireland and & Newfoundland in 1858 and failed after 26 days of operation.[12] A new type of undersea (telegraph) cable was laid in 1866, which utilized copper to telegraph messages at 12 words a minute.[13] This cable had three layers of gutta percha insulation wrapped around a core of seven strands of copper. There were 300 tons of gutta percha insulation utilized for the 2,500 nautical miles journey between the United Kingdom (UK) and U.S and they were described as the eighth wonder of the world emphasizing cooperation between the UK and the U.S.[14]

The next phase of undersea cable capabilities came in 1884; when the first underwater telephone cable service was established from San Francisco to Oakland.[15] The shortwave radio revolutionized global communications in the 1920s because of its capability to carry voice, picture and telex traffic via radio waves. In 1947, polyethylene replaced gutta percha as a preferred insulator. The invention of repeaters in 1940 allowed the cable to have a capacity of 36 telephone calls at a time, and costed $12 for the first 3 minutes.[16] Repeaters are critical equipment associated with analogue cables,

and installed along the cable to boost the signal along the route from point A to B.[17] Repeaters were first utilized in the 1956 trans-Atlantic (TAT-1) and started a shift to high quality telephone calls across the globe. There was also a technology shift towards a higher quality global network capability in 1961 which provided the capability to transmit multiple calls at one time and carried a few hundred words per minute.

The largest technology jump in undersea cable networks took place with the development of the first international fiber-optic cable between Belgium and the UK in 1986. In 1988, the first Atlantic fiber-optic cable, (TAT-8) was installed and had a capacity for 40,000 simultaneous phone calls, which was ten times that of the most capable copper cable of the day. In terms of today's undersea cable capabilities, each fiber pair within a cable has the capacity to carry information, including video, equivalent to 150,000,000 simultaneous phone calls.[18] Almost all transoceanic telecommunications are now routed via the submarine cable networks and fiber-optic cables can carry up to 30 million telephone channels per minute.[19]

Modern undersea cables rely on a property of pure glass fibers, where light is transmitted by internal reflection. Because the light signal loses strength from point A to B, optical amplifiers are installed to boost the signal. In order for information to reach its destination, these new cables rely on optical amplifiers (repeaters) to boost the glass strands which contain an element called erbium.[20] These strands are spliced at intervals along a cable and then energized by lasers that cause eribium doped fibers to boost optical signals to a capacity that is currently near nine tera bits per second (Tbps).[21] In telecommunications, bit rate or data transfer rate is the average number of bits, characters, or blocks per unit time passing between equipment in a data

transmission system. The importance of modern fiber-optic cables to connect the world at such high speeds utilizing “tbps” allows the financial world to transmit trillions of dollars daily in a region like the U.S., London, Taiwan, China, and Hong Kong.[22]

Cable repair vessels are specifically built to spool the cable out of huge holding tanks and are suited to lay cable in the deepest oceans of the world. Cable repair is an expensive and challenging marine operation requiring highly trained crews and engineers. Some of these vessels have the technological capability to dynamically position their vessel without the use of anchors and utilize state of the art equipment such as underwater remote operated vehicles (ROVs). These repair vessels are able to maintain position in weather conditions up to Beaufort number 7 sea state, while laying and/or repairing cables.[23]

Since cable repairs are not directed by national governments, but by contracts, cable owners charter vessels that are strategically located in a particular region around the globe. Contractually, they are obligated to sail with a trained crew and spare parts for repair within 24 hours of a cable fault notification.[24] It takes an average of one to two weeks for a cable break to be fixed by one of these repair vessels.[25] The uninterrupted dependability of undersea cables maintaining continuity is becoming a challenge due to globalization. Globalization is requiring the dependency on instantaneous data amongst countries, and in order to maintain around the clock vigilance on undersea cables, the network will either require additional cable repair vessels to quickly fix breaks or have additional cables as a back-up.[26]

Undersea Cable Vulnerabilities and Threats

The U. S. has an appetite for internet usage that is second only to China. In order to supply this appetite of information movement around the globe, undersea

cables are inter-connected amongst various countries such as Taiwan, China, England, and Norway. Undersea cables connect the U.S. on both the East and West coast to the outside world via 36 undersea cables, each the diameter of a garden hose.[27] The beginning and ending points of undersea cable systems are landing stations. Landing stations serve as a termination point for the undersea cables and provide a gateway to landline communication networks.[28] Due to the large amount of movement (human traffic) such as fishing boats and underwater infrastructure such as gas and water pipelines near beaches, (especially on the East Coast of the U.S.), cable companies have limited access to coastal areas to connect the undersea cables to the landing stations.[29] The limited access to the landing station has developed congested chokepoints for cables and presents a vulnerability because they tend to be located near large population centers such as New York City or Los Angeles.

All except one U.S. transatlantic cable "lands within the same 30 mile radius"[30] on the East Coast of the U.S. The situation is similar for trans-Pacific cables.[31] The causes of damage to cables vary from storm induced cable exposure and abrasions, to vessel traffic, people, animals and debris. A major cause of cable breaks and/or faults are caused by fisherman.[32] Most faults occur on the continental shelf in depths of less than 200 meters.[33] In addition, these cables provide emergency routing alternatives to existing land-based telecommunication systems that are susceptible to earthquakes, flooding, storms, and other natural phenomena.[34] For a depiction of cable systems and landings, refer to the attached link of TeleGeography's interactive submarine cable map[35]

Around the globe, undersea cables are designed around a coherent or purposeful pattern on the bottom of the seabed. Once the undersea cables depart the landing station, they are buried out to water depths up to 1000-1500m. In waters deeper than 1500m, the cables are typically laid on the ocean floor. At present, this depth is beyond the limit of fishing vessels that utilize a bottom trawler to catch fish on the ocean floor. Undersea cables are armored with a steel sheath up to around the 1000-1500m point and after that, the deep sea cables are unarmored and the size of a garden hose. Protection provided to the undersea cable at the landing stations are questionable because they are not under the jurisdiction or protection of the U.S.[36] Prior to deregulation, undersea cables used to be much more secure. The author's research tends to question whether or not the U.S. is the current leader in cable station protection.

The current technology is designed to be resilient, however cable breaks can disrupt day to day activities such as online banking, Internet shopping, defense related communications, etc. As a result, the U.S. and other governments understand the strategic value of undersea cables and are taking proactive measures to help protect them. Unfortunately, there is no global database that tracks cable faults on the ocean bottom. The ICPC and other organizations track outages or faults after they occur, but there is no authorized facility in existence to quickly identify an outage, and route to a central location that is easily accessed by an authorized government or commercial fusion center. The time it takes to locate and identify a cable fault amongst all the parties involved is cumbersome because there is no emergency response procedure available that can quickly identify what happened.

A few international organizations such as the ICPC have sought the creation of an undersea cable public or private relationship. Research has revealed that cable operators and government officials in many countries have a poor record of working together during undersea cable crises. The end result is that a cable repair can be initiated utilizing the system currently in place but, to what extent is there the capability to develop an "Early Warning System" that can prevent and/or mitigate a cable cut?

In most nations, there are many agencies involved with submarine cables. In the U.S., there is a long list of agencies that are linked with undersea cables: Department of State, Department of Defense, Department of the Navy, National Security Agency, Federal Communication s Commission, Central Intelligence Agency, U.S. Army Corps of Engineers.[37] Each of these agencies owns a piece of the submarine cable without any single agency in charge.[38] The problem of coordination and management of undersea cables increase as they extend overseas, where a quick response to repair is vital to the industry.

There was a belief that if cables could be identified through nautical charts, damage caused by fishing nets or a ship's anchor would be alleviated. Identifying undersea cables on nautical charts is a logical engineering solution for the cable industry, but it could be a security nightmare and/or vulnerability from a possible terrorist strike because the exact location of undersea cables could be exploited. If the exact location of the 36 cables in the U.S were identified, a successful attack on a few of these locations could affect roughly 95% of East coast Internet traffic.[39] There are redundancies to mitigate a terrorist strike on undersea cables but, the possibility of something like this happening is feasible. What cannot be overlooked is that the impact

of such a failure on international communications and economic stability could be devastating. Also, it is not known whether the international cable consortium and government entities involved in the protection of undersea cables has tested the system against such an attack. Research indicates that there have been no international tests of cable system defense and repairs, only limited national tests that tend to ignore the international component.[40]

Undersea cables are a valuable commodity in the 21st century global communication environment. The undersea consortium is owned by various international companies such as ATT, and these companies provide high-speed broadband connectivity and capacity for large geographic areas that are important entities of trade and communications around the globe.[41] For example, the U.S. Clearing House Interbank Payment System processes in excess of $1 trillion a day for investment companies, securities and commodities exchange organizations, banks, and other financial institutions from more than 22 countries.[42] The majority of their transactions are transmitted via undersea cables. In addition, the Department of Defense's (DoD's) net-centric warfare and Global Information Grid rely on the same undersea cables that service the information and economic spheres.[43] If undersea cables were cut or disrupted outside of the U.S. territorial waters, even for a few hours, the capability of modern U.S warfare that encompasses battle space communications and awareness, protection, and the stability of the financial networks would be at risk. As one analyst has noted, "the increase demand is being driven primarily from data traffic that is becoming an integral part of the everyday telecommunications infrastructure and has no boundaries.[44]

Maintaining the viability of these cables is extremely important. An example of the magnitude of data that reaches the international market every day is demonstrated by the Society for Worldwide Interbank Financial Telecommunications (SWIFT), which is the global provider of secure financial messaging services.[45] This organization transmits financial data between 208 countries via undersea fiber optic cables.[46] In addition, the security of international transactions via undersea cables could create chaos for global markets if the cables linking U.S., Europe and/or Asia were cut. The disproportionate importance of these cables to the nation's communication infrastructure cannot be overestimated. If all of these cables were suddenly cut, only seven percent of the U. S. traffic could be restored using every single satellite in the sky.[47] Satellites were important to the global communication industry but, were overtaken by undersea fiber-optic cable technology in terms of volume and/or capacity amongst users in 1986.[48]

There is a misconception amongst telephone, cell phones, and internet recipients around the globe that believe satellites are the primary means of communicating. There are significant limitations utilizing satellites as an efficient means of communication. Finn and Yang, note that satellites take a quarter of a second for signals to make the round trip to and from a geostationary orbit 22,000 miles above the Earth and one bounce is enough to throw off the verbal timing of a conversation. Also, the transmission quality of the satellite system could be erratic with echoes, screeches or dead-air calls.[49]

A major portion of DoD data traveling on undersea cables is unmanned aerial vehicle (UAV) video. In 2010, UAVs flew 190,000 hours, and the Air Force estimates

that it will need more than one million UAV hours annually to be prepared for future wars.[50] The Department of State and its diplomatic and consular posts are also heavily dependent on uninterrupted global undersea cable traffic. The importance of these cables makes them a potential target for other states or terrorists.

A recent RAND Corporation study highlighted the security challenges facing the public and private sectors. This study discussed current trends of using autonomous undersea vehicles (AUVs) to inspect the undersea infrastructure. The study went on to point out that the risks of using AUVs to monitor undersea systems are low. Of note, is the fact these AUVs are currently civilian owned and have no connections to the military. The RAND study further noted that manned vehicles are the only alternative to unmanned vehicles for this type of mission, and the U.S. Navy's only deep diving research submarine capable of performing this mission called the NR-1 was deactivated in 2008. There is no plan to replace NR-1 with another deep diving submarine and thus, the U.S. industry must depend on commercial systems.[51]

There is vulnerability in the usage of commercial AUV's because the U.S. military depends on an extensive infrastructure of undersea cables, the Integrated Undersea Surveillance System, and instrumented undersea ranges.[52] If commercial AUVs are capable of working in very deep regions of the seabed and have access to the exact location of undersea cables, they also have the ability to possibly render a cable inoperable due to the fact that the cables in the deepest part of the ocean are not buried but, laid "open" on the seabed.

The significance of undersea cable protection cannot be underestimated for the U.S. and international community. Brendan Nicholson, writing in an Australian

newspaper, highlighted the importance of the “Southern Cross” cable which links the U.S. with Australia, and New Zealand. He observed that the identified undersea cable landing as well as commercial/civilian owned and operated cables, are critical infrastructure for Australia and if cut, would immediately affect both their security and commercial business transactions throughout the region. Losing this cable would disrupt such areas as financial data flows, and most importantly, national security.[53] National security is an important topic in this part of the world because of the current shift in U.S. foreign policy towards the Asia-Pacific realm to deter China’s expansion. According to an article in the Wall Street Journal in November of 2011, President Obama announced that the U.S. military would be expanding their influence in the Australian region in 2012 by participating in joint exercises and providing American troops and ships “permanent and constant” access to Australian facilities.[54]

Given the world's cross-border internet and telephone traffic provided by undersea cables, it is important to recognize the importance of undersea cables to the world's infrastructure. As the global economy (Communications, Education, Business, Entertainment, and Banking & Commerce) continues to be dependent on undersea cables, it should be regarded as one of the world's critical infrastructure and held to the same standard as land-based counterparts of the Internet.[55] There should be a collective interest among cable owners and operators in continuing to make sure all paths are balanced along different routes to provide diversity in case of localized damages.[56] If localized damages are not identified quickly and diverted until new routes are opened up, they will continue to cause disruption and cost the industry respect and money.

Undersea Cable Protection Agreements and Policies

Currently, undersea cables are protected by the following international treaties: the International Convention for Protection of Submarine Cables of 1884, the Geneva Convention of the Continental Shelf, and the Geneva Convention on the High Seas are separate but, both ratified in 1958, and the U.N. Convention on the Law of the Sea (UNCLOS) of 1982. The 1958 Geneva Convention incorporates earlier treaties regarding the laying and repair of cables on the high seas. The U.S. has signed, but not ratified UNCLOS, which entered into force in 1994 and currently has 153 nations as parties.[57]

The treaties provide freedom to lay, maintain, and repair cables outside of a nation's 12 nautical mile territorial sea and obliges nations to impose criminal and civil penalties for intentional or negligent injury to cables.[58] These legal boundaries pertinent to undersea cables can be summarized as follows:

a) Territorial sea: Boundary along a nation's coast that extends its terrestrial boundaries at 12 nautical miles.
b) Exclusive economic zone (EEZ): Territorial waters are extensions of a state's laws and right of defense; EEZs are extensions of a state's rights to resources offshore. The boundaries of an EEZ go well beyond territorial waters, extending 200 miles from shore. The U.N. has allowed nations with extended and/or wide continental shelves (ECS) to extend their EEZ up to 350 miles (563 km) from shore.[59]

The Law of the Sea Treaty, formally known as the Third United Nations Convention on the Law of the Sea, or UNCLOS III, was adopted in 1982. Its purpose is

to establish a comprehensive set of rules governing the deep seabed mining regime and to replace previous U.N. Conventions on the Law of the Sea that were believed to be inadequate.[60] (A link is provided for additional information on the provisions of the 1958 Geneva Convention on the High Seas that the U.S. is party to and was later incorporated into UNCLOS.[61])

The 2010 ROGUCCI report highlighted an important item regarding UNCLOS in that some coastal nations do not comply or have failed to enact legislation that enforces the protection of undersea cables.[62] Notwithstanding concerns raised about UNCLOS, the U.S. Congress has not ratified UNCLOS, even after a strong showing before the Senate Committee on Foreign Relations (SCFR) in 2007 pertaining to the 1994 UNCLOS Ratification Agreement. The testimony of Douglas Burnett before the SCFR speaks to the conclusion: "It would be in the best interest of the U.S. to ratify this treaty because the U.S. telecom and power companies, the U.S. Navy and scientists, can seek the assistance of the U.S. government to enforce the rights of cable owners to lay, repair, and maintain cables outside of territorial seas and to prevent these rights from being diminished without U.S. involvement.[63]" Currently, a vote of the entire U.S. Senate has yet to be scheduled. Without passing this legislation, the U.S. can only resort to the 1884 Convention rules on telegraph cables in the event it seeks to enforce cable protection.[64]

International governments should recommend language within UNCLOS to urge everyone to update legislation to ensure the protection of undersea cables and to make it an international crime among states to intentionally damage undersea cables or the respective cable infrastructure. In addition, the threats of non-state actors such as

terrorists need to be addressed. International legislation pertinent to undersea cables needs to be streamlined in order for states (governments) to collaborate on cable system design, construction, repair, and security.[65]

If the signing of the treaty was delayed, the enforcement of undersea cable protection for the U.S. and international community would ensure added risks because cable security oversight would be minimal and disruptions possible. Because this option is in keeping with past cable policy, there is risk with outdated cable laws that have not been updated and are inadequate. The current fine for a cable break is punishable up to a misdemeanor with only one year in jail and a $5,000 fine, or both.[66]

A cable fault was detected in the waters off of Southeast Asia on March 23, 2007. It was later determined that over 180 km of undersea cables had been removed from the seabed by Vietnamese fishing trawlers who intended to sell the cables on the black market because of their copper value. The cable theft took over three months to repair at a cost of roughly $8 million. Repair costs do not take into account the loss of electronic data traffic between the U.S. and Southeast Asia. The culprits were not prosecuted because no national or international treaty exists that prevents such a crime from taking place or, prosecuting the culprits. This incident underscores a gap in the legal protection for undersea cables outside of territorial seas, a gap that needs to be addressed.[67]

According to my research data, it is safe to say that undersea cables are secure within the Exclusive Economic Zone (EEZ) of the U.S. The EEZ encompass state's laws and right of defense and are extensions of a state's rights to resources extending 200 miles from shore. Undersea cables originating in the U.S. EEZ are much safer than

on the open floor of the ocean and at their destination end, which in turn, can severely disrupt the U.S's economic well-being if they are severed purposefully or inadvertently.

In essence, international undersea cable treaties should provide the freedom to lay, maintain, and repair cables outside of a nation's 12 nautical mile territorial sea. Also, international cable treaties obligate nations to impose criminal and civil penalties for intentional or negligent injury to cables and provide universal access to national courts to enforce treaty obligations. In addition, cable treaties provide special status for ships laying and repairing cables. Finally, these treaties indemnify vessels who sacrifice anchors or fishing gear to avoid injury to cables and obligate owners with new cables that are laid over existing cables and pipelines for repair costs for any damages that may have occurred.[68]

Recommendations

This paper examined undersea cables and their impact on U.S National security, as well as the global community. Insights into vulnerable areas that are in need of protection were identified. The absence of an international organization tasked with providing global oversight for undersea cable protection and security was noted. Since an overarching organization tasked to coordinate information amongst the various governmental, civilian and commercial cable entities do not exist, one may assume there is an increased possibility that the ramifications of any future cable attack would be highly undetectable, disruptive and possibly catastrophic to the current and future network. The lack of any agreed-upon international, tiered-protection scheme for global undersea cable routes or a global grid restoration plan represents critical global infrastructure vulnerability.

An option to pursue is a new undersea cable construction regulatory regime potentially modeled after the Maritime Safety & Security Information System – MSSIS. The author was exposed to the MSSIS program while mobilized to active duty to support the Global War on Terrorism (GWOT) fusion cell for United States Fleet Forces Command (USFFC), Norfolk, VA. MSSIS was conceived by the Commander of U.S. Navy Sixth Fleet and the U.S. Department of Transportation's Volpe Center as an unclassified, multinational, freely shared, automatic identification system (AIS) network that tracks the location of merchant ships.[69] MSSIS provides clients with real-time AIS data derived from shore side, waterborne, and airborne platforms.

By sharing data on vessel locations near undersea cable locations, MSSIS participant countries can view a picture of the maritime domain that far exceeds the data they can gather alone. Currently, there are 69 countries around the globe sharing AIS data via MSSIS. If these countries are able to share and monitor data of cable locations, they have the capacity to prevent or mitigate a cable break by sending a warning message to the vessel from the regional operating center that monitors these particular cables. Utilizing a program similar to MSSIS, countries would be able to provide a baseline to share data freely on undersea cable locations through a common, open exchange that promotes international trust, and improves cable security and access to global cable information. The MSSIS model can be the trigger for undersea cable mitigation and response coordination amongst cable repair ships, industry and government entities responsible for cable network management.

The U.S. should continue with the current cable protection policy utilizing the legal regimes of UNCLOS, GCHS, GCCS, and ICPSC that target responsive responses

to cable disruptions. The legal regime governing submarine cables are old and date back to 1884. The current legal issues can be summarized by four major problems: (1) Many states have not enacted measures to protect cables from competing activities both within territorial and outside of territorial waters; (2) there exists an ongoing threat of international terrorism against undersea cables; (3) states have not adjusted laws to reflect the vulnerability that undersea cables possess regarding critical communication; and (4) there needs to be an establishment of a lead international agency via UNCLOS for the coordination of permit requirements and cable security monitoring.

Thus, the global undersea cable network is a global critical infrastructure that is the central nervous system of the globalized economy. Despite the potentially severe impact of a major disruption to undersea cables, the importance of the undersea cable infrastructure in ensuring continuity of U.S. government, military, economic activity and global communication is not well understood. The message of this paper is that these are all issues worthy of further discussion and analysis, and should be the focus of deeper strategic thought and planning.

Endnotes

[1] NSTAC, NSTAC: Cyber Collaboration Report, May 21, 2009. Accessed at http://www.ncs.gov/nstac/reports/2009/NSTAC%20CCTF%20Report.pdf, (accessed December 19, 2011), 26.

[2] The International Cable Protection Committee (ICPC) website, "*A Short History of Submarine Cables*," http://www.iscpc.org/publications/About_Cables_in_PDF_Format.pdf, (accessed December 19, 2011).

[3] Gillian Cookson, "*The TransAtlantic Telegraph Cable," History Today*, March 2000, http://www.historytoday.com/gillian-cookson/transatlantic-telegraph-cable-eighth-wonder-world, (accessed December 19, 2011), 1.

[4] NSTAC, NSTAC: Cyber Collaboration Report, May 21, 2009, http://www.ncs.gov/nstac/reports/2009/NSTAC%20CCTF%20Report.pdf, (accessed December 19, 2011), 26.

[5] Michael Sechrist, *Cyberspace in Deep Water: Protecting Undersea Communication Cables by Creating an International Public-Private Partnership*, (Harvard Kennedy School, March 23, 2010), 5.

[6] Stephen Malphrus, Keynote address at the "*Global Summit on Reliability of Global Undersea Communications Cable Infrastructure (ROGUCCI) conference*," Dubai, U.A.E., October 19, 2009.

[7] Michael Sechrist, *Cyberspace in Deep Water: Protecting Undersea Communication Cables by Creating an International Public-Private Partnership*, (Harvard Kennedy School, March 23, 2010), 38.

[8] Ibid, 6.

[9] Ibid.

[10] The International Cable Protection Committee (ICPC) website, *"A Short History of Submarine Cables,"* Telstra Last modified: 28th September, 1998, http://www.iscpc.org/information/History_of_Cables.htm (accessed December 19, 2011).

[11] Ibid.

[12] The Great Transatlantic Cable website, http://www.pbs.org/wgbh/amex/cable/peopleevents/e_gutta.html (accessed November 23, 2011).

[13] Ibid.

[14] Ibid.

[15] The International Cable Protection Committee (ICPC) website, *"Learn About Submarine Cables,"* http://www.iscpc.org/ (accessed December 21, 2011).

[16] Ibid.

[17] Karl Frederick Rausher, Keynote address at the "*Global Summit on Reliability of Global Undersea Communications Cable Infrastructure (ROGUCCI) conference*, The Report, Issue 1, rev 1, (2010 IEEE Communications Society), (accessed January 16, 2011),66 and 86.

[18] Ibid.

[19] The International Cable Protection Committee (ICPC) website, *"Learn About Submarine Cables,"* http://www.iscpc.org/ (accessed December 21, 2011).

[20] Ibid.

[21] Ibid.

[22] Michael Sechrist, *Cyberspace in Deep Water: Protecting Undersea Communication Cables by Creating an International Public-Private Partnership*, (Harvard Kennedy School, March 23, 2010), 18.

[23] Global Security.org, *Cable ships*, http://www.globalsecurity.org/military/systems/ship/offshore-cableship.htm, (accessed October 16, 2011). (Beaufort number 7 includes winds between 28 to 33 knots with average wave heights up to 19 feet.)

[24] Douglas Burnett, *"Cable Vision,"* Proceedings: U.S. Naval Institute 137, no. 8, 2011, August 2011 edition, http://www.squiresanders.com/cable_vision_august_2011/ (Accessed November 29, 2011), 67.

[25] Michael Sechrist, *Cyberspace in Deep Water: Protecting Undersea Communication Cables by Creating an International Public-Private Partnership*, (Harvard Kennedy School, March 23, 2010), 20.

[26] Ibid.

[27] Douglas Burnett, *"Cable Vision,"* Proceedings: U.S. Naval Institute 137, no. 8, 2011, August 2011 edition, http://www.squiresanders.com/cable_vision_august_2011/ (Accessed November 29, 2011), 67.

[28] Karl Frederick Rausher, Keynote address at the "*Global Summit on Reliability of Global Undersea Communications Cable Infrastructure (ROGUCCI) conference*, The Report, Issue 1, rev 1, (2010 IEEE Communications Society), (accessed January 21, 2012), 60.

[29] Frank W. Lacroix, Robert W. Button, Stuart E. Johnson, and John R. Wise, "*A Concept of Operations for a New Deep-Diving Submarine*." (2002, RAND Corporation), 141.

[30] David Lloyd, "The Need For Physical Diversity For Submarine Cable Routing," Hibernia Atlantic website, October 2008, http://www.hiberniaatlantic.com/documents/DaveysCorner-oct2008.pdf, (accessed February 20, 2012).

[31] Ibid.

[32] Karl Frederick Rausher, Keynote address at the "*Global Summit on Reliability of Global Undersea Communications Cable Infrastructure (ROGUCCI) conference*, The Report, Issue 1, rev 1, (2010 IEEE Communications Society), (accessed January 21, 2012), 60.

[33] Ibid.

[34] *Submarine Bandwidth 2002*, http://www.dri.co.jp/auto/report/telegeo/ tgisbo2.htm. See also Hui Pan and Paul Polishuk, "Submarine Fiber Optic Capacity Demand in the Asia Pacific Region," *Underwater Magazine,* September/October 2001, 5.

[35] The International Cable Protection Committee (ICPC) website, *"A Short History of Submarine Cables,"* Telstra Last modified: 28th September, 1998, http://www.telegeography.com/telecom-resources/telegeography-infographics/submarine-cable-map/ (accessed December 19, 2011).

[36] Karl Frederick Rausher, Keynote address at the "*Global Summit on Reliability of Global Undersea Communications Cable Infrastructure (ROGUCCI) conference*, The Report, Issue 1, rev 1, (2010 IEEE Communications Society), (accessed January 21, 2012), 61.

[37] Douglas Burnett, *"Cable Vision,"* Proceedings: U.S. Naval Institute 137, no. 8, 2011, August 2011 edition, http://www.squiresanders.com/cable_vision_august_2011/ (Accessed November 29, 2011), 70.

[38] Ibid.

[39] [39] Karl Frederick Rausher, Keynote address at the "*Global Summit on Reliability of Global Undersea Communications Cable Infrastructure (ROGUCCI) conference*, The Report, Issue 1, rev 1, (2010 IEEE Communications Society), (accessed January 21, 2012), 141.

[40] The International Cable Protection Committee (ICPC) website, *"A Short History of Submarine Cables,"* Telstra Last modified: 28th September, 1998, http://www.iscpc.org/ information/History_of_Cables.htm (accessed December 19, 2011).

[41] Douglas Burnett, *"Cable Vision,"* Proceedings: U.S. Naval Institute 137, no. 8, 2011, August 2011 edition, http://www.squiresanders.com/cable_vision_august_2011/ (Accessed November 29, 2011), 67.

[42] Ibid.

[43] Michael Sechrist, *Cyberspace in Deep Water: Protecting Undersea Communication Cables by Creating an International Public-Private Partnership*, (Harvard Kennedy School, March 23, 2010), 4.

[44] Frank W. Lacroix, Robert W. Button, Stuart E. Johnson, and John R. Wise, "*A Concept of Operations for a New Deep-Diving Submarine."* (2002 RAND Corporation), 141.

[45] Michael Sechrist, *Cyberspace in Deep Water: Protecting Undersea Communication Cables by Creating an International Public-Private Partnership*, (Harvard Kennedy School, March 23, 2010), 5.

[46] Ibid.

[47] Douglas Burnett, *"Cable Vision,"* Proceedings: U.S. Naval Institute 137, no. 8, 2011, August 2011 edition, http://www.squiresanders.com/cable_vision_august_2011/ (Accessed November 29, 2011), 68.

[48] The International Cable Protection Committee (ICPC) website, *"Learn About Submarine Cables,"* http://www.iscpc.org/ (accessed December 21, 2011).

[49] Bernard Finn and Daquing Yang, *Communications Under the Seas: The Evolving Cable Network and Its Implication* (Cambridge, Massachusetts and London, England: MIT Press, 2009), 46.

[50] *Submarine Bandwidth 2002*, http://www.dri.co.jp/auto/report/telegeo/ tgisbo2.htm. See also Hui Pan and Paul Polishuk, "Submarine Fiber Optic Capacity Demand in the Asia Pacific Region," *Underwater Magazine,* September/October 2001, 5.

[51] Robert W. Button, John Kamp, Thomas B. Curtin, and James Dryden, "*A Survey of Mission for Unmanned Undersea Vehicles,*" (2009 RAND National Defense Research Institute), xviii.

[52] Ibid, 159.

[53] Brendan Nicholson, "*Undersea cables key to security,"* September 2, 2011. Lexis Nexis article from *The Australian*, http://lexisnexis.com/Inacui2api/delivery/PrintDoc.do (accessed December 27, 2011).

[54] Laura Meckler, "U.S. to Build Up Military in Australia," *Wall Street Journal,* November 11, 2011. http://online.wsj.com/article/SB10001424052970203537304577028490161890480.html (accessed November 22, 2011).

[55] Michael Sechrist, *Cyberspace in Deep Water: Protecting Undersea Communication Cables by Creating an International Public-Private Partnership*, (Harvard Kennedy School, March 23, 2010), 21.

[56] Ibid, 22.

[57] U.S. Department of State, Law of the Sea Convention, http://www.state.gov/g/oes/ocns/opa/convention/ (accessed November 6, 2011).

[58] The International Cable Protection Committee (ICPC) website, *"Learn About Submarine Cables,"* http://www.iscpc.org/, (accessed December 19, 2011).

[59] The U.S. Extended Continental Shelf (ECS) Project is to establish the full extent of the continental shelf of the United States, consistent with international law, http://continentalshelf.gov/missions/10arctic/background/shelf.html, (accessed January 5, 2012).

[60] The United Nations Law of the Sea Treaty Information Center, http://www.unlawoftheseatreaty.org/, (accessed December 19, 2011).

[61] The International Cable Protection Committee (ICPC) website, *"A Short History of Submarine Cables,"* Maritime legal jurisdiction over international submarine cables, Last modified: 28th September, 1998, http://www.iscpc.org/ information/History_of_Cables.htm (accessed December 19, 2011).

[62] Karl Frederick Rausher, Keynote address at the "*Global Summit on Reliability of Global Undersea Communications Cable Infrastructure (ROGUCCI) conference ROGUCCI, The Report*, Issue 1, rev 1, (2010 IEEE Communications Society), (accessed January 21, 2012), 76.

[63] Testimony of Douglas Burnett before the Senate Committee on Foreign Relations on Accession to the United Nations Convention on the Law of the Sea and Ratification of the 1994 Agreement regarding Part IX of the Convention, Hearing held on October 7, 2007, 1.

[64] Michael Sechrist, *Cyberspace in Deep Water: Protecting Undersea Communication Cables by Creating an International Public-Private Partnership*, (Harvard Kennedy School, March 23, 2010), 59.

[65] Douglas R. Burnett and Mick P. Green, *Security of International Submarine Cable Infrastructure – Time to Rethink?* Ocean Conference on Legal Challenges in Maritime Security (Heidelberg, Germany, May 2007).

[66] Sechrist, *Cyberspace in Deep Water: Protecting Undersea Communication Cables by Creating an International Public-Private Partnership*, (Harvard Kennedy School, March 23, 2010), 68.

[67] Douglas R. Burnett and Mick P. Green, *Security of International Submarine Cable Infrastructure – Time to Rethink?* Ocean Conference on Legal Challenges in Maritime Security (Heidelberg, Germany, May 2007), 2.

[68] The International Cable Protection Committee (ICPC) website, *"Learn About Submarine Cables,"* http://www.iscpc.org/, (accessed December 19, 2011).

[69] Maritime Security & Safety Information System, https://mssis.volpe.dot.gov/Main/home/ (Accessed November 6, 2011).