2019

Submarine Cables and Infrastructure Vulnerabilities: Threats from Private and State Actors

Alexander Bennett

Submarine Cables and Infrastructure Vulnerabilities:

Threats from Private and State Actors

I. Introduction

The internet is the modern-day equivalent of the high seas in the 18th century. In the 1700s merchant ships carried goods across oceans which were not under the control of any nation. The more time that passed, the more it became apparent that protections needed to be put in place to prevent abuse of the seas. The lawlessness of the ocean enticed people who sought to profit into ventures of theft and commandeering. These pirates plundered ships and eventually caused the international community to create laws to combat their activities, thus criminalizing and effectively reducing the amount of piracy. The analogy of the high seas being the unregulated highway by which goods move internationally is directly on point to what the internet is today. The internet is not governed by any one nation and this chaos has attracted unruly behavior just like that of the pirates of centuries past. Similarly, these malicious internet actors can be likened to pirates in a sense, yet there seems to be little interest in passing proactive legislation on the international level to scale down the threat of internet crime.

Although often thought of as existing a cloud, somewhere high up, linked via satellites and connecting a world of people instantaneously, the internet is truly the equivalent of the high seas with underwater cables stretching entire oceans between countries. In fact, only a minor portion of internet data is even transmitted via satellite connections with between 95 to 99

percent of data flowing beneath the surface of the oceans.[1] Additionally these underwater routes operate at up to 8 times faster than any satellite connection, making them very efficient.[2] These oceanic lines are limited to about 448 separate cables which each are normally as wide as a household garden hose and at most as wide as a soda can. [3]

In this paper, we will examine security risks surrounding the undersea cables networks by weighing the criteria set forth by the Department of Homeland Security (DHS). The DHS offers an evaluative matrix tool called the Facility Security Level. I have evaluated the internet cables according to these standards and have rendered a score of "Level IV" for the cable infrastructure. The decisions process and weighing of factors will be explored later in this paper. Additionally, we will discuss the attractiveness of targeting undersea cables by both terrorists and state actors. Lastly, we will examine the broader scope of how undersea cables, and cyberspace, fit into the definitions of war and international law of human rights.

This paper is an argument for the government of the United States to pressure the world community to draft treaties to protect the undersea internet cables, establishing criminal liabilities, prosecutorial procedures, and a body of representatives (similar to the United Nations)

---

[1] Douglas Main, *Undersea Cables Transport 99 Percent of International Data*, NEWSWEEK, (Apr. 2, 2015, 12:39 PM), http://www.newsweek.com/undersea-cables-transport-99-percent-international-communications-319072.
[2] *Id.*
[3] *Submarine Cables Frequently Asked Questions*, TELEGEOGRAPHY, https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions, (last visited Mar. 20, 2018).

to oversee security provisions. It is the recommendation of this position paper for the United States to take initiative to pressure the international community, through the United Nations, to provide protection to the undersea cables, both physically and virtually, through deterrent measures including physical force and proportional countermeasures aimed at aggressors (independent and state actors) to hold them accountable for actions in cyberspace.

II. History

Underwater lines for data communication are not a new phenomenon, it is a practice which has been in practice for nearly 170 years. Beginning in the 1850s companies began to utilize underwater cables to transmit telegraph traffic internationally across oceans with the first transmission occurring in August 1858 between the United States and Great Britain with Queen Victoria congratulating President Buchanan.[4] The initial message took 17 hours to transmit but a second attempt took only 67 minutes.[5]

III. Security Classification

The US Department of Homeland Security chairs a committee called the Interagency Security Committee (ISC). The ISC was created by an executive order by President Bill Clinton six months after the Oklahoma City Bombing in 1995.[6] The purpose of this committee was to

[4] Donard de Cogan, *Dr E.O.W. Whitehouse and the 1858 Trans-Atlantic Cable*, HISTORY OF TECHNOLOGY, http://atlantic-cable.com/Books/Whitehouse/DDC/index.htm, (last visited Mar. 22, 2018).
[5] *Id.*
[6] *Interagency Security Committee*, U.S. DEP'T OF HOMELAND SEC, https://www.dhs.gov/interagency-security-committee, (last visited Mar. 19, 2018).

establish an interdepartmental cooperative among more than two dozen federal agencies to analyze and assess risks to "enhance the quality and effectiveness of security in and protection of buildings and facilities in the United States occupied by Federal employees for nonmilitary activities"[7].

The ISC in its examination of federal facilities states that critical infrastructure features such as dams, highways, and bridges are generally not included under the definition of "facilities" yet are rather classified as "high risk symbolic or critical infrastructure".[8] The definition of infrastructure according to Merriam Webster is: the system of public works of a country, state, or region; also : the resources (such as personnel, buildings, or equipment) required for an activity.[9] The undersea cables which will be examined in this paper should be classified as a form of infrastructure as they are equipment which serves as a system of public works by providing internet, just as water lines and power plants are parts of infrastructure. As part of the critical infrastructure set forth in the DHS Report the ISC added that the report was "not written with application to these structures in mind, the methodology upon which it is based

[7] Exec. Order No. 12977, 60 Fed. Reg. 54411 (Oct. 24, 1995).
[8] *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard (November 2016/2nd Edition)*, U.S. DEP'T OF HOMELAND SEC, https://www.dhs.gov/publication/isc-risk-management-process, (last visited Mar. 18, 2018).
[9] *Infrastructure*, Merriam Webster Dictionary (2018)

is applicable [to infrastructures]".[10] Therefore we will examine the threats posed to undersea cables with the same methodology which is used to examine federal facilities.

The standard by which risks to a structure are formulated into the Facility Security Level (FSL) determinations range from levels I through V. After determinations are made it is the responsibility of tenants (in our case, owners) to establish risk management plans and provide appropriate funds to countermeasure risks.[11] The FSL has correspondence to a security matrix which measures a variety of criteria and assigns point values to each factor which is then calculated to determine the proper FSL level. There are five factors in the matrix which are equally weighted and appointed point values of 1,2,3, or 4. [12] The sum of these values determine which classification of threat is present.

a. Mission Criticality

The first factor in the matrix is called "mission criticality" and is weighed by the function of the location and its importance to the federal government. It is acknowledged that there is an attraction for adversaries of the United States to seek to disrupt important government functions and missions.[13] Under the first factor of mission criticality one of the criteria to be assigned a value of 4 ("very high") is that the location houses essential communications and necessary

[10] *See* The Risk Management Process for Federal Facilities, *supra* note 4.
[11] *Id*.
[12] *Id*. at 6
[13] *Id*. at 8

equipment with an example being listed as “intelligence community facilities, including communications”.[14] It seems appropriate that the cables which supply internet would be included under this criteria for essential communications. Additionally, other criteria within the 4 point range is facilities which house specialized equipment to regulate national fiscal or monetary policies. The undersea cables transmit the information required to operate national and international financial markets, yet another compelling reason they should be assigned a point value of 4 in the first mission criticality factor.

b. Symbolism

The next factor in the threat matrix is labeled as “symbolism” and essentially is calculated by the attractiveness of the location as a target as well as the consequence of a would-be attack. The symbolic attractiveness is based on things such as appearance, publicized operations, or perceived importance. The ISC also lists communication centers as examples of targets which would be prioritized by groups which seek to damage the American economy.[15] It can be assumed that the effects of an attack would be catastrophic if carried out effectively. Also, as a communication medium which would disrupt and damage the American economy the physical embodiment of the internet is highly symbolic and attractive to terrorist or foreign

[14] *Id*.
[15] *Id*. at 10-11

forces. Given the gravity of an attack coupled with the attractiveness I classify this factor as a 3 on the matrix ("high").

c. Facility Population

The third factor of the matrix is Facility population. The ISC states that many terroristic goals include the mass casualties associated with attacks.[16] On the matrix scale the lowest point level of 1 includes the criteria of less than 100 people. It can be assumed with a high level of certainty that an attack on any undersea cable would result in less than 100 deaths. The cables are mostly unmanned and the motivation for such attacks is based more on the structural compromise than the threat to human life. For these reasons, I classify the third factor on the matrix as a level 1 threat ("low").

d. Facility Size

The fourth factor is called "facility size" and relates to the square footage which the targeted area takes up. The space of the target typically correlates to the amount of media coverage which is associated with an attack; i.e. if terrorists were to destroy a single post office location it would likely get moderate to high coverage in local and regional media depending on circumstances, yet if a large mail sorting facility or national mail facility were targeted the coverage would be more widespread and in depth. The space which the undersea cables occupy is beyond vast with some single cables spanning 25,000 miles. The ISC considers that size may

[16] *Id*. at 12

also be a deterrent for facilities to be attacked because "large facilities require a more substantial attack to create catastrophic damage, entailing more planning and preparation by adversaries that could be a deterrent".[17] The deterrent effect in relation to size is not present in the case of internet cables due to the fact that the area which cables occupy are no large but are not centralized, they are spread for miles and miles with little supervision of most of the space. Also the notion that larger targets require a very substantial attack are unable to be applied to this scenario as the unguarded cables are only 6 inches in diameter at most points. For all of these reasons the classification should be a 4 on the matrix ("very high").

e. Threat to Tenant Agencies

The fifth and final factor of the FSL threat matrix is classified as "threat to tenant agencies". This factor is somewhat unrelated to the idea of an undersea cable, yet based on criteria set forth in the matrix, any facility with little to no contact with the public falls into a score of 1 ("low"). I will disagree with this assessment of the internet cables for several reasons. Part of the consideration in this section of the matrix calls for an evaluation of the interaction between the target facility and the public. Also, past and credible threats against the target are used as criteria for determining this factor. The cables, being in the middle of the ocean has obviously caused there to be virtually no interaction with the cables and the public. Also, previous threats should not be determinative to the risk assessment of any target. Previous threats

[17] *Id*. at 13

are not always precursors to future attack or threats. Another point of interest in this fifth factor is whether the facility is located in a high, moderate, or low crime area. This is hardly a consideration which terrorist groups consider when planning attacks. The symbolism and attractiveness of a target far outweigh the fact of what type of crime area it is located within. Regardless of my disagreement with the considerations present in this factor of the matrix, I will follow the criteria in order to maintain analytical consistency with the rest of the model and thus assign a point value of 1 for this factor.

In summation of the five FSL matrix factors my analysis concludes with a raw score of 13 points by combining the scores of each factor. This score according to the matrix places the internet cables at a level III FSL.

IV. Implications and Fragility of the Cables as Infrastructure

Legal experts estimate that the daily traffic of financial institutions which flows over the undersea cable has a valuation of well over $1 trillion dollars. Global banking, stock exchange, and other commodity markets traded over the internet are gravely affected by any disruption. A good way to measure and appreciate the detriment which these interruptions cause is to examine times in which inadvertent interruptions took place. In December 2006 an earthquake damaged 9 undersea cables near Taiwan. The repair took approximately 49 days to be completed by several teams of ships. Chunghwa Telecom, which is one of Taiwan's largest telecom companies reported outages of 100 percent of its communications into Hong Kong and a 74 percent

interruption in communications to China. The two largest internet providers in China reported about 90 percent outages on all internet traffic flowing from China to the United States and Europe. [18]

The damages which have occurred to undersea cables up to today have been the result of natural disaster or human error. Many cables are damaged each year by things such as anchors dropped or dragged by ships and fishing nets which are trawled along the ocean floor to catch fish.[19] Additionally in an effort to minimize the unintentional damage from commercial practices like fishing, the locations of cables are publicly available information[20](See also; Exhibits B and C). The reason for releasing this information is so that vessels traversing the ocean are aware of the locations and avoid damaging the cables, yet by making this information public it could potentially be used for other means.

V. International Coalitions

The International Cable Protection Committee (ICPC) is an organization devoted to the preservation of undersea cables and provides leadership and guidance on issues related to

[18] Winston Qiu, *Submarine Cables Cut after Taiwan Earthquake in Dec 2006*, SUBMARINE CABLE NETWORKS, (Mar. 19, 2011), https://www.submarinenetworks.com/news/cables-cut-after-taiwan-earthquake-2006.
[19] Michael Matis, *The Protection of Undersea Cables: A Global Security Threat*, U.S. ARMY WAR COLLEGE, CABLE NETWORKS, (July. 3, 2012), www.dtic.mil/get-tr- doc/pdf?AD=A DA561426.
[20] *Id*.

undersea cable security and reliability.[21] The committee has membership with countless companies and governments across the globe, with members including the United States Navy, JP Morgan Chase, Sprint, AT&T and over 170 other organizations. Through their research, the ICPC has been able to place a dollar value on the cost of outages across undersea cables. They estimate that any single high-bandwidth undersea cable suffering an outage can cost companies and governments about 1.5 million dollars in revenue for every hour that the outage continues.[22]

VI. Attack Probability

There is potential for terrorist organizations or even state actors to wage an attack on the undersea cable network for a variety of reasons. This potential for attack or damage is evidenced by past events in which malicious damage was done to undersea cables. In 2007, following a provincial decree by the Vietnamese government, several fishing companies were granted permission to salvage undersea copper cables which were laid prior to 1975 and were no longer in use.[23] In excess of the specific permission granted to gather the defunct cables the fishing trawlers also pulled up 27 miles of fiber optic cables used to transmit internet traffic between

[21] *About the ICPC*, INT'L CABLE PROT. COMM., https://www.iscpc.org/about-the-icpc/, (last visited Mar. 15, 2018).
[22] Michael Sechrist, *Cyberspace in Deep Water: Protecting Undersea Communication Cables by Creating an International Public-Private Partnership*, HARVARD KENNEDY SCHOOL, (Mar. 23, 2010) , https://www.belfercenter.org/sites/default/files/legacy/files/PAE_final_draft_-_043010.pdf.
[23] Staff, *Vietnamese Fishermen "Salvage" Internet Lines*, REUTERS, (June. 7, 2007 1:24 AM), https://www.reuters.com/article/us-vietnam-cable/vietnamese-fishermen-salvage-internet-lines-idUSHAN1727620070607.

Vietnam, Thailand, and Hong Kong.[24] The cables were owned by a private Singaporean telecommunication company which had to replace the stolen lengths of cable at an estimated cost of 5.8 million dollars. This cost was the amount needed to physically replace the cable and did not include the amount of money being lost through the decreased or disrupted internet traffic caused by this cable theft. The perpetrators of this theft were not prosecuted due to lacking international agreement and treaties regarding such damage. This example of failure to prosecute crimes carried out against privately owned internet cables are representative of the problem which prompted the writing of this position paper. It is my position that governments should come together in an international treaty, like NATO, and design a framework to prosecute criminals who seek to damage undersea cables. The international community has done little to address these concerns and rather sits in wait for a major terror or state-initiated incident to occur.

VII. Parallels to Piracy in International Law

We will now examine how the crime of piracy is handled by international, maritime, and United States law and make an argument for the meddling and destruction of undersea cables to be protected under the same type of laws. In the United States the crime of piracy is addressed within the United States Constitution itself, in Article I §8 Cl. 10: "[t]o define and punish

[24] *Id.*

Piracies and Felonies committed on the high Seas, and Offences against the Law of Nations".[25] Those seeking to commit bad acts or destruction against undersea cables are committing such acts "on the high seas" which would also fall into the category of "[f]elonies". Article I §8 established the enumerated powers bestowed upon congress so that they may provide for the common defense and welfare of the United States. Congress, in 1948 enacted into the U.S. Code entitled "Crimes and Criminal Procedure" the following: "[w]hoever, on the high seas, commits the crime of piracy as defined by the law of nations, and is afterwards brought into or found in the United States, shall be imprisoned for life".[26]

Under international law it is acknowledged by the United Nations that piracy is executed with the intent to deprive people of property and interrupt activities of commerce.[27] Additionally the motivation for preventing and criminalizing piracy is similar- economics. The economical difficulties posed by pirates is dwarfed in comparison to the disruptions which could potentially result from internet connections being destroyed. The United Nations Convention on the Law of the Sea (UNCLOS) defines and proscribes procedures for nations to combat piracy. In UNCLOS Article 105 the UN authorizes the military or governmental ships of any state or nation to arrest pirates and seize their vessels if found outside of the waters of any nation (international

[25] U.S. Const. art.I §8 cl. 10.
[26] 18 U.S. Code § 1651 (2006)
[27] http://www.un.org/depts/los/piracy/piracy.htm

waters).[28] Further the UNCLOS states that the nation which has arrested and seized pirates is able to decide the punishment for those captured.[29] Within the same UNCLOS the United Nations addresses undersea cables in the sense that they may be laid by nations in international water and that nations are permitted to repair and maintain these international cables, yet no protection or prosecutorial procedures (like those for piracy) are set forth. Based upon the time periods in which laws regarding piracy were created in the United States it is probable that, had they had the insight, drafters of those laws would have included undersea cables in a protected class against harmful behaviors. Piracy laws are aimed to protect private ships which are defenseless for the most part and whose importance to the world economy was evident. There is virtually no difference; the cables are privately owned and deliver billions if not trillions to the national and world economy every day through transactions.

VIII. Maritime Sovereignty

The ocean is separated into different sections, or zones, based upon the distance from a nation's shoreline. The first zone is known as territorial waters and extends up to 12 nautical miles from the shore of the nation. The contiguous zone stretches another 12 miles further out beyond the territorial zone. The third zone is known as the exclusive economic zone and reaches outward from shores to a maximum of 200 nautical miles. Anything beyond the 200-nautical

[28] *Convention on the Law of the Sea*: *Article 105,* UNITED NATIONS, 10 December 1982, available from http://www.un.org/depts/los/convention_agreements/texts/unclos/closindx.htm
[29] *Id.*

mile point is considered the high seas, also known as international waters. The zone within economic control is miniscule when considering the long distances which exist between nations, the distances which intercontinental cables must traverse. It is for this reason that most of the undersea cable components will be found in international waters and outside of the control of individual countries. For example, the Coast Guard of the United States is responsible for patrolling the entire exclusive economic zone of the United States which is 4.5 million miles square, larger even than the United States which, itself, measures only 3.7 million miles square.[3031] The patrol and security of the coastlines of many countries will likely deter terrorists and other bad actors from engaging in attacks in those areas closest to shore but there is plenty of space which frankly cannot be guarded. Therefore, given the fact that the cables run mostly in international waters, combined with the fact that offenses against them are more likely to take place outside of the jurisdiction of any nation, would suggest the fact that there should be an international body responsible for promulgating legislation to punish those who destroy the cables.

[30] *U.S. Coast Guard Overview,* U.S. COAST GUARD, https://www.overview.uscg.mil/Portals/6/Documents/PDF/ USCG_Overview.pdf?ver=2016-10-21-114442-890, (last visited Mar. 17, 2018).
[31] *State Area Measurements and Internal Point Coordinates*, U.S. CENSUS BUREAU, https://www.census.gov/geo/ reference/state-area.html, (last visited Mar. 20, 2018).

IX. Prosecuting Piracy and why it Should be Applied to Undersea Cables

The punishments for terrorists and other actors who destroy cables should be modeled after those set forth in the United States Code. The code for piracy was challenged in the court case *United States v. Said* in which the Court of Appeals for the Fourth Circuit ultimately ruled that life imprisonment for piracy under U.S.C. §1651 was not in violation of the eighth amendment protection against cruel and unusual punishment. The court below in *Said* ruled on the trial of a group of seven Somalian pirates for illegally boarding another vessel. [32] The pirates in that case were convicted under §1651 yet the court for the Eastern District of Virginia declined to impose the mandatory life sentence attached to the statute because they interpreted it as a violation of the 8th Amendment.[33] The lack of international attention on undersea cables means that people who destroy the cables may have a lesser chance of being prosecuted by individual countries. There should be a UN- backed agreement which places penalties on destruction or attempted destruction of the undersea cables. The importance of this type of law will be exemplified further in the rest of this paper. In most cases the individual terrorist or even terrorist organization will lack resources and technology to carry out attacks where the cables are most vulnerable.

[32] United States v. Said, 798 F.3d 182, 185 (4th Cir. 2015)
[33] United States v. Said, 798 F.3d 182, 185 (4th Cir. 2015)

The vulnerable parts of the deep sea cables are most open to attack from another agressor- state actors. In the last year major developments have occurred in the threat to internet cables by state actors, particularly Russia.

X. Russian and the Threat to Undersea Cables and the Internet

Since the fall of the Soviet Union, Russia has had difficulty in establishing a strong set of armed force branches. In recent years the totalitarian power has begun increases in activity to grow its naval force and has vowed to have the second largest navy by 2027. See Exhibit D for an example of the military expenditures as percentage of the GDPs of Russia contrasted with the United States from 1991 (fall of the USSR) until 2016. As of 2016 Russia spent 5.39 percent of their GDP on military expenditures up from a low of 2.9 percent in 1998, while the United States closely outpaced Russian with 3.0 percent in 1998 the US has only spent 3.28 percent in 2016.[34] Additionally, with the uptick in military growth for Russia, has been an increased interest in alternative forms of warfare being explored by the Federation.

On March 15, 2018 new threats to internet security were made apparent in a release by the United States Computer Emergency Readiness Team (US- CERT) which is a division within the Department of Homeland Security. The theme of this release titled: "US- CERT Alert TA18-

[34] *Military Expenditure (% of GDP)*, THE WORLD BANK, https://data.worldbank.org/indicator /MS.MIL.XPND.GD.ZS?end=2016&locations=RU-US&page&start=1991&view=chart. (This link features an interactive data sheet which may be changed and adjusted to particular time periods and countries in order to cross- reference the expenditures on militaries based off of the gross domestic product (GDP) for each country.)

074A" outlines the national security threat to infrastructure targets by foreign governments, specifically Russia. The report states that since March of 2016 Russians have been intentionally targeting the infrastructure systems of the United States in an apparent effort to destroy, infiltrate, influence, or disrupt the operation of these systems.[35] In an article from December 2017 the Washington Post reported that Russian submarines were discovered conducting exploration and activity in the North Atlantic Ocean. The activities of these submarines was specifically close to the undersea cables in that region. According to senior US military officials the Russian exercises are "part of a more aggressive naval posture that has driven NATO to revive a Cold War-era command".[36] The focus of the submarines was evident to be connected with the data lines in the region which can be destructed or in certain circumstances "hacked" in order to intercept data while not necessarily interrupting connectivity.[37] In response to this suspicious activity by Russia the allies of NATO have begun planning and moving towards bolstering defensive measures which have not been seen since the cold war.[38] These measures

[35]*Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors,* U.S. DEP'T OF HOMELAND SEC., https://www.us-cert.gov/ncas/alerts/TA18-074A, (last visited Mar. 19, 2018).
[36] Michael Birnbaum, *Russian Submarines are Prowling Around Vital Undersea Cables It's Making NATO Nervous*, THE WASHINGTON POST, https://www.washingtonpost.com/world/europe/russian-submarines-are-prowling-around-vital-undersea-cables-its-making-nato-nervous/2017/12/22/d4c1f3da-e5d0-11e7-927a-e72eac1e73b6_story.html?noredirect=on&utm_term=.7b7517f09a18, (last visited Mar. 20, 2018).
[37] *Id*.
[38] Michael Birnbaum, *Facing Russian Threat, NATO Boosts Operations for the First Time Since the Cold War*, THE WASHINGTON POST, https://www.washingtonpost.com/world/facing-russian-

include increasing the amount of NATO Commands, increasing personnel, and other defensive measures. NATO plans to increase the amount of submarine detection planes which can be an early alert system to submarine activities and also plan to increase anti-submarine defense systems. The Russian government has sparked a renewed interest in their own naval forces by revamping 13 Cold-War-era submarines beginning in 2014 which has brought the number of their active submarines to 60 compared to the United States' 66 active submarines.[39] Along with this renewal of the Russian Navy was the transformation of an older ballistic submarine into what can essentially be referred to as a underwater carrier with the ability to carry other smaller submarines all the way to the ocean floor.[40] These smaller subs at such depths pose a tangible threat to undersea cables more so than the terrorist organizations who may not have financing or equipment to reach those depths. At these depths it is predicted that Russian will either be able to cut or at the very least monitor and surveil American and NATO internet communications for information gathering purposes.

In the US-CERT Alert it details how Russian "threat actors" implement various forms of internet hacks to infiltrate US systems, specifically systems of infrastructure. The CERT defines two separate types of targets, there are staging targets and intended targets, with the staging

threat-nato-boosts-operations-for-the-first-time-since-the-cold-war/2017/11/08/9b47f542-c49b-11e7-9922-4151f5ca6168_story.html?utm_term=.e74cb7386e1e, (last visited Mar. 20, 2018).
[39] Birnbaum, *supra* note 36.
[40] Id.

targets acting as a sort of doorway or threshold leading to the true intended targets. These two types of targets are identical to the relationship between the privately-owned companies which maintain the undersea cables and the intended targets- the American people. In the CERT documents it is explained that staging targets usually have a long pre-existing relationship with the intended targets of the threat actors. The staging targets are mostly organizations (private) with relatively softer lines of cyber defense when compared to the harder intended targets and therefore are easier to be compromised.[41] The threat actors would compromise the staging targets systems by using schemes such as "spear phising"[42] in order to gain user credentials which are then paired with a password (obtained by cracking software) in order to enter a system disguised as a normal and authorized user. At one point the DHS was able to retrieve a screenshot of what the hackers saw on their end of the process, the image was that of a control program for what electrical power plant operators use to run machinery in the power plants. See Exhibit A. By using this control program, the infiltrators could shut off or damage systems used for power generation, manufacturing, nuclear and water energy, and aviation.[43] As noted earlier the internet

[41] *See* Russian Government Cyber Activity Targeting Energy, *supra* note 35.
[42] *Id*. ("Spear-phising" implements a method of email fraud in which users are sent a seemingly legitimate email containing a PDF document which has a hyperlink to an external site, when clicked the user is asked to input email and password information to the site in order to gain access to documents. The information entered by the user was then collected by threat actors and used to access target systems, create administrator type accounts which appeared legitimate, and disable firewalls etc.)
[43] *Id*.

cables in the ocean are owned, operated, and maintained by private companies which may be more susceptible to infiltration just like the staging targets outlined in the CERT alert.

Michael Sechrist of the Harvard University Belfer Center for Science and International Affairs stated that the worst case scenario for a hack of the internet cables could be the following:

> What is the nightmare scenario? A hacker penetrates a cable management system, gains administrative rights, and hacks into the presentation server. Presentation servers can host webbased [sic] applications for numerous cable operators and handle management system data for multiple cable systems. Hacking into a presentation server can therefore provide attackers with access to control of multiple cable management systems. Hackers could then attain unprecedented toplevel [sic] views of multiple cable networks and data flows, discover physical cable vulnerabilities, and disrupt and divert data traffic. With that access, hackers/attackers can gain a potential "kill click" – with a click of a mouse they can delete wavelengths and, potentially, significantly disrupt or alter global Internet traffic routes.

This nightmare scenario is all too realistic as the companies which operate the undersea cables use commonplace operating systems like Linux and Windows.[44] The network management systems which these companies use enable them to remotely control entire cables from a remote location at the company. These connectivity possibilities make maintaining the lines and gathering information about the cables very convenient, yet the connections are also vulnerable to virtual hijacking in a scenario as described above by Mr. Sechrist. [45]

[44] Garrett Hinck Birnbaum, *Cutting the Cord: The Legal Regime Protecting Undersea Cables,* LAWFARE BLOG, (Nov. 21, 2017 7:00 A.M.), https://www.lawfareblog.com/cutting-cord-legal-regime-protecting-undersea-cables, (last visited Mar. 24, 2018).
[45] *Id*.

XI. International Law, the Law of War, and International Humanitarian Law

Whether their motive is information mining or to attack infrastructures it is evident that the preventative NATO measures being planned are paramount to the ongoing threat to the cables. The threat by Russian activities is also an unexplored area of law for the most part. The term "cyber warfare" is relatively new and also very ambiguous as it relates to attacks by one country on another. The International Humanitarian Law ("IHL") "applies to cyber operations occurring during […] or triggering[…] an armed conflict. However, determining the beginning of an armed conflict remains tricky in situations[…] short of any kinetic use of force."[46] So basically, given the present-day principles of IHL, a country can launch a cyber-attack such as interrupting infrastructure communications without maintaining a physical presence in the victim nation thus not implicating the traditional "Laws of War".

The Laws of War are part of international law that include s provisions to regulate the appropriate and justifiable reasons to engage in war between states (jus ad bellum) and the acceptable conduct during war (jus in bello).[47] The goals of these laws of war as part of the larger picture of IHL, which aim to limit the suffering caused by armed conflict between nation

[46] *Cyber-Warfare*, INT'L COMM. OF THE RED CROSS, https://casebook.icrc.org/highlight/cyber-warfare, (last visited Mar. 15, 2018). (The ICRC is a committee by the Red Cross devoted to the research and education of international humanitarian law, also known as IHL. The committee seeks to research: the distinctions of civilians and combatants, principles of proportionality, human rights, different types of conflicts, and state responsibility.)
[47] *Jus Ad Bellum and Jus In Bello*, INT'L COMM. OF THE RED CROSS, https://www.icrc.org/en/document/jus-ad-bellum-jus-in-bello, (last visited Mar. 15, 2018).

states. Yet cyber-attack falls outside of the traditional definition of war and therefore needs to be addressed on the international level. This uncertainty leaves many openings for very damaging attacks to occur without invoking consequences on the perpetrators.

The difficulty in defining cyber hacking and attacks as warfare is because traditional warfare takes place in some physical space while "cyberspace" is a virtual space. This difference causes a disconnect in the evaluation of such cyber-attacks. The ICRC discusses the various elements of newly emerging cyber aggression and posits that "[t]he effects of such 'bloodless' attacks could obviously be severe – for instance, if power or water supplies were to be interrupted or if a banking system were to be taken down."[48] It is this leap, from the virtual actions of foreign nations, to the physical world of a country across an ocean that has lawmakers and governments not sure how to define this new type of aggression. It is the position of this paper that such attacks on infrastructure, whether it be internet or a power grid, is a deliberate act of war by another country. This does not mean that every time a foreign country is found to have hacked the United States that war drums should sound, yet it is strongly advisable that the US respond proportionally to such threats to deter escalation.

[48] *ICRC International Humanitarian Law and the challenges of contemporary armed conflicts in 2015*, INT'L COMM. OF THE RED CROSS, https://casebook.icrc.org/case-study/icrc-international-humanitarian-law-and-challenges-contemporary-armed-conflicts-2015, (last visited April 20, 2018)

Another major threat of attacks on infrastructure like the undersea cables, both physically or virtually, is the risk of what are known as "indiscriminate attacks". The indiscriminate attacks in the traditional sense are violations of IHL. The International Court of Justice in The Hague, Netherlands issued an advisory opinion in 1996 regarding the legality of threat or use of nuclear weapons in which the court discussed indiscriminate attacks. The ICJ serves as the principal judicial organ of the UN and its purpose is to "settle, in accordance with international law, legal disputes submitted to it by States and to give advisory opinions on legal questions referred to it by authorized United Nations organs and specialized agencies."[49]

Although the opinion is about nuclear weapons the same principles to the indiscriminate nature of cyber-attack, the ICJ says weapons are prohibited "because of their indiscriminate effect on combatants and civilians."[50] Cyber weapons should be placed in this same category because attacks on infrastructure will not be limited to military installation and the accuracy of such attacks is similar to explosives in that there is peripheral damage to civilians. This peripheral damage example is strongly exemplified by the ICRC's Report: *ICRC, International Humanitarian Law and the challenges of contemporary armed conflicts in 2015*. It states:

> Most military networks rely on civilian cyber infrastructure, such as undersea [fiber]-optic cables, satellites, routers or nodes. Conversely, civilian vehicles, shipping, and air traffic controls are increasingly equipped with navigation systems that rely on global

[49] *The Court*, THE INT'L COURT OF JUSTICE, http://www.icj-cij.org/en/court, (last visited April 21, 2018).
[50] *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1. C.J. Reports 1996*, THE INT'L COURT OF JUSTICE, http://www.icj-cij.org/files/case-related/95/095-19960708-ADV-01-00-EN.pdf, (last visited April 20, 2018).

> positioning system (GPS) satellites, which are also used by the military. Civilian logistical supply chains (for food and medical supplies) and other businesses use the same web and communication networks through which some military communications pass. Thus, it is to a large extent impossible to differentiate between purely civilian and purely military cyber infrastructures.[51]

Conclusion

The connectivity of the entire globe relies on about 400 garden-hose-size cables stretching thousands of miles. The cables, which could at any time be severed and disrupted by various bad actors, as very vulnerable. Most alarming is that strong evidence points toward a Russian initiative to bolster their military power, seek alternative non-physical forms of attacks and to mask responsibility for hacking type attacks. These indicators also point toward a vulnerability of the undersea internet cables being attacked by Russia in order to limit or cut out communication within the United States and also between the United States and its allies. The days of traditional kinetic projectile warfare have not yet gone by the wayside, yet, they are slowly taking on a secondary spot in the arsenals of advanced nations. During Hurricane Sandy in 2012, the tri-state felt the effects of having power cut off. In some places power was extinguished for over a week's time and we saw the fabric of society begin to stretch thin with lines at gas stations, bare shelves at supermarkets, and a general panic of the public. The effects of an infrastructure attack through soft internet targets under the ocean could lead to this very same discord on a much larger scale.

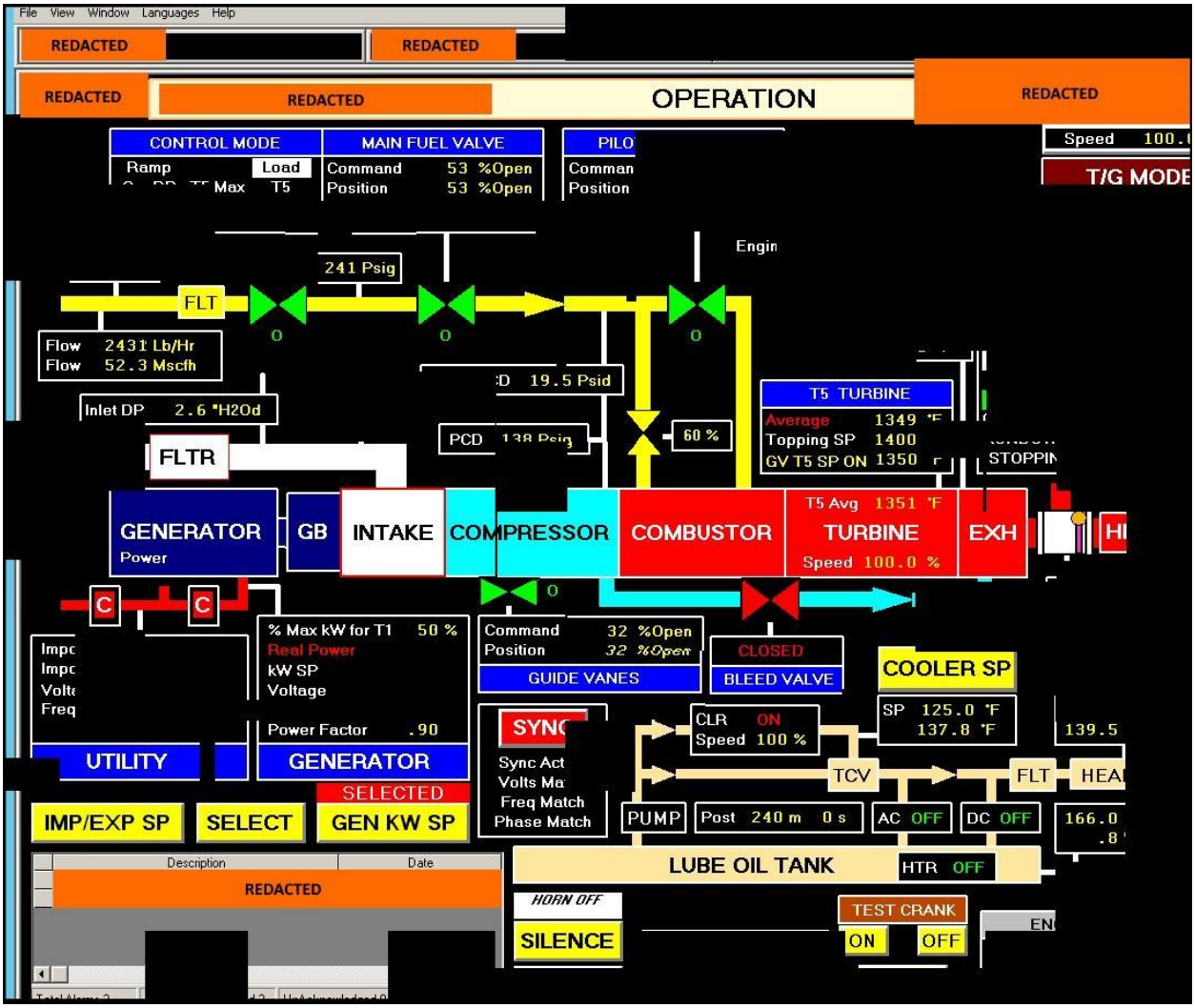
Although the United States military has taken steps to bolster cyber divisions among the branches, it is clear that the government also needs to create standards and protocol which private internet providers need to implement to prevent hacking and attacks like those on the power plant discussed above. The interconnectedness of the internet is the most powerful tool to

[51] *See* Challenges of Contemporary Armed Conflicts, *supra* note 48.

have ever existed, yet this interconnectedness also brings civilian users into the same virtual space as military users. It is the recommendation of this position paper for the United States to take initiative to pressure the international community, through the United Nations, to provide protection to the undersea cables, both physically and virtually, through deterrent measures including physical force and proportional countermeasures aimed at aggressors (independent and state actors) to hold them accountable for actions in cyberspace.

Clearly there are several strong arguments included within this paper in support of a push on the international community to revise the protections of undersea cables. The areas of law and security must be re-visited to protect the intangible internet traffic which passes through tangible connections. These cables cover far to vast of an area to not be protected. Just as laws had to be developed to control aviation when air traffic became a means of transport, the nations of the world must come together again to react to new developments and create protections and penalties applicable to the undersea systems.

Exhibit A: [52]



[52] *See* Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors, *supra* note 35.

Exhibit B:[53]

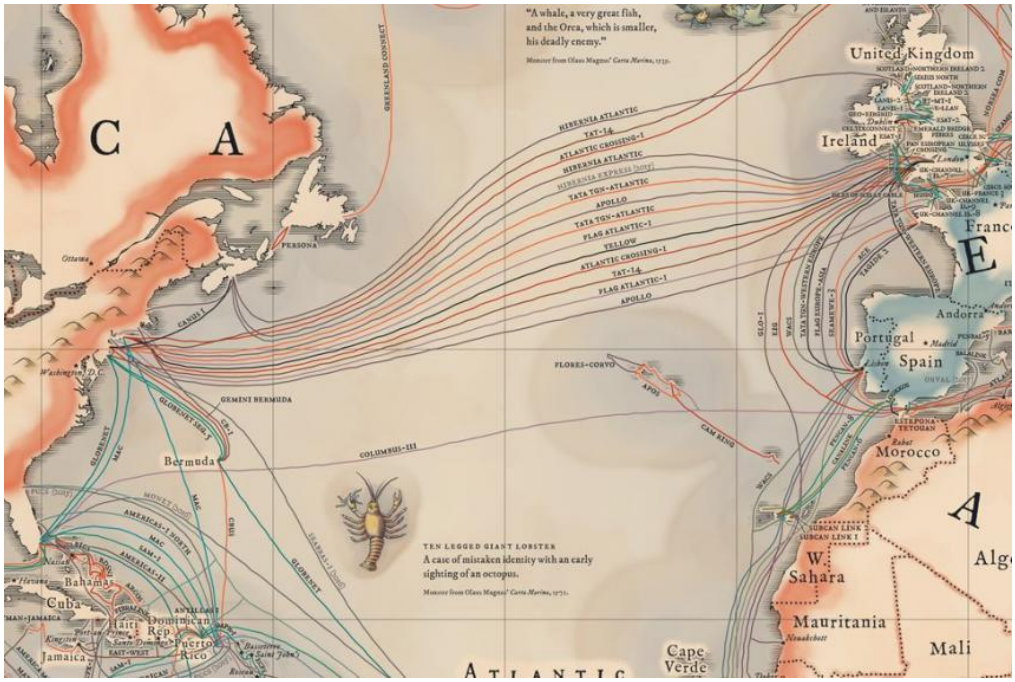
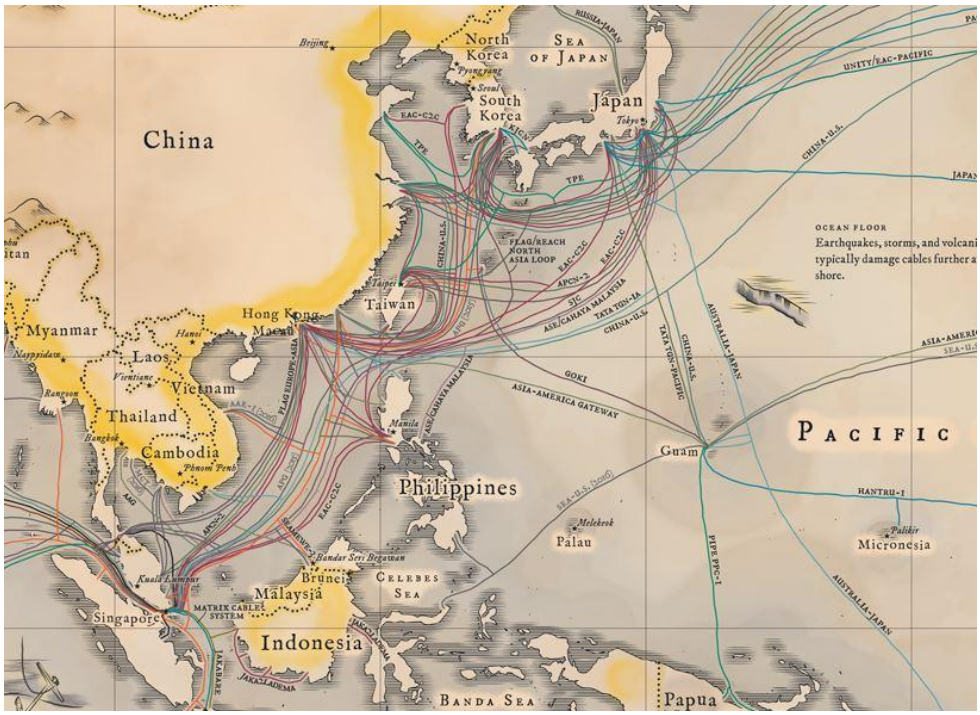


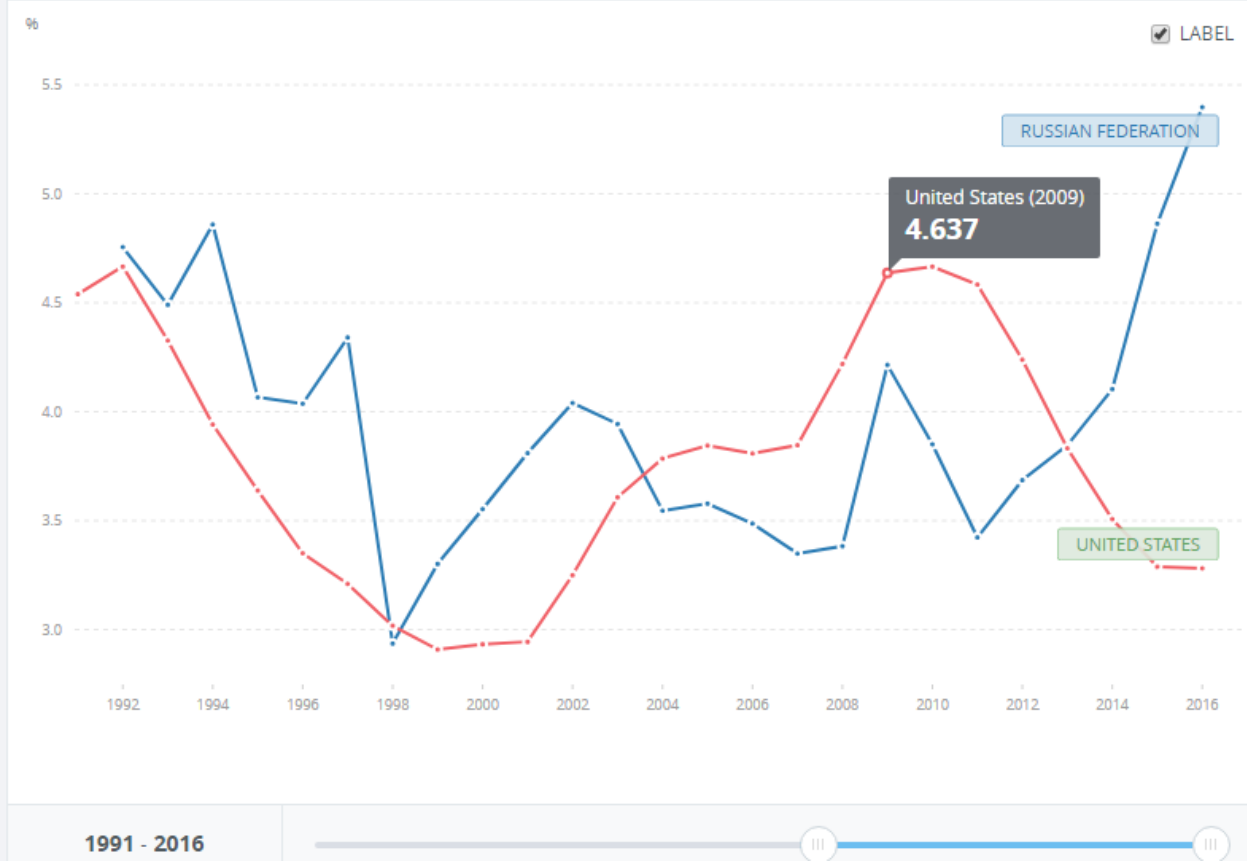
Exhibit C:[54]



[53] https://data.worldbank.org/indicator/MS.MIL.XPND.GD.ZS?end=2016&locations=RU-US&page&start=1991&view=chart

[54] https://data.worldbank.org/indicator/MS.MIL.XPND.GD.ZS?end=2016&locations=RU-US&page&start=1991&view=chart

Exhibit D [55]



[55] https://data.worldbank.org/indicator/MS.MIL.XPND.GD.ZS?end=2016&locations=RU-US&page&start=1991&view=chart