2012-06

Assessing Resilience in the Global Undersea Cable Infrastructure

Crain, John K.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

ASSESSING RESILIENCE IN THE GLOBAL UNDERSEA CABLE INFRASTRUCTURE

by

John K. Crain

June 2012

Thesis Advisor:	David L. Alderson
Second Reader:	W. Matthew Carlyle

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2012	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Assessing Resilience in the Global Undersea Cable Infrastructure			**5. FUNDING NUMBERS**
6. AUTHOR(S) John K. Crain			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ___N/A_____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

This thesis analyzes the global undersea cable infrastructure as it pertains to international telecommunications. We represent countries, cable landing stations, and undersea cables using a network structure of nodes and edges that closely imitates the real-world system. For a given geographic region, we connect individual networks associated with stand-alone cable systems to create one large network model. We use a "gravity model" to estimate the traffic demand between each pair of countries based on the number of Internet hosts in each country. We formulate and solve an Attacker-Defender (AD) model to identify the worst-case disruptions, where a "worst-case" disruption corresponds to the greatest shortage in telecommunications traffic even after the system has rebalanced flows as best as possible. Using public sources of data, we collect information about more than 220 real cable systems, and we develop a customized decision support tool that facilitates the analysis of different combinations of countries and cable systems. We demonstrate our modeling technique with an analysis of the undersea cable infrastructure connecting Europe and India. Our analysis provides insight into which components in the system are most vulnerable along with how effectively the system performs in the face of disruptions.

14. SUBJECT TERMS global undersea cable infrastructure, submarine optical fiber cables, vulnerability, Attacker Defender			**15. NUMBER OF PAGES** 103
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

ASSESSING RESILIENCE IN THE GLOBAL UNDERSEA CABLE INFRASTRUCTURE

John K. Crain
Major, United States Army
B.S., United States Military Academy, 2001

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN OPERATIONS RESEARCH

from the

NAVAL POSTGRADUATE SCHOOL
June 2012

Author: John K. Crain

Approved by: David L. Alderson
Thesis Advisor

W. Matthew Carlyle
Second Reader

Robert F. Dell
Chair, Department of Operations Research

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis analyzes the global undersea cable infrastructure as it pertains to international telecommunications. We represent countries, cable landing stations, and undersea cables using a network structure of nodes and edges that closely imitates the real-world system. For a given geographic region, we connect individual networks associated with stand-alone cable systems to create one large network model. We use a "gravity model" to estimate the traffic demand between each pair of countries based on the number of Internet hosts in each country. We formulate and solve an Attacker-Defender (AD) model to identify the worst-case disruptions, where a "worst-case" disruption corresponds to the greatest shortage in telecommunications traffic even after the system has rebalanced flows as best as possible. Using public sources of data, we collect information about more than 220 real cable systems, and we develop a customized decision support tool that facilitates the analysis of different combinations of countries and cable systems. We demonstrate our modeling technique with an analysis of the undersea cable infrastructure connecting Europe and India. Our analysis provides insight into which components in the system are most vulnerable along with how effectively the system performs in the face of disruptions.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACMA	Australian Communications and Media Authority
AD	Attacker-Defender
FSSCC	Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security
DHS	Department of Homeland Security
GAMS	General Algebraic Modeling System
Gbps	Gigabits per second
ICPC	International Cable Protection Committee
ITU	International Telecommunications Union
MILP	Mixed Integer Linear Program
MCNF	Multi-Commodity (Minimum-Cost) Network Flow
PFE	Power Feed Equipment
Tbps	Terabits per second
VBA	Visual Basic for Applications
WDM	Wavelength-Division Multiplexing

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

This thesis analyzes the global undersea cable infrastructure as it pertains to international telecommunications. We examine the resilience of this infrastructure to worst-case disruptions, where a "worst-case" disruption corresponds to the greatest shortage in telecommunications traffic even after the system has rebalanced flows as best as possible. This analysis provides insight into which components in the system are most vulnerable along with how effectively the system performs in the face of disruptions.

We represent countries, cable landing stations, and undersea cables using a network structure of nodes and edges that closely imitates the real-world system. For a given geographic region, we connect individual networks associated with stand-alone cable systems to create one large network. We use a "gravity model" to estimate the traffic demand between each pair of countries based on the number of Internet hosts in each country. We use Attacker-Defender (AD) modeling techniques to determine where the worst-case disruptions occur and how the system responds in the face of disruptions. Using public sources of data, we collect information about more than 220 real cable systems, and we develop a customized decision support tool that facilitates the analysis of different combinations of countries and cable systems. We demonstrate our modeling technique with an analysis of the undersea cable infrastructure connecting Europe and India.

Our results provide insight into this specific infrastructure and also suggest broader implications regarding undersea cable infrastructures in general. First, a country's transoceanic communications may be severely degraded without disruptions to any cables or landing stations that are actually in or near that country. Second, we highlight the important role that redundancy plays in determining the resilience of an undersea cable infrastructure. Specifically, we show that redundancy must exist in the form of both capacity redundancy and physical redundancy in order to ensure resilience across all levels of disruption. Finally, our analysis demonstrates that geography also

plays a major role in the resilience on an undersea cable infrastructure. Natural choke points and other system limitations imposed by physical geography often represent the most vulnerable locations for disruption.

Our model and analysis could easily be adapted to address scenarios of interest to the Department of Defense by focusing on specific cable systems of interest and adjusting shortage costs to prioritize certain kinds of traffic.

ACKNOWLEDGMENTS

First and foremost to my advisor, Professor David L. Alderson, to say that I could not have done this without you would be a gross understatement. Thank you for always being available and providing leadership and guidance on so many late nights. You treated this thesis and my education as if it were your own. I learned a tremendous amount from you and thoroughly enjoyed your company every step of the way! I am forever grateful.

To Professor W. Matthew Carlyle, thank you for all of your assistance and expertise in the finer details of network modeling and code development. As you intimated to me from the start, the knowledge and experience afforded by this process are truly the most valuable achievements of all.

To Professor Nedialko Dimitrov, thank you for introducing me to network modeling and providing the inspiration for my work in this fun and challenging field. I would not have attempted this thesis without your confidence in me.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Two of the most influential innovations of the latter 20th century are the Internet and mobile phones. In 1994, during the nascent stages of both these technologies, there were fewer than 20 million Internet users and 55 million mobile-cellular subscriptions worldwide. By the end of 2011, there were over 2 billion Internet users and almost 6 billion mobile-cellular subscriptions worldwide (ITU, 2011). In less than two decades, these technologies went from virtually non-existent to being a ubiquitous part of everyday life. Still, most people who use the Internet and mobile phones every day give little thought to the underlying physical infrastructure that enables near-instantaneous communication on a global scale.

A. BACKGROUND

The global undersea cable infrastructure is a physical system of optical fiber cables connecting all of the world's continents with the exception of Antarctica. According to the International Cable Protection Committee (ICPC), these undersea cables carry over 95 percent of international voice and data traffic (ICPC, 2011). Indeed, undersea telecommunications cables, along with their terrestrial counterparts, form the backbone of the information superhighway.

1. Historic Growth

Historically, transcontinental communications cables progressed across three fairly distinct eras: telegraph cables (1850–1960), coaxial telephone cables (1956–1990), and optical fiber cables (1988–present). The first transoceanic telegraph cable was laid between Ireland and Newfoundland in 1858 and used electricity and Morse code to send messages. That first cable only transmitted a single word per minute. Today, the delivery capacity of a single cable is in the terabits per second with the capability of carrying millions of simultaneous telephone calls along with large amounts of video and Internet data (Chesnoy, 2002). Figure 1 illustrates the exponential growth in the capacity of submarine cables over the years as the technology changed from telegraph to coaxial telephone to digital fiber. As the conduit for global communications and the Internet,

submarine optical fiber cables have helped revolutionize business, commerce, communications, education, and entertainment. The ownership, maintenance, protection, and usage-rights associated with each of these systems are often very complicated, involving national governments, global agencies, and a multitude of private enterprises. The Pan American Cable System, for example, was launched in 1996 by a consortium of 41 different telecommunications carriers from 27 countries (Trischitta et al., 1997).

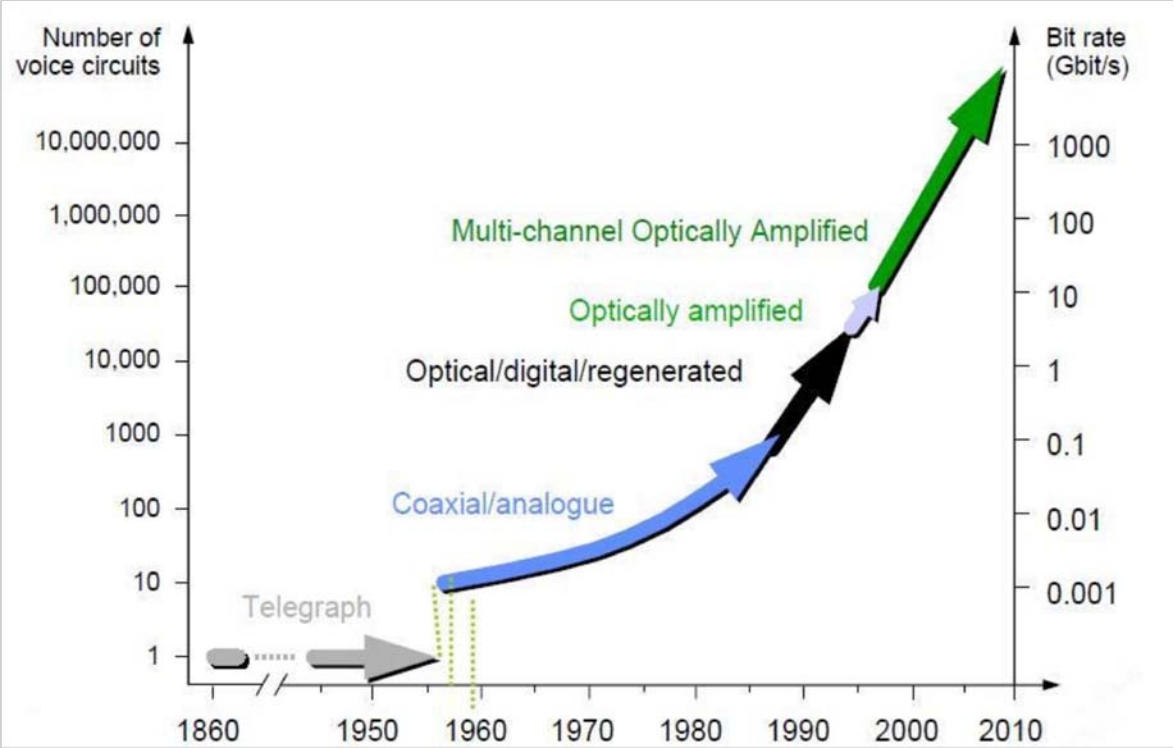


Figure 1. Capacity of undersea telecommunications cables over the years (From Alwis, 2007).

In the mid to late 1900s as the United States and the former Soviet Union vigorously competed in space exploration as a symbolic backdrop to the Cold War, it appeared that satellite technology would forever dominate global communications. In 1988, artificial satellites were the primary carrier with undersea cables accounting for only two percent of the world's transoceanic flow of communications (Mandell, 2000). However, the development of optical fiber digital technology altered that trend seemingly overnight. The first transoceanic optical fiber submarine cable system Trans-Atlantic

Telephone 8 (TAT-8) came into service in 1988 with "more capacity in a single cable than the combined capacity of all the transatlantic cables" in existence at the time (Beaufils, 2000). And while the latest optical fiber cables have more than 3000 times the capacity of their coaxial predecessors, "today's satellites have improved only modestly over theirs" (Mandell, 2000). In addition to their overwhelming advantage in capacity, submarine cables are also superior to satellites in signal quality, transmission speed, confidentiality, and service lifetime among other factors (Beaufils, 2000). Table 1 compares satellites and submarine optical fiber cables according to several key factors.

Comparison Factor	**Satellite**	**Optical Subsea**
Latency	250 milliseconds	50 milliseconds
Design life	10-15 years	25 years
Capacity	48,000 channels	160,000,000 channels
Unit cost per Mbps capacity	$737,316 US	$14,327 US
Share of traffic: 1995	50%	50%
Share of traffic: 2008	3%	97%

Table 1. Comparison of satellite versus undersea optical fiber cables across several key factors in telecommunications (Adapted from Donovan, 2009).

Satellites are still viable, particularly in one-to-many transmissions such as television broadcasts and satellite radio. They also provide critical access to remote locations. However, in the case of one-to-one transmissions between countries and continents, submarine cables clearly dominate the current landscape. According to Beaufils (2000), this dominance will expand with the advent of the next generation of the Internet and the increasing demand for bandwidth. In addition to e-mail and data browsing, the Internet now supports many more services including video and HDTV, Internet voice, file transfer, remote computing, video-conferencing, and networked devices such as smartphones and tablets along with many other multimedia applications such as 3DTV still yet to come. As a result, the global undersea communications

infrastructure continues to expand at a prolific pace. Today there are hundreds of undersea cable systems with new systems and upgrades continuing to be installed. Figure 2 shows a map of all the undersea optical fiber cable systems currently in existence.

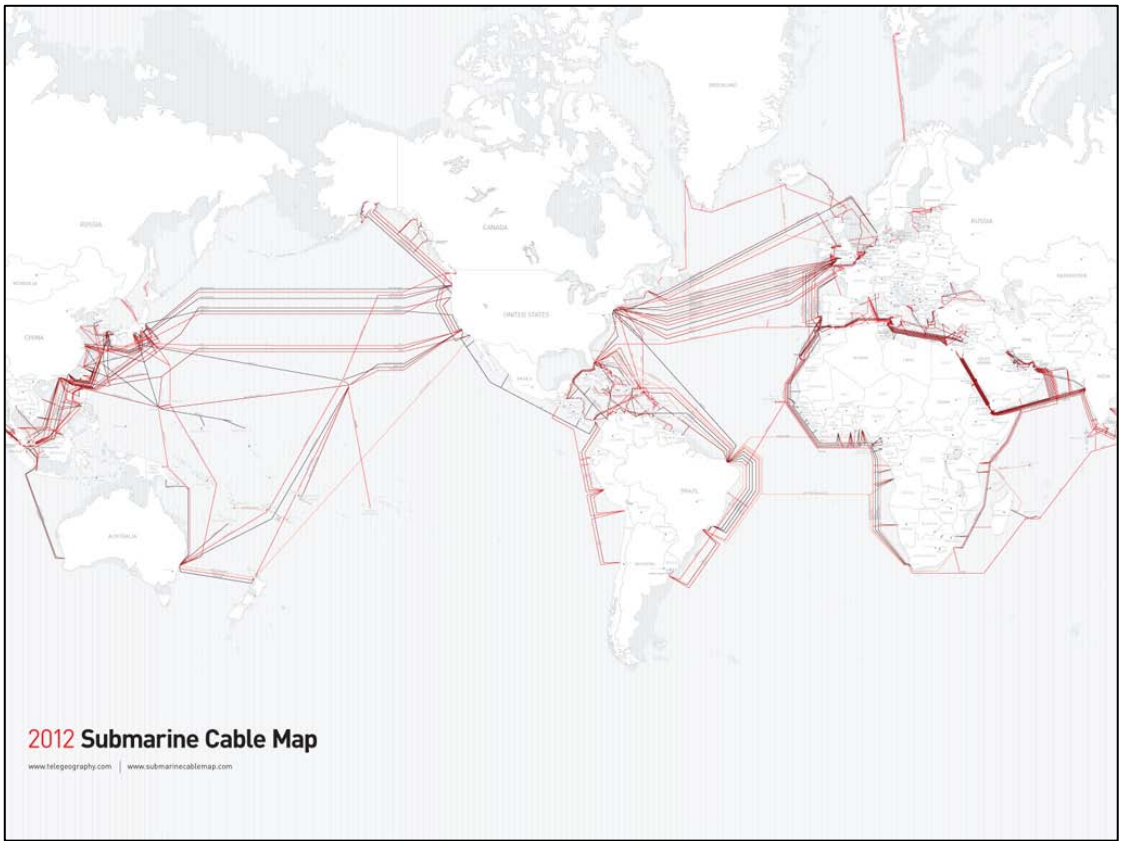


Figure 2. Map of undersea optical fiber cable systems worldwide (From Telegeography, 2012a).

2. How Undersea Cables Work

The principal components of a modern submarine optical fiber cable system include the cables themselves, repeaters, branching units, power feed equipment (PFE), and terminal equipment. Figure 3 depicts the working relationship among these components.

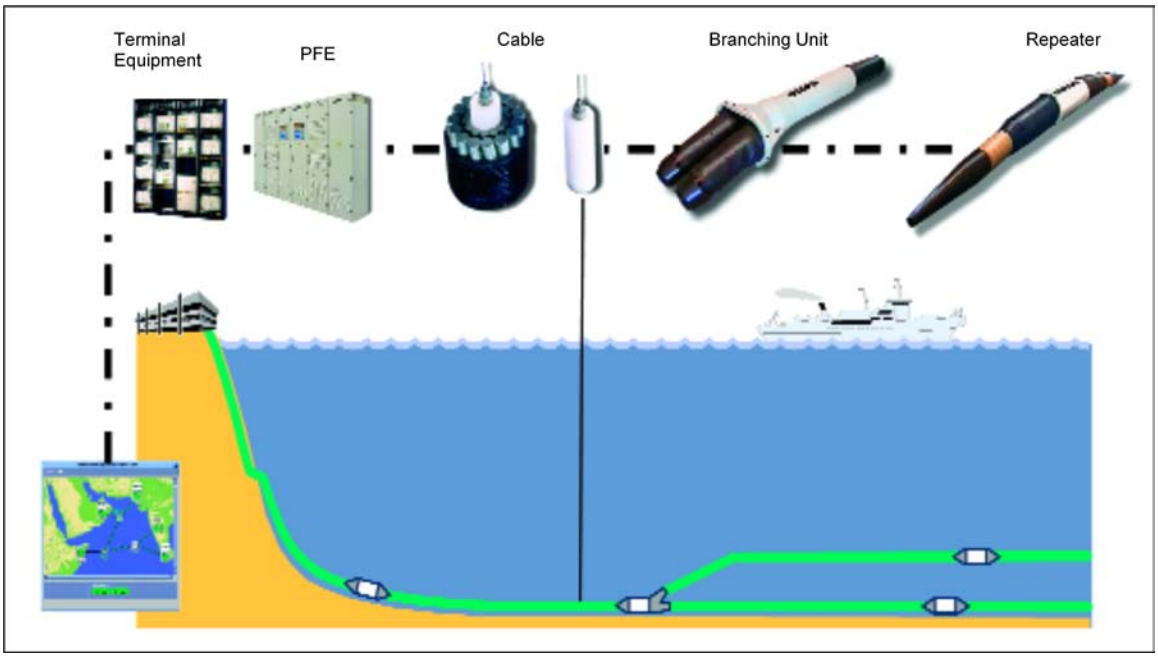


Figure 3. Principal components of a modern undersea optical fiber cable system (From Letellier, 2004).

The cables themselves are designed on a fiber-pair basis to support bidirectional traffic. Modern cables contain as many as eight fiber pairs. Since the signal is degraded as it travels along the cable, the system needs repeaters that effectively boost the signal at regular intervals along the length of the cable. Repeaters are typically located at intervals of approximately 50 to 110 kilometers apart (Letellier, 2004). In the first optical fiber cables, repeaters converted the optical signals back to the electrical domain for reamplification of the signal and then converted the signal back to the optical domain before sending it along the path. However, today's cable systems are optically amplified so that the signal remains photonic throughout the transmission path (Beaufils, 2000). The branching units often serve as repeaters themselves while also allowing for undersea fiber connections. The PFE supply electrical current to the repeaters to support the reamplification process. Finally, the terminal equipment sends and receives the signals and interfaces with terrestrial cable systems. Recent advancements in wavelength-division multiplexing (WDM) have increased the capacity for sending and receiving traffic even more dramatically. WDM technology allows the simultaneous transmission of multiple optical signals on a single optical fiber by using different wavelengths (i.e.,

colors) of laser light (Beaufils, 2000). Thus, an already established cable can be upgraded in capacity without actually adding additional fiber pairs to the cable. It only requires upgrading the terminal equipment to support the latest WDM technology. According to Letellier (2004), the latest terminal line equipment set-ups using WDM technology allow more than 100 optical channels at 10 gigabits per second (Gbps) on each channel. The newest undersea cables currently being constructed contain as many as eight fiber pairs and 128 optical channels on each fiber pair via WDM. With 10 Gbps per optical channel, the total potential capacity now exceeds 10 terabits per second (Tbps) on a single undersea cable. At that capacity, one cable "can carry approximately 160 million telephone circuits simultaneously or transfer approximately 272 DVD disks" between continents in about one second (FSSCC, 2009).

The network topology of each submarine cable system is uniquely designed to meet the particular needs of the system. Network topologies refer to both the physical and logical configuration of the cable system. In general, the physical topology relates to the undersea cable itself while the logical topology relates to the individual fiber pairs within the cable. The four basic physical configurations commonly employed are string, branched string, ring, and mesh (Beaufils, 2000). Often a single cable system will incorporate a mix of these designs. Figure 4 illustrates the basic physical topologies. The newest cable systems typically employ ring or mesh configurations because of their self-healing nature; a single cable cut does not sever any of the nodes from the network, and, assuming that sufficient capacity exists, the network can restore all traffic through re-routing.

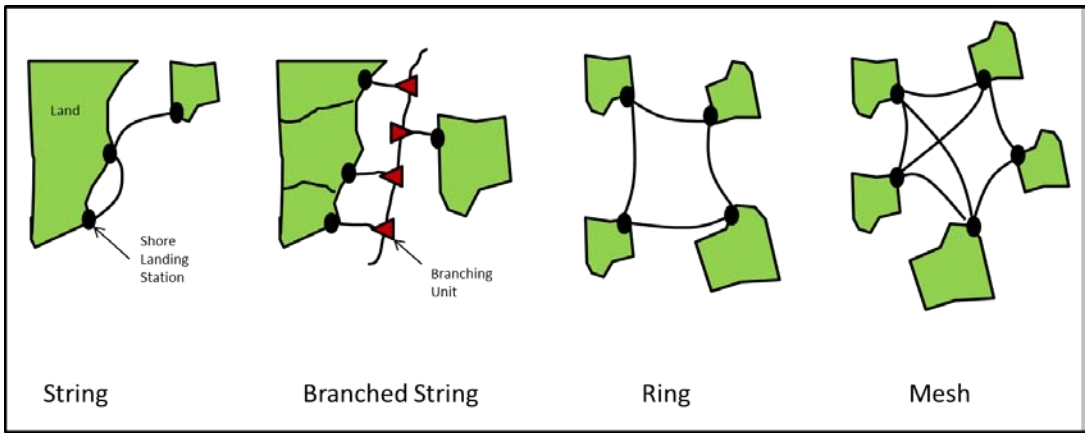


Figure 4. Basic physical topologies of undersea optical fiber cable systems.

The logical topology determines how the data is actually transmitted inside the network. Branching units provide tremendous flexibility in the routing of each fiber pair. Network operators maximize the transmission capacity between preferred routes through efficient logical configurations. The logical topology of several current submarine cable systems is shown in Figure 5. While the physical configuration of almost every submarine cable system is readily available via public source data, the logical configuration along with the quantity and location of branching units are rarely disclosed by cable owners and operators. The network topology, including both the physical and logical design, is critical to the overall performance and resilience of an undersea cable system.

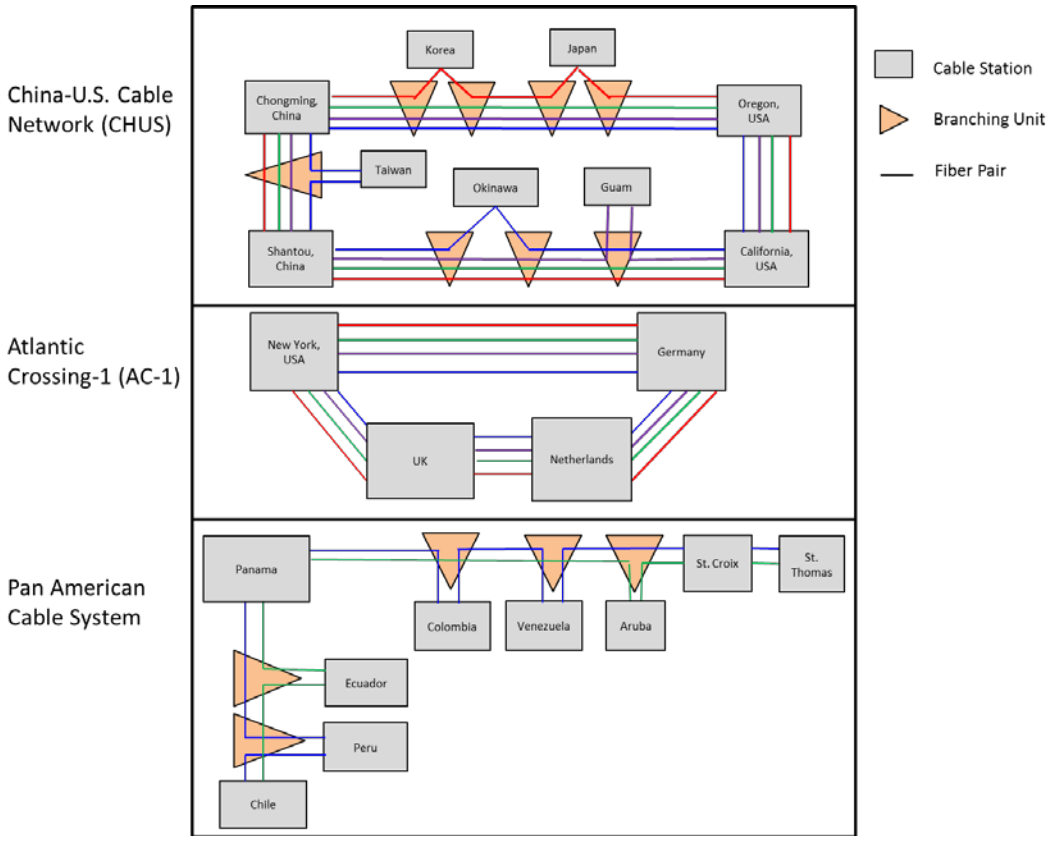


Figure 5. Logical topology of several current undersea optical fiber cable systems (After: Trischitta & Marra, 1998).

3. Impact of Disruptions

Undersea cables are susceptible to disruption from both deliberate threats (e.g., terrorism, piracy, sabotage) and non-deliberate hazards (e.g., failure, accident, natural disaster). In terms of physical security, the optical fiber cables themselves are sheathed in protective armor coatings made of high-strength steel and other synthetic materials but still only measure around 20–50 millimeters in diameter (ICPC, 2011). For further protection, the cables are typically buried in yard-deep trenches. However, they are usually left to run uncovered along the ocean floor in water depths exceeding 1,000 feet. Among non-deliberate hazards, trawl fishing and ship anchors are common disruptions. Natural hazards such as earthquakes, tsunamis, and undersea landslides occur less

frequently but typically affect multiple cables. Considering these natural and man-made obstacles they sometimes face, the garden hose-sized undersea cables are a relatively "soft" target in the ocean environment.

Major disruptions over the last several years have resulted in massive economic losses in terms of both repair costs and down time. According to the ICPC around 70 percent of all cable faults are caused by fishing and anchoring activities (ICPC, 2011). In 2007, Australia became one of the only countries to establish protection zones that prohibit fishing and anchoring activities around undersea cables (ACMA, 2007). Natural hazards, on the other hand, have much lower incidence rates than fishing and anchoring but usually result in far more severe economic consequences. The 2006 Hengchun earthquake along the southern coast of Taiwan triggered submarine landslides over large areas of the ocean floor and broke nine undersea cables in the process (ICPC, 2009). Internet telecommunications linking China, Hong Kong, Vietnam, Taiwan, Singapore, Japan, and the Philippines were seriously impaired. Cable repairs lasted around two months. During that time most traffic was successfully re-routed but with significant delays. In regards to deliberate threats, in 2007 off the coast of Vietnam piracy was blamed in the theft of active submarine cables and equipment (ICPC, 2009). In early 2008 over the span of just a few days, multiple undersea cables were cut off the coasts of Egypt and Dubai. At the time these cables collectively accounted for around three-quarters of the international communications between Europe, North Africa, the Middle East, and India. As a result, at least 14 countries lost a significant amount of connectivity. In particular, more than 80 percent of India's international service went down, while Maldives was entirely disconnected from the outside world (Sechrist, 2010a). While damage to undersea cables is common, the short time span and limited geographic area of these cuts raised troubling suspicions. Although there have been no confirmed cases of terrorism or sabotage to submarine cables, the overall security and vulnerability of the global undersea cable infrastructure remains questionable.

B. OBJECTIVES AND SCOPE

This thesis focuses on assessing resilience in the global undersea cable infrastructure as it pertains to international telecommunications. In this thesis, we define resilience as the capability of a system to maintain its functions in the face of internal and external events; this definition is consistent with that of the Critical Infrastructure Task Force (Homeland Security Advisory Council, 2006) and the National Strategy for Homeland Security (Homeland Security Council, 2007). We represent countries, cable landing stations, and undersea cables using a network structure of nodes and edges that closely imitates the real-world system. We formulate a mathematical model of the normal daily flow of international telecommunications traffic. This model of normal operations gives us an appreciation of the complexity of the global undersea cable infrastructure.

By adding the effect of cable loss to this model, we investigate the vulnerabilities of the global undersea cable infrastructure. We look at attacks against the cables themselves and attacks against cable landing stations. We also consider worst-case disruptions in regards to multiple simultaneous attacks. We define a worst-case disruption to mean a disruption that causes the greatest shortage in telecommunications traffic. Our analysis provides insight as to which components are most critical to the system.

When analyzing undersea telecommunications cables, both the physical security of the cable infrastructure along with the virtual security of the information being transmitted are important. Our analysis focuses on the physical security of the infrastructure. In other words, we consider attacks on physical components that could interrupt communications flow. We do not consider attacks against the data integrity of these flows such as from surveillance or interception of telephone or data traffic. Our geographic scope encompasses the world-wide system of undersea cables including all known cables currently in existence.

In this thesis, we make the simplifying assumption that the multitude of cable systems function collectively as if operated by a single, centralized decision maker. We

assume that link capacities are easily shared to transmit traffic as needed. In the event of failures, we assume that the network utilizes all available resources to reroute traffic in an optimal manner. We do not consider the details of routing protocols and shared ownership agreements required to make this all possible. With these assumptions we likely overestimate the ability of the network to transmit information and handle failures, but the results provide an upper bound on the network's ability to do so, and they therefore yield an optimistic estimate of the impact of attacks or disruptions on the system.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

We review three main topic areas in the academic literature that give context to this thesis. The first area of research is analyzing and modeling disruptions to the global undersea cable infrastructure. The second area of research is the use of gravity models for estimating unknown parameters. The final area of research is the Attacker-Defender (AD) style of modeling developed at the Naval Postgraduate School.

A. GLOBAL UNDERSEA CABLE INFRASTRUCTURE

Masi, Smith, and Fischer (2010) analyze the effects of natural and man-made disasters on both terrestrial and undersea optical fiber cable systems. They argue that a single cut to an optical fiber communications cable typically has little impact since the communications may be rerouted through alternative cables. However, they note that multiple simultaneous cuts, especially with undersea cables, may result in significant damage. The ability to reroute communications diminishes with each successive cable that is cut.

Collins (2011) highlights the importance of redundancy in undersea cable systems. He examines how Japan's communications infrastructure performed in the face of the catastrophic earthquake and tsunami that occurred there in early 2011. He notes that throughout the disaster, Japan sustained their international communications capabilities which allowed them to coordinate assistance from other countries in the emergency response and recovery efforts. Collins attributes that success to the redundancy gained by routing undersea cables in separate undersea trenches and bringing them ashore at different cable landing stations.

Omer, Nilchiani, and Mostashari (2009) measure the resilience of the global undersea cable infrastructure using network modeling. Their network model is highly aggregated. The nodes in the network represent major geographic regions of the world, of which they use eight total. Further, a single undirected edge between two nodes in their model represents the collection of all existing submarine cables passing between the two nodes. For example, the edge between North America and Europe represents the

combined flows and capacities of all submarine cables connecting those two regions. There are 12 total edges in their model. Their model demonstrates a broad-scale approach with possible applications to similar networked infrastructure systems. They define the "value delivery" of the infrastructure as the total amount of information that is carried through the network. They measure resiliency as the ratio of the value delivery of the system after a disruption to the value delivery of the system before the disruption. Finally, their article also highlights the critical importance of rerouting and redundant capacities for a more resilient communications infrastructure.

Sechrist (2010b) uses an analytic framework based on a "Danger Index" to determine a risk assessment for the global undersea cable infrastructure as a whole. The "Danger Index" is defined as the product of *Intention*, *Capability*, *Vulnerability*, and *Consequence*. Intention refers to the intent of those causing damage to cables, whether malicious or benign. Capability refers to the knowledge, skills, and special tools required to purposefully damage undersea cables. Vulnerability is assessed based on qualitative factors such as cable route diversity, physical security of cables and cable landing stations, and whether or not cables lie in fault-prone earthquake zones. Consequence refers to the size, duration, and economic costs associated with cable disruptions. Sechrist demonstrates that the four variables of the equation are all increasing, and subsequently concludes that the global undersea cable architecture is at an increased risk of danger. He provides a number of policy recommendations to lower the "Danger Index" for the undersea cable infrastructure including hardening of facilities, prioritizing traffic, encouraging cable protection zones, and creating disaster recovery plans.

B. GRAVITY MODELS

As described by Chang et al. (2006), gravity models take their name from Newton's law of gravitation, and are commonly used by social scientists to model or estimate the flow of people, goods, or information between geographic areas. In Newton's law of gravitation the force is proportional to the product of the masses of the two objects divided by the distance squared. Similarly, gravity models use readily available data such as population statistics (or other surrogate) and distances between

cities to develop the intensity for pair-wise interactions, such as volume of traffic flow. However, as Chang et al. (2006) point out, locality is not as large a factor in Internet traffic as with the transport of physical goods. In their gravity model of Internet traffic, the traffic exchanged between two locations is proportional to the volumes entering and exiting at those locations. More specifically, they denote network nodes by n_i, $i = 1, \ldots, k$, and the traffic matrix by T, where $T(i, j)$ denotes the volume of traffic that enters the network at node n_i and exits at node n_j. Let $T^{in}(i)$ and $T^{out}(j)$ denote the total traffic that enters the network via node n_i, and exits the network via node n_j, respectively. The gravity model is then computed by

$$T(i, j) = T^{tot} \frac{T^{in}(i)}{\sum_k T^{in}(k)} \frac{T^{out}(j)}{\sum_k T^{out}(k)} = T^{tot} p^{in}(i) p^{out}(j)$$

where T^{tot} is the total traffic across the network, and $p^{in}(i)$ and $p^{out}(j)$ denote the proportion of traffic entering and exiting the network at nodes i and j respectively. For this model, then, we still need to know the total volume of traffic that enters and exits at each node or else the total traffic across the entire network along with some good estimators for the probabilities of traffic entering and exiting at each location. Gravity models such as this are particularly useful, necessary in fact, when actual or historical data is either unavailable or too expensive to gather.

Omer, Nilchiani, and Mostashari (2009) use a simpler gravity model to approximate traffic demand in their network model of the global undersea cable infrastructure. For each node, they calculate the demand by multiplying the number of internet users by the average content downloaded per person per day. As a result, they have a demand value for traffic at each node. However, they do not explicitly state how that demand is proportioned from among the other nodes. Rather, the percentages of that demand coming from the various others nodes are assumed.

Nandi, Vasarhelyi, and Ahn (2000) also present a gravity model for estimating the flow of Internet traffic between countries. Their model is primarily based on the theory of network externality. Specifically, they assume that the flow of traffic among different countries is directly linked with the number of Internet hosts in those countries. The state

of Internet connectivity among different countries is implicitly incorporated into their model by using this information on the number of hosts. Admittedly, their model does not consider the role of language or cultural aspects in the flow of Internet traffic. The mathematical formulation of their model is similar to the one used by Chang et al. (2006) where the total traffic across the network is distributed among the different countries based on the probabilities of traffic entering or exiting the network at each country. In the model by Nandi, Vasarhelyi, and Ahn (2000), those probabilities are effectively determined by the number of Internet hosts in each country.

C. ATTACKER DEFENDER MODELING

Brown et al. (2005, 2006) present a class of network interdiction models specifically tailored to critical infrastructure systems and the intelligent adversaries (i.e., terrorists) who threaten them. These Attacker-Defender (AD) models use bi-level and tri-level optimization to pinpoint the most vulnerable components of an infrastructure, analyze worst-case scenarios, and identify optimal defense plans to enhance the resilience of the system. They start by building an "operator's model" which is a mathematical model of the normal, day-to-day operating realities of the infrastructure system. This model prescribes the network flows that optimize system performance under idealized conditions. The "attacker's model" is built on the operator's model. In the "attacker's model", an intelligent adversary attacks the infrastructure where it causes maximum damage to system performance. The capability of the attacker is adjusted to analyze various potential scenarios. Finally, the "defender's model" builds off the first two and allows the defender to mitigate disruptions by making strategic investments of limited resources for hardening, redundancy, or capacity expansion. The development of AD models allows for the systematic identification of optimal defensive plans for infrastructure systems.

Information transparency is a key assumption of the AD models. In other words, the attacker has perfect knowledge of how the defender will (or should) optimally operate the system, even after an attack. To demonstrate and test the AD style of modeling, Brown et al. (2005, 2006) often create hypothetical but realistic scenarios. They

assemble “red” teams to gather strictly open-source data on the proposed infrastructure target. The data gathered is used to inform the AD model, and it also helps with demonstrating just how easy it may be for potential terrorists to identify the vulnerabilities of a given infrastructure. We apply the AD modeling techniques, including the use of strictly open-source data, in our analysis of the global undersea cable infrastructure.

D. OUR CONTRIBUTIONS IN CONTEXT

We create the network structure and mathematical formulations to model the global undersea cable infrastructure. We then superimpose simple graphs of each individual cable system onto the larger network one by one to create a large, complex network. We analyze scenarios involving only a small number of specified countries and cables in a particular geographic region all the way up to scenarios involving all the cables in the world. We present examples of such scenarios and demonstrate their implementation in our model. Our approach follows directly from the AD modeling style developed by Brown et al. (2005, 2006) for the analysis of critical infrastructure systems. Our AD style of modeling contrasts with the risk-based approach used by Sechrist (2010b). And while Omer, Nilchiani, and Mostashari (2009) represent the global undersea cable infrastructure as a network model, we build on their approach to achieve a more realistic network model where each cable system is represented individually.

THIS PAGE INTENTIONALLY LEFT BLANK

III. MODEL FORMULATION

Our analysis proceeds in three steps. In the first step we develop a mathematical model of the undersea cable system as an Attacker-Defender (AD) model. By running the model through a variety of scenarios, we gain insight into the critical components of the infrastructure along with potential worst-case disruptions in terms of multiple simultaneous attacks. The second step in our model development is data collection. This includes gathering the key information on the real-world cable systems including the configuration, landing stations, and capacity of each cable system. We also develop a gravity model to estimate traffic demand between countries. Finally, we build our network model by abstracting all of the currently existing undersea cable systems into individual graphs. We introduce our network modeling approach with a specific example.

A. MATHEMATICAL MODEL

We model the end-to-end information flows mathematically using a multi-commodity (minimum-cost) network flow (MCNF) model. The traffic demand between each pair of countries drives the flow in our mathematical model. We measure network performance as the total cost to send all traffic through the network, with our goal being to satisfy the demand at minimum cost. Each unit of unsatisfied demand is penalized by a shortage cost which may be different for each supply and demand location. For example, the shortage cost for traffic lost from the United States to Israel may be higher than for traffic lost from South Africa to Singapore. By changing the relative shortage costs for different supply-demand combinations, we can prioritize different end-to-end traffic flows.

In order to ensure that flows are dropped only when there does not exist a feasible path through the network, we set the shortage cost for dropping one unit of flow to be larger than the cost of routing that unit along the longest possible path in the network. The longest possible path in the network can be defined as nC, where $n = |N|$ and $C = \max\{c_{ij} : (i, j) \in A\}$. We define commodities in our model in terms of their

destinations. Specifically, we let Y_{ij}^t denote the flow of traffic destined for node t that travels over arc (i, j). We let $B = [b_s^t]$ be the traffic matrix denoting the demand for traffic between all source-destination pairs $s - t$, where $b_s^t > 0$ represents the volume of traffic required to flow from node s to node $t \neq s$ in the network. We also define $b_t^t = -\sum_{s \neq t} b_s^t$ as the total flow of traffic that enters the network at node t. The remaining details of the model follow in three phases: the operator's problem, the attacker's problem, and solving the AD model.

1. Operator's Problem

We develop the operator's problem to determine the optimal flow under normal conditions. The operator's problem identifies the specific routes and quantities of flow on each route in order to satisfy demand at minimum cost. The operator's problem gives us a basic understanding of the flow of telecommunications traffic on a regular basis under ideal conditions.

Index Use

$n \in N$	Nodes (alias *i*, *j*, *s*, *t*)
$(i, j) \in A$	Directed arcs

Data [units]

c_{ij}	Flow cost over arc *(i, j)* [$/Gbps]
u_{ij}	Capacity on arc *(i, j)* [Gbps]
b_s^t	Demand for traffic between *s* and *t* [Gbps]
ρ_s^t	Per-unit shortage cost for dropped flow between *s* and *t* [$/Gbps]

Decision Variables [units]

Y_{ij}^t Total flow of traffic destined for *t* that travels over arc *(i, j)* [Gbps]

W_s^t Amount of *s*-*t* traffic that is dropped [Gbps]

Formulation [dual variables]

$$\min_{Y,W} \quad \sum_{(i,j)\in A} c_{ij} \sum_{t\in N} Y_{ij}^t + \sum_{s,t\in N} \rho_s^t W_s^t \qquad \text{(D0)}$$

$$s.t. \quad \sum_{j:(s,j)\in A} Y_{sj}^t - \sum_{i:(i,s)\in A} Y_{is}^t + W_s^t = b_s^t \qquad \forall s,t \in N, s \neq t \qquad [\alpha_s^t] \qquad \text{(D1)}$$

$$\sum_{j:(t,j)\in A} Y_{tj}^t - \sum_{i:(i,t)\in A} Y_{it}^t - \sum_{s:s\neq t} W_s^t = b_t^t \qquad \forall t \in N \qquad [\alpha_t^t] \qquad \text{(D2)}$$

$$\sum_{t\in N} Y_{ij}^t \leq u_{ij} \qquad \forall (i,j) \in A \qquad [-\beta_{ij}] \qquad \text{(D3)}$$

$$Y_{ij}^t \geq 0 \qquad \forall (i,j) \in A, \forall t \in N \qquad \text{(D4)}$$

$$W_s^t \geq 0 \qquad \forall s,t \in N \qquad \text{(D5)}$$

Discussion

The objective function (D0) includes the cost of routing flows to their destinations and the cost of any dropped flows. Constraint (D1) enforces the balance of flow for each node $s \in N$ and each commodity destination $t \in N, t \neq s$. Constraint (D2) enforces the balance of flow for each commodity destination node $t \in N$. Constraint (D3) ensures the capacity on each arc is not exceeded. Constraints (D4) and (D5) ensure all actual flows and dropped flows, respectively, are nonnegative.

Solving the operator's problem provides tremendous value, particularly in an industry where the demand often outpaces the capacity of the industry. For example, consider a telecommunications carrier looking to expand but having a limited budget for expansion. Suppose the choice is between constructing a new undersea cable from the

United States to Japan or a cable from India to Australia. Running the operator's problem for each proposed design easily reveals the extent to which those designs can meet the traffic demand.

2. Attacker's Problem

In the attacker's problem, we consider an intelligent adversary whose goal is to choose a set of arcs whose removal will create a worst-case disruption for the network operator. An attack in our model corresponds to an undersea cable that is cut or otherwise disrupted. We assume that each attack results in complete interdiction of flows traveling in both directions along the cable. We also consider scenarios where the attacker chooses to attack cable landing stations effectively interdicting flow on all of the cables entering those landing stations. To model the attacker's actions, we introduce binary variables X_{ij} for each attackable arc (i, j). We let $X_{ij} = 1$ if the attacker chooses to interdict arc (i, j), and $X_{ij} = 0$ otherwise. We assume that the attacker is limited by the number of attacks he can conduct, denoted by the scalar $\overline{attacks}$. The remaining details of the attacker's problem follow in the formulation.

Additional Index Use

$(i, j) \in B$	Arcs that may be attacked

Additional Data [units]

p_{ij}	Additive cost for sending flow over an attacked arc [$/Gbps]
$\overline{attacks}$	Number of attacks allowed [scalar]

Additional Decision Variables [units]

X_{ij}	Binary variables where $X_{ij} = 1$ if arc *(i, j)* is attacked, 0 otherwise

Formulation

$$\max_{X} \min_{Y,W} \sum_{(i,j)\in A} (c_{ij} + p_{ij} X_{ij}) \sum_{t\in N} Y_{ij}^{t} + \sum_{s,t\in N} \rho_s^t W_s^t \qquad \text{(A0)}$$

s.t. (D1), (D2), (D3), (D4), (D5)

$$\sum_{(i,j)\in B} X_{ij} \le 2 \cdot \overline{attacks} \qquad \text{(A1)}$$

$$X_{ij} = X_{ji} \qquad \forall (i,j) \in B \qquad \text{(A2)}$$

$$X_{ij} \in \{0,1\} \qquad \forall (i,j) \in B \qquad \text{(A3)}$$

Discussion

The objective function (A0) follows from the operator's problem but now includes the attack variables, X_{ij}, for each attackable arc. If an arc is attacked, any flows along it incur an additional per-unit penalty cost p_{ij}. Since we assume that an attack on an arc means complete interdiction of that arc, we set the penalty cost for using attacked arcs to be greater than the shortage cost for unsatisfied demand. The network will always drop flow rather than send flow over a more expensive, attacked arc. Hence, attacked arcs are effectively impassable. As a result, our model reflects the basic behavior of the real world system. Constraints (D1) through (D5) are unchanged from the operator's problem. Constraint (A1) limits the number of interdictions allowed by the attacker. Constraint (A2) ensures that an attack on an arc in one direction results in an attack on that same arc in the opposite direction. Modifying the scalar $\overline{attacks}$ allows us to consider various scenarios relating to the attacker's capability. Finally, constraint (A3) implements the binary restriction on each attack variable.

3. Solving the Attacker Defender Model

The attacker's problem is a bi-level max-min optimization problem. The operator wants to minimize the cost of operating the system while the attacker seeks to maximize that minimum cost. Unfortunately, this formulation is not a mixed integer linear program (MILP) and hence not easily solved using commercial integer linear programming

solvers. To solve this formulation, we fix the attack variables and treat them as constants, then take the dual of the inner problem, and finally release the attack variables to produce a MILP which can be solved directly using commercial solvers. The resulting formulation follows.

Additional Decision Variables

α_s^t Dual variable corresponding to equations (D1) and (D2) of the Operator's Problem

β_{ij} Dual variable corresponding to equation (D3) of the Operator's Problem

Formulation [dual variables]

$$\max_{\alpha,\beta,X} \sum_{s,t\in N} b_s^t \alpha_s^t - \sum_{(i,j)\in A} u_{ij}\beta_{ij} \qquad \text{(AD0)}$$

s.t. $\alpha_i^t - \alpha_j^t - \beta_{ij} - p_{ij}X_{ij} \le c_{ij}$ $\quad \forall (i,j)\in A, t\in N$ $\quad [Y_{ij}^t]$ (AD1)

$\alpha_s^t \le \rho_s^t$ $\quad \forall s,t\in N$ $\quad [W_s^t]$ (AD2)

$\alpha_t^t = 0$ $\quad \forall t\in N$ (AD3)

$\beta_{ij} \ge 0$ $\quad \forall (i,j)\in A$ (AD4)

(A1), (A2), (A3)

Discussion

The objective function (AD0) to be maximized results from the dual of the inner problem in the attacker's problem. We have one dual variable, α_s^t, for each node combination in the network and one dual variable, β_{ij}, for each arc in the network. These dual variables now serve as decision variables. Their optimal solutions reflect the relative importance of the corresponding constraints from the attacker's (primal)

problem. Constraints (AD1) through (AD4) also follow from the dual of the inner problem in the attacker's problem. Constraints (A1) through (A3), unchanged from the attacker's problem, ensure the attack plan is feasible.

Based on the number of attacks allowed, the solution to the AD problem gives us the optimal attack locations. From the eyes of an intelligent adversary with the intent of inflicting maximal damage, these attack locations reflect the components which are most attractive to attack. Further, we can transfer this interdiction plan back to the original attacker's problem and solve for the operator's new best flow plan with the interdictions in place. This yields insight into the resilience of our system. We see exactly how the system responds and how effectively it absorbs the impact of the attack plan. Looking at the increased cost in the objective function, we also see the relative damage associated with each attack plan. Finally, by modifying the attacker's capability over a range of values and analyzing the output, we determine the worst-case disruptions to system performance in regards to an increasing number of simultaneous attacks.

B. DATA COLLECTION

The data to support our model consists of two primary types: capacity and traffic demand. Capacity values for all currently existing submarine cables are straight forward and readily available on public sources. We focus primarily on the *lit capacity* of each cable system. Lit capacity refers to the actual traffic-carrying capability of a cable based on what has been equipped to date. Design or max capacity refers to the maximum traffic-carrying capability of a cable if it were fully equipped using today's technology. Design capacity combines lit and unlit (or dark) capacity.

The traffic demand between each pair of countries is considerably more difficult to quantify. For competitive and privacy reasons, privately-owned undersea cable operators seldom provide historical records of the traffic volume on their cables. Additionally, there are many different metrics used to measure the flow of telecommunications traffic. For our network model, we seek demand in bandwidth terms, namely Gbps. The used bandwidth between two locations effectively represents the demand between those locations at a snapshot in time. Obviously the used bandwidth

fluctuates throughout the day with spikes during normal business hours. In practice, most network providers use the peak traffic demand over a given time period to represent used bandwidth since "a network that is able to accommodate the daily peak load will necessarily accommodate all demand at every other second of the day" (Terabit Consulting, 2002).

We develop a gravity model to estimate international traffic flow between each pair of countries. We are not concerned with domestic traffic. On the other hand, we are concerned with both the inbound and outbound traffic for each country. On a typical route, voice data only accounts for about one percent of the total demand (Szajowski, 2010), so we focus our analysis on Internet traffic. Our gravity model for traffic is a modified version of those developed by Nandi et al. (2000) and Chang et al. (2006). As with Nandi et al. (2000), the flow of traffic among countries in our model is directly dependent on the number of Internet hosts in each country. As the population of interest, the number of Internet hosts reasonably reflects the level of connectivity within each country along with the degree to which countries communicate with each other. This measure also reflects the asymmetric nature of Internet traffic. Countries with a small share of hosts relative to the Internet world receive more traffic than they send, while countries with a large share, such as the United States, send more traffic than they receive. Additionally, these statistics are widely available in the public domain. The number of Internet hosts for each country is listed in Appendix A and is assumed to be correct for this model. Our gravity model for computing the traffic matrix $B = [b_s^t]$ follows.

Index Use

$n \in N$ Countries (alias *s*, *t*)

Data [units]

T^{tot} Total traffic across the network [Gbps]

T_s Total traffic associated with country *s* [Gbps]

T_{st} Total traffic exchanged between country *s* and country *t* [Gbps]

b_s^t Traffic from country *s* to country *t* [Gbps]

H_n Number of Internet hosts in country *n* [scalar]

Formulation

$$T_s = \frac{H_s}{\sum_{n \in N} H_n} T^{tot} \qquad \forall s \in N \qquad \text{(G0)}$$

$$T_{st} = \frac{H_t}{\sum_{n \in N} H_n} T_s \qquad \forall s,t \in N \qquad \text{(G1)}$$

$$b_s^t = \frac{H_s}{H_s + H_t} T_{st} \qquad \forall s,t \in N, s \neq t \qquad \text{(G2)}$$

$$b_t^t = -\sum_{s:s \neq t} b_s^t \qquad \forall t \in N \qquad \text{(G3)}$$

Discussion

From the total traffic across the network, equation (G0) computes the share that is associated with country *s*. From the total traffic of country *s*, equation (G1) computes the share that is exchanged with country *t*. Then, from the total traffic exchanged between

countries *s* and *t*, equation (G2) computes the share of traffic that travels from country *s* to country *t*. Finally, equation (G3) computes the total flow of traffic that enters the network at node *t*. We demonstrate our gravity model with an example. For the total traffic across the network, we use 55 Tbps, an estimate of the international demand for Internet bandwidth in 2011 (Telegeography, 2011). We use the list in Appendix A for the number of Internet hosts in each country. The resulting traffic matrix, for a small sampling of countries, is shown in Table 2. Since we define commodities in terms of their destinations, the negative values on the diagonals represent the demand of the commodity corresponding to that destination. For example, USA has a demand of approximately 352 Gbps of the commodity "USA". Correspondingly, Australia has a supply of approximately 16 Gbps of the commodity "USA", Brazil a supply of approximately 34 Gbps of the commodity "USA", and so on. The sum for each column in the traffic matrix then is equal to zero.

	USA	Australia	Brazil	China	Colombia	France	India	Israel	Japan	Singapore	UK
USA	-351.59	536.35	765.33	609.68	103.93	607.01	185.71	69.60	2016.74	40.97	286.21
Australia	16.32	-631.98	9.94	8.97	2.68	8.95	4.26	1.89	13.53	1.16	5.80
Brazil	33.67	14.37	-879.35	15.51	4.07	15.47	6.69	2.83	26.00	1.72	9.38
China	21.18	10.23	12.25	-712.23	3.12	10.93	5.02	2.19	17.15	1.34	6.91
Colombia	0.60	0.51	0.53	0.52	-131.52	0.52	0.39	0.24	0.58	0.17	0.44
France	20.99	10.17	12.16	10.88	3.10	-709.33	5.00	2.17	17.01	1.33	6.87
India	1.92	1.45	1.57	1.49	0.69	1.49	-230.82	0.53	1.79	0.35	1.18
Israel	0.27	0.24	0.25	0.24	0.16	0.24	0.20	-88.87	0.26	0.10	0.22
Japan	251.96	55.52	73.82	61.67	12.48	61.45	21.65	8.47	-2097.27	5.04	32.20
Singapore	0.09	0.09	0.09	0.09	0.07	0.09	0.08	0.06	0.09	-52.76	0.08
UK	4.58	3.05	3.41	3.19	1.23	3.18	1.83	0.90	4.13	0.58	-349.30

Table 2. Traffic matrix, based on 55 Tbps total traffic across the network, showing the demand for traffic, in Gbps, between a small sample of countries.

C. NETWORK MODEL

We model the real-world infrastructure explicitly. We prefer a high-fidelity network model because that is where the value of rigorous optimization is often realized. As described by Brown et al. (2006), in the analysis of large infrastructure systems the most damaging, coordinated attacks are not always obvious, and the most effective

defenses are not necessarily intuitive. A more detailed model also allows us to pinpoint the actual physical components that are most vulnerable which leads to recommendations that are specific and actionable.

We model each undersea cable system as its own network. All of these models taken together form the complete network. This method allows us to add or remove individual cable systems as needed. In addition to identifying all the existing cables worldwide along with their landing stations, we take special care in the configuration of each cable. The exact network configuration of each cable system is unique. While the logical topologies are almost always confidential, the physical topologies are readily available from a number of public sources in most cases. As such, we match the arcs in our network model with the physical configurations available for each cable system. We introduce our network modeling approach with a specific example of the abstraction of one undersea cable system into a network.

The Flag Falcon Cable System connects numerous countries throughout Africa, the Middle East, and South Asia. Incidentally, Flag Falcon was one of the cable systems cut during the widespread disruptions in early 2008. Figure 6 shows an overall view of the Flag Falcon Cable System.

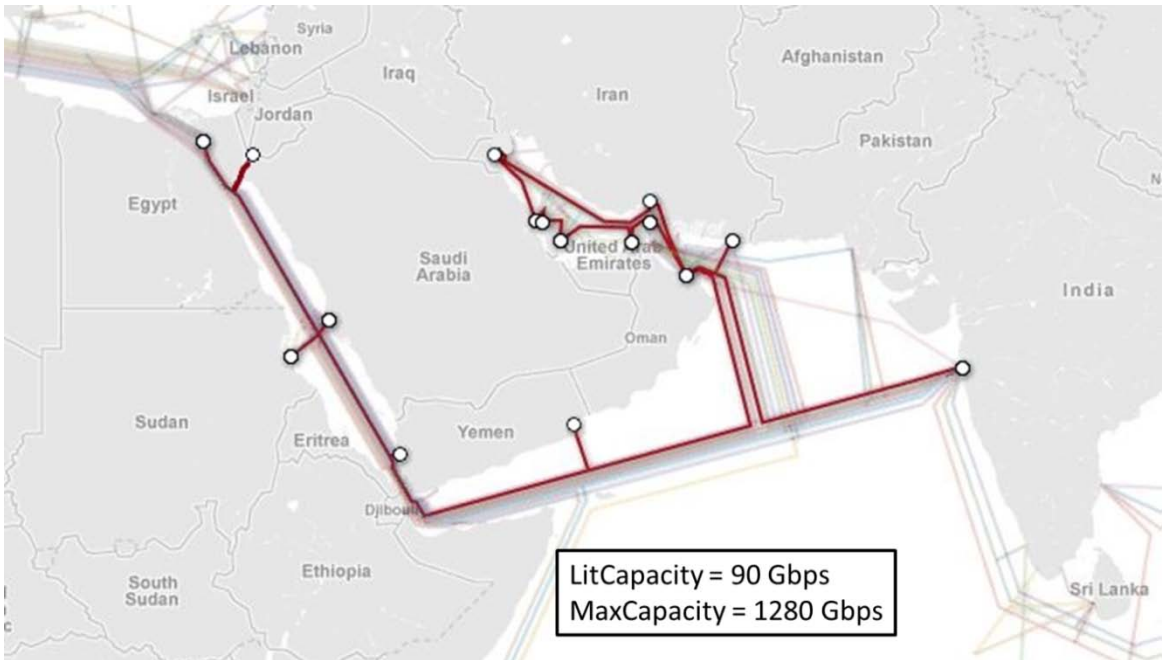


Figure 6. Physical configuration of the Flag Falcon Cable System (Adapted from Telegeography, 2012b).

The Flag Falcon Cable System consists of a mix of branched string and ring configurations. Starting in Egypt, Flag Falcon runs the length of the Red Sea and then along the southern coast of the Arabian Peninsula with branches to several countries along the way. The Persian Gulf section of the cable is a self-healing ring design with landing stations throughout the Gulf region. Finally, another branched string travels from Oman to India with a branch to Iran. There are 16 total landing stations in the cable system. Figure 7 shows a portion of the Flag Falcon Cable System and depicts our network modeling approach.

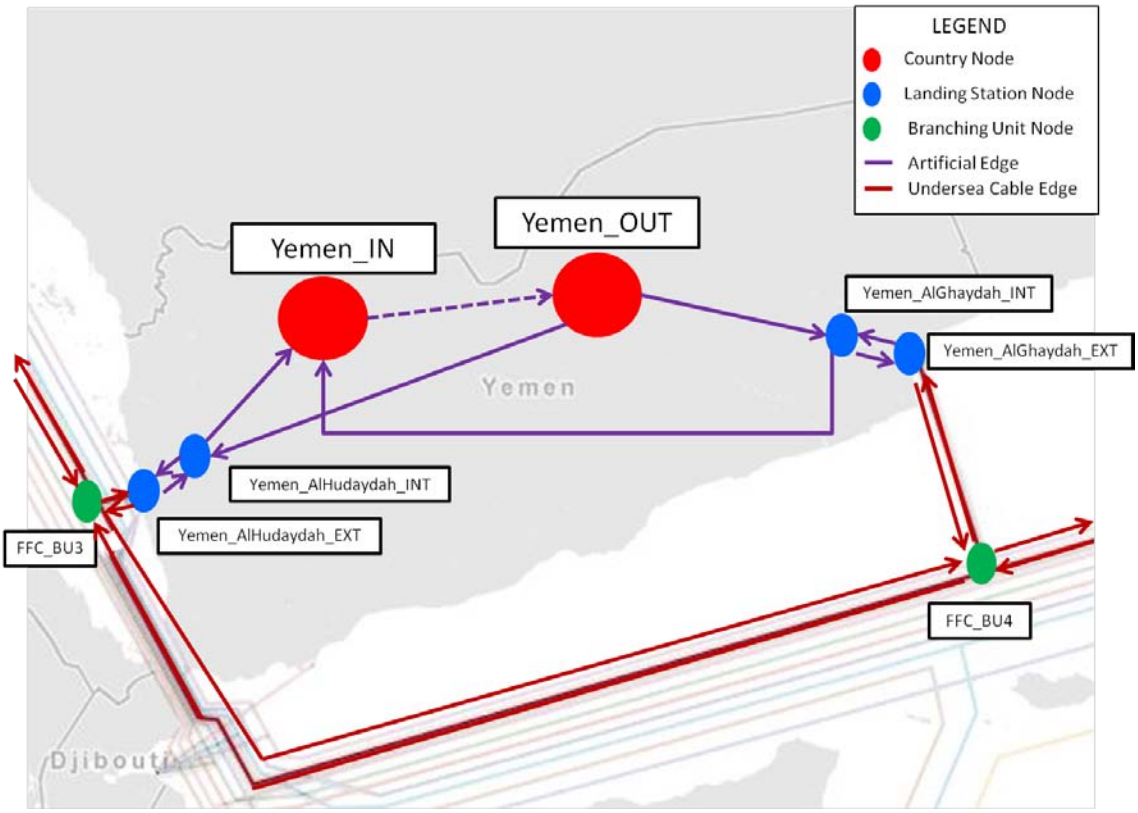


Figure 7. Network design showing a portion of the Flag Falcon Cable System (FFC) with nodes representing the country (red), landing stations (blue), and branching units (green) (Adapted from Telegeography, 2012b).

In our network design, each country involved in the cable system is represented by two nodes: an input node and an output node. The input node receives the traffic destined for that country, while the output node sends out the traffic that is destined for other countries. Each country's input node is connected to its output node by a single directed edge. The capacity on this edge is dependent on the terrestrial optical fiber cable infrastructure of the respective country. For countries with well-developed terrestrial cable systems such as the United States, we assume the capacity on this directed edge is effectively unlimited. For countries with limited terrestrial infrastructure, we assume the capacity is negligible. In effect, this assumption determines whether traffic may travel across the terrestrial systems of a country to be passed along to other undersea cable systems. In the example here, we assume the terrestrial cable infrastructure in Yemen is not sufficient to transfer traffic from one cable landing station in Yemen to the other

cable landing station in Yemen via terrestrial systems. To indicate this assumption, we represent the zero-capacity directed edge from Yemen's input node to its output node with the dotted line in Figure 7. In addition to the terrestrial cable infrastructure within each country, we also consider the terrestrial infrastructure between countries which share a land boundary such as the United States and Canada. When the terrestrial infrastructure between two countries is well-developed, we use a directed edge from the output node of one country to the input node of the other country and vice versa. This assumption allows traffic to be sent between countries via terrestrial cable systems. Further in our network design, we represent each cable landing station by a pair of nodes: an interior node and an exterior node. The landing station's interior and exterior nodes are connected by dual edges in opposite directions with abundant capacity on each edge. An attack on these edges effectively represents an attack against the corresponding landing station. Finally, each landing station is connected with its respective country with a directed edge from the landing station's interior node to the country's input node and another directed edge from the country's output node to the landing station's interior node. We assume an abundant capacity on each of these edges as well. In this manner, we create the network structure for all the countries and cable landing stations involved in the model. The only remaining task is to abstract the cable systems themselves into our network.

Since undersea cable systems are designed on a fiber pair basis to support bi-directional flow, the cable capacities represent the capacity for flow in either direction. As such, we represent each segment of a cable system with dual edges in opposite directions where each of the two edges has the given capacity of the respective cable. For each intersection in the physical configuration of a cable system, we assume that a branching unit supports that convergence. We represent each branching unit with an artificial node as shown in Figure 7. As a result, each segment of an undersea cable system starts and ends at either of two nodes: an exterior node of a cable landing station or an artificial node representing a branching unit. In the case of a ring configuration as in the Persian Gulf section of Flag Falcon, each segment of the undersea cable starts and ends at the exterior node of the associated cable landing stations.

Using the modeling technique described here, we construct the basis of our network including the nodes and edges for all countries and their associated landing stations. Then we superimpose the graph of each individual cable system to create a complex network. This modeling approach provides tremendous flexibility in regards to the specific scenarios of interest. We analyze the flow of communications between specific countries or regions in the world by adding or removing the associated cable systems as needed.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. THE EUROPE TO INDIA MODEL

In this section we demonstrate our network modeling technique for undersea cable infrastructure. We analyze the flow of communications between Europe and India. While much of the attention during the undersea cable disruptions in early 2008 in the Mediterranean Sea and Persian Gulf focused on countries in the Middle East, India was actually the most heavily affected country. India had over 2,000 network prefix outages during the disruptions, the highest number among all impacted countries (Zmijewski, 2008). And since many companies throughout Europe outsource call centers and other Internet related business to India, the disruptions created second order effects in the European economy as well. While most of the major bandwidth from India heads east, there are only six undersea cable systems that connect India to Europe. These six cable systems, along with the lit and maximum capacity for each, are listed in Table 3. The capacities shown are assumed to be correct for this analysis.

Cable System	Lit Capacity (Gbps)	Max Capacity (Gbps)
FLAG Europe-Asia (FEA)	85	200
FLAG Falcon	90	1280
IMEWE	520	3840
SEACOM/Tata TGN-Eurasia	100	1280
SeaMeWe-3	90	960
SeaMeWe-4	1350	1700

Table 3. The six undersea cable systems that connect Europe and India along with the capacity of each cable system.

We include the six cable systems from Table 3 in our network model. We use the physical configurations of these cable systems to construct their individual graphs by segment as shown in Appendix B. In regards to traffic, we include all the countries

associated with these six cable systems except those countries to the east of India. There are 35 total countries in the model. We assume the total traffic across the network is 10 Tbps. Under this assumption, the system is near 100 percent operational utilization. That is, under normal operating conditions the six cable systems, based on their lit capacity, effectively transmit all traffic with only a small amount of dropped flow. We also assume that the European countries in this model, along with India and Egypt, have effectively unlimited terrestrial capacity. As such, landing stations in these countries may pass transit traffic along to other landing stations within that same country. Additionally, we assume that the European countries sharing land boundaries also have effectively unlimited capacity via terrestrial or other systems. This assumption, in effect, allows the European countries to exchange traffic without using the six undersea cables in the model. This last assumption is very important. In practice, undersea cables are not often used when easier and less expensive transmission mediums exist. The last assumption ensures the flows on the cables in our model closely resemble the actual flows that could be expected on the corresponding real-world cables in regards to the source and destination of the traffic.

We use our model to analyze the flow of communications between Europe and India under three different scenarios. For each of the three scenarios, we analyze the impact of up to 10 simultaneous interdictions to the system. In this model, an interdiction corresponds to an attack or disruption against an undersea cable or cable landing station. We store the country data and cable system data in Microsoft Excel (Microsoft Corporation, 2012). We use the General Algebraic Modeling System (GAMS) (GAMS, 2010) to implement the mathematical model and solve utilizing CPLEX 12.02 (ILOG, 2007). Finally, we develop a custom Visual Basic for Applications (VBA) (Microsoft Corporation, 2012) user interface for automated scenario generation. The user interface generates the desired network model based on the selected countries and cable systems, computes the traffic between each pair of countries based on the gravity model, and runs the optimization in GAMS.

A. RESULTS

The operator's goal is to transmit the traffic demand for all 35 countries in the model without prejudice to any particular country or countries. Similarly, the attacker seeks to maximize the damage to the overall system rather than target any particular country or countries. In other words, the attacker does not care which countries suffer the greatest loss in telecommunications traffic but rather how much damage is inflicted on the system as a whole. Within this broader context, our analysis focuses primarily on the traffic exchanged between Europe and India. Figure 8 displays a cartoon diagram of the six cable systems in the Europe to India model. This diagram shows the general routing configuration of each cable system. Appendix B provides the exact routing configurations, including all landing stations, for each cable system.

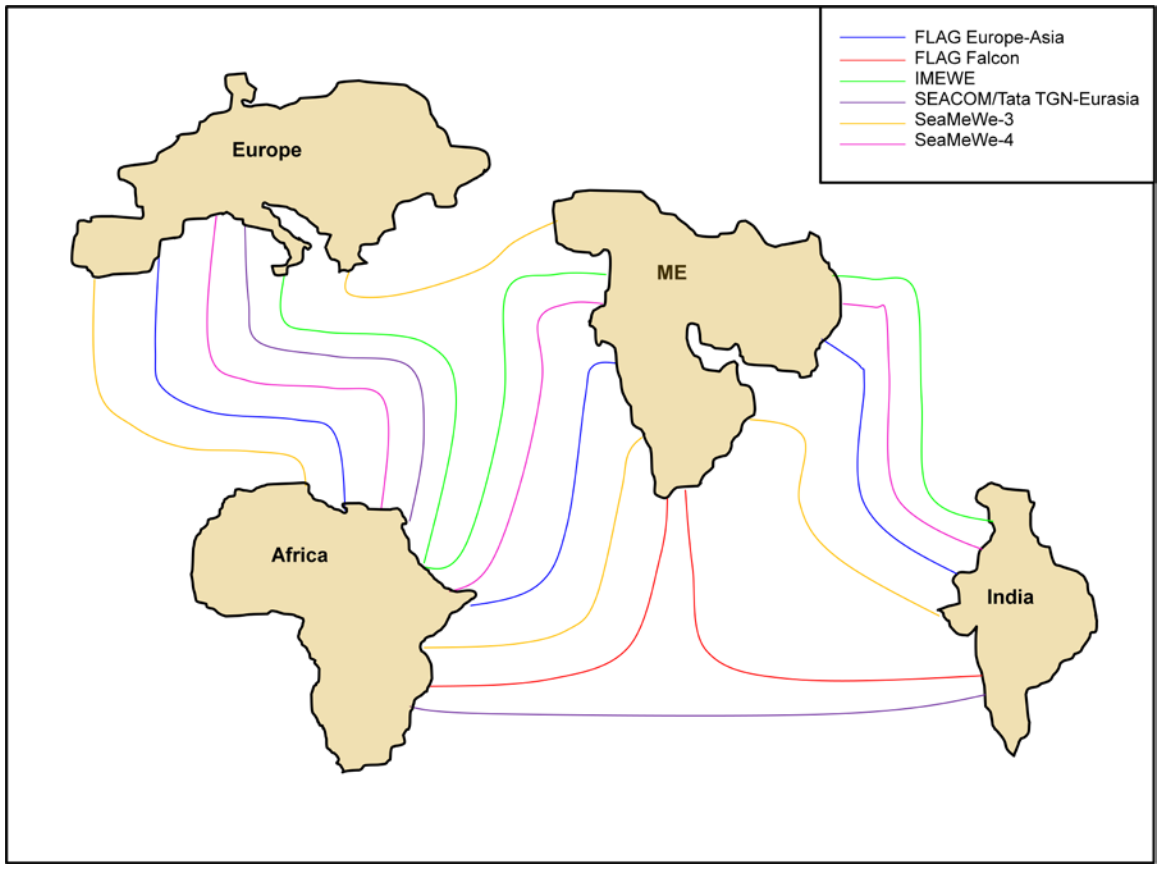


Figure 8. Cartoon diagram of the Europe to India model.

Table 4 provides a summarized version of the traffic matrix aggregated by the four geographic regions from Figure 8. This traffic matrix does not account for all of the traffic demand in this model. In particular, the traffic demand between countries in the same region is not included. We aggregate the traffic by region so we can focus on the traffic between Europe and India. Appendix D provides the complete traffic matrix by country for the Europe to India model.

	Europe	Africa	Middle East	India
Europe	-349.655	345.121	329.519	371.019
Africa	104.862	-377.815	15.511	13.193
Middle East	66.427	10.205	-367.924	8.501
India	178.366	22.489	22.894	-392.713

Table 4. Traffic matrix, in Gbps, for the Europe to India model aggregated by geographic region

1. Scenario One

In the first scenario, we assume each cable system operates at lit capacity. Additionally, we do not allow interdictions against the cable landing stations. Figure 9 shows the operator's resilience curve for scenario one. This curve shows the amount of traffic that is dropped across the entire system at each level of interdiction. Under normal conditions, with no interdictions, the system is not able to satisfy the total traffic demand. The amount of dropped traffic is approximately 400 Gbps. However, none of the traffic demand between Europe and India is dropped. Europe successfully sends approximately 371 Gbps of traffic to India and receives approximately 178 Gbps of traffic from India. Further, all traffic demand between pairs of countries in the same region is also satisfied. Most of the dropped traffic in the no-interdiction case occurs between Europe and Africa with approximately 250 Gbps of dropped flow. Traffic associated with the country of South Africa, either incoming or outgoing, accounts for almost half of that dropped flow between Europe and Africa. In this model, South Africa is an underserved country

relative to the amount of traffic demand associated with it. Only one cable system, the SEACOM Tata/TGN-Eurasia, provides access to South Africa. The consequence of too much demand along a specific route is dropped traffic.

As we introduce interdictions to the system, the amount of dropped traffic increases by a similar amount, approximately 200 Gbps, for each additional interdiction up to the case of five interdictions. Beyond five interdictions, the curve levels out with successive interdictions beyond that offering little additional value in terms of further degrading the system. Further, India is completely isolated from Europe in the case of five interdictions, and hence most of the damage to the system is already accomplished at that level.

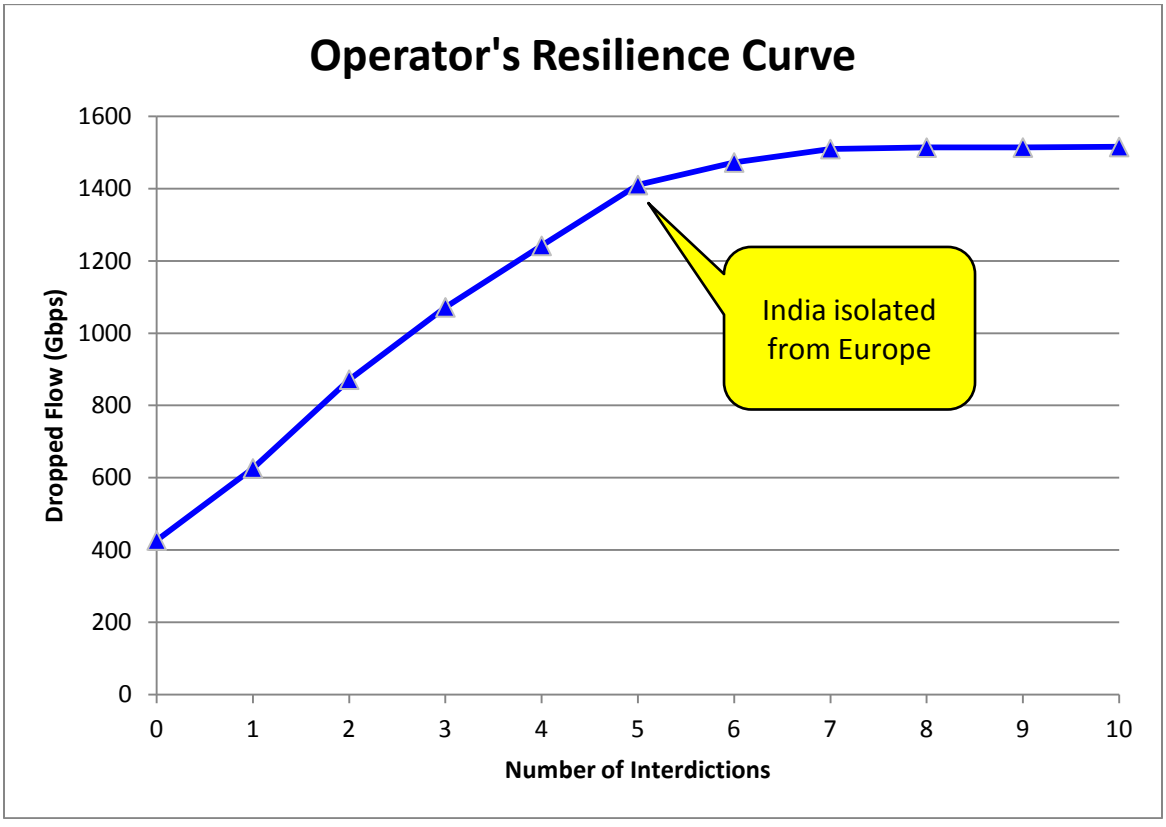


Figure 9. Operator's resilience curve for scenario one.

Figure 10 indicates which cables are interdicted along with the approximate location of the disruptions for each case up to five interdictions. Appendix C provides a

comprehensive list of these interdiction locations by the actual cable segment for each case up to ten interdictions. In Figure 10, we see that the interdiction locations are not always nested; for example, the optimal attack location in the case of one interdiction is not included in the case of two interdictions. The same is true going from four to five interdictions. Figure 10 reveals another interesting observation. Aside from the case of one interdiction, the optimal attack locations always occur between Europe and Africa in the Mediterranean Sea. In the case of two, three, or four interdictions, these attack locations tend to be in the middle of the Mediterranean Sea or near the coast of Africa. In the case of five interdictions, however, we observe the non-nested result. All of the interdiction locations still lie in the Mediterranean Sea. However, in this case the majority of attack locations lie near the coast of Europe rather than Africa.

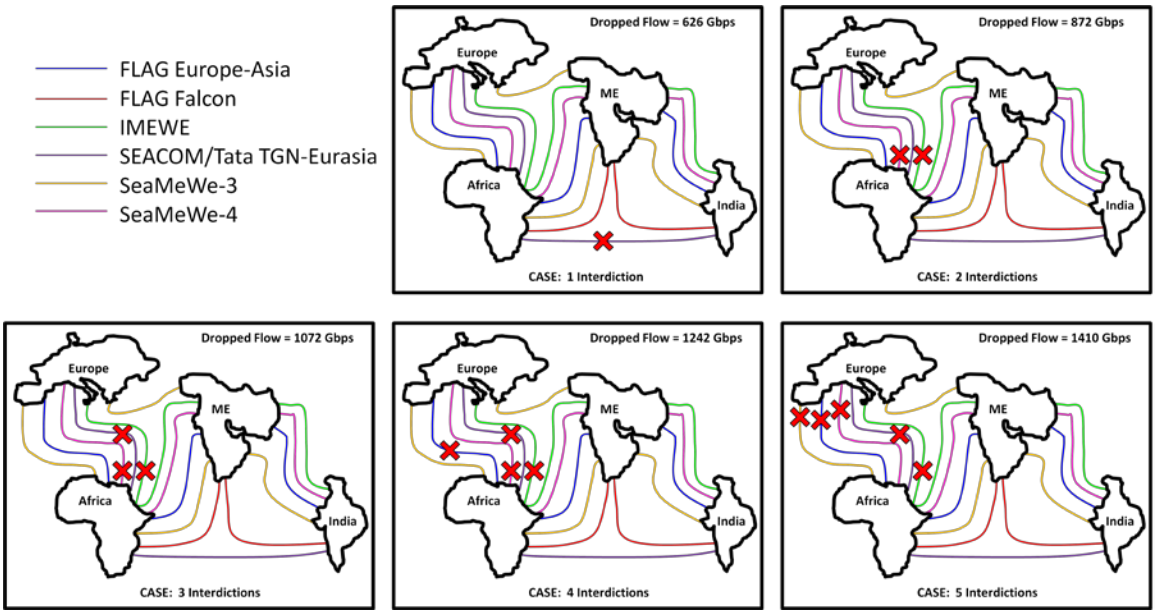


Figure 10. Cartoon diagram for scenario one showing which cables are interdicted along with the approximate location of the disruptions.

Figure 11 provides further analysis of the traffic dropped in scenario one. This chart focuses specifically on the traffic associated with India both inbound and outbound. We already know that India is completely isolated from Europe with five or more simultaneous disruptions. However, looking at Figure 11, India's traffic is actually

severely degraded much sooner than that. Figure 11 shows the percent loss in India's traffic with all other countries in the model, not just those in Europe. While India is fairly resilient in the case of one or two disruptions, almost 70 percent of the traffic destined for or coming out of India is lost with just three simultaneous disruptions. Strikingly, all of this loss to India's communications traffic occurs without a single cable disruption at or near the actual coast of India.

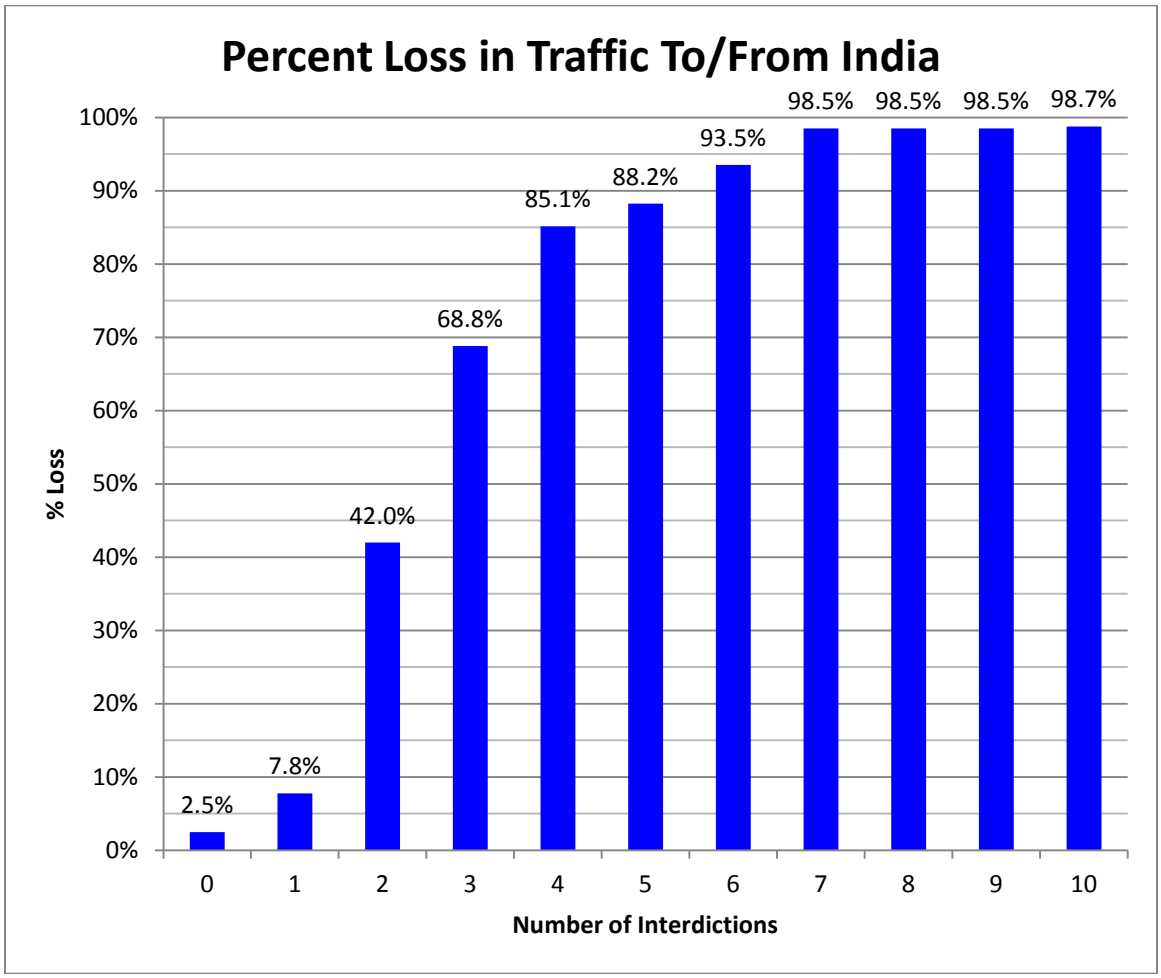


Figure 11. Percent loss in the traffic associated with India in scenario one.

2. Scenario Two

In scenario two we assume each cable system operates at maximum capacity rather than lit capacity. As in the first scenario, we do not allow interdictions against the

cable landing stations. Analyzing the model using the maximum capacity of the cables allows us to see the effect of this redundant capacity. In Figure 12, we compare the operator's resilience curves for scenarios one and two. The first difference we notice between scenarios one and two occurs when the system is operating under normal, ideal conditions with no interdictions.

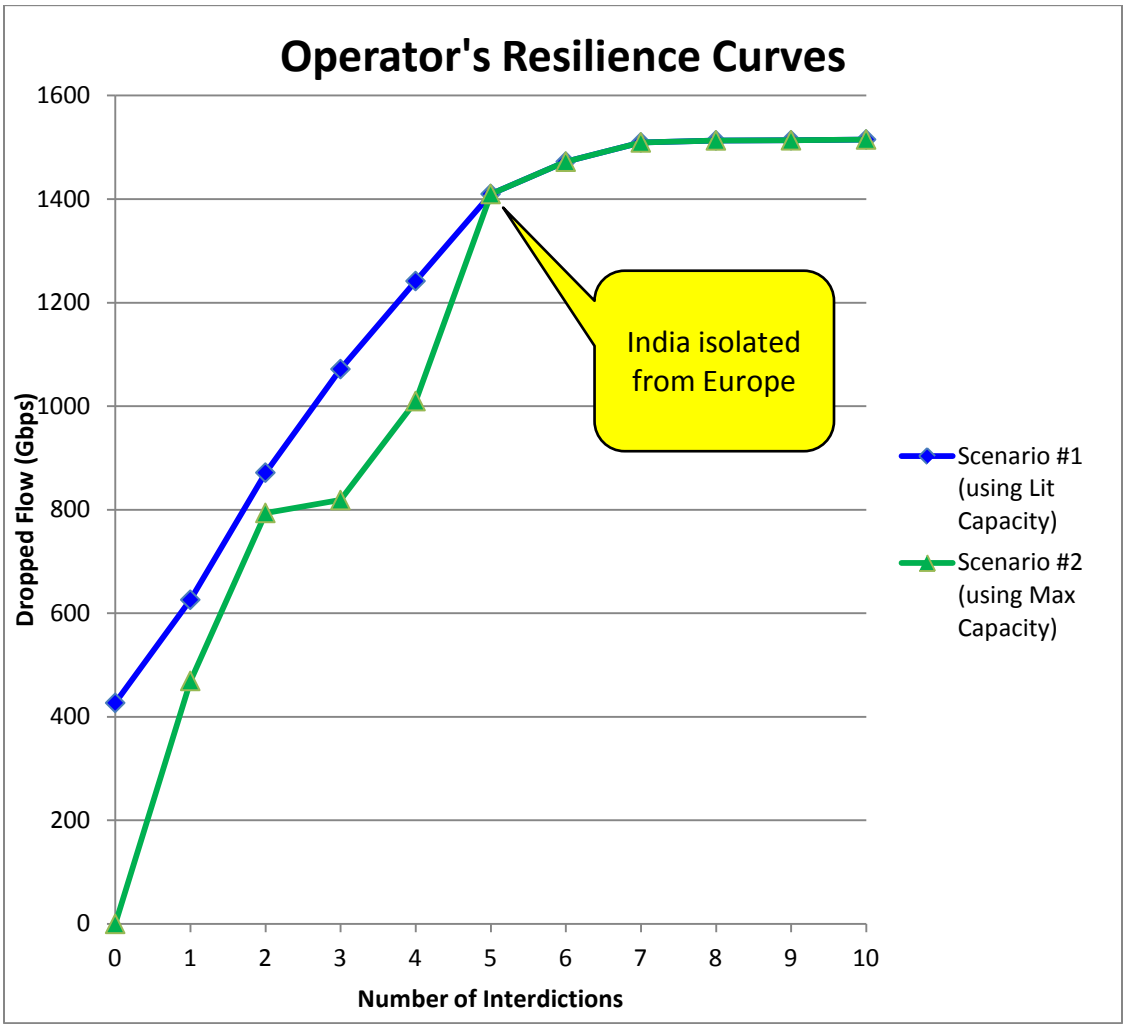


Figure 12. Operator's resilience curves for scenarios one and two

In scenario one when the cable systems operate at lit capacity, the system is not able to satisfy the total traffic demand. The amount of traffic dropped is approximately 400 Gbps. However, in scenario two when the cable systems operate at maximum capacity, the system easily satisfies the total traffic demand with no dropped flow. Figure

13 displays the operational utilization on each segment of one of the cable systems in our model, the SEACOM/Tata TGN-Eurasia, under normal operating conditions with no interdictions. In scenario one, most of the segments in this cable system are at or near 100 percent operational utilization. Meanwhile in scenario two, most of the segments are around just 30 percent operational utilization.

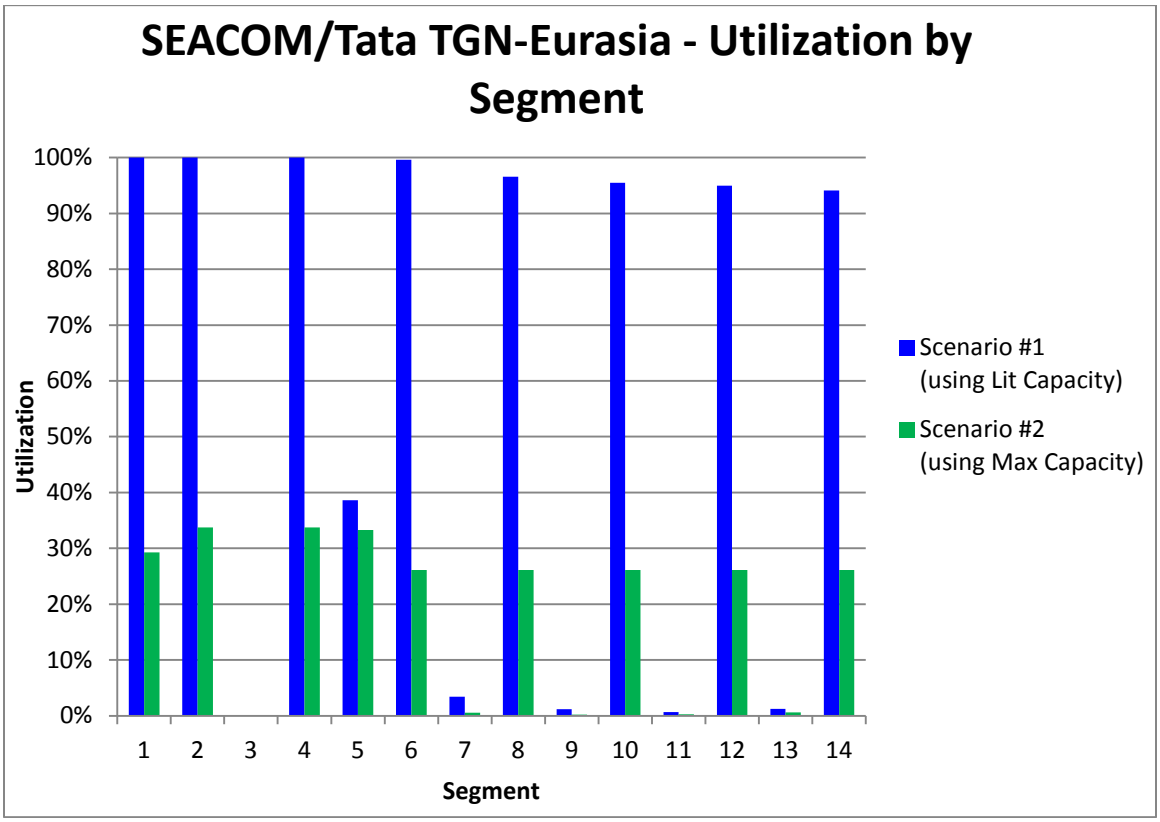


Figure 13. Operational utilization by segment of the SEACOM/Tata TGN-Eurasia cable system under normal conditions with no interdictions

With the additional capacity provided in scenario two, the system is also more resilient to disruption for cases up to four interdictions as we might expect. However, in the case of five or more interdictions, the operator's resilience curves are identical for scenarios one and two. In both scenarios, all of the cables entering Europe are disrupted for these cases. As a result, traffic cannot be re-routed into or out of Europe via excess capacity on other cables. So while the additional capacity of the cables provided by

scenario two is beneficial for small numbers of disruptions, this redundant capacity offers no help in the case of larger numbers of simultaneous disruptions. And as in scenario one, India is still isolated from Europe in the case of five or more interdictions.

Looking back at the operator's resilience curves in Figure 12, the total amount of dropped traffic across the entire system appears only slightly improved for scenario two versus scenario one. However, a closer look at the traffic associated specifically with India reveals significant improvement under scenario two. As shown in Figure 14, under scenario two the system is extremely resilient up to three interdictions in regards to the traffic associated with India. Whereas India experiences nearly 70 percent loss in traffic in scenario one in the case of three simultaneous disruptions, the loss to India is less than 10 percent in scenario two in that same case.

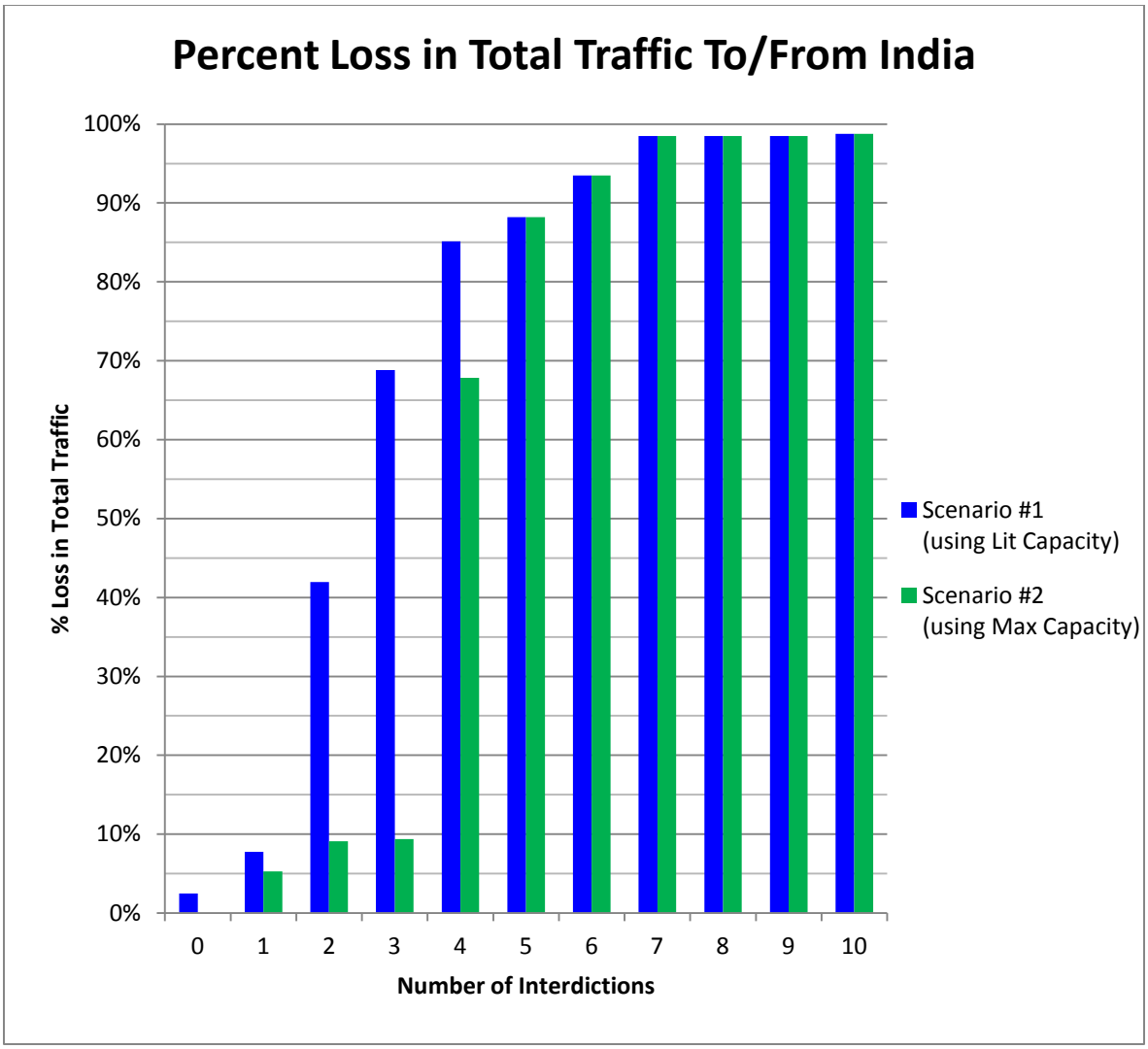


Figure 14. Percent loss in the traffic associated with India for scenarios one and two

Figure 15 indicates which cables are interdicted along with the approximate location of the disruptions for each case up to five interdictions for scenario two. As with scenario one, Appendix C provides a comprehensive list of interdiction locations for each case up to ten interdictions. In Figure 15, the interdiction locations between successive cases are always nested with one exception. Going from three interdictions to four interdictions, we see the non-nested result. In fact, none of the attack locations from the three-interdiction case are present in the four-interdiction case.

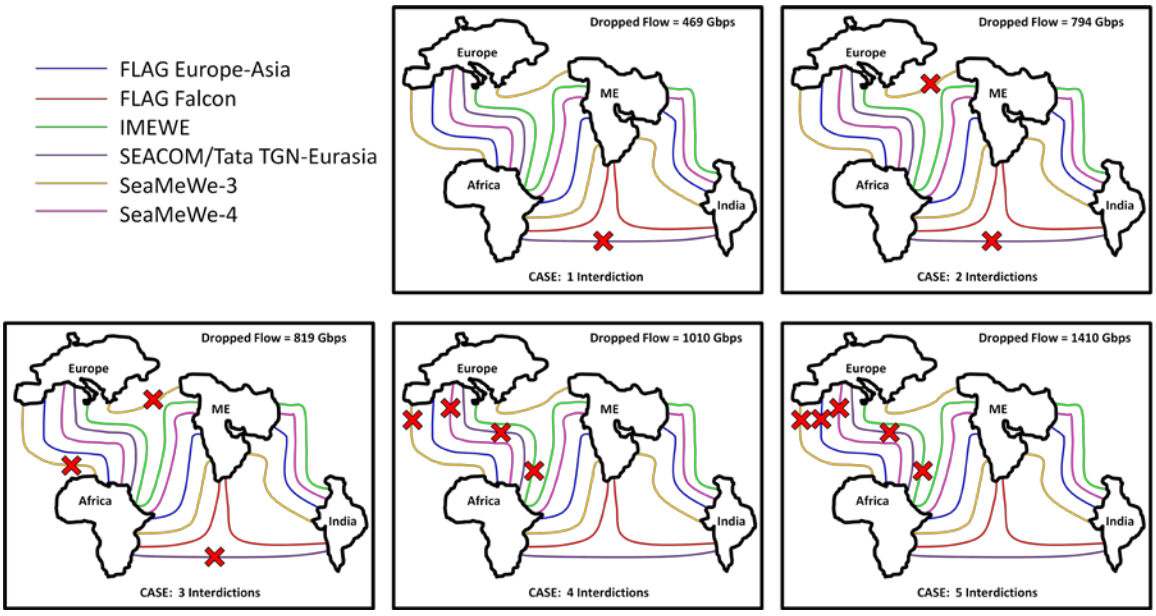


Figure 15. Cartoon diagram for scenario two showing which cables are interdicted along with the approximate location of the disruptions

3. Scenario Three

In the third and final scenario, we assume each cable system operates at lit capacity as in scenario one. However, in this scenario we allow interdictions against the cable landing stations in addition to interdictions against the cables themselves. The operator's resilience curves for all three scenarios are compared in Figure 16. As we might expect, the system is significantly less resilient to disruption in scenario three where we allow interdictions against cable landing stations. In the case of one, two, or three interdictions, the total traffic that is dropped is significantly higher in scenario three compared to scenario one. Additionally, in scenario three India is isolated from Europe with just two simultaneous interdictions compared with the five interdictions required in scenarios one and two.

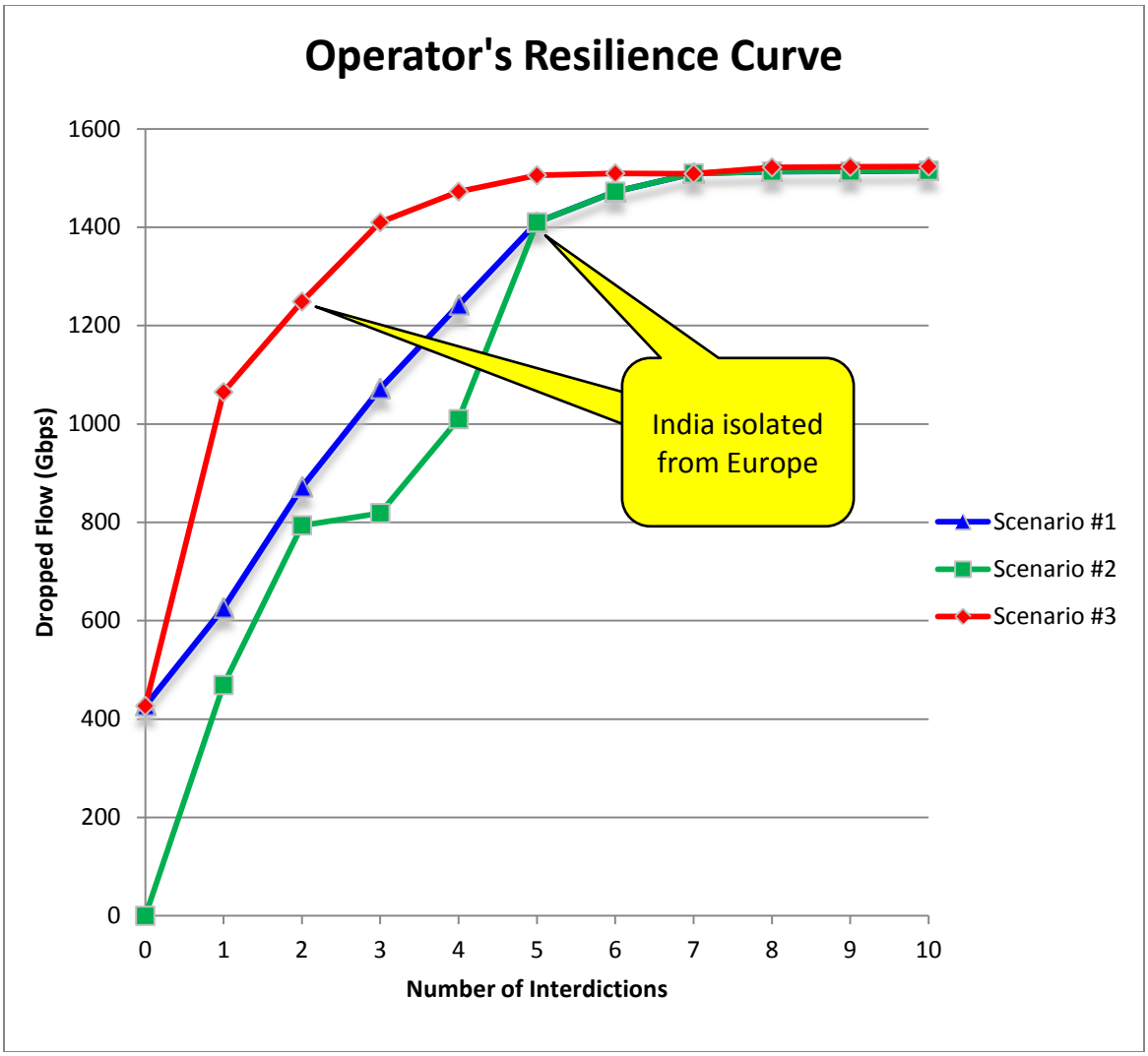


Figure 16. Operator's resilience curves for all scenarios.

As shown in Figure 17, the interdiction locations for scenario three are not nested going from one to two interdictions and also from two to three interdictions. In the case of one interdiction, the worst-case disruption occurs at the cable landing station in Marseille, France. Since three of the six cables in this model utilize this landing station as an entry point to Europe, the total amount of dropped traffic in scenario three is almost double that of scenario one for the case of one interdiction. In the case of two interdictions, the worst-case disruptions still occur at cable landing stations but here the landing stations lie along Egypt's Red Sea coast. Although not clearly evident from the cartoon diagram in Figure 17, each of the six cable systems in this model travelling from

India to Europe enter Egypt at one of these two cable landing stations. As a result, India is completely isolated from Europe with only the two interdictions. As with the first two scenarios, Appendix C provides the comprehensive list of interdiction locations for each case up to ten interdictions for scenario three.

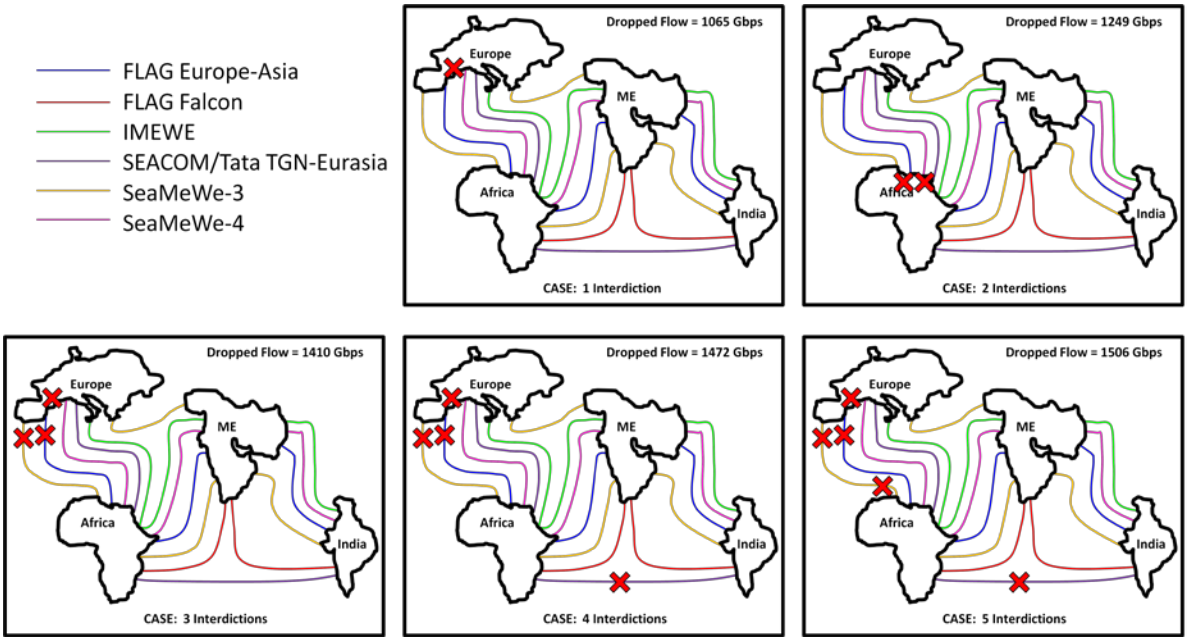


Figure 17. Cartoon diagram for scenario three showing which cables or landing stations are interdicted along with the approximate location of the disruptions.

In Figure 18, we again focus specifically on the traffic associated with India. In this figure, we compare the percent loss in Indian traffic, both inbound and outbound, across all three scenarios. As expected, scenario three produces the most catastrophic results. Even with just one interdiction, India loses over 65 percent of its total traffic. And again, we note from Figure 17 that these devastating losses occur without an actual attack at or near the coast of India. In fact, we do not see an attack at or near India until the case of seven interdictions. And in this case, India is completely isolated from all the other countries in the model not just those in Europe. Another interesting observation from Figure 18 occurs in the jump from two interdictions to three interdictions. Recall that the goal of the attacker is to inflict maximal damage on the system as a whole.

Indeed, the damage to the system in scenario three increases going from two to three interdictions as shown in the operator's resilience curve back in Figure 16. However, the damage to India actually decreases from two to three interdictions as shown in Figure 18. A closer look at the attack locations for scenario three in Appendix C reveals the reason for this decrease in damage to India. As mentioned previously, the worst-case disruptions in the two-interdiction case in scenario three both occur at landing stations on the Red Sea coast of Egypt. Since each of the cables travelling from India to Europe go through one of these two landing stations, India is isolated from Europe in this case. Furthermore, India is also isolated from all the non-European countries whose only access to undersea cables lies on the Mediterranean Sea. So in addition to being isolated from Europe, India is also isolated from Turkey, another country with relatively strong traffic demand. However, going from two to three interdictions we see another non-nested result as the landing stations in Egypt are no longer attacked. In the three-interdiction case, the worst-case disruptions switch back to the European coast. And while India is still cut off from Europe, the traffic demand between India and Turkey is satisfied in this case. As a result, we see the small decrease in the damage specifically to India going from two to three interdictions.

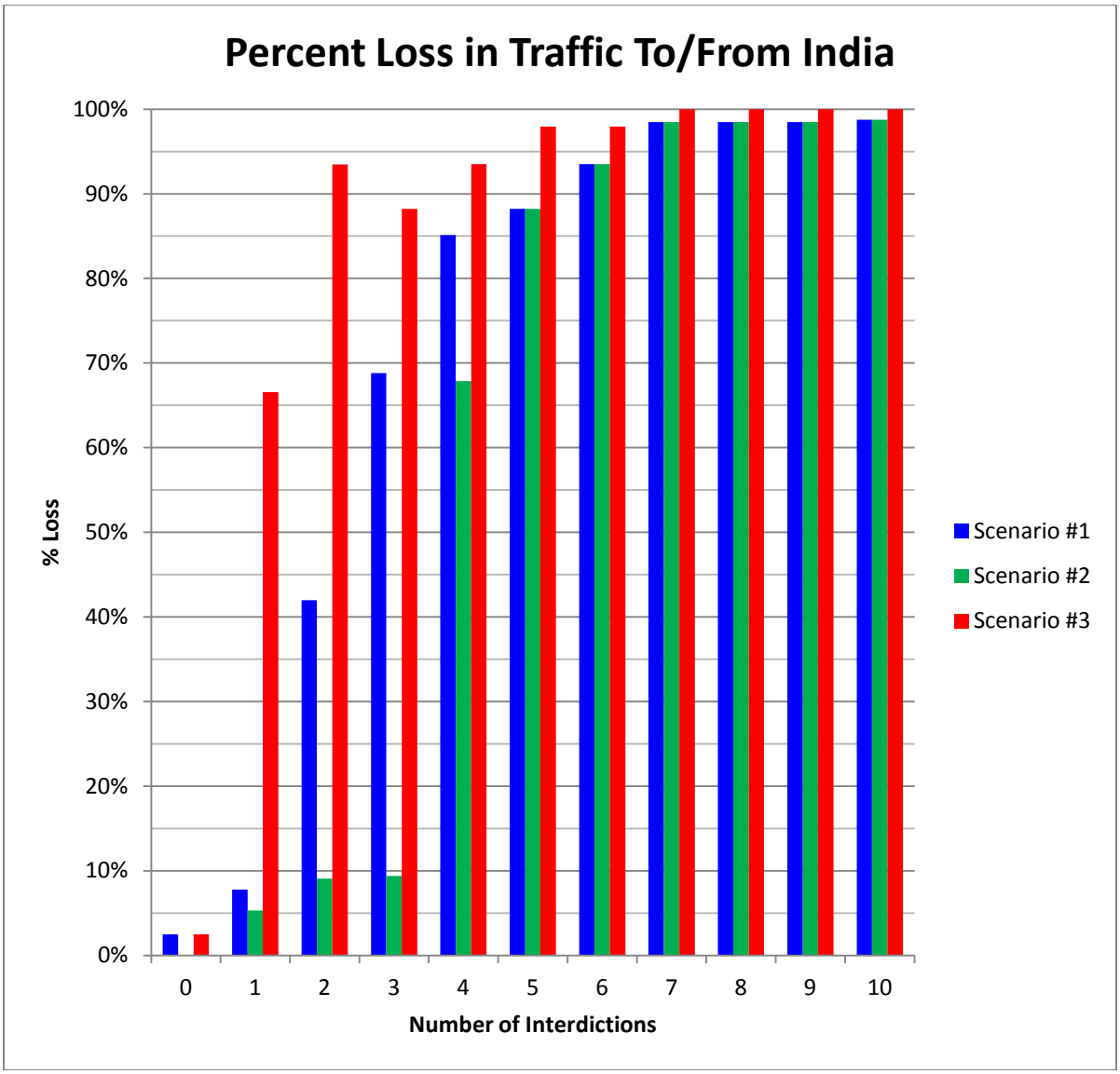


Figure 18. Percent loss in the traffic associated with India across all scenarios.

Table 5 provides additional insight into which of the six cables are targeted the most in this model. The SEACOM/Tata TGN-Eurasia and SeaMeWe-3 cable systems are the most consistently interdicted cables across all three scenarios. At first glance, this result is somewhat counterintuitive given that these two cables are not the largest capacity cables in this model. In fact, the SeaMeWe-4 and IMEWE cable systems both have much larger capacities and hence would seem the more attractive choices for interdiction. The physical configurations of the cables in Appendix B provide insight into these seemingly paradoxical results. While the SeaMeWe-4 and IMEWE cable

systems each have only two landing stations in Europe, the SeaMeWe-3 has seven landing stations in Europe. The physical redundancy afforded by this routing makes the SeaMeWe-3 more resilient to interdictions but also more attractive for interdiction at multiple locations. In all three scenarios, the SeaMeWe-3 cable system is attacked at more locations than any other cable. Meanwhile, the SeaMeWe-4 and IMEWE cable systems are almost always attacked just one time and in the same location each time. Their physical configurations present a single point of failure whereby the entire cable system is severely degraded with just one interdiction. The SeaMeWe-3 cable system, on the other hand, must be attacked at multiple different locations in order to inflict maximal damage. Physical redundancy, in the form of both path diversity and landing station diversity, allows cables to function effectively even after disruptions.

		FLAG Europe-Asia	FLAG Falcon	IMEWE	SEACOM/Tata TGN-Eurasia	SeaMeWe-3	SeaMeWe-4	Landing Station - France	Landing Station - Egypt	Landing Station - India
Scenario #1										
Interdictions	1				X					
	2			X			X			
	3			X	X		X			
	4	X		X	X		X			
	5	X		X	X	X	X			
	6	X		X	XX	X	X			
	7	X		X	XX	XX	X			
	8	X		X	XX	XXX	X			
	9	X		X	XX	XXXX	X			
	10	X	XX	X	XX	XXX	X			
Subtotal		**7**	**2**	**9**	**14**	**14**	**9**			
Scenario #2										
Interdictions	1				X					
	2				X	X				
	3				X	XX				
	4			X	X	X	X			
	5	X		X	X	X	X			
	6	X		X	XX	X	X			
	7	X		X	XX	XX	X			
	8	X		X	XX	XXX	X			
	9	X		X	XX	XXXX	X			
	10	X	XX	X	XX	XXX	X			
Subtotal		**6**	**2**	**7**	**15**	**18**	**7**			
Scenario #3										
Interdictions	1							X		
	2								XX	
	3	X				X		X		
	4	X			X	X		X		
	5	X			X	XX		X		
	6	X			X	XXX		X		
	7	X				XXX		X		XX
	8	X			X	XXX		X		XX
	9	X			X	XXXX		X		XX
	10	X			XX	XXX		X	X	XX
Subtotal		**8**	**0**	**0**	**7**	**20**	**0**	**9**	**3**	**8**
TOTAL		**21**	**4**	**16**	**36**	**52**	**16**	**9**	**3**	**8**

Table 5. Frequency of interdiction by cable or landing station across all scenarios

V. CONCLUSION

Our primary goal in this thesis is to provide a network modeling technique for analyzing resilience in the global undersea cable infrastructure. This technique can be applied at the microscopic level with just one or two cables and a few countries up to the macroscopic level with all the undersea cables and countries in the world. Our analysis of Europe to India traffic in the previous section demonstrates our technique. The results and analysis from this model also provide significant insight into the undersea cable infrastructure connecting Europe and India and still broader implications regarding undersea cable infrastructures in general.

First, as with India in our analysis, a country's ability to send and receive transoceanic communications may be severely degraded without disruptions to any cables or landing stations that are actually in or near that country. Such is the nature of undersea cables, and indeed the primary difficulty that countries face in protecting their undersea cable interests. Often, those interests stretch well beyond their own territorial boundaries.

The second major insight from our model and analysis is the importance of redundancy. In our model, adding redundancy enhances the resilience of the Europe to India cable infrastructure. And while this result merely validates what is already intuitively known about undersea cables, our model further demonstrates a more specific result regarding redundancy. In order to ensure the resilience of the infrastructure across all levels of disruptions, redundancy must exist in the form of both capacity redundancy and physical redundancy. In scenario two in our model, the additional capacity made available in the already existing cables significantly enhances the resilience of the system in the cases of three or fewer simultaneous disruptions; this capacity redundancy provides tremendous flexibility for re-routing traffic along other cables with minimal traffic loss. Of course capacity redundancy also provides adequate margins for future growth along major geographic routes such as the route from Europe to India. But capacity redundancy alone is not enough. In the face of larger scale simultaneous disruptions, physical redundancy is similarly vital. In the case of five or more simultaneous disruptions, we show that capacity redundancy is useless without physical redundancy.

Furthermore, physical redundancy must exist in multiple forms. Path diversity in the routing of cable systems, such as with the SeaMeWe-3 cable system in our model, allows cables to effectively handle disruptions and ensures that no physical or logical single points of interdiction exist. Landing station diversity is just as critical. As we demonstrate in scenario three, landing stations that host multiple undersea cables are particularly vulnerable. Since all of the cables entering Egypt via the Red Sea coast share one of two landing stations, interdictions against these two landing stations result in massive traffic loss in our model.

Finally, our model demonstrates that geography plays an important role. For any sea-bound commodity exchanged between Europe and India, the passage through Egypt from the Mediterranean Sea to the Red Sea is a natural choke point. The same is true with undersea cables. In our model, more than half of all interdictions across the first two scenarios occur at cable segments at or near the Egyptian coastline. So along with the landing stations in Egypt, the cable segments adjoined to Egypt are similarly vulnerable. Further, because of its geographic area, the Mediterranean Sea is naturally more congested with undersea cables than is the Atlantic or Pacific Oceans. As a result, destructive events, whether natural or man-made, are more likely to affect multiple cables. Unfortunately, as demonstrated across all the scenarios in our model, the Europe to India undersea cable infrastructure is not at all resilient to five or more simultaneous disruptions when those disruptions occur at key locations.

This research is a small example of the analysis on the global undersea cable infrastructure that can be undertaken with our network modeling technique. Our results are derived from data we collected through open sources. While we assume the data used here is correct, the model could easily be updated to incorporate known or measured data from the actual proprietary sources. Examples of this kind of data include the cable capacities, precise logical and physical configurations of the cables, along with historic or projected traffic demands along specified routes. This model could easily be adapted to address scenarios of interest to the Department of Defense by including specific cable systems and adjusting shortage costs to prioritize certain kinds of traffic.

Future research might also incorporate terrestrial cable systems to more accurately reflect the overall level of connectivity among countries and regions. Further, our model assumes the cost of carrying traffic is identical for each cable system. With more accurate data on the cost of carrying traffic along the different cables, further research could expand our model from simply a resilience approach to an economic or consumer goal model. As an example, consider a communications carrier that wants to lease capacity along a particular route based on their projected traffic demand. The model, then, is modified to optimally determine the cables and quantity of capacity on each cable that minimize cost. Another factor we do not consider in this research is the length of repair time associated with a particular disruption. As an improvement to our model, future work might account for variable length repair times for each disruption event based on historical data. This would allow for a better understanding of the economic losses over time that result from different levels of disruptions. In conclusion, the complex and rapidly evolving infrastructure of undersea cables offers countless possibilities for future research and analysis. We hope the network modeling technique described herein serves as a step forward in those endeavors.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A: INTERNET HOSTS BY COUNTRY

RANK	COUNTRY	INTERNET HOSTS
1	United States	498,000,000
2	Japan	63,466,000
3	Italy	25,456,000
4	Brazil	23,790,000
5	Germany	20,416,000
6	China	19,772,000
7	Australia	16,952,000
8	France	16,872,880
9	Mexico	15,165,000
10	Russia	13,758,000
11	Netherlands	13,715,000
12	Poland	12,928,000
13	Argentina	10,928,000
14	Canada	8,515,000
15	United Kingdom	8,409,000
16	India	6,738,000
17	Taiwan	6,166,000
18	Sweden	5,727,000
19	Switzerland	5,249,000
20	Belgium	5,180,000
21	South Africa	4,835,000
22	Finland	4,700,000
23	Denmark	4,285,000
24	Colombia	4,281,000
25	Spain	4,232,000
26	Czech Republic	4,140,000
27	Portugal	3,664,000
28	Turkey	3,625,000
29	Norway	3,584,000
30	Austria	3,445,000
31	Thailand	3,278,000
32	Greece	3,115,000
33	Hungary	3,064,000
34	New Zealand	3,028,000
35	Romania	2,702,000
36	Israel	2,179,000

RANK	COUNTRY	INTERNET HOSTS
37	Ukraine	1,997,000
38	Singapore	1,932,000
39	Chile	1,854,000
40	Slovakia	1,387,000
41	Ireland	1,380,000
42	Indonesia	1,342,000
43	Lithuania	1,184,000
44	Serbia	1,102,000
45	Uruguay	945,826
46	Bulgaria	937,195
47	Venezuela	888,028
48	Hong Kong	861,516
49	Estonia	848,009
50	Croatia	725,521
51	Moldova	696,685
52	Philippines	452,050
53	Slovenia	417,984
54	Dominican Republic	404,057
55	United Arab Emirates	371,969
56	Malaysia	363,007
57	Iceland	360,910
58	Georgia	358,109
59	Guatemala	346,834
60	Pakistan	340,834
61	Latvia	315,889
62	Belarus	302,560
63	Korea, South	293,862
64	Paraguay	278,473
65	Morocco	278,075
66	Luxembourg	253,959
67	Cyprus	252,990
68	Trinidad and Tobago	241,640
69	Peru	232,515
70	Egypt	200,336
71	Armenia	192,541
72	Nicaragua	176,985
73	Vietnam	175,612
74	Bolivia	167,769
75	Iran	167,453

RANK	COUNTRY	INTERNET HOSTS
76	Ecuador	162,281
77	Saudi Arabia	147,202
78	Costa Rica	146,164
79	Bosnia and Herzegovina	146,152
80	Tuvalu	138,579
81	Kyrgyzstan	116,586
82	Mozambique	82,804
83	Niue	78,927
84	Namibia	77,948
85	Turks and Caicos Islands	72,591
86	Kenya	69,914
87	Bangladesh	69,285
88	Kazakhstan	65,988
89	Lebanon	64,525
90	Macedonia	62,718
91	Ghana	60,282
92	Cocos (Keeling) Islands	58,130
93	Uzbekistan	56,334
94	British Indian Ocean Territory	54,452
95	Mauritius	51,123
96	Brunei	49,403
97	Jordan	49,083
98	Bahrain	46,035
99	Nepal	41,532
100	Aruba	40,894
101	French Polynesia	37,360
102	New Caledonia	33,904
103	Yemen	33,279
104	Uganda	33,082
105	Madagascar	32,537
106	Zimbabwe	30,650
107	Azerbaijan	29,968
108	Andorra	28,131
109	Honduras	27,074
110	Tanzania	25,832
111	Monaco	25,674
112	Guyana	24,840
113	Cayman Islands	23,079
114	Fiji	22,754

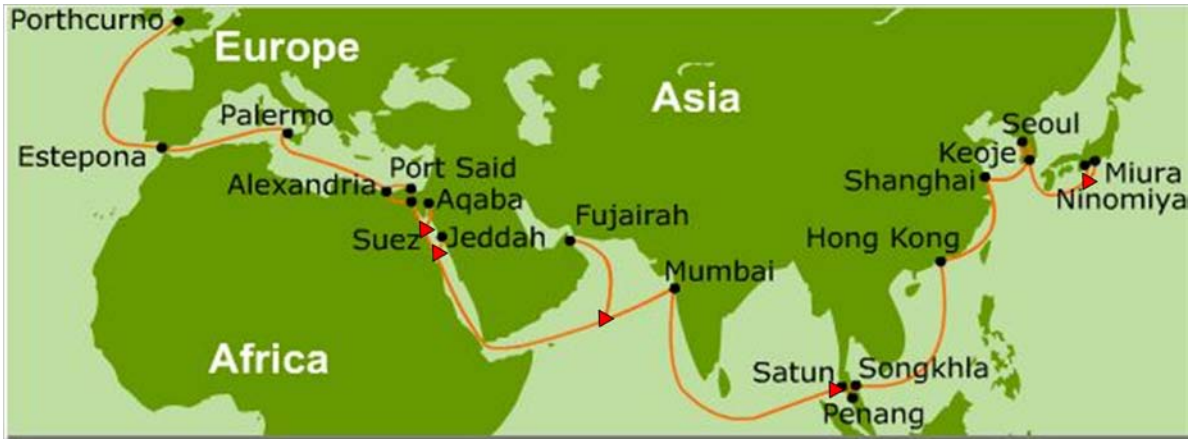
RANK	COUNTRY	INTERNET HOSTS
115	El Salvador	22,372
116	Mongolia	20,865
117	Tonga	20,766
118	Bahamas, The	20,674
119	Bermuda	20,527
120	Angola	20,269
121	Samoa	18,074
122	Libya	17,787
123	Zambia	16,372
124	Greenland	15,639
125	Albania	15,505
126	Bhutan	14,714
127	Malta	14,687
128	Cambodia	13,768
129	Oman	13,488
130	Antigua and Barbuda	11,844
131	San Marino	11,097
132	Panama	10,984
133	Liechtenstein	9,969
134	Montenegro	9,915
135	Cameroon	9,553
136	Sri Lanka	8,652
137	Cote d'Ivoire	8,598
138	Nauru	8,161
139	Antarctica	7,763
140	Faroe Islands	7,595
141	Belize	7,464
142	Saint Helena, Ascension, and Tristan da Cunha	6,724
143	Vanuatu	5,656
144	Virgin Islands	4,876
145	Papua New Guinea	4,847
146	Micronesia, Federated States of	4,638
147	Solomon Islands	4,354
148	Tajikistan	4,268
149	Jamaica	3,897
150	Cook Islands	3,565
151	Gibraltar	3,445
152	Christmas Island	3,265
153	Cuba	3,196

RANK	COUNTRY	INTERNET HOSTS
154	Maldives	3,054
155	Wallis and Futuna	2,750
156	Kuwait	2,730
157	Swaziland	2,706
158	Botswana	2,674
159	Congo, Democratic Republic of the	2,514
160	Montserrat	2,470
161	American Samoa	2,368
162	Burkina Faso	1,833
163	Sao Tome and Principe	1,646
164	Lesotho	1,581
165	Tokelau	1,550
166	Laos	1,526
167	Barbados	1,522
168	Rwanda	1,277
169	Togo	1,165
170	Malawi	1,092
171	Burma	1,033
172	Nigeria	936
173	Qatar	887
174	Isle of Man	881
175	Eritrea	870
176	Dominica	722
177	Turkmenistan	717
178	Tunisia	575
179	Algeria	561
180	Haiti	541
181	British Virgin Islands	505
182	Benin	495
183	Gambia, The	491
184	Puerto Rico	458
185	South Georgia and South Sandwich Islands	441
186	Mali	438
187	Syria	420
188	Saint Vincent and the Grenadines	336
189	Kiribati	328
190	Macau	284
191	Anguilla	283
192	Sierra Leone	280

RANK	COUNTRY	INTERNET HOSTS
193	Jersey	255
194	Seychelles	238
195	Burundi	236
196	Niger	229
197	Guernsey	224
198	Senegal	217
199	Timor-Leste	210
200	Djibouti	209
201	Suriname	186
202	Ethiopia	167
203	Afghanistan	121
204	Norfolk Island	120
205	Somalia	113
206	Falkland Islands (Islas Malvinas)	111
207	Gabon	103
208	Holy See (Vatican City)	102
209	Saint Lucia	90
210	Sudan	90
211	Guinea-Bissau	86
212	Grenada	71
213	Saint Kitts and Nevis	52
214	Congo, Republic of the	43
215	French Southern and Antarctic Lands	34
216	Cape Verde	31
217	Mauritania	28
218	Pitcairn Islands	27
219	Iraq	23
220	Central African Republic	20
221	Northern Mariana Islands	17
222	Comoros	15
223	Guinea	15
224	Liberia	7
225	Korea, North	7
226	Equatorial Guinea	7
227	Bouvet Island	6
228	Chad	5
229	Palau	4
230	Marshall Islands	3
231	Saint Pierre and Miquelon	2

APPENDIX B: PHYSICAL CONFIGURATIONS AND SEGMENTS OF THE UNDERSEA CABLES IN THE EUROPE TO INDIA MODEL

Cable: FLAG Europe Asia

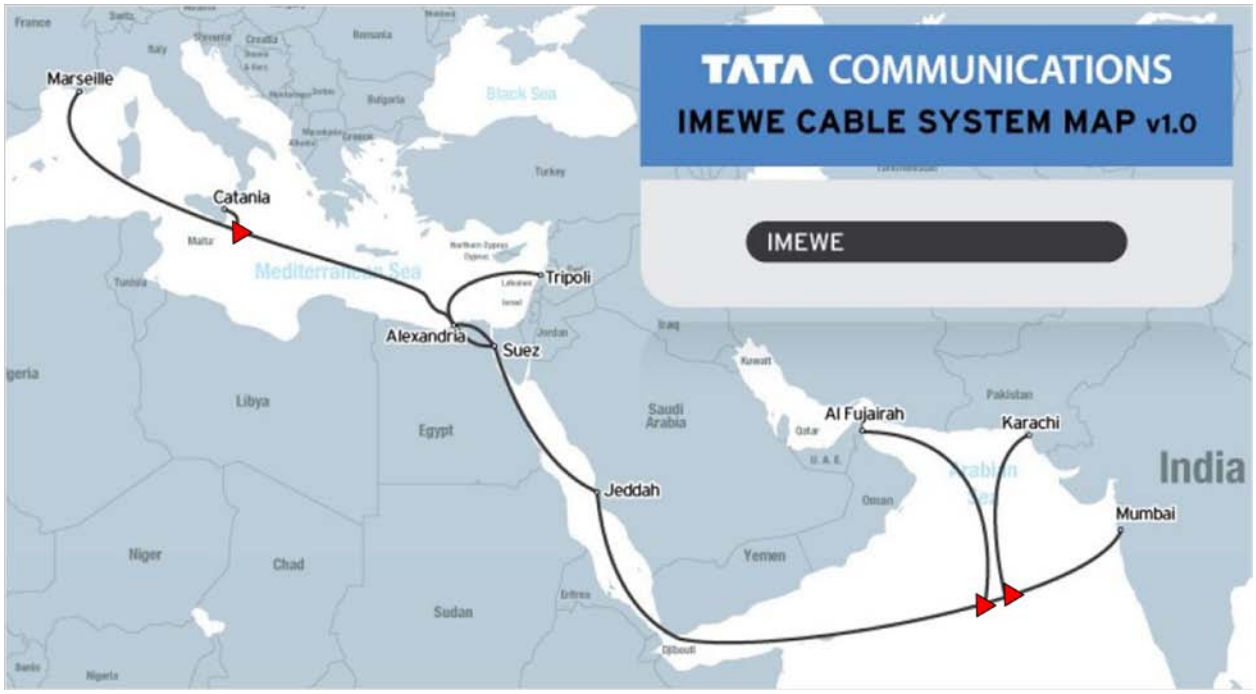


Segment	End Point 1	End Point 2	Lit Capacity (Gbps)	Max Capacity (Gbps)
1	Porthcurno, UK	Estepona, Spain	85	200
2	Estepona, Spain	Palermo, Sicily	85	200
3	Palermo, Sicily	Alexandria, Egypt	85	200
4	Alexandria, Egypt	Port Said, Egypt	85	200
5	Suez, Egypt	Branching Unit 1	85	200
6	Al Aqabah, Jordan	Branching Unit 1	85	200
7	Branching Unit 1	Branching Unit 2	85	200
8	Jeddah, Saudi Arabia	Branching Unit 2	85	200
9	Branching Unit 2	Branching Unit 3	85	200
10	Fujairah, UAE	Branching Unit 3	85	200
11	Branching Unit 3	Mumbai, India	85	200
12	Mumbai, India	Branching Unit 4	85	200
13	Branching Unit 4	Penang, Malaysia	85	200
14	Branching Unit 4	Satun, Thailand	85	200
15	Satun, Thailand	Songkhla, Thailand	85	200
16	Songkhla, Thailand	Lantau Island, Hong Kong	85	200
17	Lantau Island, Hong Kong	Shanghai, China	85	200
18	Shanghai, China	Keoje, South Korea	85	200
19	Keoje, South Korea	Branching Unit 5	85	200
20	Branching Unit 5	Ninomiya, Japan	85	200
21	Branching Unit 5	Miura, Japan	85	200

Cable: FLAG Falcon

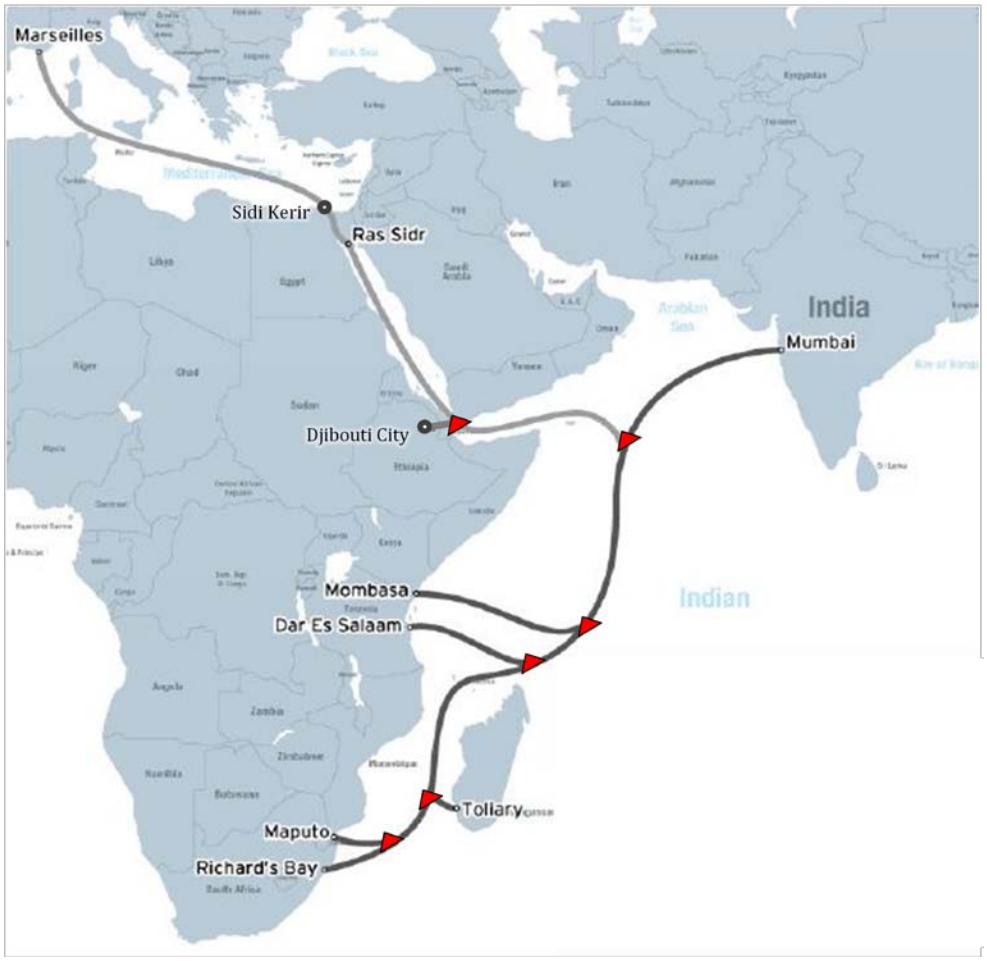
Segment	End Point 1	End Point 2	Lit Capacity (Gbps)	Max Capacity (Gbps)
1	Suez, Egypt	Branching Unit 1	90	1280
2	Al Aqabah, Jordan	Branching Unit 1	90	1280
3	Branching Unit 1	Branching Unit 2	90	1280
4	Jeddah, Saudi Arabia	Branching Unit 2	90	1280
5	Port Sudan, Sudan	Branching Unit 2	90	1280
6	Branching Unit 2	Branching Unit 3	90	1280
7	Al Hudaydah, Yemen	Branching Unit 3	90	1280
8	Branching Unit 3	Branching Unit 4	90	1280
9	Al Ghaydah, Yemen	Branching Unit 4	90	1280
10	Branching Unit 4	Al Seeb, Oman	90	1280
11	Al Seeb, Oman	Branching Unit 5	90	1280
12	Chabahar, Iran	Branching Unit 5	90	1280
13	Branching Unit 5	Mumbai, India	90	1280
14	Al Seeb, Oman	Khasab, Oman	90	1280
15	Khasab, Oman	Dubai, UAE	90	1280
16	Dubai, UAE	Doha, Qatar	90	1280
17	Doha, Qatar	Manama, Bahrain	90	1280
18	Manama, Bahrain	Al Khubar, Saudi Arabia	90	1280
19	Al Khubar, Saudi Arabia	Kuwait City, Kuwait	90	1280
20	Kuwait City, Kuwait	Bandar Abbas, Iran	90	1280
21	Bandar Abbas, Iran	Al Seeb, Oman	90	1280

Cable: IMEWE



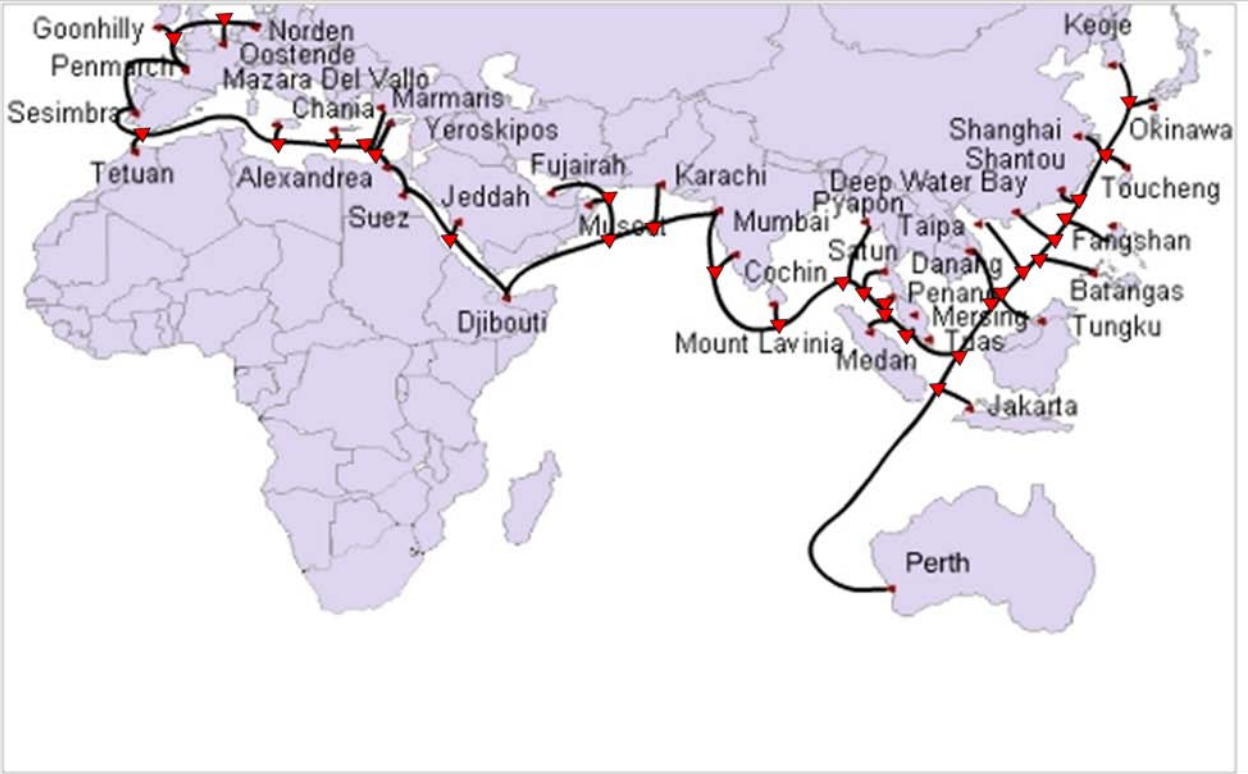
Segment	End Point 1	End Point 2	Lit Capacity (Gbps)	Max Capacity (Gbps)
1	Marseille, France	Branching Unit 1	520	3840
2	Catania, Sicily	Branching Unit 1	520	3840
3	Branching Unit 1	Alexandria, Egypt	520	3840
4	Alexandria, Egypt	Tripoli, Lebanon	520	3840
5	Suez, Egypt	Jeddah, Saudi Arabia	520	3840
6	Jeddah, Saudi Arabia	Branching Unit 2	520	3840
7	Fujairah, UAE	Branching Unit 2	520	3840
8	Branching Unit 2	Branching Unit 3	520	3840
9	Karachi, Pakistan	Branching Unit 3	520	3840
10	Mumbai, India	Branching Unit 3	520	3840

Cable: SEACOM/Tata TGN-Eurasia



Segment	End Point 1	End Point 2	Lit Capacity (Gbps)	Max Capacity (Gbps)
1	Marseille, France	Sidi Kerir, Egypt	100	1280
2	Ras Sidr, Egypt	Branching Unit 1	100	1280
3	Djibouti City, Djibouti	Branching Unit 1	100	1280
4	Branching Unit 1	Branching Unit 2	100	1280
5	Branching Unit 2	Mumbai, India	100	1280
6	Branching Unit 2	Branching Unit 3	100	1280
7	Mombasa, Kenya	Branching Unit 3	100	1280
8	Branching Unit 3	Branching Unit 4	100	1280
9	Dar Es Salaam, Tanzania	Branching Unit 4	100	1280
10	Branching Unit 4	Branching Unit 5	100	1280
11	Toliary, Madagascar	Branching Unit 5	100	1280
12	Branching Unit 5	Branching Unit 6	100	1280
13	Maputo, Mozambique	Branching Unit 6	100	1280
14	Mtunzini, South Africa	Branching Unit 6	100	1280

Cable: SeaMeWe-3

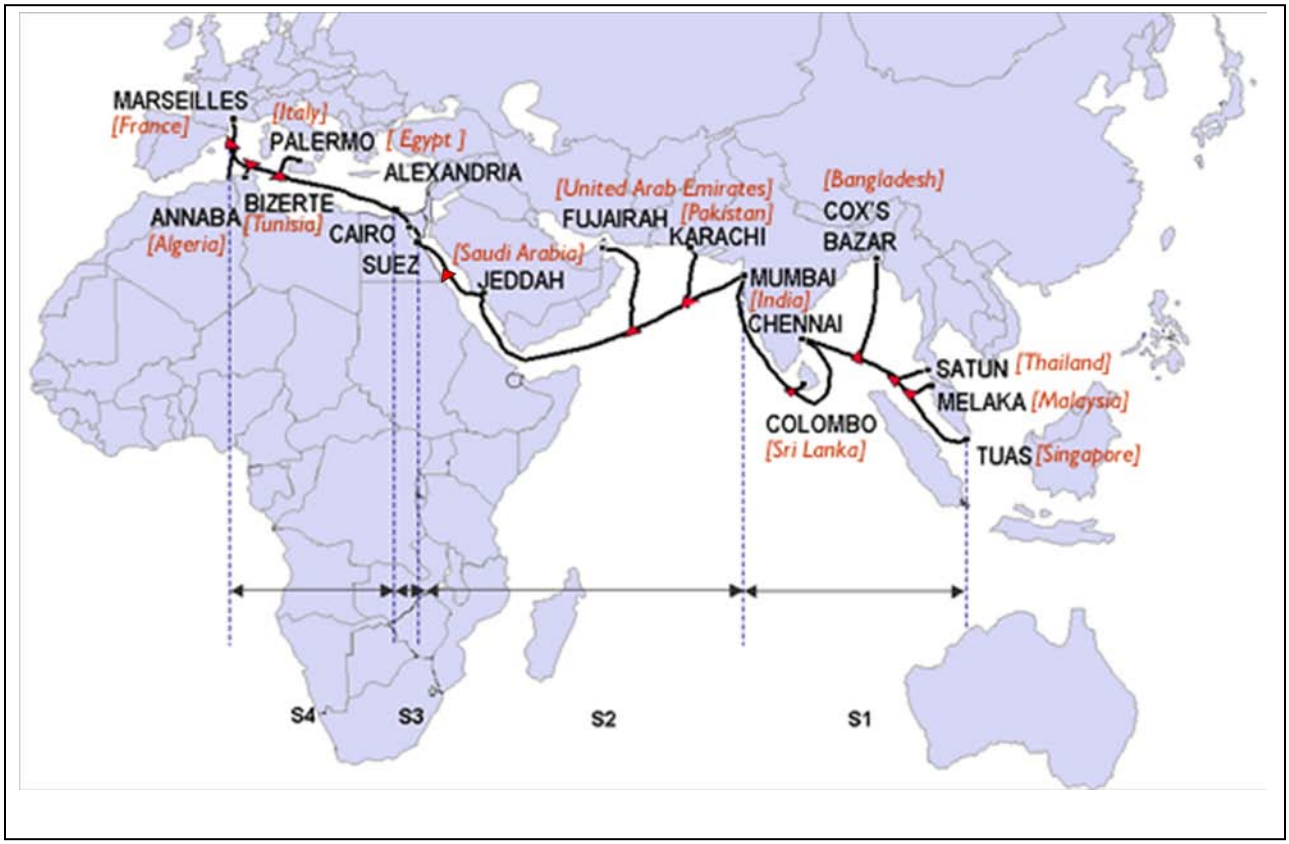


Segment	End Point 1	End Point 2	Lit Capacity (Gbps)	Max Capacity (Gbps)
1	Norden, Germany	Branching Unit 1	90	960
2	Ostend, Belgium	Branching Unit 1	90	960
3	Branching Unit 1	Branching Unit 2	90	960
4	Goonhilly Downs, UK	Branching Unit 2	90	960
5	Branching Unit 2	Penmarch, France	90	960
6	Penmarch, France	Sesimbra, Portugal	90	960
7	Sesimbra, Portugal	Branching Unit 3	90	960
8	Tetouan, Morocco	Branching Unit 3	90	960
9	Branching Unit 3	Branching Unit 4	90	960
10	Mazara del Vallo, Sicily	Branching Unit 4	90	960
11	Branching Unit 4	Branching Unit 5	90	960
12	Chania, Crete	Branching Unit 5	90	960
13	Branching Unit 5	Branching Unit 6	90	960
14	Marmaris, Turkey	Branching Unit 6	90	960
15	Branching Unit 6	Branching Unit 7	90	960
16	Yeroskipos, Cyprus	Branching Unit 7	90	960
17	Branching Unit 7	Alexandria, Egypt	90	960

Segment	End Point 1	End Point 2	Lit Capacity (Gbps)	Max Capacity (Gbps)
18	Suez, Egypt	Branching Unit 8	90	960
19	Jeddah, Saudi Arabia	Branching Unit 8	90	960
20	Branching Unit 8	Djibouti City, Djibouti	90	960
21	Djibouti City, Djibouti	Branching Unit 9	90	960
22	Branching Unit 9	Branching Unit 10	90	960
23	Muscat, Oman	Branching Unit 10	90	960
24	Fujairah, UAE	Branching Unit 10	90	960
25	Branching Unit 9	Branching Unit 11	90	960
26	Karachi, Pakistan	Branching Unit 11	90	960
27	Branching Unit 11	Mumbai, India	90	960
28	Mumbai, India	Branching Unit 12	90	960
29	Cochin, India	Branching Unit 12	90	960
30	Branching Unit 12	Branching Unit 13	90	960
31	Mount Lavinia, Sri Lanka	Branching Unit 13	90	960
32	Branching Unit 13	Branching Unit 14	90	960
33	Pyapon, Myanmar	Branching Unit 14	90	960
34	Branching Unit 14	Branching Unit 15	90	960
35	Satun, Thailand	Branching Unit 15	90	960
36	Branching Unit 15	Branching Unit 16	90	960
37	Penang, Malaysia	Branching Unit 16	90	960
38	Branching Unit 16	Branching Unit 17	90	960
39	Medan, Indonesia	Branching Unit 17	90	960
40	Branching Unit 17	Branching Unit 18	90	960
41	Mersing, Malaysia	Branching Unit 18	90	960
42	Branching Unit 18	Tuas, Singapore	90	960
43	Tuas, Singapore	Branching Unit 19	90	960
44	Branching Unit 19	Branching Unit 20	90	960
45	Jakarta, Indonesia	Branching Unit 20	90	960
46	Perth, Australia	Branching Unit 20	90	960
47	Branching Unit 20	Branching Unit 21	90	960
48	Danang, Vietnam	Branching Unit 21	90	960
49	Branching Unit 21	Branching Unit 22	90	960
50	Tungku Beach, Brunei	Branching Unit 22	90	960
51	Branching Unit 22	Branching Unit 23	90	960
52	Taipa, Macao	Branching Unit 23	90	960
53	Branching Unit 23	Branching Unit 24	90	960
54	Batangas Bay, Philippines	Branching Unit 24	90	960
55	Branching Unit 24	Branching Unit 25	90	960

Segment	End Point 1	End Point 2	Lit Capacity (Gbps)	Max Capacity (Gbps)
56	Deep Water Bay, Hong Kong	Branching Unit 25	90	960
57	Branching Unit 25	Branching Unit 26	90	960
58	Fangshan, Taiwan	Branching Unit 26	90	960
59	Branching Unit 26	Branching Unit 27	90	960
60	Shantou, China	Branching Unit 27	90	960
61	Branching Unit 27	Branching Unit 28	90	960
62	Shanghai, China	Branching Unit 28	90	960
63	Toucheng, Taiwan	Branching Unit 28	90	960
64	Branching Unit 28	Branching Unit 29	90	960
65	Okinawa	Branching Unit 29	90	960
66	Keoje, South Korea	Branching Unit 29	90	960

Cable: SeaMeWe-4



Segment	End Point 1	End Point 2	Lit Capacity (Gbps)	Max Capacity (Gbps)
1	Marseille, France	Branching Unit 1	1350	1700
2	Annaba, Algeria	Branching Unit 1	1350	1700
3	Branching Unit 1	Branching Unit 2	1350	1700
4	Branching Unit 2	Bizerte, Tunisia	1350	1700
5	Branching Unit 2	Branching Unit 3	1350	1700
6	Branching Unit 3	Palermo, Sicily	1350	1700
7	Branching Unit 3	Alexandria, Egypt	1350	1700
8	Suez, Egypt	Branching Unit 4	1350	1700
9	Branching Unit 4	Jeddah, Saudi Arabia	1350	1700
10	Jeddah, Saudi Arabia	Branching Unit 5	1350	1700
11	Fujairah, UAE	Branching Unit 5	1350	1700
12	Branching Unit 5	Branching Unit 6	1350	1700
13	Karachi, Pakistan	Branching Unit 6	1350	1700
14	Branching Unit 6	Mumbai, India	1350	1700
15	Mumbai, India	Branching Unit 7	1350	1700
16	Colombo, Sri Lanka	Branching Unit 7	1350	1700
17	Branching Unit 7	Chennai, India	1350	1700
18	Chennai, India	Branching Unit 8	1350	1700
19	Coxs Bazar, Bangladesh	Branching Unit 8	1350	1700
20	Branching Unit 8	Branching Unit 9	1350	1700
21	Satun, Thailand	Branching Unit 9	1350	1700
22	Branching Unit 9	Branching Unit 10	1350	1700
23	Melaka, Malaysia	Branching Unit 10	1350	1700
24	Branching Unit 10	Tuas, Singapore	1350	1700

APPENDIX C: INTERDICTION LOCATIONS BY SEGMENT FOR EACH SCENARIO IN THE EUROPE TO INDIA MODEL

SCENARIO 1			Location of Interdiction	
Num Interdictions	Cable	Segment	End Point 1	End Point 2
1	SEACOM/Tata TGN-Eurasia	6	Branching Unit 2	Branching Unit 3
2	IMEWE	3	Alexandria, Egypt	Branching Unit 1
	SeaMeWe-4	7	Alexandria, Egypt	Branching Unit 3
3	IMEWE	3	Alexandria, Egypt	Branching Unit 1
	SEACOM/Tata TGN-Eurasia	1	Sidi Kerir, Egypt	Marseille, France
	SeaMeWe-4	7	Alexandria, Egypt	Branching Unit 3
4	FLAG Europe-Asia (FEA)	3	Alexandria, Egypt	Palermo, Sicily
	IMEWE	3	Alexandria, Egypt	Branching Unit 1
	SEACOM/Tata TGN-Eurasia	1	Sidi Kerir, Egypt	Marseille, France
	SeaMeWe-4	7	Alexandria, Egypt	Branching Unit 3
5	FLAG Europe-Asia (FEA)	2	Estepona, Spain	Palermo, Sicily
	IMEWE	3	Alexandria, Egypt	Branching Unit 1
	SEACOM/Tata TGN-Eurasia	1	Sidi Kerir, Egypt	Marseille, France
	SeaMeWe-3	7	Sesimbra, Portugal	Branching Unit 3
	SeaMeWe-4	1	Marseille, France	Branching Unit 1
6	FLAG Europe-Asia (FEA)	2	Estepona, Spain	Palermo, Sicily
	IMEWE	3	Alexandria, Egypt	Branching Unit 1
	SEACOM/Tata TGN-Eurasia	1	Sidi Kerir, Egypt	Marseille, France
	SEACOM/Tata TGN-Eurasia	6	Branching Unit 2	Branching Unit 3
	SeaMeWe-3	7	Sesimbra, Portugal	Branching Unit 3
	SeaMeWe-4	1	Marseille, France	Branching Unit 1
7	FLAG Europe-Asia (FEA)	3	Alexandria, Egypt	Palermo, Sicily
	IMEWE	3	Alexandria, Egypt	Branching Unit 1
	SEACOM/Tata TGN-Eurasia	1	Sidi Kerir, Egypt	Marseille, France
	SEACOM/Tata TGN-Eurasia	6	Branching Unit 2	Branching Unit 3
	SeaMeWe-3	7	Sesimbra, Portugal	Branching Unit 3
	SeaMeWe-3	17	Alexandria, Egypt	Branching Unit 7
	SeaMeWe-4	7	Alexandria, Egypt	Branching Unit 3
8	FLAG Europe-Asia (FEA)	3	Alexandria, Egypt	Palermo, Sicily
	IMEWE	3	Alexandria, Egypt	Branching Unit 1
	SEACOM/Tata TGN-Eurasia	1	Sidi Kerir, Egypt	Marseille, France
	SEACOM/Tata TGN-Eurasia	6	Branching Unit 2	Branching Unit 3
	SeaMeWe-3	7	Sesimbra, Portugal	Branching Unit 3

SCENARIO 1			Location of Interdiction	
Num Interdictions	Cable	Segment	End Point 1	End Point 2
	SeaMeWe-3	14	Marmais, Turkey	Branching Unit 6
	SeaMeWe-3	17	Alexandria, Egypt	Branching Unit 7
	SeaMeWe-4	7	Alexandria, Egypt	Branching Unit 3
9	FLAG Europe-Asia (FEA)	3	Alexandria, Egypt	Palermo, Sicily
	IMEWE	3	Alexandria, Egypt	Branching Unit 1
	SEACOM/Tata TGN-Eurasia	1	Sidi Kerir, Egypt	Marseille, France
	SEACOM/Tata TGN-Eurasia	6	Branching Unit 2	Branching Unit 3
	SeaMeWe-3	7	Sesimbra, Portugal	Branching Unit 3
	SeaMeWe-3	13	Branching Unit 5	Branching Unit 6
	SeaMeWe-3	14	Marmais, Turkey	Branching Unit 6
	SeaMeWe-3	16	Yeroskipos, Cyprus	Branching Unit 7
	SeaMeWe-4	7	Alexandria, Egypt	Branching Unit 3
10	FLAG Europe-Asia (FEA)	3	Alexandria, Egypt	Palermo, Sicily
	FLAG FALCON	6	Branching Unit 2	Branching Unit 3
	FLAG FALCON	13	Mumbai, India	Branching Unit 5
	IMEWE	3	Alexandria, Egypt	Branching Unit 1
	SEACOM/Tata TGN-Eurasia	1	Sidi Kerir, Egypt	Marseille, France
	SEACOM/Tata TGN-Eurasia	6	Branching Unit 2	Branching Unit 3
	SeaMeWe-3	7	Sesimbra, Portugal	Branching Unit 3
	SeaMeWe-3	14	Marmais, Turkey	Branching Unit 6
	SeaMeWe-3	17	Alexandria, Egypt	Branching Unit 7
	SeaMeWe-4	7	Alexandria, Egypt	Branching Unit 3

SCENARIO 2			Location of Interdiction	
Num Interdictions	Cable	Segment	End Point 1	End Point 2
1	SEACOM/Tata TGN-Eurasia	6	Branching Unit 2	Branching Unit 3
2	SEACOM/Tata TGN-Eurasia	6	Branching Unit 2	Branching Unit 3
	SeaMeWe-3	14	Marmaris, Turkey	Branching Unit 6
3	SEACOM/Tata TGN-Eurasia	6	Branching Unit 2	Branching Unit 3
	SeaMeWe-3	8	Tetouan, Morocco	Branching Unit 3
	SeaMeWe-3	14	Marmaris, Turkey	Branching Unit 6
4	IMEWE	3	Alexandria, Egypt	Branching Unit 1
	SEACOM/Tata TGN-Eurasia	1	Sidi Kerir, Egypt	Marseille, France
	SeaMeWe-3	7	Sesimbra, Portugal	Branching Unit 3

SCENARIO 2			Location of Interdiction	
Num Interdictions	Cable	Segment	End Point 1	End Point 2
	SeaMeWe-4	1	Marseille, France	Branching Unit 1
5	FLAG Europe-Asia (FEA)	2	Estepona, Spain	Palermo, Sicily
	IMEWE	3	Alexandria, Egypt	Branching Unit 1
	SEACOM/Tata TGN-Eurasia	1	Sidi Kerir, Egypt	Marseille, France
	SeaMeWe-3	7	Sesimbra, Portugal	Branching Unit 3
	SeaMeWe-4	1	Marseille, France	Branching Unit 1
6	FLAG Europe-Asia (FEA)	2	Estepona, Spain	Palermo, Sicily
	IMEWE	3	Alexandria, Egypt	Branching Unit 1
	SEACOM/Tata TGN-Eurasia	1	Sidi Kerir, Egypt	Marseille, France
	SEACOM/Tata TGN-Eurasia	6	Branching Unit 2	Branching Unit 3
	SeaMeWe-3	7	Sesimbra, Portugal	Branching Unit 3
	SeaMeWe-4	1	Marseille, France	Branching Unit 1
7	FLAG Europe-Asia (FEA)	3	Alexandria, Egypt	Palermo, Sicily
	IMEWE	3	Alexandria, Egypt	Branching Unit 1
	SEACOM/Tata TGN-Eurasia	1	Sidi Kerir, Egypt	Marseille, France
	SEACOM/Tata TGN-Eurasia	6	Branching Unit 2	Branching Unit 3
	SeaMeWe-3	7	Sesimbra, Portugal	Branching Unit 3
	SeaMeWe-3	17	Alexandria, Egypt	Branching Unit 7
	SeaMeWe-4	7	Alexandria, Egypt	Branching Unit 3
8	FLAG Europe-Asia (FEA)	3	Alexandria, Egypt	Palermo, Sicily
	IMEWE	3	Alexandria, Egypt	Branching Unit 1
	SEACOM/Tata TGN-Eurasia	1	Sidi Kerir, Egypt	Marseille, France
	SEACOM/Tata TGN-Eurasia	6	Branching Unit 2	Branching Unit 3
	SeaMeWe-3	7	Sesimbra, Portugal	Branching Unit 3
	SeaMeWe-3	14	Marmaris, Turkey	Branching Unit 6
	SeaMeWe-3	17	Alexandria, Egypt	Branching Unit 7
	SeaMeWe-4	7	Alexandria, Egypt	Branching Unit 3
9	FLAG Europe-Asia (FEA)	3	Alexandria, Egypt	Palermo, Sicily
	IMEWE	3	Alexandria, Egypt	Branching Unit 1
	SEACOM/Tata TGN-Eurasia	1	Sidi Kerir, Egypt	Marseille, France
	SEACOM/Tata TGN-Eurasia	6	Branching Unit 2	Branching Unit 3
	SeaMeWe-3	7	Sesimbra, Portugal	Branching Unit 3
	SeaMeWe-3	14	Marmaris, Turkey	Branching Unit 6
	SeaMeWe-3	16	Yeroskipos, Cyprus	Branching Unit 7
	SeaMeWe-3	17	Alexandria, Egypt	Branching Unit 7
	SeaMeWe-4	7	Alexandria, Egypt	Branching Unit 3
10	FLAG Europe-Asia (FEA)	3	Alexandria, Egypt	Palermo, Sicily

SCENARIO 2			Location of Interdiction	
Num Interdictions	Cable	Segment	End Point 1	End Point 2
	FLAG Falcon	6	Branching Unit 2	Branching Unit 3
	FLAG Falcon	13	Mumbai, India	Branching Unit 5
	IMEWE	3	Alexandria, Egypt	Branching Unit 1
	SEACOM/Tata TGN-Eurasia	1	Sidi Kerir, Egypt	Marseille, France
	SEACOM/Tata TGN-Eurasia	6	Branching Unit 2	Branching Unit 3
	SeaMeWe-3	7	Sesimbra, Portugal	Branching Unit 3
	SeaMeWe-3	14	Marmaris, Turkey	Branching Unit 6
	SeaMeWe-3	17	Alexandria, Egypt	Branching Unit 7
	SeaMeWe-4	7	Alexandria, Egypt	Branching Unit 3

SCENARIO 3				Location of Interdiction	
Num Interdictions	Interdict (Cable or LS)	Cable or LS Name	Segment	End Point 1	End Point 2
1	LS	Marseille, France	n/a	Marseille, France	Marseille, France
2	LS	Ras Sidr, Egypt	n/a	Ras Sidr, Egypt	Ras Sidr, Egypt
	LS	Suez, Egypt	n/a	Suez, Egypt	Suez, Egypt
3	Cable	FLAG Europe-Asia	2	Estepona, Spain	Palermo, Sicily
	LS	Marseille, France	n/a	Marseille, France	Marseille, France
	Cable	SeaMeWe-3	7	Sesimbra, Portugal	Branching Unit 3
4	Cable	FLAG Europe-Asia	2	Estepona, Spain	Palermo, Sicily
	LS	Marseille, France	n/a	Marseille, France	Marseille, France
	Cable	SEACOM	6	Branching Unit 2	Branching Unit 3
	Cable	SeaMeWe-3	7	Sesimbra, Portugal	Branching Unit 3
5	Cable	FLAG Europe-Asia	2	Estepona, Spain	Palermo, Sicily
	LS	Marseille, France	n/a	Marseille, France	Marseille, France
	Cable	SEACOM	6	Branching Unit 2	Branching Unit 3
	Cable	SeaMeWe-3	7	Sesimbra, Portugal	Branching Unit 3
	Cable	SeaMeWe-3	17	Alexandria, Egypt	Branching Unit 7
6	Cable	FLAG Europe-Asia	2	Estepona, Spain	Palermo, Sicily
	LS	Marseille, France	n/a	Marseille, France	Marseille, France
	Cable	SEACOM	6	Branching Unit 2	Branching Unit 3
	Cable	SeaMeWe-3	7	Sesimbra, Portugal	Branching Unit 3
	Cable	SeaMeWe-3	14	Marmaris,Turkey	Branching Unit 6
	Cable	SeaMeWe-3	17	Alexandria, Egypt	Branching Unit 7
7	LS	Chennai, India	n/a	Chennai, India	Chennai, India

SCENARIO 3				Location of Interdiction	
Num Interdictions	Interdict (Cable or LS)	Cable or LS Name	Segment	End Point 1	End Point 2
	Cable	FLAG Europe-Asia	2	Estepona, Spain	Palermo, Sicily
	LS	Marseille, France	n/a	Marseille, France	Marseille, France
	LS	Mumbai, India	n/a	Mumbai, India	Mumbai, India
	Cable	SeaMeWe-3	7	Sesimbra, Portugal	Branching Unit 3
	Cable	SeaMeWe-3	14	Marmaris,Turkey	Branching Unit 6
	Cable	SeaMeWe-3	29	Cochin,India	Branch Unit 12
8	LS	Chennai, India	n/a	Chennai, India	Chennai, India
	Cable	FLAG Europe-Asia	2	Estepona, Spain	Palermo, Sicily
	LS	Marseille, France	n/a	Marseille, France	Marseille, France
	LS	Mumbai, India	n/a	Mumbai, India	Mumbai, India
	Cable	SEACOM	14	Mtunzini, S. Africa	Branching Unit 6
	Cable	SeaMeWe-3	7	Sesimbra, Portugal	Branching Unit 3
	Cable	SeaMeWe-3	14	Marmaris,Turkey	Branching Unit 6
	Cable	SeaMeWe-3	29	Cochin, India	Branch Unit 12
9	LS	Chennai, India	n/a	Chennai, India	Chennai, India
	Cable	FLAG Europe-Asia	2	Estepona, Spain	Palermo, Sicily
	LS	Marseille, France	n/a	Marseille, France	Marseille, France
	LS	Mumbai, India	n/a	Mumbai, India	Mumbai, India
	Cable	SEACOM	14	Mtunzini, S. Africa	Branching Unit 6
	Cable	SeaMeWe-3	7	Sesimbra, Portugal	Branching Unit 3
	Cable	SeaMeWe-3	14	Marmaris,Turkey	Branching Unit 6
	Cable	SeaMeWe-3	17	Alexandria, Egypt	Branching Unit 7
	Cable	SeaMeWe-3	29	Cochin,India	Branch Unit 12
10	LS	Chennai, India	n/a	Chennai, India	Chennai, India
	Cable	FLAG Europe-Asia	2	Estepona, Spain	Palermo, Sicily
	LS	Marseille, France	n/a	Marseille, France	Marseille, France
	LS	Mumbai, India	n/a	Mumbai, India	Mumbai, India
	Cable	SEACOM	2	Ras Sidr, Egypt	Branching Unit 1
	Cable	SEACOM	14	Mtunzini, S. Africa	Branching Unit 6
	Cable	SeaMeWe-3	7	Sesimbra, Portugal	Branching Unit 3
	Cable	SeaMeWe-3	14	Marmaris,Turkey	Branching Unit 6
	Cable	SeaMeWe-3	29	Cochin,India	Branch Unit 12
	LS	Suez, Egypt	n/a	Suez, Egypt	Suez, Egypt

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D: COMPLETE TRAFFIC MATRIX BY COUNTRY FOR THE EUROPE TO INDIA MODEL

	Algeria	Bahrain	Belgium	Crete	Cyprus	Djibouti	Egypt	France	Germany	India	Iran	Italy	Jordan	Kenya	Kuwait	Lebanon	Madagascar	Morocco	Mozambique	Oman	Pakistan	Portugal	Qatar	Saudi Arabia	Sicily	South Africa	Spain	Sri Lanka	Sudan	Tanzania	Tunisia	Turkey	UAE	UK	Yemen
Algeria	-0.1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Bahrain	0.0	-4.5	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Belgium	0.0	0.2	-330.9	0.5	1.2	0.0	1.0	19.6	20.5	14.5	0.8	21.3	0.2	0.3	0.0	0.3	0.2	1.3	0.4	0.1	1.6	10.6	0.0	0.7	2.3	12.4	11.5	0.0	0.0	0.1	0.0	10.6	1.7	15.9	0.2
Crete	0.0	0.0	0.0	-9.6	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Cyprus	0.0	0.0	0.1	0.0	-23.8	0.0	0.0	0.1	0.1	0.1	0.0	0.1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.1	0.0	0.0	0.0	0.1	0.1	0.0	0.0	0.0	0.0	0.1	0.0	0.1	0.0
Djibouti	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Egypt	0.0	0.0	0.0	0.0	0.0	0.0	-15.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
France	0.0	0.7	64.0	1.6	4.0	0.0	3.2	-576.3	149.2	77.8	2.7	163.9	0.8	1.1	0.0	1.0	0.5	4.4	1.3	0.2	5.4	48.6	0.0	2.4	7.8	60.7	54.4	0.1	0.0	0.4	0.0	46.2	5.9	90.6	0.5
Germany	0.0	0.9	80.7	1.9	4.9	0.0	3.9	180.5	-580.9	99.0	3.2	221.4	1.0	1.4	0.1	1.3	0.6	5.4	1.6	0.3	6.6	60.7	0.0	2.9	9.5	76.4	68.5	0.2	0.0	0.5	0.0	60.2	7.1	116.4	0.6
India	0.0	0.3	18.9	0.6	1.6	0.0	1.3	31.1	32.7	-391.9	1.1	34.4	0.3	0.4	0.0	0.4	0.2	1.7	0.5	0.1	2.1	15.3	0.0	0.9	3.0	18.2	16.8	0.1	0.0	0.2	0.0	15.2	2.3	24.1	0.2
Iran	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	-15.9	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Italy	0.0	1.1	104.9	2.4	6.1	0.0	4.8	247.2	276.0	123.8	4.1	-548.3	1.2	1.7	0.1	1.6	0.8	6.7	2.0	0.3	8.2	78.0	0.0	3.6	11.9	99.0	88.4	0.2	0.0	0.6	0.0	77.3	8.9	154.0	0.8
Jordan	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	-4.8	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Kenya	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	-6.7	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Kuwait	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	-0.3	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Lebanon	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	-6.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Madagascar	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	-3.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Morocco	0.0	0.0	0.1	0.0	0.0	0.0	0.0	0.1	0.1	0.1	0.0	0.1	0.0	0.0	0.0	0.0	0.0	-26.1	0.0	0.0	0.0	0.1	0.0	0.0	0.0	0.1	0.1	0.0	0.0	0.0	0.0	0.1	0.0	0.1	0.0
Mozambique	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	-8.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Oman	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	-1.3	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Pakistan	0.0	0.0	0.1	0.0	0.0	0.0	0.0	0.1	0.1	0.1	0.0	0.1	0.0	0.0	0.0	0.0	0.0	0.1	0.0	0.0	-31.7	0.1	0.0	0.0	0.1	0.1	0.1	0.0	0.0	0.0	0.0	0.1	0.1	0.1	0.0
Portugal	0.0	0.2	7.5	0.3	0.8	0.0	0.7	10.6	10.9	8.3	0.6	11.2	0.2	0.2	0.0	0.2	0.1	0.9	0.3	0.0	1.1	-258.4	0.0	0.5	1.5	7.3	6.9	0.0	0.0	0.1	0.0	6.4	1.2	8.9	0.1
Qatar	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	-0.1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Saudi Arabia	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	-14.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Sicily	0.0	0.0	0.2	0.0	0.1	0.0	0.1	0.2	0.2	0.2	0.1	0.2	0.0	0.0	0.0	0.0	0.0	0.1	0.0	0.0	0.1	0.2	0.0	0.1	-45.7	0.2	0.2	0.0	0.0	0.0	0.0	0.2	0.1	0.2	0.0
South Africa	0.0	0.2	11.6	0.5	1.1	0.0	0.9	17.4	18.1	13.0	0.7	18.8	0.2	0.3	0.0	0.3	0.2	1.2	0.4	0.1	1.5	9.6	0.0	0.7	2.1	-315.6	10.4	0.0	0.0	0.1	0.0	9.6	1.6	14.2	0.2
Spain	0.0	0.2	9.4	0.4	1.0	0.0	0.8	13.7	14.2	10.5	0.7	14.7	0.2	0.3	0.0	0.3	0.1	1.1	0.3	0.1	1.3	8.0	0.0	0.6	1.8	9.1	-287.3	0.0	0.0	0.1	0.0	7.9	1.4	11.4	0.1
Sri Lanka	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	-0.8	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Sudan	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Tanzania	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	-2.5	0.0	0.0	0.0	0.0	0.0
Tunisia	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	-0.1	0.0	0.0	0.0	0.0
Turkey	0.0	0.2	7.4	0.3	0.8	0.0	0.7	10.4	10.7	8.2	0.6	11.0	0.2	0.2	0.0	0.2	0.1	0.9	0.3	0.0	1.1	6.3	0.0	0.5	1.5	7.2	6.8	0.0	0.0	0.1	0.0	-256.4	1.2	8.8	0.1
UAE	0.0	0.0	0.1	0.0	0.1	0.0	0.0	0.1	0.1	0.1	0.0	0.1	0.0	0.0	0.0	0.0	0.0	0.1	0.0	0.0	0.1	0.1	0.0	0.0	0.1	0.1	0.1	0.0	0.0	0.0	0.0	0.1	-34.5	0.1	0.0
UK	0.0	0.4	25.8	0.8	2.0	0.0	1.6	45.2	47.5	30.1	1.3	50.5	0.4	0.6	0.0	0.5	0.3	2.2	0.7	0.1	2.6	20.5	0.0	1.2	3.8	24.7	22.7	0.1	0.0	0.2	0.0	20.4	2.9	-445.1	0.3
Yemen	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	-3.2

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Alderson, D.L., M. Carlyle. 2009. How to design communication networks to be resilient to worst-case disruptions. Working paper, Naval Postgraduate School, Monterey, CA.

Alwis, C. 2007. Use of optical fibers towards global village. Presentation for *The Institution of Engineering and Technology (IET)*. Retrieved from http://www.christiealwis.com/Papers.htm.

Australian Communications and Media Authority (ACMA). 2007. *Protection zones around submarine cables of national significance*. Retrieved from http://www.acma.gov.au/WEB/STANDARD/pc=PC_100223.

Beaufils, J. 2000. How do submarine networks web the world? *Optical Fiber Technology* **6**(1) 15–32.

British Broadcasting Corporation (BBC). 2008. *Severed cables disrupt internet*. Retrieved from http://news.bbc.co.uk/2/hi/technology/7222536.stm.

Brown, G., M. Carlyle, J. Salmeron, K. Wood. 2005. Analyzing the vulnerability of critical infrastructure to attack and planning defenses. *Tutorials in Operations Research: Emerging Theory, Methods, and Applications* 102-123.

Brown, G., M. Carlyle, J. Salmeron, K. Wood. 2006. Defending critical infrastructure. *Interfaces* **36**(6) 530–544.

Brown, G., R. Dell. 2007. Formulating integer linear programs: A rogues' gallery. *INFORMS Trans. Ed*. **7**(2) 153–159.

Central Intelligence Agency (CIA). 2012. *The world factbook: Internet hosts by country*. Retrieved from https://www.cia.gov/library/publications/the-world-factbook/rankorder/2184rank.html.

Chang, H., M. Roughan, S. Uhlig, D.L. Alderson, W. Willinger. 2006. The many facets of Internet topology and traffic. *Networks and Heterogeneous Media* **1**(4) 569-600.

Chesnoy, J. 2002. *Undersea Fiber Communication Systems*. Academic Press, London.

Collins, L. 2011. Comms redundancy proves its value. *Engineering and Technology* **6**(4) 58–59.

Department of Homeland Security (DHS). 2009. *National infrastructure protection plan*. Retrieved from http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

Donovan, C. 2009. Twenty thousand leagues under the sea: A life cycle assessment of fibre optic submarine cable systems. Master's thesis. The Royal Institute of Technology (RTH), Stockholm, Sweden.

Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC). 2009. *Resilient international telecommunications guidelines for the financial services sector*. Retrieved from http://www.fsscc.org/.

Flag Telecom. 2012. *Flag Europe-Asia cable map*. Retrieved from http://sdc.flagtelecom.com/network/flag_europe_asia.html.

GAMS Development Corporation. 2010. *General Algebraic Modeling System (GAMS) 23.6*. Washington, D.C.

Homeland Security Advisory Council. 2006. *Report of the critical infrastructure task force*. U.S. Department of Homeland Security, Washington, D.C.

Homeland Security Council. 2007. *National strategy for homeland security*. The White House, Washington, D.C.

ILOG. 2007. *ILOG CPLEX 11.0 User's Manual*. Retrieved from http://www-eio.upc.es/lceio/manuals/cplex-11/html/.

International Cable Protection Committee (ICPC). 2009. *Submarine cable network security*. Retrieved from http://www.iscpc.org/.

International Cable Protection Committee (ICPC). 2011. *About submarine telecommunications cables*. Retrieved from http://www.iscpc.org/.

International Telecommunications Union (ITU). 2011. *Handbook for the collection of administrative data on telecommunications/ICT*. Retrieved from http://www.itu.int/ITU-D/ict/index.html.

Letellier, V. 2004. Submarine systems: From laboratory to seabed. *Optics and Photonics News* **15**(2) 30–35.

Mandell, M. 2000. 120000 leagues under the sea. *Institute of Electrical and Electronics Engineers (IEEE) Spectrum* **37**(4) 50–54.

Masi, D., E. Smith, M. Fischer. 2010. Understanding and mitigating catastrophic disruption and attack. *Sigma: Rare Events* **10**(1) 16–22.

Microsoft Corporation. 2012. *Microsoft Office*. Retrieved from http://office.microsoft.com/en-us/.

Nandi, B., M. A. Vasarhelyi, J. Ahn. 2000. Network demand model and global Internet traffic forecasting. *Convergence in Communications and Beyond*. Eds. Bohlin, K., K. Brodin, A. Lundgren, B. Thorngren. Elsevier Science Publishers, Amsterdam. 87–100.

Omer, M., R. Nilchiani, A. Mostashari. 2009. Measuring the resilience of the trans-oceanic telecommunication cable system. *Institute of Electrical and Electronics Engineers (IEEE) Systems Journal* **3**(3) 295–303.

Seacom. 2012. *SEACOM/Tata TGN-Eurasia cable map*. Retrieved from http://www.seacom.mu/network.

Sechrist, M. 2010a. Cyberspace in deep water: Protecting the arteries of the Internet. *Harvard Kennedy School Review* **10** 40–44.

Sechrist, M. 2010b. Cyberspace in deep water: Protecting undersea communication cables by creating an international public-private partnership. *Harvard Kennedy School Policy Analysis Exercise*.

Sintelsat. 2012. *India-Middle East-Western Europe (IMEWE) cable map*. Retrieved from http://www.sintelsat.com/fibernetworks/IMEWE.html.

Sri Lanka Telecom. 2012a. *Sea-Me-We-3 cable map*. Retrieved from http://www.seamewe3.com/inpages/cable_system.asp.

Sri Lanka Telecom. 2012b. *Sea-Me-We-4 cable map*. Retrieved from http://www.seamewe4.com/inpages/cable_system.asp.

Szajowski, P., G. Soloway, S. Thomas. 2010. Managing the economic lifecycle of a submarine cable system. *Proc. 32nd Annual Pacific Telecommunications Conference 2010 (PTC '10)*, Honolulu, HI.

Telegeography. 2011. *Meeting the global appetite for bandwidth*. Retrieved from http://www.telegeography.com/telecom-resources/telegeography-presentations/index.html.

Telegeography. 2012a. *2012 submarine cable map*. Retrieved from http://www.telegeography.com/telecom-maps/submarine-cable-map/index.html.

Telegeography. 2012b. *Interactive submarine cable map*. Retrieved from http://www.submarinecablemap.com/.

Terabit Consulting. 2002. *The Undersea Cable Report 2002*. Published by Terabit Consulting, Cambridge, MA.

Trischitta, P., A. Medina, R. Remedi. 1997. The Pan American cable system. *Institute of Electrical and Electronics Engineers (IEEE) Communications Magazine* **35**(12) 134–140.

Trischitta, P., W. Marra. 1998. Applying WDM technology to undersea cable networks. *Institute of Electrical and Electronics Engineers (IEEE) Communications Magazine* **36**(2) 62–66.

Zmijewski, E. 2008. Threats to Internet routing and global connectivity. *20th Annual FIRST Conference*, Vancouver, Canada. Retrieved from http://www.first.org/conference/2008/program/presentations.html.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. David L. Alderson
   Director, Center for Infrastructure Defense
   Naval Postgraduate School
   Monterey, California

4. Gerald G. Brown
   Executive Director, Center for Infrastructure Defense
   Naval Postgraduate School
   Monterey, California

5. Harrison Schramm, CDR, USN
   Naval Postgraduate School
   Monterey, California

6. Douglas R. Burton, CDR, USN
   Naval Postgraduate School
   Monterey, California

7. Jeffrey E. Kline, CAPT (Ret), USN
   Naval Postgraduate School
   Monterey, California