Design of a Transoceanic Cable Protection System

Isaac Geisler, Kumar Karra, Felipe Cardenas, and Dane Underwood
George Mason University, ggeisler, skarra, fcarden2, dunderw@masonlive.gmu.edu

***Abstract* - A system of underwater fiber optic cables spanning the world's oceans carries 99% of international communication data. Billions of dollars are invested into this network, resulting in 36% annual growth over the last 7 years. Over 150 cable damage incidents occur per year, causing significant losses to available cable bandwidth. Sixty percent of the faults are caused by human action, such as fishing and anchoring. Twenty percent are caused by random natural events and component failures, while the remaining 20% of fault causes are unknown. In addition, repairing a fault takes on average 13 days and costs $6 million, with more incurred costs due to the inability to provide bandwidth to its customers. This paper describes a design and operation to protect these cables by deployment of Transoceanic Cable Protection System (TCPS). The system consists of a Mission Control Center to accomplish three functions: (1) Threat Identification, (2) Damage Prevention, and (3) Coordination of Cable Repair. A probabilistic Monte Carlo simulation was developed to determine the effects of the TCPS on cable downtime, threat detection, mean time between failure, and cost per fault. The model evaluates the performance of TCPS based on the input distributions for threat generation, threat inter-arrival time, identification of threats, damage prevention, and repair time. A utility vs. cost analysis factoring in prevention, identification, cable downtime, lifespan, and environmental impact indicates that a passive hydrophone array is the most effective design for the Threat Identification function.**

Index Terms - cable protection, fiber optic cable, transoceanic cable

CONTEXT

A system of underwater fiber optic cables spanning the world's oceans transmits 99% of all international communication data, including internet traffic, phone calls, and text messages. There are over 300 cables currently in service, with dozens more planned to go online in the next few years [1]. Cables are the most cost-effective alternatives for long-distance telecommunications, because they offer high bandwidth at a fraction of the cost of satellite or microwave systems. Cables span over 500,000 miles on the seafloor, and individual cables can be over 3,000 miles long. The cost of cables range from tens of millions to billions of dollars to construct and maintain [2][3]. They come in a variety of capabilities, and the current network consists of a patchwork of technologies, with many cables from the early 1990s still in service [4].

The most important of these cables are the 53 transoceanic cables that interconnect the continents. These cables are critical infrastructure for governments and businesses. As of 2014, the transoceanic network provided 87 Tbps of bandwidth and has been growing exponentially at a 36% increase per year. [5]. This growth has been fueled by 11.8 billion dollars of investment since 2008 [5]. 4.8 billion dollars is planned to be invested in new transoceanic cables coming online in the next couple of years as well [5]. In all, planned cable systems coming online through 2020 will increase the global transoceanic bandwidth to 742 Tbps [5]. Newer cable technologies are now significantly increasing the bandwidth capacities of new cables, allowing this exponential growth to continue.

Cable owners rent out bandwidth at the rate of $85,000 to $100,000 per 10 Gbps unit per month to land-based ISPs, other telecommunication industries, governments, and technology companies [6][7][8]. Newer, high capacity cables can be worth up to $30 million per month in bandwidth rentals. This makes any cable downtime or damage a significant loss. Cable faults are categorized into 6 major causes, as shown in Figure 1. Accidental fishing and anchoring incidents cause 60% of the faults. Natural causes and component failure causes 20% of the faults, while the remaining 20% of the causes of the faults are unknown.

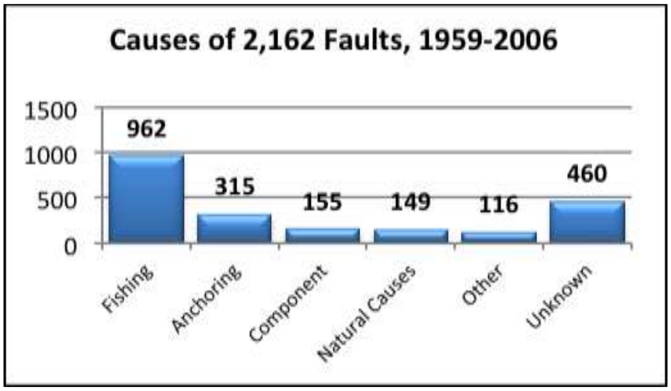

FIGURE I
DISTRIBUTION OF CABLE FAULT CAUSES

Intentional hostile human action, such as sabotage and espionage threats are not captured in the aforementioned research. Known incidents of sabotage in Indonesia, Egypt, and Libya blacked out regions for several days. Sightings of the Russian ship *Yantar*, equipped with 2 submersibles capable of cutting cables, increased fear of espionage and sabotage in the U.S. last fall [9].

Current methods of cable protection include using layers of armoring and insulation. While this steel armoring provides some protection, it can only be used in depths less than 2,000 meters [4]. The burial rate is 0.2-0.5 km/hr and costs about $12,000 per hour. Cables are also protected by the International Cable Protection Committee (ICPC) and Atlantic Cable Maintenance & Repair Agreement (ACMA). Protections include cable protection zones and procedures for criminal and civil charges. However, there is no active cable surveillance of marine activity monitoring to prevent cable damage.

Repair operations take on average 13 days with standard deviation of 1.07 days for finding delays, 1.26 days for repair ship travel, and 2.02 days for actual repair. The average total cost is $6 million [10]. Repairs can be significantly delayed by factors such as weather, difficulty locating the cable, or errors in reinstallation. During cable downtime, cable owners face significant losses due to repair costs and the loss of cable bandwidth.

STAKEHOLDER ANALYSIS

I. Cable Owners

Eighty percent of cable ownership resided with consortiums of telecommunication companies as of 2013 [1]. Their objective is to have uninterrupted data transmission through these lines at minimal costs. Repairing cable faults can accumulate cost throughout a cable's lifetime. Furthermore, telecommunication companies have shifted their focus on enhancing existing cables over building new ones since the early 2000's [1].

II. Maritime Industry

Members of the maritime industry are directly affected because of the risk and/or damage caused by accidental fishing and anchoring incidents. Seafarers and fishermen can face litigation from telecommunication companies in case of a fault.

III. Direct Access Entities

These entities are concerned with cable installation and repair services. Their objectives include the expansion of the cable system along with benefitting from a high fault rate of the cables [11].

IV. Governments

Governments in the United States, Latin America, Europe, Southeast Asia, and Africa are concerned with the threat of espionage due to the classified nature of the information passed through the submarine cables.

V. Stakeholder Tensions

While cable owners and governments want to decrease the number of cable faults, cable repair services benefit from a high cable failure rate. The maritime industry wants to reduce the number of faults caused by shipping and fishing vessels, but there is lack of clarity in the location of underwater cables that could make incidents preventable.

PROBLEM AND NEED

I. Problem

Despite massive dependence on these cables, they are left unguarded and poorly protected. More than 150 cable faults occur every year and about 60% are caused by humans. There is also increasing fear of sabotage and espionage due to government tensions and historical events.

II. Need

There is a need to provide active protection of cables to decrease the number of faults, increase the rate of detection, and improve the mean notification time of damaged cables. This inadvertently minimizes cable damage, decreases the cost in repairing cables, and deters future threats from happening.

CONCEPT OF OPERATIONS

The proposed solution is the Transoceanic Cable Protection System (TCPS). The TCPS will have three functions: (1) Threat Identification, (2) Prevention, and (3) Repair Coordination. The basic procedure of the system starts with identifying and detecting threats. Once a threat is detected, prevention efforts are initiated. If damage does occur, the next objective is to reduce cable downtime by coordinating repair.

I. Concept of Operations

The TCPS encompasses the need to perform three functions from a central Mission Control Center. First, the Threat Identification function aims to identify surface-level and underwater threats using different technologies that will send data to Mission Control. Using this data, the system will identify threats to the cables.

Second, the Prevention function will stem from forecasting and communication. Forecasting is performed by gathering data per region. For example, majority of cable faults occur in depths less than 200 meters and are more common in certain regions [7]. By knowing that volume will be higher in this region, we can forecast that it is more likely for cable faults to occur. In this case, the system would heavily monitor ship activity near in these regions. Mission Control will then facilitate communication through either messages to marine traffic or messages to appropriate authorities.

Third, if damage is not prevented and a fault occurs, Mission Control will begin the Repair Coordination process, which will involve sending messages to repair companies. The Mission Control will be the basis for the different functions as all will be operated from this location.

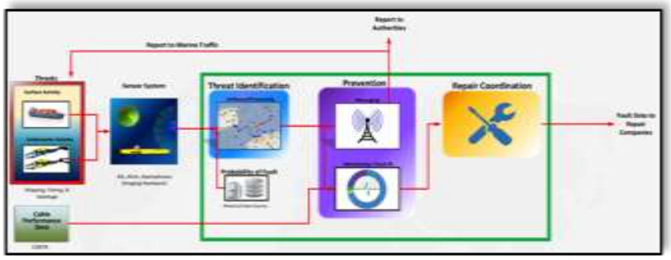

FIGURE 2
MISSION CONTROL FUNCTIONAL BREAKDOWN

II. Requirements

Requirements for the system are shown in Table I.

TABLE I
MISSION REQUIREMENTS

NUMBER	DESCRIPTION
MR.1.0	TCPS shall monitor cables 24 hours a day.
MR.1.1	The system shall survey and monitor 50% of the total cable length.
MR.1.2	The system shall be able to monitor at least 50% of littoral zones.
DR.1.3	The system shall provide real-time information to Mission Control.
DR.1.4	The system shall differentiate between hostile and non-hostile threats.
MR.2.0	TCPS shall provide real-time threat information to appropriate authorities.
MR.3.0	TCPS shall detect fault location to within 100 meters.
FR.3.1	The system shall provide real-time information to cable owner and repair companies within one hour.

THREAT IDENTIFICATION DESIGN ALTERNATIVES

Design alternatives for the Identification Function include two categories: surface-level and underwater surveillance systems. A survey for the suitability of various technologies identified the following alternatives:

I. SURFACE LEVEL: AUTOMATIC IDENTIFICATION SYSTEM

Automatic Identification System (AIS) is a transponder that is required by law to be placed on all ships over 299 tons. The transponder communicates with on-shore stations via satellite. AIS provides location, speed, identification, and movement data in real time. AIS is limited to a 200 nm range from the shore and cannot provide data on underwater movement [12].

II. ACTIVE UNDERWATER ALTERNATIVES

For active underwater surveillance, autonomous underwater vehicles (AUVs) will be utilized. AUVs are submersibles that have the ability to travel a predetermined path or operate autonomously for a period of time. They will be equipped with Synthetic Aperture Sonar (SAS) for high resolution imaging capabilities. The following three AUVs are the alternative for active cable surveillance systems:

- **Liquid Robotics Wave Glider:** The Wave Glider is a low power, long duration AUV capable of up to one year endurance before maintenance. It uses a combination of solar and wave power for propulsion [13].
- **Kongsberg Seaglider:** The Seaglider is widely used in oceanographic surveys. It is also a low power, long duration AUV. It is battery powered and has a payload capable of carrying multiple sensors [14].
- **Kongsberg HUGIN:** The HUGIN is used for both oceanographic surveys and oil and gas drilling inspection. It has a very large payload capacity and is capable of diving to 6,000 meters in depth. HUGIN is currently used in civilian and military operations [15].

III. PASSIVE UNDERWATER ALTERNATIVE: HYDROPHONES

Ocean Sonics icListen Audio Frequency Smart Hydrophones (hydrophones for short) are passive acoustic sensors that listen for sound within a region, such as engine noise. The hydrophones will be set up in an array consisting of a buoy, tether, hydrophone and anchor. The array will be placed along the length of a cable with the hydrophone device residing in the Sound Fixing and Ranging (SOFAR) region. The SOFAR region is approximately 1,000 meters below the surface. Its pressure and temperature range allows sound waves to travel undisturbed for thousands of kilometers. The hydrophone will be anchored to the seabed with a tether attached to the hydrophone, which is connected to a surface buoy that can transmit real time data. This hydrophone array meets the requirements of our threat identification function [16].

V. SUMMARY

Table 3 shows the capabilities of the design alternatives and approximate costs.

TABLE 3
DESIGN ALTERNATIVES SUMMARY

ALTERNATIVE	CAPABILITIES	COST
AIS	200 nm range Tracks location, speed, movement Required on ships over 299 tons	$10,000/year
WAVEGLIDER	Up to 1 year endurance Built-in AIS receiver 2 knots average speed	$200,000/unit
HUGIN	72 hour endurance 6,000 meter depth rating 4.1 knots average speed	$5 million/unit
SEAGLIDER	7,200 hour endurance 1.7 knots average speed 1,000 meter depth rating	$250,000/unit
HYDROPHONES	Up to 16 km listening range	$5,000/unit

The image below further illustrates the use of the design alternatives in TCPS.

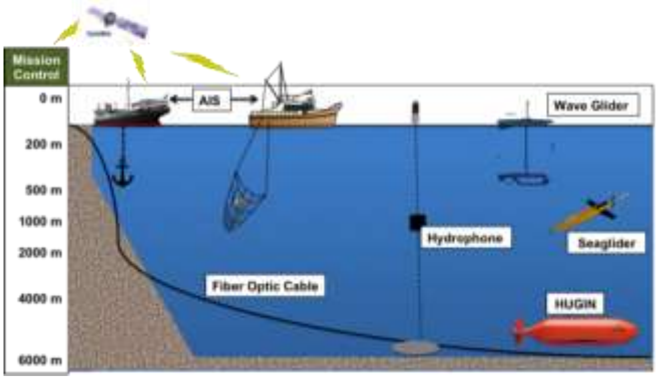

FIGURE 3
DESIGN ALTERNATIVES FOR IDENTIFICATION FUNCTION

METHOD OF ANALYSIS

The primary method of analysis for the proposed system is through a computer simulation of two representative transoceanic cables. The cables are the SEA-US and the APX-East, both located in the Pacific Ocean. These specific cables were chosen as examples of the types of cables planned to be installed over the next 10 years. These cables are ideal candidate customers for the Transoceanic Cable Protection System. An image of the SEA-US cable is shown with cable landing stations in California, Hawaii, Guam, and the Philippines.

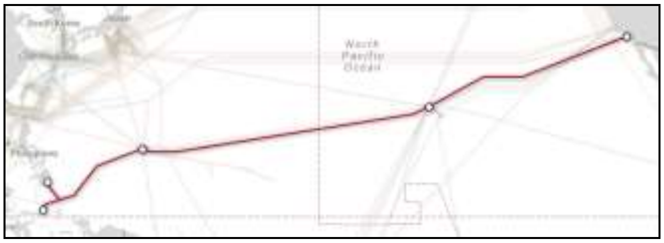

FIGURE 4
SEA-US CABLE

I. Simulation Parameters and Variables

The simulation has two inputs: a depth profile representing the cable to be simulated, and a list of the specific TCPS alternatives actively monitoring the cable. The list of TCPS alternatives includes operating range, speed, and sensor types.

Threats are generated via a Poisson distribution. Currently, real world threats to cable systems are not tracked since there is little to no surveillance of these cables. To model threats, known fault occurrences were utilized. The number of each threat type per year was obtained by estimating the threat to fault conversion probability of each fault type. From these threat rates, the threat interarrival time in hours was estimated and used for the threat generation. See Table 4 for specific threat/fault types and associated probabilities.

TABLE 4
THREAT GENERATION

	Probability of Fault Type	Normalized Probability of Fault type	P * 0.5 faults/year	Threat-Fault conversion probability	Threats per year of each type	Threats per hour of each type	Threat Interarrival rate in hours
Fishing	0.44	0.54	0.27	0.05	5.41	6.2x10^{-4}	1,619
Anchoring	0.16	0.19	0.095	0.25	0.38	4.3x10^{-5}	23,051
Component	0.07	0.09	0.045	1.00	0.04	5x10^{-6}	199,776
Natural	0.07	0.08	0.04	0.10	0.42	4.8x10^{-5}	20,846
Espionage	0.04	0.05	0.025	0.00	0.02	3x10^{-6}	365,000
Sabotage	0.04	0.05	0.025	1.00	0.02	3x10^{-6}	359,598
Total	0.82	1	0.5	2.4	6.30	0.00071	**1,390**

When threats are generated, they are assigned loiter times with a normal distribution. The simulation clock counts down this loiter time until 0. Based on its threat to fault conversion probability, the threat either generates a fault or is removed from the simulation.

If a fault has occurred, the simulation generates three delay times (notification, travel, and repair) based on distributions calculated from real world data. The travel and repair delays are multiplied by the repair cost rate to generate the total repair cost. All three delays combined become the total cable downtime, which are used to analyze lost bandwidth costs based on the total cable bandwidth and the monthly rental rate for that cable.

II. Design of Experiment and Simulation Configuration

The simulation runs for 10 years, updating all TCPS agents, threats and faults every hour on its internal clock. When initialized, TCPS agents are placed on the cable profile as appropriate based on the input agent list.

When the simulation clock reaches the next interarrival time, a threat is generated at a random but appropriate depth and location on the cable.

Every hourly clock tick, all agents are updated, moving and scanning for threats along the cable. If a TCPS agent is within sensor range of a threat, it has a 95% chance of detecting the threat. If the threat can be identified, warning messages are sent to the threat to deter possible cable damage. The messages have a 25-50% chance of removing the threat, increasing based on the type of sensor that has detected the threat. Success probabilities are conservative estimates with more information yielding higher success rates. The Design of Experiment for the SEA-US is shown in Table 5.

TABLE 5
DESIGN OF EXPERIMENT FOR SEA-US SIMULATION

Cable	**System Type**	**TCPS Technologies**	**TCPS Coverage**		
			Insta nt	**Per 24 hrs**	**Total**
SEA-US	None	None	0%	**0%**	**0%**
SEA-US	AIS Only	4 AIS	8%	**8%**	**8%**
SEA-US	AUV Only	26 HUGIN	6%	**37%**	**100%**
SEA-US	AUV Only	50 Seaglider (SG)	11%	**18%**	**100%**
SEA-US	Hydrophone Only	1000 Hydrophone Buoys (HB)	100%	**100%**	**100%**
SEA-US	AUV Only	30 Wave Glider (WG)	80%	**98%**	**100%**
SEA-US	Full Hybrid	4 AIS, 19 HUGIN, 9 SG	14%	**38%**	**100%**

SEA-US	Full Hybrid	4 AIS, 1000 HB	100%	**100%**	**100%**
SEA-US	Full Hybrid	4 AIS, 81 HB, 20 HUGIN	30%	**54%**	**100%**
SEA-US	Full Hybrid	4 AIS, 81 HB, 12 WG	57%	**64%**	**100%**
SEA-US	Partial Hybrid	4 AIS, 231 HB	32%	**32%**	**32%**
SEA-US	Partial Hybrid	4 AIS, 7 WG	15%	**31%**	**33%**
SEA-US	Partial Hybrid	4 AIS, 231 HB, 7 WG	32%	**32%**	**33%**

Each simulation is replicated 7700 times and the aggregate data is used for analysis. The number of replications was determined by calculating the number of replications needed for a 95% confidence interval based on the mean and standard deviation of all parameters from an initial 1000 replication run.

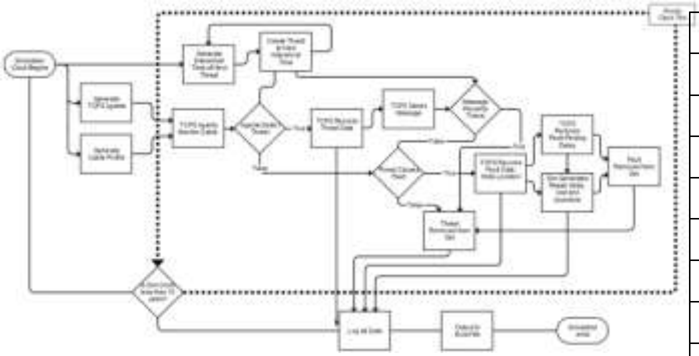

FIGURE 5

FUNCTIONAL ARCHITECTURE OF THE TCPS SIMULATION

III. Simulation Validation

To validate the as-is case simulation, the results are to be compared to historical data using a two-sample test within a 95% confidence interval. In contrast, there is no hard data to compare to the TCPS simulation output as a similar system does not exist. To ensure accuracy of data, input parameters for each case are verified.

IV. Utility Analysis

The following graphic shows the utility hierarchy and their associated weightings. The four main categories of weights are prevention, identification, downtime, lifespan, and environmental impact as to correlate with the mission requirements. Each category is further broken down into the relevant simulation outputs. The weights for each measure are based on each cable and the unique requirements they have. Figure 6 shows the weights used for the SEA-US cable.

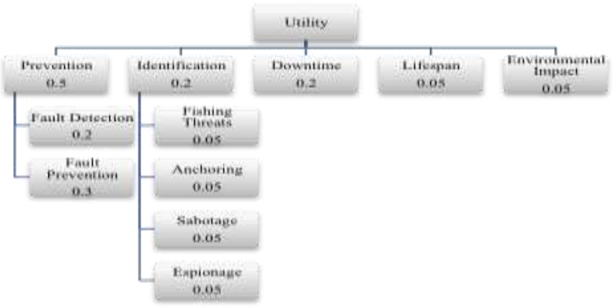

FIGURE 6

UTILITY HIERARCHY

RESULTS AND UTILITY ANALYSIS

I. Simulation Results

The "Hydrophone + AIS", Hybrid Case 2, exhibits the highest utility at 0.68, at a cost of $12.76 million. This case successfully detected 92% of threats, prevented 56% of faults, reduced cable downtime by 57% and reduced repair costs and lost bandwidth costs by $57 million over 10 years.

TABLE 6

RESULTS OF SEA-US SIMULATION

	Threats Detected	Faults Prevented	Cable Downtime (hrs)	Repair Costs ($M)	Bandwidth Losses ($M)
As-Is	0%	0%	1325.9	10.69	90.31
AIS	21%	13%	1151.8	9.28	78.45
HUGIN	11%	4%	1270.0	10.26	86.50
SeaGlider	11%	4%	1265.0	10.21	86.16
Hydrophone	92%	53%	619.1	5.05	42.17
Wave Glider	74%	45%	737.7	5.98	50.25
Hybrid Case 1	30%	16%	1102.4	8.91	75.09
Hybrid Case 2	92%	56%	576.3	4.70	39.26
Hybrid Case 3	35%	21%	1056.8	8.54	71.98
Hybrid Case 4	45%	28%	954.9	7.72	65.04

Utility vs. Cost analysis is shown in Figure 7. Alternatives in the upper left hand side of the prove to be the best options.

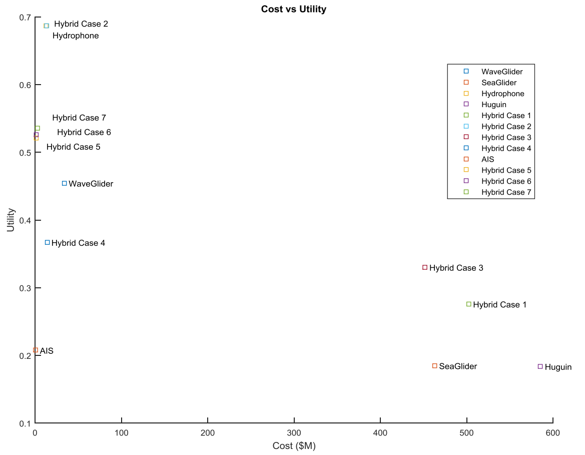

FIGURE 7

COST VS. UTILITY FOR SEA-US SIMULATION

II. Sensitivity

Each of the utility measure's weighting are varied between 0%-100% in order to analyze the sensitivity of the results.

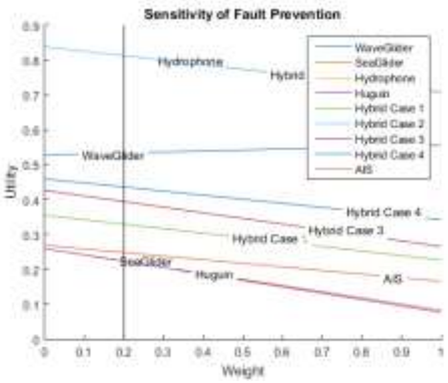

FIGURE 8
SENSITIVITY OF FAULT PREVENTION FOR SEA-US CABLE

The sensitivity chart shows the Sensitivity of Fault Prevention measure for the SEA-US cable. The leading design alternative, the “Hydrophone only” case, continues to have dominant utility throughout the variation of the weighting. This remains the case for the other measures as well concluding that the results are not very sensitive.

RECOMMENDATIONS

Based on analysis of the utility function, our recommendation is the installation of a hydrophone and AIS based TCPS on any cable desiring protection from cable fault incidents. Simulation results indicate that the hydrophone and AIS alternative was able to detect 92% of cable threats, and prevented 56% of cable faults. This alternative reduced cable downtime by 57%, repair costs by $6 million and lost bandwidth costs by $51 million. The study positively concludes that by implementing underwater surveillance on transoceanic cables, cable downtime, bandwidth losses and repair costs may be significantly reduced.

There is a gap in the market that can be filled by TCPS. The business case developed is based on the costs for two periods: (1) set-up period, and (2) operational period. Set-up period will have nonrecurring costs for Mission Control of $1,350,000. Recurring costs for Mission Control will be $1,018,000 per year. For each protected cable, the nonrecurring cost is expected to be $1,300,000 with a recurring cost of $58,000 per year.

Customers will subscribe to the system on a yearly basis with a 5-year monitoring contract. Subscription price is a function of cable length, number of cable landing stations (CLS), and coverage desired by the customer. For example, the SEA-US cable has 4 CLS and is 15,000 km in length. For 100% coverage with the Hydrophone + AIS alternative, the subscription price is $1,634,000 per year. Initial investment in TCPS includes the nonrecurring Mission Control costs and the first year of operating expenses, resulting in $2,368,000.

This protection method will provide the owners of SEA-US $4.7 million in repair cost savings and $24.7 million in downtime cost savings over 10 years. Further business case analysis indicates that by following a 5-year subscription model, the optimistic break-even point will be reached in one year (optimistic) and two years (pessimistic). TCPS will see an optimistic 1132% ROI and a pessimistic 231% ROI.

ACKNOWLEDGEMENT

Special thanks to: Dr. Lance Sherry, Faculty Advisor; George Blaha of Raytheon, Sponsor; and Bahram Yousefi, GMU Graduate Teaching Assistant.

REFERENCES

[1] TeleGeography. (2015, September 15). Submarine Cable Map [Online]. Available: http://www.submarinecablemap.com/#/

[2] L. Hedges. (2015, March 19). Top five telecoms projects [Online]. Available: http://www.hibernianetworks.com/corp/wp-content/uploads/2013/02/Top-five-telecoms-projects-2015_Capacity-Magazine_April-2015.pdf

[3] F. Lardinois. (2015, May 11). Microsoft invests in 3 undersea cable projects to improve its data center connectivity [Online]. Available: http://techcrunch.com/2015/05/11/microsoft-invests-in-3-undersea-cable-projects-to-improve-its-data-center-connectivity/#.hhwwya:w2DQ

[4] L. Carter et al. “Submarine cables and the oceans: connecting the world” UNEP-WCMC/UNEP/ICPC. Cambridge, UK, Biodiversity Series No. 31, 2009.

[5] Y. Ruggeri et al. “Submarine Telecoms Industry Report” Terabit Consulting. Cambridge,MA, Issue 3, 2014.

[6] M. Islam. (2015, May 8). Submarine Cable plans to sell bandwidth to Italian firm at low price [Online]. Available: http://www.thedailystar.net/business/submarine-cable-plans-sell-bandwidth-italian-firm-low-price-80342

[7] “Global Bandwidth Research Service Executive Summary” TeleGeography. Washington D.C. 2015

[8] “Australia & Pacific Bandwidth Review” TeleGeography. Washington D.C. February, 2015.

[9] B. Gertz. (2015, September 22). *Russian Spy Ship Makes Port Call in Caribbean* [Online]. Available: http://freebeacon.com/national-security/russian-spy-ship-makes-port-call-in-caribbean/

[10] W. Rain. (2009, December 14). Problems faced by Industry in the repair of damaged submarine telecommunications cables inside maritime jurisdictional claims [Online]. Available: http://cil.nus.edu.sg/wp/wp-content/uploads/2009/10/Wolfgang-Rain-Session-3.pdf

[11] Reuters. (2015, August 26). Libya's land phone line system breaks down after cables were damaged [Online]. Available: https://www.dailystar.com.lb/News/Middle-East/2015/Aug26/312843-libyas-land-phone-line-system-breaks-down-after-cables-were-damaged.ashx

[12] “Satellite AIS Data” *Marine Traffic*, 2016. [Online]. Available: http://www.marinetraffic.com/en/p/satellite-ais

[13] “Wave Glider - How it works,” *Liquid Robotics*, 2016. [Online]. Available: http://liquid-robotics.com/technology/waveglider/how-it-works.html.

[14] “Autonomous Underwater Vehicle - Seaglider,” *Kongsberg Marine*, 2015. [Online]. Available: http://www.km.kongsberg.com/ks/web/nokbg0240.nsf/AllWeb/EC2FF8B58CA491A4C1257B870048C78C?OpenDocument.

[15] “Autonomous Underwater Vehicle - HUGIN,” *Kongsberg Marine*, 2015. [Online]. Available: http://www.km.kongsberg.com/ks/web/nokbg0240.nsf/AllWeb/B3F87A63D8E419E5C1256A68004E946C?OpenDocument.

[16] “icListen Smart Hydrophones,” *Ocean Sonics*, 2015. [Online]. Available: http://oceansonics.com/iclisten-smart-hydrophones/.

AUTHOR INFORMATION

All authors are undergraduates of the Systems Engineering and Operations Research Department at George Mason University.