CYBERSPACE IN DEEP WATER:

Protecting Undersea Communication Cables By Creating an International Public-Private Partnership

MICHAEL SECHRIST
HARVARD KENNEDY SCHOOL
MARCH 23, 2010

CYBERSPACE IN DEEP WATER:
PROTECTING UNDERSEA COMMUNICATION CABLES

By Creating an International Public-Private Partnership

Prepared by:
Michael Sechrist
Harvard Kennedy School

Prepared for:
Rand Beers
Under Secretary for National Programs and Protection Directorate,
Department of Homeland Security

Faculty Advisor: Eric Rosenbach

External Advisor: Richard Clarke
CEO, Good Harbor Consulting, LLC

Seminar Leader: Monica Toft

Harvard Kennedy School of Government
Policy Analysis Exercise

March 23, 2010

ACKNOWLEDGEMENTS

Undersea communication cables became an academic interest of mine a few years ago. I was fascinated by the subject and shocked to learn how little is known about them. In 2008, I wrote a research proposal on a public-private partnership for cables and received a Department of Homeland Security Fellowship to attend Harvard Kennedy School to study the issue further. This work is a culmination of that proposal and process.

I owe many thanks to the Oak Ridge Institute for Science and Education and the Department of Homeland Security for supporting me in this research. Some of it was developed this summer while working for the Department of Homeland Security ALERT Center of Excellence at Northeastern University. To my project mentors at ALERT, Michael Silevitch and John Beaty, I owe a debt of gratitude for developing my initial ideas and barring with me through my first presentations.

I especially want to thank Eric Rosenbach, my faculty advisor, who appreciated the significance of this project enough to find funding for me to attend professional conferences on the subject. His overall guidance was truly beneficial, particularly since he has been my interface with my client throughout the year.

Overall, this paper incorporates research collected from presentations delivered at two professional conferences, the Reliability of Global Undersea Communication Cables Infrastructure (ROGUCCI) Summit and the Pacific Telecommunications Council (PTC) 2010, several dozen interviews and informal conversations with industry experts, a vast literature review, as well as source documents provided to me from the Department of Homeland Security.

ORISE ACKNOWLEDGEMENT

This research was performed under an appointment to the U.S. Department of Homeland Security (DHS) Scholarship and Fellowship Program, administered by the Oak Ridge Institute for Science and Education (ORISE) through an interagency agreement between the U.S. Department of Energy (DOE) and DHS. ORISE is managed by Oak Ridge Associated Universities (ORAU) under DOE contract number DE-AC05-06OR23100. All opinions expressed in this paper are the author’s and do not necessarily reflect the policies and views of DHS, DOE, or ORAU/ORISE.

EXECUTIVE SUMMARY

A "September 10th" mindset permeates relations between the United States ("U.S.") government and undersea communications cable companies. Communication before and after a cable break is sparse, disjointed and compartmentalized. For catastrophic cable outages, no coordinated mitigation plan exists. Nor is there adequate defense-in-depth in place. There is plenty of room for improvement among all parties. To improve the process, this paper proposes that the Department of Homeland Security create an international public-private partnership to prevent and prepare for the world's next major cable outage.

Cables are vital to global communications and U.S. interests. In the U.S., approximately 95% of all international internet and phone traffic travel through undersea cables.[1] Nearly all government traffic, including sensitive diplomatic and military orders, travels these cables to reach officials in the field.

In the military, DoD's net-centric warfare and Global Information Grid (e.g., DoD's information interoperable system) rely on undersea cables.[2] The GIG uses undersea communication cables to provide large segments of DoD personnel living and working overseas with fast, reliable and relatively cheap communication.[3] [4]

[1] NSTAC, NSTAC: Cyber Collaboration Report, May 21, 2009. Page 26. Accessed at http://www.ncs.gov/nstac/reports/2009/NSTAC%20CCTF%20Report.pdf

[2] "CHIPS - The Department of the Navy Information Technology Magazine," DON CIO Spectrum and Telecommunications Team, Jan-March 2005, Accessed at http://www.chips.navy.mil/archives/05_Jan/web_pages/spectrum.htm

[3] Ibid.

[4] James Dunnigan, "The Unstoppable Signal From Space," Strategypage.com, February 15, 2008. Accessed at http://www.strategypage.com/dls/articles/200821522200.asp

A major portion of DoD data traveling on undersea cables is unmanned aerial vehicle (UAV) video.[5] In 2010, UAVs "will fly 190,000 hours"[6] and the Air Force estimates that "it will need more than one million UAV hours annually to be prepared for future wars."[7] Without ensured cable connectivity, the future of modern warfare is in jeopardy.

The stability of the modern financial system is also at risk. Companies use cables to transfer trillions of dollars every day. For example, the Society for Worldwide Interbank Financial Telecommunication (SWIFT), which describes itself as "the global provider of secure financial messaging services," uses undersea fiber-optic communications cables to transmit financial data between 208 countries.[8]

In 2004 alone, nine million messages and approximately $7.4 trillion a day was traded on this network.[9] Today, nearly 15 million messages a day are sent over it. The CLS Bank, which "operates the largest multi-currency cash settlement system," conducts over one million transactions and trades over $4.7 trillion dollars a day on the same undersea cables.[10] As Stephen Malphrus, Chief of Staff to Federal Reserve Chairman Bernanke recently noted, "When communications networks go down, the financial services sector does not grind to a halt, rather it snaps to a halt."[11]

[5] Brian Mocheknhaupt, "We've Seen the Future, and It's Unmanned," *Esquire Magazine*, October 14, 2009. Accessed at http://www.esquire.com/features/unmanned-aircraft-1109

[6]Ibid.

[7] Ibid.

[8] Address by Stephen Malphrus, ROGUCCI conference

[9] Ibid.

[10] Ibid.

[11] Stephen Malphrus, "Keynote Address," ROGUCCI conference, Dubai, U.A.E., October 19, 2009.

When a cable does lose service, the economic impact is difficult to quantify. One estimate from the International Cable Protection Committee's legal advisor states that "…service interruptions of these high-bandwidth underwater fiber optics communications systems can result in excess of $1.5 million revenue loss per hour."[12] His estimate deals primarily with losses from cable operator, not those from companies or government entities that own bandwidth on the disrupted cable. In that respect, as well as the fact the estimate is five years old, it can be considered quite low.

The Department of Homeland Security has the statutory authority to create the partnership to better ensure cable connectivity worldwide. Under Homeland Security Presidential Directives (HSPD) 5 and 7, as well as Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, DHS is to direct the National Communications System and provide for the security of telecommunications critical infrastructure protection. DHS oversees the President's National Security Telecommunications Advisory Committee (NSTAC), as well as Information Sharing Analysis Centers (ISACs) for Information Technology and Communication. These groups evaluate the security of undersea cables in one form or another. Moreover, DHS is charged with conducting "bilateral discussions with close allies and others to further international cyber security awareness"[13] and leads the inter-agency "Team Telecom" group that assesses undersea cable permits and licenses.[14]

[12] Douglas Burnett, "Submarine Cable Infrastructure Defense Against Terrorists," *Sea Technology Magazine*, July 2005. Accessed at http://findarticles.com/p/articles/mi_qa5367/is_200507/ai_n21376410/pg_2/?tag=content;col1

[13] *NSTAC Report to the President on International Communications,* NSTAC, August 16, 2007. Page D-5. Accessed at http://www.ncs.gov/nstac/reports/2007/NSTAC%20International%20Report.pdf

[14] Kent Bressie, "More Unwritten Rules: Developments in U.S. National Security Regulation of Undersea Cable Systems," Presentation to the 2009 PTC conference, January 18, 2009. Accessed at http://www.harriswiltshire.com/siteFiles/News/7DF1C8D035660E8FBEF0AAC7BA8DA103.pdf

Research produced herein shows that the global undersea cable architecture is at an increased risk of danger. In this paper, Larson's "Danger Index" is used as the analytic framework to determine this risk assessment for the undersea cable infrastructure. The "Danger Index" is a quantitative application of a qualitative concept. It is equivalent to *Intention* multiplied by *Capability*, *Vulnerability* and *Consequence*.[15] Most, if not all, these terms of the equation are increasing and thus the associated level of danger is also growing. To decrease the danger variable, the partnership should be designed to lessen the underlying causes for the increases. Specific policy recommendations tackle these causes.

The ultimate goals of the partnership are to develop industry best practices, high-level operational exercises, reporting structures and comprehensive lists with single points of contact. The international community is best served if the partnership forms as a voluntary, non-institutional body, similar in respects to the Department of State's Global Initiative to Combat Nuclear Terrorism. Lastly, the paper proposes steps to enact the partnership in this respect.

[15] Randell Larson, *Our Own Worst Enemy: Asking the Right Questions About Security to Protect You, Your Family, and America,* Hachette Book Group, New York, 2007. Page 68.

TABLE OF CONTENTS

A RECENT WAKE-UP CALL[16]

Fridays are typically slow days for federal officials. But December 19, 2008 was no ordinary Friday.

On just his second day on the job, Lieutenant General Carroll Pollett, the Director of the Defense Information Systems Agency (DISA), faced a major problem.[17] For reasons unknown at the time, three of the world's largest cables from Italy to Egypt had been severed. These cables, although seemingly far away in the Mediterranean Sea, are major contributors to overall DoD global connectivity.

As the CEO of Verizon noted last year, "DISA relies on commercial networks for 95 percent of the infrastructure [used] for strategic communications."[18] In this case, the cable outage quickly caused "a 60 percent loss of both commercial and military capacity in the Gulf Region."[19] It was a nightmare scenario for Pollett. The U.S. needed a fast, uninterrupted bandwidth connection to communicate to the Middle East and all eyes looked at him to get it.

An ad-hoc team quickly assembled with staff from U.S. Strategic Command's Joint Functional Component Command for Network Warfare (STRATCOM – JFCC-NW) and the Joint Task Force for Global Network Operations (JTF-GNO). The team sought to restore the lost capacity, but cable repairs are not a quick fix. In some

[16] Information from this section was collected from a variety of sources, the most helpful of which came from Nick Lordi, Senior Director at Telcordia Technologies, Inc., in an unpublished paper entitled, "Air Force Cybersecurity Article Points." Senior leadership within DHS should read it in conjunction with this section to get a full understanding.

[17] Ivan Seidenberg, "Keynote Address: Customer Partnership Conference," Defense Information Systems Agency (DISA) Customer Partnership Conference, April 21, 2009. Accessed at http://www22.verizon.com/Content/ExecutiveCenter/Ivan_Seidenberg/defense_information_systems/defense_information_systems.htm

[18] Ibid.

[19] Ibid.

cases, cable breaks take several weeks to re-splice. Other routes and other technologies would be needed to mitigate the loss.

As DISA, JFCC-NW and JTF-GNO all went into overdrive, the U.S. Air Force unmanned aerial vehicle (UAV) targeting teams' work slowed to a halt. In a February 20th, 2009 briefing, Lieutenant Colonel Donald Fielden, 50th Communications Squadron Commander at Shriever Air Force, stated the cable breaks decreased UAV flights operating out of Balad Air Force base in Balad, Iraq from "hundreds of combat sorties per day" to "tens of sorties a day."[20] Since "a single Global Hawk UAV requires 500Mbps bandwidth"[21] to operate, undersea cables[22] are needed to provide for fast, large and inexpensive connection. Milliseconds matter when you are in the UAV business and undersea cables shave off hundreds of them compared to satellites. But without a reliable connection, U.S. military technicians sitting within the 42nd Attack Squadron at Creech Air Force Base outside Las Vegas, Nevada or elsewhere in Europe would have been of little use. UAV operations at Balad, America's "biggest base in Iraq,"[23] were nearly frozen. It is not publicly known if UAV operations in Pakistan or elsewhere were also hampered, but when 80% connectivity is lost between Europe and the Middle East, it is a safe assumption.

In the end, industry insiders believe that a couple of ships, inadvertently, caused the breaks. Ships are known to drag their anchors long distances along the relatively flat Mediterranean Sea bottom; in this case, ships' anchors caught three cables and bent them beyond a workable point. With the breaks, essential fiber optic links that

[20] Nick Lordi, "Air Force Cybersecurity Article Points," Telcordia Technologies, Inc., unpublished article.

[21] "CHIPS - The Department of the Navy Information Technology Magazine," DON CIO Spectrum and Telecommunications Team, Jan-March 2005, Accessed at http://www.chips.navy.mil/archives/05_Jan/web_pages/spectrum.htm

[22] For a definition of undersea cables, please see Appendix A.

[23] Lordi, Telcordia, unpublished article – see appendix.

keep connections streaming between U.S. military forces in the Gulf and U.S. UAV ground control stations were significantly degraded.[24]

When UAV missions "are the only game in town,"[25] global network reliability is paramount. Undersea cables play a vital role in executing sensitive military operations and the loss of the three fiber optic cables can disrupt significant connectivity. The same losses can occur in the financial, diplomatic and social sectors.

Key Takeaway

Cable breaks halfway across the world threaten U.S. vital national security interests. They can also threaten the sustainability of U.S. companies, U.S. citizens and U.S. interests operating abroad. NSTAC presented a similar picture to the President three years ago: "cyber threats to global infrastructures may originate from international sources *beyond the jurisdiction* of U.S. and allied authorities…increasing concerns about the security and availability of *domestic* [National Security/Emergency Preparedness] communications and the global communications on which many key U.S. functions and economic interests rely."[26]

Undersea cables are one of the most important global cyber infrastructures in existence. Simply put: any effort to protect cables must also be international. An effort led by the U.S. to protect cables landing only in the U.S. will never be enough because international cable disruptions have large secondary effects, much like that of the 2008 global financial crisis. The resulting solution must also be global.

[24] Mockenhaupt, *Esquire Magazine*.

[25] Noah Schactman, "CIA Chief: Drones 'Only Game in Town' for Stopping Al Qaeda," *Wired Magazine*, May 19, 2009. Accessed at http://www.wired.com/dangerroom/2009/05/cia-chief-drones-only-game-in-town-for-stopping-al-qaeda/#ixzz0e8GDppPM

[26] NSTAC Report to the President on International Communications, NSTAC, 2007.

METHODOLOGY

The analytical framework used within the report originates from Randell Larson's book, *Our Own Worst Enemy: Asking the Right Questions About Security to Protect You, Your Family, and America*, and Snow, Hoag and Weckman's follow-on study and presentation delivered to the *Seventh International Conference on Networks*. The risk management equation is applicable to fiber optic transmission systems.[27]

The idea and model for an international public-private partnership came from the Global Initiative to Combat Nuclear Terrorism, started in 2006. That Initiative began in the Office of the Under Secretary for Arms Control and International Security, in which I worked, and was spearheaded by Thomas Lehrman, under the guidance of then Under Secretary Bob Joseph. It was endorsed by the National Security Council and agreed to by Presidents Bush and Putin in St. Petersburg, Moscow in 2006. The Initiative formed from a core group of partner nations into a voluntary, non-institutional partnership that was led from the Office of the Under Secretary after Presidential endorsement. Like the Initiative before it, this cable partnership would seek similar things to be successful: initial partner nation buy-in, a voluntary, non-institutional structure and Under Secretary-level support within DHS.

Literature Review

In researching vulnerabilities, threats and trends, an exhaustive search of undersea cable material was conducted within Harvard and MIT library system. Source documents were provided by the National Communications System; the most helpful are classified For Official Use Only (FOUO) and cannot be discussed in this paper. However, the President's National Security Telecommunications Advisory

[27] Snow, Hoag and Weckman, "Understanding danger to critical telecom infrastructure: a risky business," IEEE Computer Society: 2009 Eighth International Conference on Networks, pg. 453.

Committee (NSTAC) produced several papers that can be mentioned here of note, namely:

- *NSTAC: Cyber Collaboration Report*, NSTAC May 21, 2009.
- *NSTAC Response to the Sixty-Day Cyber Study Group*, NSTAC, March 12, 2009.
- *NSTAC Report to the President on International Communications,* NSTAC, August 16, 2007.
- *NSTAC Report to the President on Emergency Communications and Interoperability,* NSTAC, January 16, 2007.
- *NSTAC Global Infrastructure Resiliency Report,* NSTAC, December 2006.
- *International Collaboration on Cyber Security Research and Development: Leveraging Global Partnerships for the Security of Free Nations and All Sector Preparedness and Response,* NSTAC's Industry Executive Subcommittee's Research and Development Task Force, September 21-22, 2006.

Other notable source documents include:

- *Connecting America: The National Broadband Plan*, the Federal Communications Commission, March 16, 2010.
- *Cyberspace Policy Review*, The White House, May 2009.
- *NSPD 54/HSPD 23* - *The Comprehensive National Cybersecurity Initiative,* The White House, March 2, 2010.
- Asia-Pacific Economic Cooperation (APEC) Submarine Cable Workshop Group reports
- International Cable Protection Committee Recommendations 1 through 12
- Submarine Cable Improvement Group (SCIG) recommendations

Several books on the subject were helpful, including *Blind Man's Bluff* by Sontag, *Breakpoint* by Clarke, *Undersea Fiber Communication Systems* by Chesnoy and

Communications Under the Sea by Finn and Yang. All other books on undersea cables provided historical background, which was great for understanding how today's undersea communication lines closely follow the routes and positions of telegraph lines from yesteryear.

I am also indebted to the WorldCat interlibrary loan for finding me the only inter-library copy of the 2002 *Undersea Cable Report* produced by Terabit Consulting, located in Cambridge, MA. The 942-page report provided detailed facts and figures about all in-service fiber-optic cable lines. Since few lines have been added to U.S. trans-oceanic supply since 2002, the report was a great resource.

All SubTel Forum magazine and Porthcurno Telegraph Museum magazine articles were read and consulted for the project. The DHS Daily Open Source Infrastructure Update Report was also monitored for cable-related articles for the past ten months.

Throughout the past year, a collection of over ten telegraph and fiber-optic cable maps were collected, including the most recent Telegeography world cable map, which is recognized as the seminal map in the field.

Conference Presentations

Papers and PowerPoint presentations were collected from two conferences attended, the Reliability of Global Undersea Communication Cables Infrastructure (ROGUCCI) Summit hosted by the Institute of Electrical and Electronics Engineers (IEEE) in Dubai, U.A.E. and the 2010 Pacific Telecommunications Council (PTC) hosted in Honolulu, Hawaii. The ROGUCCI Summit provided cutting-edge research on vulnerabilities and industry trends, particularly from cable operators; the PTC conference contributed significantly to my knowledge of cable insurance and cable upgrade costs. Both conferences generated enough material for several papers, let alone one.

Previous PTC conference presentations, from 2004 through 2009, were consulted and studied for the project. I also collected all cable-related presentations delivered to the North American Network Operators Group (NANOG) and to three SubOptic conferences (i.e. 2001, 2004 and 2007). The research produced some interesting facts and got me up to speed on many issues.

Interviews and Consultations

Approximately 40 interviews were conducted for this project. Most interviewed discussed matters on background due to the sensitive nature of the subject. Consultations with Douglas Burnett from the International Cable Protection Committee, Nicholas Lordi from Telcordia, Carl Foster from the DHS National Communications System, Alan Maudlin from Telegeography, Hunter Newby from Allied Fiber, Fred Nichols and Bill Gunnels from DoD's Networks Information and Integration office, Pete Guevara from JP Morgan Global Networks, Keith Schofield at Pioneer Consulting and Fiona Beck from Southern Cross Cable Network were most helpful in understanding the cable industry. All interviewed, except one, emphasized that a lack of communication and information sharing exists within the cable industry, between companies and governments alike. All expressed the hope that it would soon change.

BACKGROUND AND SIGNIFICANCE OF UNDERSEA CABLES

> "When communications networks go down, the financial services sector does not grind to a halt, rather it snaps to a halt."[28] -- Stephen Malphrus, Chief of Staff to Chairman of the U.S. Federal Reserve Ben Bernanke, referring to undersea cables at the ROGUCCI conference, Dubai, UAE, October 2009.

Undersea cables are the technology of choice to move large amounts of data around the world quickly. There is no other technology that compares. Cable is cheap, fast and reliable.

Jim Hayes, President of the California-based, Fiber Optic Association notes that "99 percent of the world's long-distance communications travel through fiber links. The remaining 1 percent are… satellite-based, mainly in places like Africa, South America and less developed parts of Asia."[29] Most countries prefer undersea cables to satellites for many reasons. Satellite communication is comparatively too expensive, slow and unreliable. For example, satellites add at least 400 milliseconds to any transmission.[30]

In the world of global network operations, every millisecond counts and an extra 400 adds an eternity. Today, too many missions depend on real-time feeds and pinpoint data to be successful. Satellite latency, coupled with its smaller bandwidth capacity and greater packet loss, just doesn't cut it. In fact, no other technology can single-handedly restore the millions of lost connections cables carry.[31] For these

[28] Stephen Malphrus, "Keynote Address," ROGUCCI conference, Dubai, U.A.E., October 19, 2009.

[29] Declan McCullagh, "NSA Eavesdropping: How it might work," ZDnet.com, February 7, 2006. Accessed at http://news.zdnet.com/2100-1009_22-146683.html

[30] See CISCO systems, "Reliable Signaling System 7 (SS7) Transport Over Satellite Links," White Paper, 2005. Accessed at http://www.cisco.com/en/US/prod/collateral/wireless/wirelssw/ps1862/prod_white_paper0900aecd802e3b77.pdf

[31] Laurie Doyle presentation, slide 39.

reasons, approximately 95% of all United States (U.S.) international internet and phone traffic travel through undersea cables.[32]

Nearly all U.S. government traffic, including sensitive diplomatic and military orders, travels these cables in order to reach officials in the field. Companies use them to transfer trillions of dollars every day. And other companies, many foreign owned, operate most of them.

According to the Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs, "the private sector owns the preponderance of [U.S.] critical infrastructure -- estimates range from 85 percent to 95 percent."[33] For undersea cables, the figure is closer to 100%. Moreover, the budgets of undersea cable companies cannot compare to the budgets of those governments' reliant on them. Therefore, 'when the private sector has to implement more rigorous security systems to be compliant, they'll look at the most cost effective means of doing that…'"[34]

Financial Flows

When these companies and governments lose connectivity, they lose millions of dollars and the confidence of the public. A 2005 article estimate that "…service interruptions of these high-bandwidth underwater fiber optics communications

[32] NSTAC, NSTAC: Cyber Collaboration Report, May 21, 2009. Page 26. Accessed at http://www.ncs.gov/nstac/reports/2009/NSTAC%20CCTF%20Report.pdf

[33] Anne La Lena, "PCII & You," *DCIP News*, November 2009. Accessed at http://policy.defense.gov/sections/policy_offices/hd/assets/downloads/DCIP%20Newsletter_November%202009.pdf

[34] Martha Entwistle, "Market Watch: Critical Infrastructure," *Security Director News*, August 2008. Accessed at http://www.securitydirectornews.com/article/sd200808LPJLXD/Critical%20Infrastructure

systems can result in excess of $1.5 million revenue loss per hour."[35] This estimate deals strictly with the costs for cable operators; it does not deal with the revenue lost for those whose traffic goes down on that cable system. In that respect, as well as the fact the estimate is five years old, it can be considered quite low.

Some of the most important data to traverse these cables is financial. The Society for Worldwide Interbank Financial Telecommunication (SWIFT), which describes itself as "the global provider of secure financial messaging services," uses undersea fiber-optic communications cables to transmit financial between 208 countries.[36] In 2004 alone, nine million messages and approximately $7.4 trillion a day was traded on this network.[37] Today, nearly 15 million messages a day are sent over it. The CLS Bank, which "operates the largest multi-currency cash settlement system," conducts over one million transactions and trades over $4.7 trillion dollars a day on the same undersea cables.[38] With trillions traded daily, a multi-cable outage, especially in a regional financial hub like Taiwan/China/Hong Kong, has enormous ramifications on the trust and soundness of the global financial order.

Taiwan 2006

Such was the case during the 2006 Hengchun earthquake off the coast of Taiwan. After the quake, it took eleven cable repair ships seven weeks to fix all disrupted cables.[39] When millisecond delays lose millions for real-time trading companies, 49

[35] Douglas Burnett, "Submarine Cable Infrastructure Defense Against Terrorists," *Sea Technology Magazine*, July 2005. Accessed at http://findarticles.com/p/articles/mi_qa5367/is_200507/ai_n21376410/pg_2/?tag=content;col1

[36] Address by Stephen Malphrus, ROGUCCI conference

[37] Ibid.

[38] Ibid.

[39] Mick Green, et al. "Submarine Cable Network Security," Presentation to APEC Submarine Cable Workshop Group, September 2009. Accessed at

days is unacceptable. Without a reliable and quick back-up plan in place, communication carriers and end-users jeopardize profit and investor confidence. Even with a pre-arranged plan, the cost differential in service restoration can be huge. In the Hengchun quake case, the cost differential over land was 30 times the cost over water.[40] Additional latency is typically another problem companies' face in these situations too. Satellite back-up, as discussed earlier, is typically not a feasible option.

Secondary Effects

Secondary effects with cable outages are also significant. A recent simulation in Australia proved just how important. An Australian government official involved in the simulation stated that his government soon realized that if one or more cables went down, air traffic controllers wouldn't be able to land planes because they couldn't check who was on them.[41] Even background checks performed on incoming passengers, he said, can be halted in the event of a cable outage. This example is one of many proving cables' significant first, second and even third-order effects.

Resiliency

Because of the consequences, cables are designed to be extremely reliable and resilient. Today's cable systems seek to operate with 99.999% (5-9s) consistency, which equates to a mere five minutes of downtime per year.[42] Companies continue

http://74.125.113.132/search?q=cache:9yxrwo21PBIJ:www.iscpc.org/information/Openly%2520Published%2520Members%2520Area%2520Items/Submarine_Cable_Network_Security.ppt+hengchun+earthquake+eleven+ships+cable&cd=3&hl=en&ct=clnk&gl=us

[40] Mick Green, ICPC Presentation to the ROGUCCI conference, October 19, 2009.

[41] Comments made by Australian official to ROGUCCI conference members, October 22, 2009.

[42] See Laurie Doyle presentation to Pacific Telecommunications Council meeting 2007, accessed at http://www.ptc.org/past_events/my2007/presentations/Satellite%20Submarine%20-

to seek the elusive 99.9999% (6-9s) through mesh networking arrangements. Even when a cable loses service, service can be rerouted on other cables in many cases. This rerouting is good news since a cable breaks, on average, once every three days somewhere around the world.[43] When cables break, they can be fixed by ships within one to two weeks on average.[44] All in all, cables have been one of the most dependable technologies ever created.

Their dependability, most likely, has been the reason governments have not spent too much time worrying about their continuity. But recent breaks within the past decade have changed that feeling. Events like that in Taiwan 2006 and Middle East 2008 prove that multi-cable outages can occur and severely hamper day-to-day operations. At least seven serious outages have occurred in the last seven years and the frequency of these events is becoming more prevalent.

Cables, now more than ever, are an essential critical infrastructure that deserves constant watch and constant protection. They also require physical diversity to avoid tail-end catastrophic losses.

Physical Diversity

Despite the importance of cables, many laypersons would be astonished to learn that all but one U.S. transatlantic cable "land[s] within the same 30-mile radius."[45] Moreover, "most transatlantic traffic shares the same congested waterways, entry

%20Doyle.pdf Also see RNAL (cable system). Accessed at http://en.wikipedia.org/wiki/RNAL_(cable_system)

[43] Ryan Singel, "Cable Cut Fever Grips the Web," *Wired Magazine*, February 6, 2008. Accessed at http://www.wired.com/threatlevel/2008/02/who-cut-the-cab/

[44] Interview with Fiona Beck, CEO of Southern Cross Cable System, January 20, 2010.

[45] David Lloyd, "The Need For Physical Diversity For Submarine Cable Routing," Hibernia Atlantic website. October 2008. Accessed at http://www.hiberniaatlantic.com/documents/DaveysCorner-oct2008.pdf

points and backhaul connecting NYC Metro area."[46] One industry official noted privately that almost all the traffic from New York to London arrives in an 18-inch pipe underneath an unprotected manhole next to 60 Hudson Street in downtown Manhattan. Similar facts can be presented for traffic arriving from the West Coast. In other countries, the problem of physical diversity is likely even worse.

Coastal geography, backhaul costs on land and historical permitting processes are three main reasons cables continue to land in the same places. The first two cannot be changed with policy, but the third can. Legal efforts to streamline permitting at the federal, state and local level would be helpful in diversifying cable landing spots. But undersea cable companies normally do not have the political backing to push for these changes. Policymakers also typically do not have the technical knowledge to recognize the importance of cables. A partnership between policymakers and cable companies can change that, but it must go global to be effective.

Value of Partnership

As the world awaits the next massive undersea cable outage, policymakers can take steps now to reduce the chances of such an event, as well as improve recovery efforts after it happens.

With the rise of internet and telecommunications growth, more and more governments and companies rely on undersea cables. Many of us use undersea communication cables every day too. We call friends abroad or we read newspapers online from worldwide websites. Each time we hit send, our message travels along these cables. Despite the importance of cables, they have vulnerabilities that remain woefully unaddressed by the international community as a whole.

[46] Ibid.

A new international public-private forum would first and foremost be an education and awareness platform. It should champion the cause of undersea cable security in all its forms. Secondly, it should help formalize the non-existent relationship between companies and government. It can formulate a disaster recovery plan among members, and organize and perform operational exercises with key officials to keep it updated and accurate. With this partnership, the U.S. government can lead the world in undersea cable protection and assure its own networks are more resilient and redundant than before.   It may be the only way to ensure the future protection of this critical infrastructure and bring all stakeholders together in the security process.

MOTIVATION FOR CYBERSECURITY PUBLIC-PRIVATE PARTNERSHIPS

The Obama Administration understands the need for public-private partnerships in cyber security. The 60-day Cyber Security Review published in March 2009 mentioned the idea of public-private partnerships no less than 11 times and devoted an entire section on it. It is not the first time the idea of a telecommunications public-private partnership has been mentioned.

Since 1991, NSTAC has recommended that the President create a "a cyber collaboration capability" that can establish "an initial operational capability that allows all appropriate players to share information, establish a baseline understanding of the threats to our Nation's critical infrastructures, and take action to detect, prevent, mitigate, and respond to cyber threats."[47] In this arrangement, companies and governments would work side-by-side. The group would also receive undersea cable outage reports.

In February 2010, David Bodenheimer, a legal cybersecurity specialist, testified to the House Armed Services Committee's Subcommittee on Terrorism, Unconventional Threats and Capabilities that "virtually every top official, cybersecurity expert, and major review has reached the same conclusion – public-private partnerships are vital to any successful cybersecurity strategy."[48] He then provided a concise list of those in favor of public-private partnerships, reproduced for the reader below:

[47] NSTAC, *NSTAC: Cyber Collaboration Report*, May 21, 2009. Page 11. Accessed at http://www.ncs.gov/nstac/reports/2009/NSTAC%20CCTF%20Report.pdf

[48] "Statement to the House Armed Services Committee's Subcommittee on Terrorism, Unconventional Threats and Capabilities," David Bodenheimer, February 10, 2010. http://armedservices.house.gov/pdfs/TUTC022510/Bodenheimer_Testimony022510.pdf

• President Obama. "...we will strengthen the public/private partnerships that are critical to this [cybersecurity] endeavor."[49]

• Senator Rockefeller. "We need a coordinated public-private response. Currently, this does not exist."[50]

• Representative Lipinski. "Improving the security of cyberspace is of the utmost importance and it will take the collective effort of the Federal government, private sector, our scientists and engineers, and every American to succeed." [51]

• DNI Director Blair. "Acting independently, neither the U.S. government nor the private sector can fully control or protect the country's information infrastructure."[52]

• The NSTAC May 2009 report. It stated that "there is an urgent need to improve upon coordination of existing U.S. and international cyber incident capabilities in both public and private sectors. The need for this capability is growing over time."[53]

• CSIS Report. "The U.S. government should rebuild the public- private partnership on cybersecurity to focus on key infrastructures and coordinated preventive and responsive activities."[54]

[49] "Remarks by the President on Securing Our Nation's Cyber Infrastructure," The White House Office of the Press Secretary (May 29, 2009).

[50] Cybersecurity: Assessing Our Vulnerabilities and Developing an Effective Response: Hearings Before Senate Comm. on Commerce, Science, and Transportation, 111th Cong., p. 2 (Mar. 19, 2009) (statement of Sen. Rockefeller).

[51] "Subcommittee Chairman Lipinski's Floor Speech on H.R. 4061," House Subcomm. on Science and Technology (Feb. 3, 2010) (http://science.house.gov/press/PRArticle.aspx?NewsID=2736).

[52] Blair, "Director of National Intelligence's Annual Threat Assessment," Government Info Security (Feb. 2, 2010) (http://www.govinfosecurity.com/articles.php?art_id=2154&rf=011610eg)

[53] Ibid.

•Industry. "[G]overnment and industry must develop a much more thoughtful, fundamental and contemporary relationship to address their mutual (not just government's) cyber security needs."[55]

• Experts Generally. "The key strategy improvements identified by cybersecurity experts [include]: . . . Bolster public-private partnerships through an improved value proposition and use of incentives."[56]

Momentum for an Undersea Public-Private Partnership

More specifically, a few organizations have sought the creation an undersea cable public-private partnership. Most studying the issue recognize that cable operators and government officials in many countries have a poor record of working together during undersea cable crises. They have an even poorer record of communicating before a crisis or after to implement lessons learned and best practices. No coordinated, public effort exists within the U.S. or elsewhere to address undersea cable security. Below are a few organizations that have sought a partnership:

- In the 2005, the Heritage Foundation issued a report stating that "… no organization [is] tasked with monitoring the global cable network to determine if it is the target of a concerted attack. Cable companies monitor their own cables and work with each other to repair outages quickly, but they provide no feedback to governments. For the overall system, it seems unlikely that governments would even be aware that an attack is occurring until well after the event."[57]

[54] CSIS Commission Report, p. 6 (Dec. 2008).

[55] Internet Security Alliance, "The Cyber Security Social Contract Policy Recommendations for the Obama Administration and 111th Congress," p. 3 (2008).

[56] GAO, "Cybersecurity: Continued Efforts Are Needed to Protect Information Systems from Evolving Threats," p. 15 (GAO-10-230T) (Nov. 17, 2009).

[57] James Carafano et al. Heritage Foundation report, 2005. Page 13.

- In 2009, NSTAC stated “adequate cyber defense could only occur through international cooperation,” and that its 2006 Global Infrastructure Resiliency Report discusses the “restoration of [undersea cable] infrastructure requires international cooperation.”[58]

- In 2009, Telcordia released a report stating that “The time is right for a multi-national, cross-industry forum comprised of the undersea cable infrastructure community, major enterprise customers, ISPs, and data hosting centers that monitor their global infrastructure to develop models for global infrastructure resiliency.” [59]

[58] NSTAC Cybersecruity Collaboration Report

[59] Spilios Makris, “'Undersea Cable System Outages and Global Infrastructure Resiliency – A Discussion of Issues in Managing Third-Party Expectations,” Presentation delivered to IEEE. Slide 24. Accessed at http://www.ieee-cqr.org/2009/FINAL%20UPLOAD/DAY%203%20-%20THR/SPILIOS%20MAKRIS%20-%20Lordi_CQR2009_final.pdf

THE ROLE OF THE DEPARTMENT OF HOMELAND SECURITY

The Department of Homeland Security (DHS) has the statutory authority to create the partnership to better ensure cable connectivity worldwide. Under the recently declassified National Security Presidential Directive (NSPD) 54/Homeland Security Presidential Directive (HSPD) 23 *Comprehensive National Cybersecurity Initiative*, DHS is given authority to execute Initiative 12, which defines "the Federal role for extending cybersecurity into critical infrastructure domain."[60]

Under HSPD 5 and 7, as well as Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, DHS is to direct the National Communications System and provide for the security of telecommunications critical infrastructure sector. DHS oversees the President's National Security Telecommunications Advisory Committee (NSTAC), the National Cybersecurity Center, the National Communication System and the NCS' National Coordinating Center (NCC). The Deputy Under Secretary for National Protection and Programs Directorate is also the Director of the National Cybersecurity Center within DHS and the NCS. Within the NCS' NCC, Information Sharing Analysis Centers (ISACs) exist for Information Technology and Communication, respectively. These two ISACs have authority to evaluate the security of undersea cables in one form or another.

NCS and DHS Sector Coordinating Councils

The National Communications Service (NCS), now under DHS, serves to provide resilient and redundant communication in times of emergency. NCS provides

[60] NSPD 54/HSPD 23 - *The Comprehensive National Cybersecurity Initiative,* The White House, March 2, 2010. Accessed at http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

certain users with the Government Emergency Telecommunication Service (GETS) and the Telecommunication Service Priority (TSP) programs. These services provide customers priority status in making telephone calls, particularly in times of emergencies when communication towers are likely to suffer outages.

To increase communication between cable companies and government officials, NSTAC recommends the development of public-private partnerships in this realm. The Presidential group discussed undersea cable cuts in its 2006 Global Infrastructure Resiliency Report and in follow-on documents.[61] It applauded the effort to create the IT and Communication Sector and Government Coordinating Councils within DHS to address the lack of a public-private forum. Yet the report calls for more communication, not just domestically.[62]

Moreover, DHS is charged with conducting "bilateral discussions with close allies and others to further international cyber security awareness"[63] and leads the inter-agency "Team Telecom" group that assesses undersea cable permits and licenses.[64]

DHS and "Team Telecom"

DHS leads the "Team Telecom" process. "Team Telecom" studies undersea cable landing license applications for national security purposes, particularly to ensure that foreign ownership of telecom companies does not provide other governments'

[61] NSTAC, *NSTAC: Cyber Collaboration Report*, May 21, 2009. Page 26. Accessed at http://www.ncs.gov/nstac/reports/2009/NSTAC%20CCTF%20Report.pdf

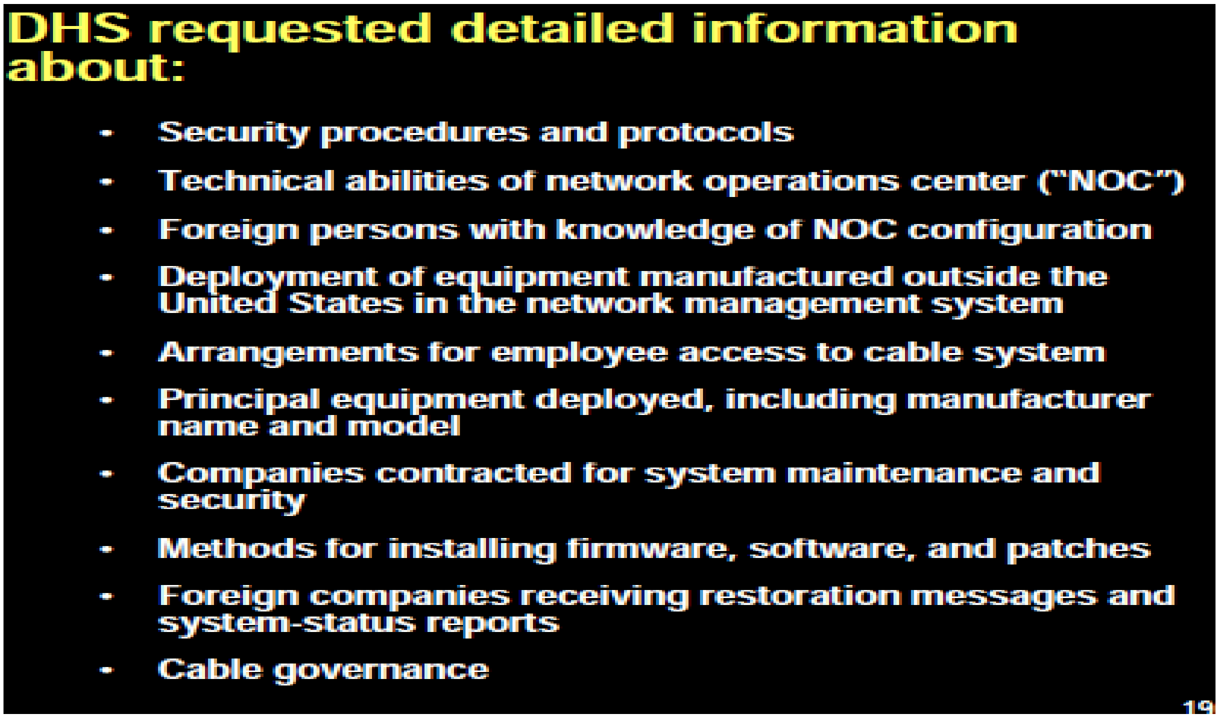
[62] Ibid., page 30.

[63] *NSTAC Report to the President on International Communications,* NSTAC, August 16, 2007. Page D-5. Accessed at http://www.ncs.gov/nstac/reports/2007/NSTAC%20International%20Report.pdf

[64] Kent Bressie, "More Unwritten Rules: Developments in U.S. National Security Regulation of Undersea Cable Systems," Presentation to the 2009 PTC conference, January 18, 2009. Slide 7. Accessed at http://www.harriswiltshire.com/siteFiles/News/7DF1C8D035660E8FBEF0AAC7BA8DA103.pdf

access to U.S. national security information.[65] Team Telecom is comprised of officials from the Departments of Defense, State, Justice, Homeland Security, Central Intelligence Agency, National Security Agency and the Office of the Director of National Intelligence.[66]

In 2008, DHS, the FCC and the Office of Science and Technology Policy in the White House (OSTP), asked all undersea cable companies doing business in the United States to submit detailed information about their systems.[67] DHS voluntary asks for these items below:[68]



DHS requested detailed information about:

- Security procedures and protocols
- Technical abilities of network operations center ("NOC")
- Foreign persons with knowledge of NOC configuration
- Deployment of equipment manufactured outside the United States in the network management system
- Arrangements for employee access to cable system
- Principal equipment deployed, including manufacturer name and model
- Companies contracted for system maintenance and security
- Methods for installing firmware, software, and patches
- Foreign companies receiving restoration messages and system-status reports
- Cable governance

19

Source: Kent Bressie, presentation to PTC conference, 2009. Slide 19.

[65] Ibid.

[66] Kent Bressie, "New Barriers to U.S. Market Entry for Undersea Cable Operators: Recent Developments with 'Team Telecom'," Presentation to the 2008 PTC conference, January 13, 2008. Accessed at www.ptc.org/ptc08/participants/speakers/papers/BressieFinalSlides.pdf

[67] Information collected from Bressie, PTC presentation, 2009.

[68] Ibid.

With DHS heavy involvement in cybersecurity affairs, the Under Secretary for National Protection and Programs Directorate can best lead the charge to develop an international undersea cable partnership.

But what issues should the partnership tackle?

In this paper, a framework is used to identify current issues affecting cable reliability, redundancy and security. Ratings are given and recommendations are made to decrease high scoring issues. A discussion of the Larson framework and its use in the paper follows below.

THE LARSON FRAMEWORK

The Larson Framework was developed by Colonel Randell Larson, USAF (Ret) in a 2007 book.[69] He is currently the Director of The Institute for Homeland Security and the National Security Advisor to the Center for Biosecurity, University of Pittsburgh Medical Center. He also was the first in the nation to design a graduate course on homeland security.

His framework encompasses a Danger Index equation, which involves four variables and blends MITRE Corporation's of risk with Yacov Haimes' definition of risk.[70] The equation is defined as:

DANGER = INTENTION X CAPABILITY X VULNERABILITY X CONSEQUENCE

The Danger term is also equivalent to both definitions of risk and can take values between [0, 10000]. In the equation, all other variables have a range of [0, 10].

The four variables listed in the equation are assessed under certain criteria.

[69] Larson, 2007. Page 68,

[70] Snow, Hoag and Weckman, "Understanding danger to critical telecom infrastructure: a risky business," IEEE Computer Society: 2009 Eighth International Conference on Networks, pg. 451.

FRAMEWORK CRITERIA[71]

Consequence	• Size of outage • Duration of outage • Economic Impact
Vulnerability	• Weakness or a state of susceptibility which opens the infrastructure to a possible outage due to attack or circumstance • Adherence to design, operations, and maintenance best practices
Intention	• Benign intention (installation, operations and maintenance) • Malicious intention (intentional, high value of target)
Capability	• Skill of exploiting or triggering personnel (could be detrimental in two situations – low skill for benign intention and high skill for malicious intention) • Knowledge of vulnerability • Devices to exploit or trigger vulnerability into a disruptive event.

Andrew Snow, John Hoag and Gary Weckman showed that the equation can be applied to the telecommunication infrastructure.[72] In their paper, they apply the criteria above to evaluate the danger from a fault in a wired cable SONET ring (see Appendix B for cable topologies). Their table and comments are reproduced below:

[71] Ibid. See Page 452.

[72] Ibid. Page 452.

Snow, Hoag and Weckman analysis of SONET Fault Ring, 2008[73]

	SONET Ring 32	Comments
Consequence	9	270,000 users
Vulnerability	2	Fault tolerant ring. Outage requires (1) two fiber cuts, (2) one fiber cut and node failure, or (3) two node failures. Requires food operation and maintenance to replace/repair if ring goes to protect mode.
Intention	4	Value of target moderate to high for terrorist, vandals or theif's might mistake for copper
Capability	2	Hard to locate fiber, nodes in buildings
Danger Index	144	1.4% normalized to 100%

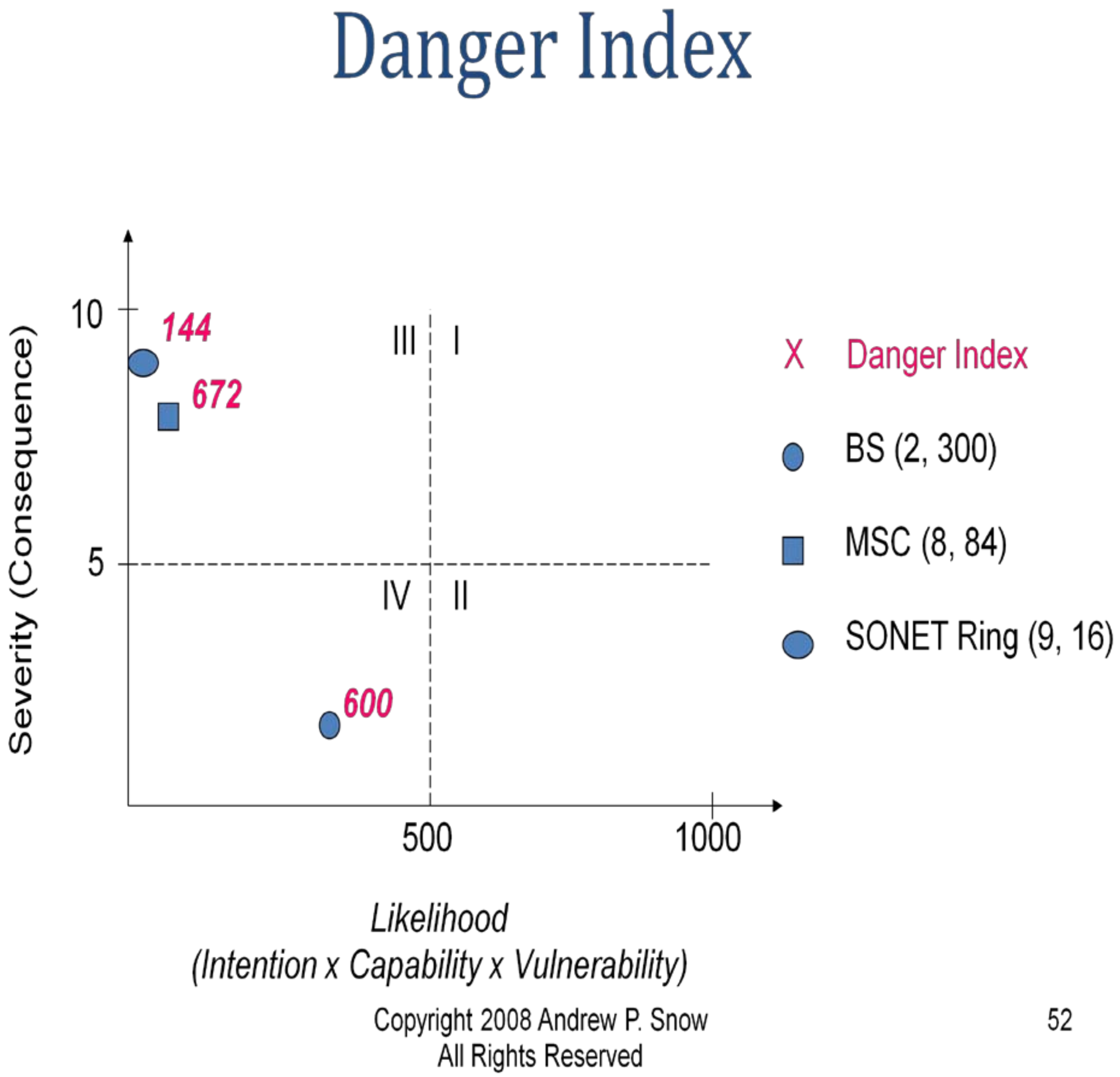
Here, the consequence of an attack on a SONET ring is among the highest found, yet the danger is low due to low scores for vulnerability, capability and intention.

SONET rings exist in undersea communication cable networks, as well, and can be evaluated using the same framework. Yet, the more important topic for an undersea cable partnership is the overall threat to the entire international architecture.[74]

[73] Ibid.

[74] Describing the undersea cable architecture as a complete, entire system has been labeled as incorrect by some. Robert Work notes: "The global undersea cable infrastructure is a balkanized conglomeration of point-to-point connections and self-healing loop networks operated by large telecommunications consortia and a smaller number of financially-distressed private carriers. There is no single entity responsible for continuity of global cable service; international carriers enter into cooperative service agreements with other carriers to provide backup for their own network services. Any use of the terms *global network* or *global system* to describe the world-wide submarine cable infrastructure is thus misleading." Robert Work, "The Undersea Telecommunications Infrastructure: A Global Net Assessment," unpublished paper, p. i. Accessed at http://www.csbaonline.org/4Publications/Archive/R.20051024.QDR06/R.20051024.QDR06.pdf Page 71-72.

In a related presentation, Snow and Weckman show the danger existing in other architectures.[75] Their graph is reproduced here:



Danger Index

Copyright 2008 Andrew P. Snow
All Rights Reserved

52

KEY: *BS = Personal Communications System (PCS) Base Station; MSC = PCS Mobile Switching Center*

[75] See Drs. Andy Snow[1] and Gary Weckman, "Tutorial: Protecting Critical Telecommunications and Networking Infrastructure," The Seventh International Conference on Networking ICN 2008. Slide 52.

Research collected herein shows that the danger to the international undersea cable architecture, as a whole, is much higher than other architectures studied. The undersea cable architecture falls into Quadrant III but at a much higher overall rating. The ratings associated with the vulnerability, capability and intention terms are higher, pushing the danger index to a high level. To be consistent in evaluating the terms in the equation, I will use the framework criteria provided in the Snow, et. al. article.

CONSEQUENCE

Background: The consequences from a cable break can be enormous in places that rely on only one cable. However, most countries have at least two cable systems connected together in the form of a ring (See Appendix B on cable topologies). The ring topology network means that if one cable is out, the second cable takes on the additional capacity using spare bandwidth. When two or more cables are out, countries and/or cable systems can be in trouble. Nowadays, more and more companies are switching to mesh networking, which allows for two or more landing sites to each be connected to two or more cables. However, not all countries and cable companies have created a mesh network. It is likely that not every U.S. government agency has a mesh network for all its priority services as well.

The Snow, et. al. study uses size of outage, duration of outage and economic impact to assess the consequence variable. Important facts to consider for this term are as follows:

- 99% of the international data and phone connectivity relies on cables.
- 95% of U.S. international data and phone traffic travels over cables.
- The U.S. Department of Defense lost 60% of its commercial and military connectivity in the December 2008 breaks. U.S. UAV flights diminished from in the hundreds to into the tens during the cable breaks.
- The SWIFT network, the CLS bank and NYSE Euronext use cables for international-real-time trading. Millisecond delays can impact day-traders from making millions in profit.
- In the past five years, countries like India, Pakistan, Egypt, Vietnam, Maldives, Qatar, Taiwan and several in West Africa have lost over 80% capacity in one or more instances.

Below is a table that analyzes nine significant cable outages over the past seven years. Approximately 85 newsworthy cable breaks have occurred since 1999[76]; the ones highlighted are just the most notable from my research. All information has been pulled from research collected and inserted into Appendix D; references and background information on each break is in that section.

[76] Nick Lordi, Spilios Makris, and Melvin Linnell, Analysis of Newsworthy Undersea Cable Infrastructure Outages (1999 – 2009), Telcordia Technologies, Inc. Presentation made to ROGUCCI Summit, Dubai, October, 2009.

SIGNIFICANT CABLE BREAKS SINCE 2003[77]

DATE	LOCATION	CAUSE	# OF CABLES	AFFECTED	DURATION (# of days)	ECONOMIC LOSS
May 21, 2003	NEAR ALGERIA	Earthquake	5 cables	Unknown	45 days	Unknown
June 27, 2005	PAKISTAN	Fishing Trawler	1 Cable	Pakistan = 100% loss initially; 50% of internet users and 80% of phone users lost int'l service	11 days	Millions of dollars, including $10-$20 million in investment losses
December 26, 2006	NEAR TAIWAN	Earthquake	9 cables and 21 faults	Taiwan = Int'l calling to U.S. down 60% and to surrounding countries 98%; internet access significantly impaired to/from China, Hong Kong, Vietnam, Taiwan, Singapore, Japan, Phillippines	49 days	Most likely, millions; South Korean currency trading halted; trade and online stock prices significantly disrupted
November 2007	BANGLADESH	Intentional sabotage	1 cable; two cuts	Bangladesh = 100% int'l communications lost	At least one week	Bangladesh Telegraph and Telephone Board lost $1.05 million in revenue
January 23-February 4, 2008	NEAR EGYPT	Ship anchors	5 cables in 4 locations	2500 networks; India = 60 million users lost, Pakistan = 12 million lost, Egypt = 6 million lost and Saudi Arabia = 4.7 million lost	At least 14 days	Unknown, but India's call center/ outsourcing industry decreased connectivity by upwards of 60%
December 19, 2008	EGYPT AND ITALY	Ship anchors	3 cables	Lost service: Maldives = 100% India = 82% Qatar = 73% Djibouti = 71% UAE = 68% Zambia = 62% U.S. military Egypt = 52% Pakistan = 51%	Unknown	Unknown

[77] All information presented herein was collected from sources footnoted in Appendix D. See that section for further referencing.

DATE	LOCATION	CAUSE	# OF CABLES	AFFECTED	DURATION (# of days)	ECONOMIC LOSS
April 4, 2009	UNITED STATES (CALIFORNIA)	Intentional sabotage	10 cables in 3 locations	1.5 million services lost in California, including ATM and credit card processing; 52,000 Verizon landlines lost service; wireless, Internet, phone and emergency service lost	12 hours	Unknown but significant
July 30, 2009	NEAR NIGERIA	Unknown	1 cable	Benin, Togo, Niger = 100% loss;[78] Nigeria = 70% bandwidth loss	Several days	In Nigeria, banking, government and mobile phone networks nearly or all down
August 12, 2009	NEAR TAIWAN	Typhoon, earthquake	10 cables in 20 locations	Qatar and Singapore = major disruptions; Indonesia, Philippines, South Korean and Japan = significant disruptions	At least 14 days	Unknown, but minimal in Taiwan

[78] "More Never Agains IV," The Availability Digest, February 2010 http://www.availabilitydigest.com/public_articles/0502/more_never_agains_4.pdf

Theft of expensive undersea fiber-optic communications cable can also create serious consequences. Below is a chart of recent cable thefts around the world and their associated impact.

RECENT UNDERSEA COMMUNICATION CABLE THEFTS

DATE	LOCATION	AMOUNT STOLEN	AFFECTED	ECONOMIC LOSS	AFTERMATH
August 2006 – March 2007	VIETNAM	500 Kilometers	82% of voice/data traffic lost; internet delays for up to 3 months after thefts	$5.8 million to restore cable loss	Prime Minister begins public awareness campaign of cable significance; Vietnam's socio-economic, national security and prestige significantly diminished
2008	JAMAICA	Unknown; in one case, thieves stole cable at one end while it was being replaced at the other	Unknown	Cable and Wireless Jamaica lost $1.5 million	Cable and Wireless offering $15,000 reward for arrest of cable thieves
2008	South Africa	Unknown	Unknown	Over $100 million each year	Unknown

Clearly, the consequences of a significant undersea cable break or cable theft is very, very high. Based on the data above, it is at least a 9 on a 10 point scale.

RATING:

Consequence	**Receives a 9 out 10**	**Comment: Size, duration and economic costs of outages were very high in most cases. An advanced industrialized country would suffer incredibly from such losses. Almost all the world's internet and voice traffic travels over cables. Satellite typically can only pick up between 5-10% of traffic maximum.**

VULNERABILITY

The factors determining the vulnerability variable are provided on the left hand side of the below charts. The scores of these factors are averaged at the end of the section to provide a quantitative score to the qualitative variable of vulnerability.

Weakness and Susceptibility	Factors Increasing Score	Factors Decreasing Score
U.S. CABLE ROUTE DIVERSITY	All but one U.S. transatlantic cable "land[s] within the same 30-mile radius"[79] on the East Coast of the U.S.	More carriers, Verizon, Comcast, switching to mesh networking to avoid route homogeneity
	"Most transatlantic traffic shares the same congested waterways, entry points and backhaul connecting NYC Metro area."[80]	Oversupply of bandwidth on both trans-Pacific and trans-Atlantic routes for the next four years; thus if multi-cables drop, other cables can pick up dropped capacity.
	Backhaul vulnerability: One industry official noted privately that almost all the traffic from New York to London arrives in an 18-inch pipe underneath an unprotected manhole next to 60 Hudson Street in downtown Manhattan.	
	The situation is similar for trans-Pacific cables, which funnel into the carrier hotel building at One Wilshire Boulevard, Los Angeles, California.	
U.S. Route Diversity Rating = 8 out of 10 **REASON: Mesh networking decreases threat, but the vulnerability on the East Coast and near East Coast carrier hotels remains quite high.**		

[79] David Lloyd, "The Need For Physical Diversity For Submarine Cable Routing," Hibernia Atlantic website. October 2008. Accessed at http://www.hiberniaatlantic.com/documents/DaveysCorner-oct2008.pdf

[80] Ibid.

Weakness and Susceptibility	Factors Increasing Rating	Factors Decreasing Rating
WORLDWIDE CABLE ROUTE DIVERSITY	31° 11.738' N, 29° 54.108'E - These coordinates identify the "intersection between El Horreya and El Nabi Streets" Alexandria, Egypt.[81] This location is a "center of the fiber world." In this building, five cables, "FLAG, SEA-ME-WE 1, 2, and 3, AFRICA-1 all converge."[82] It is the "single cross-connect for all cable between Africa, Europe and Asia."[83] At least 80% of all European to Middle Eastern connectivity passes through this building.	
	Other bottlenecks exist in the Mediterranean Sea, India, Hawaii and Guam.[84]	
	Many countries do not have funds to support multiple cable landing stations or routes.	
	Lack of investment necessary to create redundant lines in multiple locations.	
Worldwide Route Diversity Rating = 8 out of 10 **REASON: 80% of international connectivity for three continents passes through one building. The vulnerability rating is high to reflect that fact. Single points of failure at this level are also beyond acceptable.**		

[81] Hank Nussbacher, "Undersea Cables: Jan 20 IDC" IDC Seminar presentation, January 20, 2004. Accessed at http://www.interall.co.il/presentations/undersea-2004.pdf

[82] Ibid.

[83] Ibid.

[84] D. Dominey-Howes and J. Goff, "Hanging on the line," Natural Hazards Earth Systems Science, 9, 2009. Page 607. Accessed at www.nat-hazards-earth-syst-sci.net/9/605/2009/

Weakness and Susceptibility	Factors Increasing Score	Factors Decreasing Score
PHYSICAL SECURITY OF STATIONS AND WET CABLES	The building in Alexandria, Egypt has considerable deficiencies. According to a 2004 presentation, the building was "built on the ruins of the Great Library of Alexandria…in 1933 by British to house [Postal Telephone and Telegraph]."[85] It is fairly dilapidated, containing at least one "wrought iron elevator and broken windows."[86] The old telegraph stations, like those found in Egypt, need to be completely revamped since so much of today's society relies upon their operational success.	Since 9/11, federal funding has been allocated to states to increase cable landing station security. It is unclear what the result has been.
	The UK's Centre for Protected Infrastructure noted in a 2006 report that cable landing stations "are relatively poor in terms of physical security. In a number of cases (for example Land's End) the car park is uncontrolled and immediately adjacent to the building – an obvious risk. Access to manned buildings is via a traditional front door backed up with CCTV camera although the security achieved at that level depends on processes and how the station staff handles unexpected visitors."[87]	The ICPC recommends instituting air or sea patrols of cable routes in cases where a cable protection zone has not been implemented. The patrols are meant to ward off threats to cables from other ships, fishing trawlers and dredgers.
	The report goes further, noting that "inside the building, any amount of damage could be inflicted by electronic or physical means, for example any of the 'electronic attack' scenarios below could be achieved using the local PCs and control systems. A less technical attack could directly cripple the batteries or power supplies, or just	

[85] Ibid.

[86] Ibid.

[87] *An Overview of the Use of Submarine Cable Technology by UK PLC*, Centre for the Protection of National Infrastructure, March 2006. Accessed at http://www.cpni.gov.uk/Docs/Submarine-cables.pdf

Weakness and Susceptibility	Factors Increasing Score	Factors Decreasing Score
	swinging an axe in the equipment rooms could easily stop traffic using no technical knowledge at all."[88]	
	In the U.S., many cable landing stations are located in well-trafficked areas and contain minimal security measures around its perimeter.	
	Most cable companies in the U.S. and abroad do not invest, nor have the money to invest, in cable landing security. Very few governments make the security of these stations a priority enough to provide this type of funding as well.	

Physical Security Rating = 8 out of 10

REASON: Little good news was found to offset the said vulnerabilities of cable landing station security. Most interviewed in this report stated the relative ease in disrupting the physical security of landing stations.

[88] Ibid.

Weakness and Susceptibility	Factors Increasing Rating	Factors Decreasing Rating
MULTIPLE CROSSINGS	59.58.93°N, 009.25.47°W[89] - The publicly available Kingfisher cable maps website lists this exact coordinates of major cable crossing. For instance, at this point, the Atlantic-Crossing 1 (AC1) and TAT-14 cables cross in international waters in the North Sea, not too far above Scotland.[90]	Multiple crossings, generally, are difficult to locate on publicly available websites.
	Another important fact to note is that cables rarely run in a straight parallel line to one another. In fact, cables tend to cross one another all the time. Moreover, some triple-crossings do exist, mainly in place closer to a shoreline as the cables funnel into a particular landing station.[91]	Most websites, other than Kingfisher, have been removed from the Internet and do not appear on the Internet's Wayback Time Machine.
	The International Cable Protection Committee recommends providing exact coordinate route position lists of all cables to ship/boat owners at their request. They do so to avoid inadvertent cuts. However, this recommendation provides an easy way for seafarers to conduct malicious activity.	

Multiple Crossings Rating = 7 out of 10

REASON: Route position sites now require ship documentation in order to receive route position lists. Yet this information does not receive more protection than that. Some multiple crossings can still be located on public websites.

[89] TAT-14-Segment K-North Western Approaches, Cable Awareness Chart, Kingfisher Charts. Accessed at www.kisca.org.uk.

[90] Ibid.

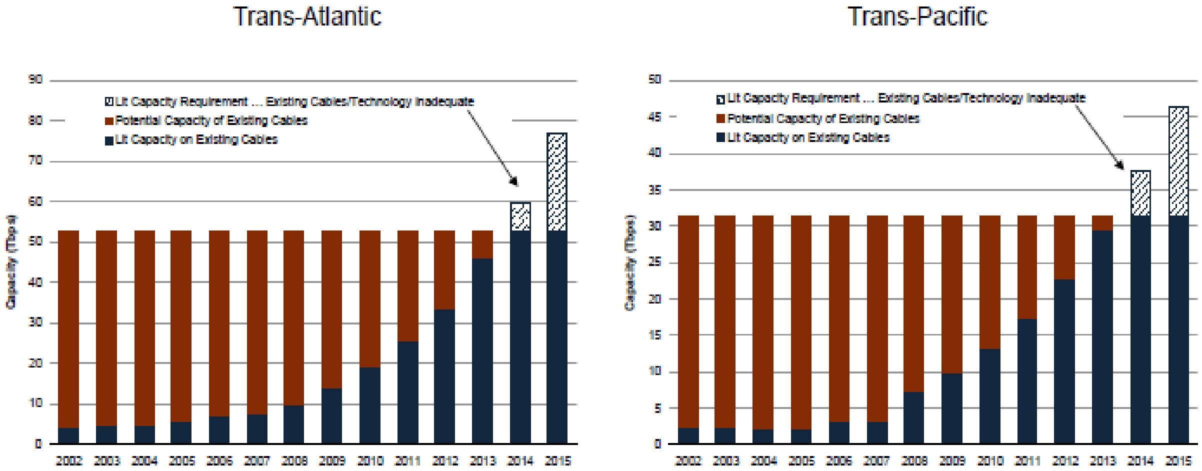
[91] R.Hoshina and J.Featherstone, "Improvements in submarine cable system protection," Submarine Cable Improvement Group. Accessed at http://www.scig.net/section10e.pdf

Weakness and Susceptibility	Factors Increasing Rating	Factors Decreasing Rating
FUTURE CAPACITY	A summer 2009 report published by industry consultants, Telegeography, Inc., shows that trans-Atlantic bandwidth may dry up by 2014. Bandwidth projections show a 33% cumulative annual growth rate (CAGR) every year over the next five years.[92] Currently, over 10 terabits per second flow over transatlantic cables, but that could reach near 53 terabits per second and max out cable capacity by 2014. Unless current cable systems upgrade their 10 gigabit per second technology to 40 gigabit or replace old cables, the system will not be able to deal with the rise in relative yearly rise in traffic demand.	Telegeography analysts have assured industry leaders that capacity will be added to existing routes or new cables will be laid.
	40G transmission signals need to be more accurate to function and can be prone to more signal errors.	The technology has recently been proven to work on long cable lines. Now it needs further fine-tuning to be placed on all long-haul systems.
	Upgrades to 40G for cable systems can cost cable operators 10-20% of the total cost of a system[93] (the equivalent of a $50-100 million investment in some systems).	
Future Capacity Rating = 5 out of 10 **REASON: Despite assurances, cable upgrades are not certain, especially given the costs. Cable companies will seek to avoid operating at cost in the future and may shy away from this investment.**		

[92] Stephen Beckert, "Trans-Atlantic bandwidth – the hangover lingers," Telegeography *Comms Update*. June 22, 2009. Accessed at http://www.telegeography.com/cu/article.php?article_id=28963

[93] Fiona Beck, "View from the CEO's chair," Presentation to PTC 2010 conference, January 16, 2010.

Most recent bandwidth projections from Telegeography below:[94]



Source: Stephen Beckert, "TeleGeography International Telecom Trends Seminar," Presentation to PTC 2010 conference, January 17, 2010. Slide 24.

Weakness and Susceptibility	Factors Increasing Rating	Factors Decreasing Rating
CABLE LAYING IN FAULT-PRONE ZONES	Historical precedent: Earthquakes around Algeria (2003), Taiwan (2006) and Taiwan (2009) caused multi-cable outages.	Cables in these regions are most likely laid with rock/double-armor
	A 2009 report recently proved that an earthquake of magnitude 6.2 or greater would break cables at certain depths around the Luzon Strait, near Taiwan.[95] The cable examined, SEA-ME-WE-3, is similar to others placed elsewhere. In the trans-Atlantic, cables cross the Mid-Atlantic ridge, which is prone to 6.0+ earthquakes - the latest coming just three weeks ago.	Seismologists and geologists typically determine work with other team members for cable operators to find the safest/best route positions available.

[94] Stephen Beckert, "TeleGeography International Telecom Trends Seminar," Presentation to PTC 2010 conference, January 17, 2010.

[95] Liu Aiwen, "Response analysis of a submarine cable under fault movement," Earthquake Engineering and Engineering Vibration (2009) 8:159-164. March 2009. Accessed at http://www.springerlink.com/content/k80726225p754328/fulltext.pdf

Weakness and Susceptibility	Factors Increasing Rating	Factors Decreasing Rating
	It is unknown if Hawaii's short geological history makes cables susceptible to geohazards. Other natural hazards areas near cables are common, "earthquakes at the Cascadia margin and Hellenic Arc, volcanic eruptions in Indonesia, and hurricanes in the Caribbean."[96]	
Cables on Faults Rating = 4 out of 10 **REASON: Recent research by Aiwen is cause for concern, but not enough to assign a higher rating. Geologists and seismologists are intricately involved in determining cable positions.**		

Weakness and Susceptibility	Factors Increasing Rating	Factors Decreasing Rating
ADHERENCE TO BEST PRACTICES	Unclear as to how best practices internationally, as well as domestically, are implemented, if at all.	12 recommendations/best practices are given out by the International Cable Protection Committee.
	Due to the expense of cables, operators sometimes run cables at or marginally above the cost of these systems, placing downward pressure on cost control and adherence to best practices in the process.	In the U.S., the Network Reliability and interoperability Council provides a public list of over 730 best practices for both cable and wireline operators, providers, personnel, etc.
Best Practices Rating = 2 out of 10 **REASON: Cost control does place pressure on cable companies to implement only recommendations that are absolutely necessary; however, little data is found on their implementation.**		

[96] D. Dominey-Howes and J. Goff, Natural Hazards Earth Systems Science, Page 607.

VULNERABILITY CALCULATION

VULNERABILITY = Average (U.S. CABLE ROUTE DIVERSITY, WORLD CABLE ROUTE DIVERSITY, PHYSICAL SECURITY OF CABLES/LANDING STATIONS, MULTIPLE CROSSINGS, FUTURE CAPACITY, CABLE IN FAULT PRONE ZONES, ADHERENCE TO BEST PRACTICES)

VULNERABILITY = (8 + 8 + 8 + 7 + 5 + 4 + 2) / 7

VULNERABILITY = 6

Vulnerability	**6 out of 10**	**Comment: Identified lack of route diversity, as well as specified cable threats, pushed rating higher.**

INTENTION

INTENTION	Factors Increasing Rating	Factors Decreasing Rating
MALICIOUS	CABLE TERRORISM: The CPNI in the U.K. is "aware of a case in Spain where a system was badly damaged by a bomb planted in the terminal station."[97]	No state or non-state actor has declared its intention to purposefully harm cables or cable landing stations.
	5 of twelve profiled major breaks were caused intentionally through sabotage or theft; Bangladesh (man-made cuts), Vietnam (theft and sabotage), Jamaica (theft), South Africa (theft), California (man-made cuts)	UNCLOS ratification increases states' abilities to protect cables and dole out penalties for malicious acts.
	Numerous efforts in past to commit cable espionage, most notably Operation Ivy Bells. The U.S. Navy operation successfully spied on Soviet cables for almost ten years in the '70s.	Australia and New Zealand are among the first to create cable corridors that shield cables a mile on each side from ship traffic.
	Non-state actors seek to disrupt U.S. economy and military operations so cables would be high on their list	
	Poor legal regime preventing malicious actors; most countries' cable laws stem from the 1884 Submarine Cable Convention	
	Many cable landing facilities and/or carrier hotels exist close to street traffic with little or no security; car bomb at these sites can significantly halt undersea cable traffic.	
	Elimination of communication networks becomes states' first priority in conventional conflict; U.S. cut cables during 1898 Spanish-American War; Germans and British did the same in World War I.	

Malicious Rating = 6 out of 10

REASON: Unspoken international norm that cables are extremely important to global operations and would be targeted in any military conflict or espionage planning

[97] Ibid.

INTENTION	Factors Increasing Rating	Factors Decreasing Rating
BENIGN	Fleet of cable repair ships continue to age	Very few problems discovered regarding installation, operations and maintenance
	Quantities of spare cable are not uniformly determined; varies by cable system	Cable companies are known to be very conservative before making any changes that might affect the system. Reliability is the prize owners seek
Benign Rating = 2 out of 10 **REASON: Cables typically do not suffer outages from benign causes**		

INTENTION CALCULATION

INTENTION = AVERAGE (BENIGN AND MALICIOUS)

INTENTION = (6 + 2) / 2

INTENTION = 4

Intention	**Receives a 4 out 10**	**Comment: Some malicious precedent and threats exist, but not enough to justify high rating**

CAPABILITY

CAPABILITY	Factors Increasing Rating	Factors Decreasing Rating
Skill for Exploitation	Low level of skill to cut cables. Cables can be cut by anchors, fishing trawlers and clam dredgers. All those vessels can be operated by many, many people throughout the world. An “inadvertent” anchor cut at a cable crossing point, such as the one mentioned in the vulnerability section, would take out one-half of two major rings. This cut would take at least 7 days to repair, maybe up to 21 days since it would be a multiple cable fix. It would also leave the other section of the ring highly vulnerable. If a coordinated cut did follow, the attack would eliminate 820 Gigabytes-per-seconds of service, nearly 1/8 of all trans-Atlantic communication.	Within 2000 meters of coastline, the ICPC recommends that cables be buried at least 1.5 meters below the ocean floor to ward against inadvertent human activity.
	Illiterate Vietnamese fishermen were able to pull up cable in numerous locations and steal giant pieces.	Remote operating vehicles (ROVs), as well as cable splicing ships, are difficult to operate. Both are best at catching cable lying on the seabed.
	If cable is caught, very little skill is needed to break or bend the line beyond its radius and stop service	Cables move often on the seafloor making it difficult to find cable even with coordinates in some cases.

Skill for Exploitation Rating = 6 out of 10

REASON: Growing proliferation of pirated ships, ROVs, as well as fishing/clam boats in cable zones can disrupt cables. Not much skill is needed in these vessels is needed to disrupt cables other than lowering an anchor or a trawler in most cases.

CAPABILITY	Factors Increasing Rating	Factors Decreasing Rating
Knowledge of Vulnerability	All the data collected on vulnerabilities pulled from publicly available sources. Much data exists for non-governmental and non-industry groups to readily collect.	Most of the information on this topic is classified or confidential within each respective agency. Data on cable landing station/cable security is typically sensitive within companies as well, and falls under the protected critical infrastructure information (PCII) designation in the U.S.
	Cable route position lists are made available to many ship owners per their request.	ICPC annual sessions are closed to the public and presentations are not made publicly available.

Knowledge of Vulnerability Rating = 5 out of 10

REASON: Government and companies have tried to limit public information on cables in the last five years, but lots of public information still exists.

CAPABILITY	Factors Increasing Rating	Factors Decreasing Rating
Devices for Exploitation	Proliferation of manufacturers selling submarines and remotely operated vehicles (ROVs) that can cut, splice and connect cables at depths of nearly 1,000 meters.[98]	ROVs sell for $450,000 and above.[99]
	Ships with anchors, fishing trawlers and clam dredgers; ship can also be pirated to do the same.	
	Cable pliers can bend/break cables.	
	Car bomb can be set outside cable landing stations within close proximity in a variety of cases	

Devices for Exploitation Rating = 7 out of 10

REASON: Most every state has the capability to break cables and there is an increased probability that non-state actors could purchase ROVs for this purpose. Ship anchors, as well as fishing trawlers and clam dredgers, could easily disrupt cable lines. ICPC recommends, and cable companies typically do, bury cables in the ocean floor out to 2000 meters from shore.

[98] Karl Hasslinger, "Undersea warfare: The hidden threat," Armed Forces Journal, March 2008. Accessed at http://www.armedforcesjournal.com/2008/03/3348196

[99] Ibid.

CAPABILITY CALCULATION:

CAPABILITY = Average (Skill for Exploitation, Knowledge of Vulnerability, Devices for Exploitation)

CAPABILITY = (6 + 5 + 7) / 3

Capability	**Receives a 6 out 10**	**Comment: Cables are relatively easy to disrupt with a variety of tools available on most ships/boats. The locations of cable landing stations, including some cable positions, are readily found on the internet and elsewhere.**

REVISED DANGER INDEX FOR INTERNATIONAL UNDERSEA CABLE ARCHITECTURE

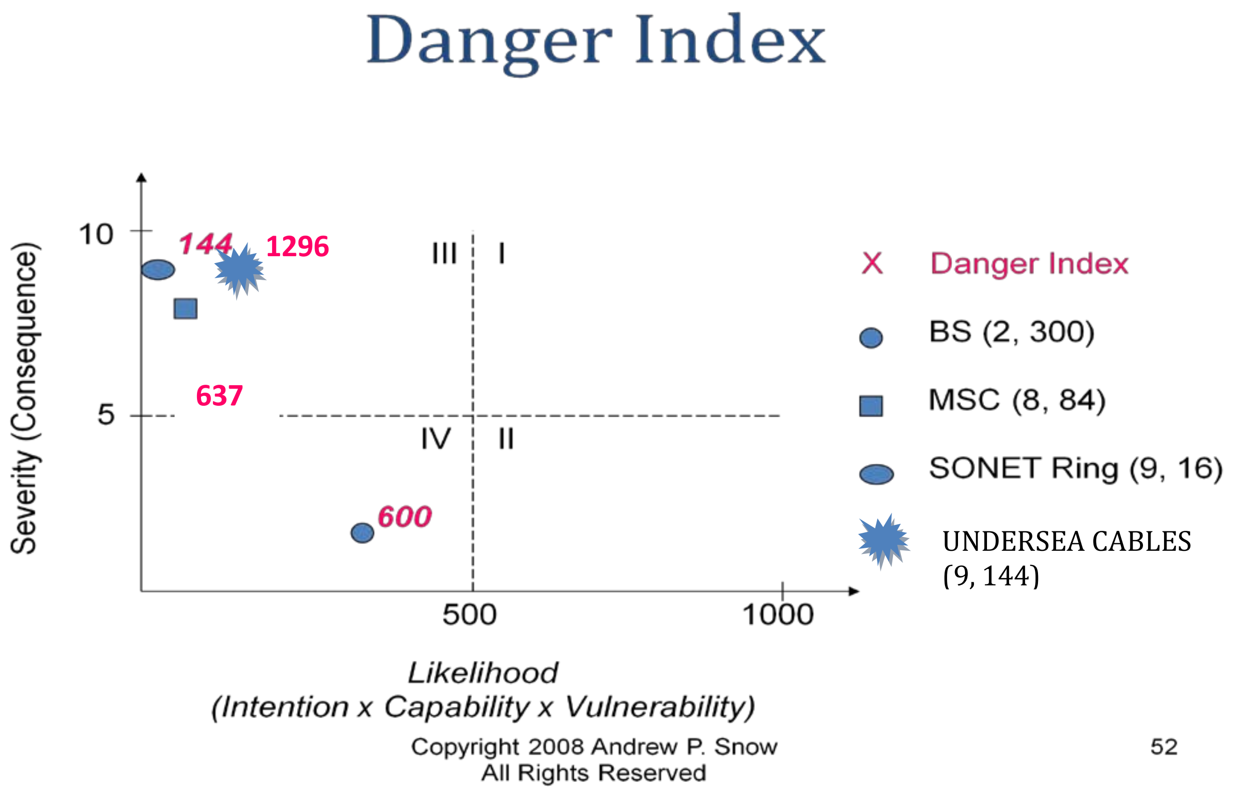
DANGER INDEX = CONSEQUENCE X VULNERABILITY X INTENTION X CAPABILITY

DANGER INDEX = (9 X 6 X 4 X 6)

DANGER INDEX = 1296 (out of 10,000)

DANGER INDEX **= 12.96% if normalized to 100%. This estimate states that a 12.96% danger exists to one or more cables/nodes within the international cable system. It is a relatively conservative estimate, seeing as it averages the threats within each subcategory.**

When applied to the Snow, Hoag and Weckman's Danger Index[100], the new chart looks like:



[100] Drs. Andy Snow[1] and Gary Weckman, "Tutorial: Protecting Critical Telecommunications and Networking Infrastructure," The Seventh International Conference on Networking ICN 2008. Slide 52.

In order of relative danger, undersea communication cables rank the highest at 1296; the personal communications service base station (PCS – BS) and the personal communications service mobile switching center (PCS – MSC) have the next highest danger ratings. A 12.96% danger is particularly high for an architecture that prides itself on reliability and quality of service (QoS), as it strives to achieve 6-9s of dependability on all systems. Final recommendations are listed to decrease the 12.96% danger index into a more manageable figure.

Before those recommendations are discussed, some important cable issues have not been addressed in the danger analysis. The next section walks through other issues that should be considered in making cable policy recommendations.

CABLE ISSUES UNADDRESSED IN FRAMEWORK

United Nations Convention on the Law of the Seas (UNCLOS) Un-Ratified

The U.S. is a signatory to the United Nations Convention on the Law of the Seas (UNCLOS), but Congress has not ratified it, even after a strong push by the Bush Administration in 2007. The UNCLOS provides the most comprehensive form of international law protection for undersea cables. It would increase cable security and enhance monetary and legal penalties for inadvertent and intentional cable cuts. Without passing this legislation, the U.S. can only resort to the 1884 Convention rules on telegraph cables in the event it seeks to prosecute an individual or entity for a cable cut.

The Looming Bandwidth Price Increase

Cable companies that have to upgrade or replace systems will price their costs at a much more competitive level in the future, driving up costs.

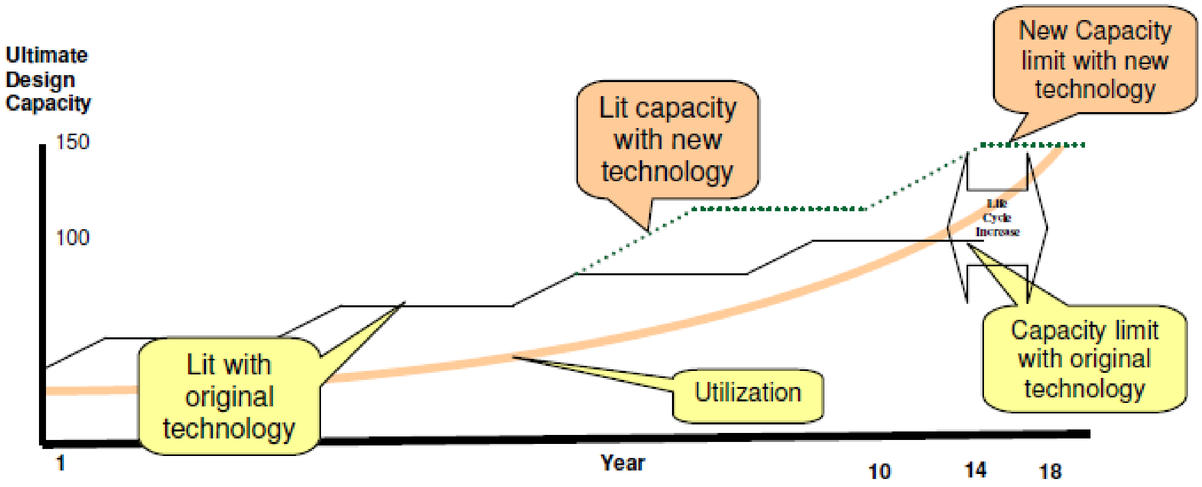
If prices go up to accommodate this increase, who will pay for it? As one Telegeography analyst notes, “Trans-Atlantic cable operators and wholesale buyers are facing a slow-motion crisis," since "the cost of circuits on a new cable built today would be far higher than prices prevailing in the market."[101] This cost increase is a problem since cable operators only make enough now to cover cable operating costs. Bandwidth prices per unit cost have dropped nearly 70% over the last decade.[102] This steady drop is attributed to the massive over-supply of bandwidth produced during the dot-com boom and bust from 1997-2002. Prices for customers have dropped consistently ever since 1997 and most have become accustomed to bandwidth always becoming cheaper. But that might not be the case much longer.

[101] “Trans-Atlantic Capacity Faces Exhaust by 2014,” *XChange Magazine*, June 30, 2009. Accessed at http://www.xchangemag.com/hotnews/trans-atlantic-capacity-faces-exhaust-by-2014.html

[102] Stephen Beckert remarks, PTC 2010 presentation.

Replacing Old Systems

Some of the cables in use today may not be able to be replaced because the technology is outdated. From the list of U.S. cables, one can see that many cables are almost a decade old. A recent study pointed out that a cable system's life now averages 18 years (see graph below).[103]



Source: Sam Thomas, paper to PTC presentation, January, 2010. Page 14.

Many systems will soon reach their 25-year half-life (see Appendix C). It is also important to note that many were built before the events of 9/11 and the creation of DHS. Critical infrastructure protection, especially involving cables and cable landing stations, was not on the radar of cable builders when these systems were being laid. Thus if new systems are built, the U.S. government will have or needs to create an opportunity to influence cable operators to build route diversity into the projects. Finding a way to build extra, possibly more expensive security measures into cable systems will require more capital (CAPEX) and operational (OPEX) expenditures. Implementing government security plans into the bottom line profit motive of

[103] Sam Thomas, "Managing the Economic Life Cycle of a Submarine Cable System," Presentation to PTC 2010, January 19, 2010. Graph accessed at http://www.ptc.org/ptc10/program/images/papers/papers/Paper_Sam%20Thomas_FS4.pdf

companies is a daunting challenge, particularly because a lack of communication exists today.

Other expenses

In addition to the costs of new or upgraded systems, cable companies also face an aging fleet of cable repair ships and cable landing stations that could use extra security. The Heritage Foundation noted five years ago that "while network repair capacity is able to meet current threats (e.g., trawlers, earthquakes, sharks), it would be incapable of repairing in a timely manner the damage caused by a targeted or systematic attack. Due to low market prices and high O&M costs, the number of ships and trained crews capable of conducting repairs is declining, as are worldwide spare parts inventories."[104] In order to increase these inventories, costs will go up. Upgrading both ships and landing stations will translate into higher CAPEX and OPEX that customers may have to bear in higher prices.

Mesh networking is the future

With Verizon, AT&T and TATA Communications now advertising their switch to mesh networking, more companies see mesh networking as the way to protect against cable breaks. It is up to IT and network operators within government agencies and private companies to design and purchase the excess bandwidth capacity needed to ensure their organization has mesh connectivity.

The founder of the first around-the-world cable system recently proposed an idea which uses the excess 'unlit' cable capacity that exists in the world today in a more

[104] James Carafano and Alane Kochems, "Making the Sea Safer: A National Agenda for Maritime Security and Counterterrorism," *Heritage Foundation*, February 17, 2005. Page 13. Accessed at http://74.125.93.132/search?q=cache%3A2Z6hFDVVqM8J%3Awww.heritage.org%2Fresearch%2Fhomelanddefense%2Fupload%2F74871_4.pdf+undersea+cable+CRS+report&hl=en&gl=us

constructive way.[105] The 'unlit' capacity could be used for disaster recovery purposes via a mesh network should one or many systems suffer from an outage for whatever reason. The plan would seek to prevent widespread outages like that which took place all over the world in the previous decade (see Appendix D).

The U.S. Cable Permitting Process

The FCC approves all submarine cable licenses after reviewing the license application. This authority has been delegated via Presidential Executive Order 10530, Section 5.[106]

In order to make a full inter-agency decision, the FCC is now required to send all cable licenses to the Committee of Foreign Investment in the United States (CFIUS) for review first. Within CFIUS, a "Team Telecom" studies undersea cable landing license applications for national security purposes, particularly to ensure that foreign ownership of telecom companies does not provide other governments' access to U.S. national security information.[107] Team Telecom is comprised of officials from the Departments of Defense, State, Justice, Homeland Security, Central Intelligence Agency, National Security Agency and the Office of the Director of National Intelligence.[108] Below is a list of the FCC Cable Landing Licenses processing

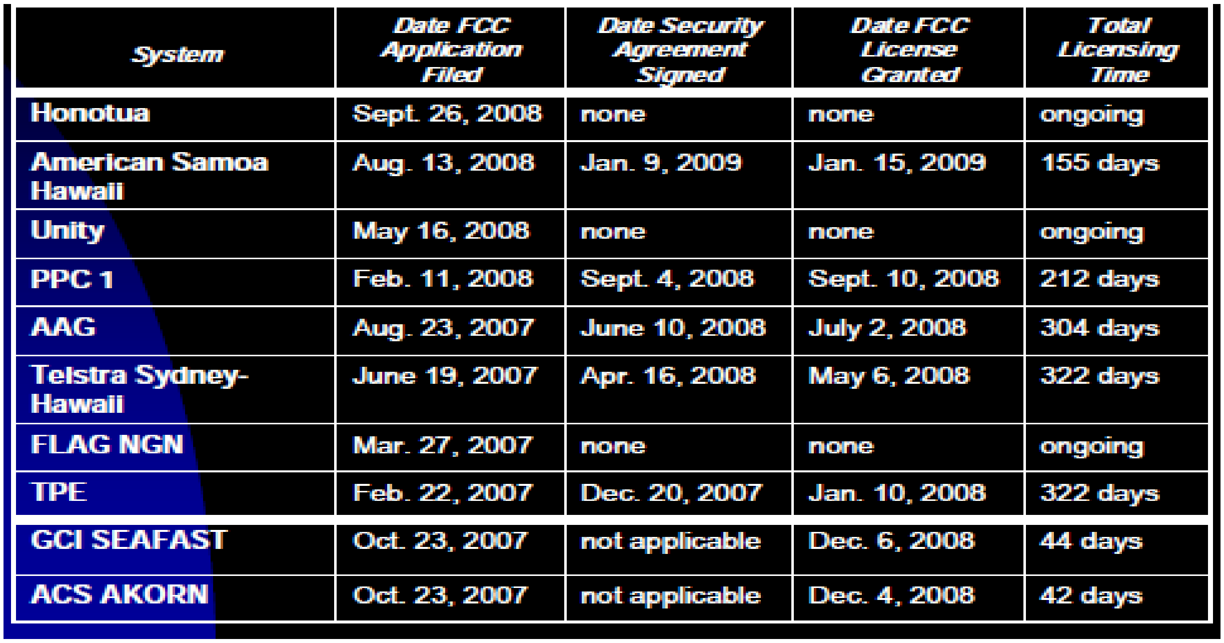
[105] Neil Tagare, PTC 2010 presentation

[106] See E.O. 10530 at http://www.archives.gov/federal-register/codification/executive-order/10530.html

[107] Kent Bressie, "More Unwritten Rules: Developments in U.S. National Security Regulation of Undersea Cable Systems," Presentation made to the 2009 PTC conference, January 18, 2009. Accessed at http://www.harriswiltshire.com/siteFiles/News/7DF1C8D035660E8FBEF0AAC7BA8DA103.pdf

[108] Kent Bressie, "New Barriers to U.S. Market Entry for Undersea Cable Operators: Recent Developments with 'Team Telecom'," Presentation to the 2008 PTC conference, January 13, 2008. Accessed at www.ptc.org/ptc08/participants/speakers/papers/BressieFinalSlides.pdf

times for recent pacific-ocean systems.[109] From the chart, one can see that some licenses can be in process for nearly two years.



System	Date FCC Application Filed	Date Security Agreement Signed	Date FCC License Granted	Total Licensing Time
Honotua	Sept. 26, 2008	none	none	ongoing
American Samoa Hawaii	Aug. 13, 2008	Jan. 9, 2009	Jan. 15, 2009	155 days
Unity	May 16, 2008	none	none	ongoing
PPC 1	Feb. 11, 2008	Sept. 4, 2008	Sept. 10, 2008	212 days
AAG	Aug. 23, 2007	June 10, 2008	July 2, 2008	304 days
Telstra Sydney-Hawaii	June 19, 2007	Apr. 16, 2008	May 6, 2008	322 days
FLAG NGN	Mar. 27, 2007	none	none	ongoing
TPE	Feb. 22, 2007	Dec. 20, 2007	Jan. 10, 2008	322 days
GCI SEAFAST	Oct. 23, 2007	not applicable	Dec. 6, 2008	44 days
ACS AKORN	Oct. 23, 2007	not applicable	Dec. 4, 2008	42 days

Source: Kent Bressie, presentation to PTC conference, 2009. Slide 14.

In addition to receiving, Team Telecom, CFIUS and FCC approval, a cable cannot land in the U.S. without some sort of approval from the U.S. Army Corps of Engineers, the Department of State, the National Oceanic and Atmospheric Administration and the U.S. Coast Guard at the federal level. It is an uncoordinated mess essentially.

At the state and local level, cable companies need to receive zoning and environmental approvals as well. For instance, in states, such as New Jersey, California and Florida, environmental requirements are stiff, and permitting can hold the cable development process up to a year. The uneven permit process is a constant complaint among cable operators. It is also uneven when applying for permits to repair cables within states' maritime boundaries. Some states take weeks to do so and charge high fees to enter their waters.

[109] Kent Bressie, "More Unwritten Rules: Developments in U.S. National Security Regulation of Undersea Cable Systems," Presentation made to the 2009 PTC conference, January 18, 2009.

The International Permitting Process

The cable permitting process is also onerous in many other countries. One example, provided by the ICPC, is found below:[110]

Permits required for a repair in Territorial/EEZ Waters

1.	Ministry of Home Affairs –	28 days
2.	Ministry of Defence –	14 days
3.	Specific Period Licence –	14 days
4.	Indian Coastal Conference –	14 days
5.	Vessel Temporary Importation –	3 days
6.	Importation Duty – Consumables –	3 days
7.	Naval Security Inspection –	1 day

Minimum period to obtain permit for repair = items 1 + 5 + 7 = 32 days

It is nearly impossible to predict how long the process can take and if it is long, it can greatly affect that system's profitability.

[110] Information collected from Mick Green, et al. "Submarine Cable Network Security," Presentation to APEC Submarine Cable Workshop Group, September 2009. Accessed at http://74.125.113.132/search?q=cache:9yxrwo21PBIJ:www.iscpc.org/information/Openly%2520Published%2520Members%2520Area%2520Items/Submarine_Cable_Network_Security.ppt+hengchun+earthquake+eleven+ships+cable&cd=3&hl=en&ct=clnk&gl=us

POLICY RECOMMENDATIONS

Certain policies can address these issues, while lowering the danger index rating in the process. Those policies are recommended below.

1. Create a uniform permitting structure.

Recommendation	Industry Priority	Government Priority	Chances Public-Private Partnership can impact
Create a Uniform Permitting Structure	**HIGH**	**LOW**	**HIGH**

PROBLEM: Currently, companies cannot be sure how long it will take to receive a permit to land a cable in the U.S. or other countries. In some instance, the process can add years to business development timeline. The uncertainty negatively affects company profit, which in turn limits the economic life-span of a cable.[111] When the economic life-span is shortened, cables are decommissioned quicker and more volatility exists in the market.[112] Companies also lose more money than it would have, some of which could be applied to increasing security on land or via sea patrols.

Permits are also required by some states to even to repairs in or around their territorial waters. States charge fees for these permit repair licenses in some instances. In the case of the Hengchun earthquake near Taiwan, it took cable repair ships days to obtain the necessary permits to fix the cables. This was unnecessary time that cable operators and cable users could not afford.

[111] Sam Thomas, Presentation to PTC 2010, January 19, 2010. Page 1.

[112] Ibid. Page 13.

SOLUTION: Permits and permit fees for cable landings should be uniformly structured. Permits and fees for repairs should be discarded. For private cable companies, permit changes is more important than all other issues. The public-private partnership should deal with them accordingly.

SUPPORT: Every industry insider supports permit streamlining. U.S. Federal officials want to collect information before issuing a permit and state and local officials seek to collect revenue from cable landings. Streamlining the permitting process is less of an issue to U.S. officials, at least.

Decreased Danger: The consequences of a cable break would decrease as cable repair ships could arrive quicker to fix broken cables. Cables could also be laid quicker if permitting timelines were streamlined. Both efforts would lessen the consequence term.

2. Pursue defense-in-depth

Recommendation	Industry Priority	Government Priority	Chances Public-Private Partnership can impact
Pursue Defense-in-Depth	**LOW**	**HIGH**	**MEDIUM**

PROBLEM: Cables are vulnerable to intentional and benign disruption in a variety of ways on land and in water. No one security policy by itself can protect cables from the many threats they face.

SOLUTION: Defense-in-Depth, also referred to as layered security, is a comprehensive policy approach that "denotes the practice of having multiple, redundant, and independent layers of safety systems" to "mitigate the risk of one component of the defense being compromised or circumvented."[113]

It typically relates to nuclear security and information technology security. The CERT, a federally funded research and development center, lists multiple components for defense-in-depth related to IT security; they include compliance management, risk management, identity management, authorization management, accountability management, availability management, configuration management and incident management. Many of the recommendations made in this paper could fall into one of these categories. This concept should be employed by the public and private sectors in any future partnership. [114]

Examples of defense-in-depth for cables might include evaluating security for all elements of undersea cable systems: payload, human, power, software, hardware, policy, networks and environment, as described by Karl Rauscher.[115]

SUPPORT: Governments, worldwide, favor defense-in-depth as it provides multiple levels of protection.

[113] See "Defense-in-Depth" Wikipedia entry. Accessed at http://en.wikipedia.org/wiki/Defence_in_depth

[114] For more information see Christopher May, et al., "Defense in Depth: Foundations for Secure and Resilient IT Enterprises," *CERT organization,* September 2006 www.cert.org/archive/pdf/Defense_in_Depth092106.pdf

[115] Karl Rauscher, "ENISA Expert Group on Research Priorities in the Areas of Networking and Information Security for Resilient Networks," ENISA Workshop, Athens Greece, May 2009. Slide 14. Accessed at http://www.enisa.europa.eu/act/it/inf/procent/eg1/rauscher

Decreased Danger: A stated policy for defense-in-depth would lessen cable vulnerability to threats on land and in water, as well as threats that might lead to a cascading failure. The intention and capability terms might also be reduced under good defense-in-depth strategies.

3. Seek legal changes

Recommendation	Industry Priority	Government Priority	Chances Public-Private Partnership can impact
Legal changes	**MEDIUM**	**MEDIUM**	**MEDIUM**

PROBLEM: In many countries, the laws related to incidental or purposeful cable cuts are outdated. Most have not been updated since the 1884 Convention on Submarine Cables. The current U.S. domestic laws are woefully inadequate. Submarine cable injury and punishment falls under United States Code 47, Chapter 2, Section 21. The legislation states that anyone who willfully breaks a submarine cable is punishable up to a misdemeanor with up to 1 year in jail and a $5,000 fine, or both.[116]

SOLUTION: The partnership should push the U.S., and all member states with undersea cable landings, to sign and ratify UNCLOS, as well as enact strict domestic legislation to be in compliance with the legislation. UNCLOS provides the broadest measure of protection under international law although it does have some gaps in coverage.[117] States that have ratified

[116] FCC Cable Landing License Act, the FCC. Accessed at http://www.fcc.gov/ib/pd/pf/clla.html

[117] See Robert Beckman, Tara Davenport, "WORKSHOP ON SUBMARINE CABLES AND LAW OF THE SEA REPORT," Center for International Law, National University of Singapore, December 2009. Page 7. Accessed at http://cil.nus.edu.sg/wp/wp-content/uploads/2009/10/Workshop-Report-29-Jan-2010.pdf

UNCLOS also need to implement national legislation to protect cables; since the U.S. has not ratified the treaty, no domestic legislation has been updated.

Good examples of strict domestic legislation are found in Australia and New Zealand, where the fine for cable damage can be upwards of $250,000 and 10 years jail time.[118] Punitive damages can also be sought by affected companies up to $750,000 per day a cable is broken.[119] Countries reliant of cable system should be particularly encouraged to update their laws similar to Australia and New Zealand.

SUPPORT: The Bush Administration supported UNCLOS ratification, but it is unclear where the Obama Administration stands. Industry generally favors any law that can prevent inadvertent or malicious acts that disrupt undersea cables.

Decreased Danger: The intention and capability terms in the equation would be reduced with stiffer penalties, as more people would be deterred from affecting cable connectivity.

[118] See "Submarine Cables and Pipeline," Land Information New Zealand office, Government of New Zealand. Accessed at http://www.linz.govt.nz/docs/hydro/ntm/summary/annual/nz13.pdf

[119] Ibid.

4. Incentivize upgrades to 40G

Recommendation	Industry Priority	Government Priority	Chances Public-Private Partnership can impact
Incentivize upgrades to 40G	**MEDIUM**	**LOW**	**LOW**

PROBLEM: On high-traffic routes, like the Trans-Atlantic, cable capacity may be in short supply in a few years. With congested cables, the chances of a cable break creating cable disruptions and outages are much higher. Since cable companies are hesitant to upgrade because of additional costs, governments may have to monitor and incentivize companies to go to 40G to ensure supply and keep risks low.

SOLUTION: In the U.S., one way to do this is to allow cable companies to apply for stimulus funding in order to upgrade. The partnership can monitor this activity and also provide mechanisms, like an insurance scheme with low premiums for companies that invest in higher bandwidth technology.

SUPPORT: Any incentive to reduce upgrade costs would entice private sector support. In cases where a bandwidth crunch looms, such as in the Trans-Atlantic, government may not have a choice but to incentivize the market through grants or other mechanisms.

Decreased Danger: With bandwidth increased to 40G wavelengths, the consequence and vulnerability to a cable system suffer some level of outage would diminish.

5. Create Disaster Recovery Plans

Recommendation	Industry Priority	Government Priority	Chances Public-Private Partnership can impact
Create Disaster Recovery Plans	**HIGH**	**HIGH**	**HIGH**

PROBLEM: Taiwan's Hengchun earthquake taught cable operators in East Asia that disaster recovery arrangements need to be in place before a crisis. If not, network operators will scramble trying to re-route traffic during one.

SOLUTION: One of the goals of the partnership would be to highlight the importance of undersea cables to network operators and ensure that they are ready for potential crises should these systems go down in a variety of ways in the future. This effort will help companies, users and nations save money and ensure service. Mesh networking should be touted to all members in order to stave off risks associated with linear and ring cable topologies.

States may also consider the idea of designing a global mesh network that uses spare capacity in emergency situations to ensure connectivity. The founder of the first cable system to connect around the world (the FLAG cable) thought up this idea and seeks stimulus funding now to enact it.[120]

SUPPORT: Cable companies and governments are beholden to providing their customers/citizens with high quality service, with minimal interruptions, even in the case of an emergency. Ensuring backup and recovery plans exist is one way to diminish the risk.

[120] Neil Tagare, presentation to PTC 2010 conference, January 19, 2010.

Decreased Danger: The consequence or vulnerability of a cable system would lessen if careful thought is given now to plans that devise alternative routing schemes in order to avoid the next big cable outage.

6. Designate Single Points of Contact

Recommendation	Industry Priority	Government Priority	Chances Public-Private Partnership can impact
Designate Single Points of Contact	**HIGH**	**MEDIUM**	**HIGH**

PROBLEM: The APEC Submarine Cable Working Group noted, as well as others like Telcordia Technologies, that no single point of contact exists within the U.S., or other governments, to report a cable outage. If there is information about an outage, it is not communicated widely to other government agencies. Moreover, the process is not formalized or a transparent.

SOLUTION: The partnership should identify single points of contact, including alternates, in all member agencies with the authority to distribute the information widely. The process should also be clearly communicated to members within the organization as well as on the Internet to ensure openness.

SUPPORT: Companies continue to ask for officials within their respective governments they can contact in the event of a cable issue or outage emerges. Governments seemingly want the idea to, but have not designated officials yet to provide a response to the request.

Decreased Danger: The consequence of an outage and vulnerability of a system to an unaddressed issue would diminish with points of contact lists.

7. Encourage Cable Protection Zones

Recommendation	Industry Priority	Government Priority	Chances Public-Private Partnership can impact
Cable Protection Zones	**HIGH**	**MEDIUM**	**HIGH**

PROBLEM: Most countries rely on cables heavily for international communications. Yet few have made it policy to implement cable protection zones, so that fishing trawlers, clam dredgers and ship anchors don't inadvertently cut off lines of communication to the outside world.

SOLUTION: Any partnership should push member states to use these zones so that this vital critical infrastructure is better protected.

SUPPORT: Most every cable company would support such a measure, but many groups, like the fishing or shipping association, might oppose such cable zones as it might affect their profitability in a slightly negative way. Because of their opposition, governments might be lukewarm on the issue of cable zones; however, the consequences are too high not to at least evaluate such a recommendation.

Decreased Danger: Vulnerability, intention and capability would all decrease, minimizing the likelihood of cable faults in the process.

8. Promote Cable Route Diversity and Security

Recommendation	Industry Priority	Government Priority	Chances Public-Private Partnership can impact
Cable Route Diversity and Security	**LOW**	**HIGH**	**HIGH**

PROBLEM: Cables cross too often, especially as they approach coast lines. Crossings and similar routes create the problem of bottlenecks and easy targets. Moreover, these routes and landing stations are sometimes found on Internet websites like Spyglass, Cryptome and even Wikipedia. The Internet Wayback Machine also allows easy location for information previously uploaded.

SOLUTION: No critical infrastructure should be an easy target this day in age. Thus the partnership should address the need to space cables further apart and secure cable crossings, particularly on high-traffic cables. Companies may need government involvement in order to receive some benefit for route diversity in future cable planning.

Cable crossings in the water are a different problem. The ICPC recommends that all cables be protected by double-armor/rock-armor coverings when crossing one another. This armor prevents the cable being penetrated or broken if an anchor dropped on that location. The partnership should push the industry the ICPC Regulation #2 regarding these cable crossing procedures.[121]

SUPPORT: Government seeks these security measures, but wishes to push the costs on to the private sector. The private sector would consider this a low priority as they are more concerned with delivering a profit and return on

[121] Recommendation No. 2: Recommended Routing and Reporting Criteria for Cables in Proximity to Others, ICPC. Page 6. Published January 26, 2007.

investment. Providing security for tail-end probabilities is typically not a lucrative business model. However, with the odds of tail-end probabilities seemingly increasing, it is time companies start to move towards investment in this recommendation, possibly with some government assistance.

Decreased Danger: Again, both consequence and vulnerability would diminish with investment in more resilient and physically diverse routes. The Taiwan 2006 and Mediterranean 2008 cuts would not have been so significant if this recommendation had been made a priority sooner.

9. Harden facilities

Recommendation	Industry Priority	Government Priority	Chances Public-Private Partnership can impact
Harden Facilities	**LOW**	**MEDIUM**	**MEDIUM**

PROBLEM: More protections need to be made to secure backhaul routes to cable landing stations, cable landing stations themselves, and undersea cables extending within territorial waters and beyond. Yet multiple companies operate multiple systems in these three areas; multiple government agencies also have jurisdictions in all three areas.

SOLUTION: The partnership would provide an opportunity for appropriate parties to work together to secure these sites. The overlapping authorities in the various governments may need to be streamlined so that one agency can implement the necessary physical security additions all three sites need.

SUPPORT: Government, again, favors more security, while cable companies see increased costs with adding more security. It is important to try and reach agreement between both parties on site security and the partnership would facilitate that discussion.

Decreased Danger: Hardened facilities with decrease physical vulnerabilities, keep malcontents away and reduce the chances that one could damage a landing station through means like a car bomb.

10. Prioritize Traffic

Recommendation	Industry Priority	Government Priority	Chances Public-Private Partnership can impact
Create a Uniform Permitting Structure	**LOW**	**HIGH**	**MEDIUM**

PROBLEM: Currently, the U.S. National Communication Services has three programs to ensure emergency communication stays connected in the event of a crisis: the Wireless Priority Service, the Government Emergency Telecommunication Service and the Telecommunication Service Priority program. However, no publicly available program exists to sift and ensure high priority international internet data traffic continues to connect international in the event of a crisis. The recent National Broadband Plan would change that for domestic broadband communications.

SOLUTION: It is now time to seek something similar for international broadband communications. NCS should work with other nations, through the partnership to develop a traffic priority scheme for undersea cable communications should an outage occur.

SUPPORT: In March, the U.S. Federal Communications Commission (FCC) released the National Broadband Plan. Recommendation 16.11 in the document states that the "FCC and the National Communications System (NCS) should create priority network access and routing for broadband communications."[122]

[122] *National Broadband Plan*, Federal Communications Commission, March 16, 2010. Page 322.

Decreased Danger: Both consequence and vulnerability terms would decrease.

11. Promote Cable Education and Public Awareness

Recommendation	Industry Priority	Government Priority	Chances Public-Private Partnership can impact
Education and Awareness	**HIGH**	**MEDIUM**	**MEDIUM**

PROBLEM: Despite being one of our societies' most critical underpinnings, few within the government or commercial sectors realize the importance of undersea cables. This lack of awareness hinders cable companies and the industry more generally from receiving the protection and funding it deserves.

SOLUTION: Begin a public awareness campaign to highlight the importance of cables. Focus company and government energy on evaluating efforts they can make to improve the cable architecture.

SUPPORT: The U.S. government has previously been tight-lipped about the role and existence of undersea cables and that policy would need to change. Some efforts are being made within the government, NSTAC for example, to bring policy awareness on cable matters to the attention of senior officials. Other governments, such as Australia, which raised cable awareness at APEC and the Vietnam, which created its own public awareness campaign, would concur with this recommendation.

Decreased Danger: This recommendation would reduce cable vulnerability, as well as benign intention that might induce cable problems.

RECOMMENDATIONS OVERVIEW

#	SPECIFIC POLICY RECOMMENDATIONS	INDUSTRY PRIORITY	GOVT PRIORITY	CONSEQUENCE REDUCTION	VULNERABILITY REDUCTION	INTENTION REDUCTION	CAPABILITY REDUCTION	International Cable Partnership Could Impact
1	Create a uniform permitting structure	🔴	🟡	☑	------- -------	-------- --------	---------- ----------	☑
2	Pursue defense-in-depth	🟡	🔴	-------- --------	☑	☑	☑	☑
3	Seek legal changes	🔵	🔵	-------- --------	------- -------	☑	☑	☑
4	Incentivize upgrades to 40G	🔵	🟡	☑	☑	-------- --------	---------- ----------	--------- ---------
5	Create Disaster Recovery Plans	🔴	🔴	☑	☑	-------- --------	---------- ----------	☑
6	Designate Single Points of Contact	🔴	🔵	☑	☑	-------- --------	---------- ----------	☑
7	Encourage Cable Protection Zones	🔴	🔵	☑	☑	☑	---------- ----------	☑
8	Promote Cable Route Diversity and Security	🟡	🔴	☑	☑	-------- --------	---------- ----------	☑
9	Harden Facilities	🟡	🔵	-------- --------	☑	☑	☑	☑
10	Prioritize Traffic	🟡	🔴	☑	☑	-------- --------	---------- ----------	☑
11	Educate and Improve Public Awareness	🔴	🔵	-------- --------	☑	☑	---------- ----------	☑
	INTERNATIONAL PUBLIC-PRIVATE PARTNERSHIP	🔴	🔴	☑	☑	☑	☑	--------- ---------

High Priority = 🔴 Medium Priority = 🔵 Low Priority = 🟡

INTERNATIONAL EFFORTS UNDERWAY

Some organizations and countries are addressing a variety of these recommendations, in a limited way. Below is a list of some of the main efforts taking place to address undersea cable issues.

Pacific Partner Members (PPM) Committee No. 2

ACTION: After the 2006 Hengchun earthquake, a group of 14 major telecommunication companies was formed within the existing Pacific Partner Members organization. [123]

PURPOSE: The earthquake had served as a giant wake-up call in the industry; it exposed the weakness of ring topology and pushed operators to move to mesh topology. It also pushed cable companies to decide to avoid laying cables in earthquake fault-prone areas. As a response, the companies within the committee developed new restoration agreements with another should another major incident happen again.[124] The partnership is a result of those efforts.

RESULT: The partnership meets at least twice a year and pro-actively focuses on disaster recovery situations. The partnership paid off when much less connectivity was lost during Typhoon Morakot and Taiwanese earthquake than would have been if no partnership had existed.

[123] See "Meeting No. 1: Report to PPM Principals," The Pacific Partners Members Committee No. 2, Jun 2007. Accessed at http://www.pacificpartner.org/conpage.php?conid=43

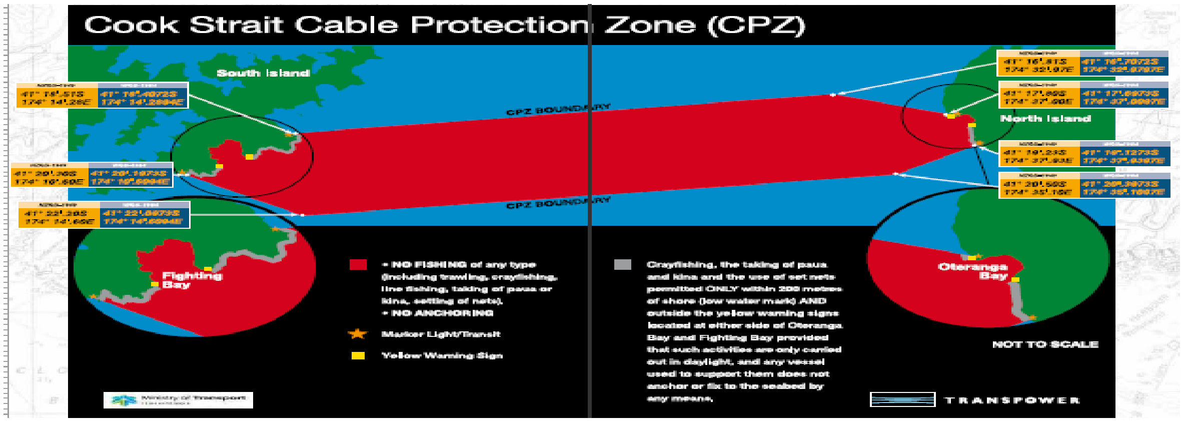
[124] "PPM Committee 2 Report (Disaster Recovery)," *Pacific Partners Members Committee No. 2,* August 28, 2008. Accessed at www.pacificpartner.org/document/PPM%20Committee%202%20Report.ppt

The Government of New Zealand

ACTION: In 1996, the New Zealand government passed the Submarine Cables and Pipelines Protection Act.[125]

PURPOSE: The Act gave the government the ability to regulate fishing and anchoring along cable route position lists.[126] New Zealand was way ahead of other states in passing additional legislation to protect cables. Currently, all permitting is done in one central location, through a government submarine cable protection office.

RESULT: New Zealand has implemented a cable protection zone that others have also followed. See the New Zealand Cook Strait Protection Zone map below:[127]


Cook Strait Cable Protection Zone (CPZ)
South Island
North Island
CPZ BOUNDARY
CPZ BOUNDARY
Fighting Bay
Oteranga Bay
• NO FISHING of any type (including trawling, crayfishing, line fishing, taking of paua or kina, setting of nets).
• NO ANCHORING
Marker Light/Transit
Yellow Warning Sign
Crayfishing, the taking of paua and kina and the use of set nets permitted ONLY within 200 metres of shore (low water mark) AND outside the yellow warning signs located at either side of Oteranga Bay and Fighting Bay provided that such activities are only carried out in daylight, and any vessel used to support them does not anchor or fix to the seabed by any means.
NOT TO SCALE
Ministry of Transport
TRANSPOWER

Source: Cook Strait Submarine Cable Protection Booklet, page 11, October 2008

[125] See "Submarine Cables and Pipeline," Land Information New Zealand office, Government of New Zealand. Accessed at http://www.linz.govt.nz/docs/hydro/ntm/summary/annual/nz13.pdf

[126] Ibid.

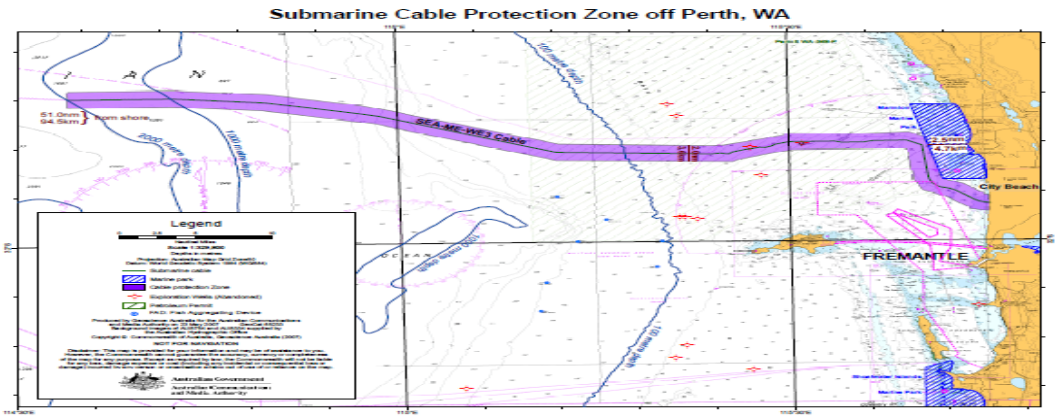
[127] The Cook Strait Submarine Cable Protection Zone booklet, October 2008. Page 11. Accessed at https://transpower.co.nz/f2462,11793265/cook-strait-cable-2008.pdf

The Government of Australia

ACTION: In September 2005, the Australian Parliament passed the Telecommunications and Other Legislation Amendment (Protection of Submarine Cables and Other Measures) Act.[128]

PURPOSE: Similar to the New Zealand act, the Australian version institutes greater penalties for all forms of submarine cable sabotage. The Australian Communications and Media Authority even signed a memorandum of understanding with its Defense Department so it could properly regulate security activities in the cable zone.[129]

RESULT: Australia followed New Zealand in creating cable protection zones around its most important cable lines. See one zone below. Australia continues to push for stronger international efforts to protect cables, as it did at APEC in 2009.



Source: Australia Communication and Media Authority; http://www.acma.gov.au/webwr/_assets/main/lib100668/wa_protection_zone_map.pdf

[128] "Protection zones around submarine cables of national significance," Australian Communication and Media Authority, Government of Australia. Accessed at http://www.acma.gov.au/WEB/STANDARD..PC/pc=PC_100223

[129] Ibid.

Asia-Pacific Economic Cooperation (APEC)

ACTION: At last year's 2009 APEC meeting, Australia convened the first ever "Submarine Cable Protection Workshop," within the Security and Prosperity Steering Group. During the workshop, 12 presentations were delivered.

PURPOSE: The workshop sought to agree on a set of recommendations that could be inserted into the final ministerial declaration issued at the end of 2009.

RESULT: One of the major recommendations made was to designate a single point of contact (SPOC) in each APEC country to handle cable issues.[130] Currently, no SPOC exists for companies to report cable outages in various governments, one of which is the U.S.

Reliability of the Global Undersea Communications Cable Infrastructure (ROGUCCI) Summit

ACTION: The first ever Summit designed to focus on the security and reliability of undersea communication cables took place in Dubai, UAE in October 2009.

PURPOSE: Hosted by the IEEE, the Summit noted specific vulnerabilities that need to be addressed in order to protect cable systems.

RESULT: One of the outcomes of the Summit was that much more needs to be done in regards to international dialogue, education and awareness on cable issues. Interestingly, no U.S. government representative attended the event. Very few government officials in general participated overall.

[130] "Report on the Outcomes of the Submarine Cable Information Sharing Workshop," APEC meeting, September 2009. Accessed at http://aimp.apec.org/Documents/2009/TEL/TEL40-SPSG/09_tel40_spsg_010.doc

The International Cable and Protection Committee (ICPC)

BACKGROUND: On May 22, 1958, six major cable owners met in London to form the Cable Damage Committee. By 1967, the Cable Damage Committee had become the ICPC, with a "principal purpose is to promote the safeguarding of submarine telecommunication cables against manmade and natural hazards."[131] Today, the ICPC meets annually and does not actively recruit government officials to attend. It appears that government officials rarely attend.

ACTION: The 2010 annual meeting is titled, "Protecting the global submarine cable network**:** New and evolving challenges for operators, governments and stakeholders in the expanding submarine cable community."[132] The issue of increasing government and cable company coordination and communication is sure to top the discussion list. Undersea cable policy is clearly becoming more important to advanced countries as well as international organizations.

PURPOSE: The goal of the ICPC is "to exchange information and establish countermeasures among seabed users for protecting the cables."[133] The organization "also serves as an industry forum for cable owners to share cable fault information and to develop standard procedures as 'ICPC Recommendations'."[134]

[131] "About the ICPC," ICPC. Accessed at http://www.iscpc.org/information/About_ICPC.htm

[132] ICPC Homepage. Accessed at www.iscpc.org

[133] Masakuni Kuwazuru, Ryoji Hoshina, "Regulatory Aspects of Undersea Cable Protection," KDD Submarine Cable Systems Inc. (KDD-SCS). Accessed at www.scig.net/Section07a.pdf.

[134] Ibid.

A NEW PARTNERSHIP: PUCS

These international efforts are a good start, but not enough. A new international public-private partnership - one that brings both governments and companies together in a formalized way – is the best way to implement the recommendations from the previous chart. If implemented, these recommendations will, in turn, dramatically lower the 12.96% danger index rating.

It is in the interest of DHS to push for this partnership. The agency cannot begin to address the multi-varied issues presented alone and will need unified, inter-agency support to begin this partnership. To that end, it would be of some benefit to have a member of the Executive Office of the President or National Security Council oversee the inter-agency process as the partnership unfolds. The staff member would work with a member of the Under Secretary for National Protection and Programs Directorate's staff within DHS to successfully implement the partnership. The DHS NPPD Office would oversee the partnership and be responsible for reaching out to international partners.

To create this partnership, the U.S. should join with those countries most interested in protecting cables first, namely Australia, New Zealand, the United Kingdom, France, Japan, China, Singapore, Egypt and India. This core group of countries would become the first members of the partnership and its first members. International organizations, like the ICPC, NASCA, UKCPC and others would also be invited to join first.

One idea would be to call the group the Partnership for Undersea Cable Security (PUCS). PUCS would bring international industry and governments together to improve cable security, as well as:

- Develop a set of best practices
- A statement of principles

- Terms of references
- Outage reporting structures
- Lists of single points of contact
- And high-level operational exercises.

More nations and groups would be invited to join after the initial stages. PUCS would meet in its entirety at least once a year, with sub-groups meeting several times a year to address cable-specific issues. Planning operational exercises for members would be high among the list of activities.

In time, the partnership would lessen the risk of a cable outage anywhere in the world and develop ways to mitigate crises. It should be considered one of the best options the world has in order to protect this vital infrastructure and to keep us all connected to one another.

The more difficult part is going about actually creating and structuring the partnership. As stated, the goal would be to start a major international partnership run by the Office of the Under Secretary for National Protection and Programs Directorate within DHS. Here are some concrete steps the Office could take to get there.

STARTING THE PARTNERSHIP

The support of government and cable company support is vital. Below are some steps DHS could take right now, in chronological or simultaneous fashion, to start the partnership.

Steps to get U.S. Government Support

- Within DHS, seek the support of NSTAC, National Communications System, Office of Infrastructure Protection, United States Computer Emergency Readiness Team and National Cyber Security Division management for the idea.
- Once cyber-related offices in DHS approve, seek the support of the National Cyber Czar, Howard Schmidt, within the National Security Council.
- Once DHS entities and the NSC are on board, seek the support of the FCC, the U.S. Cyber Command at NSA, DISA, Department of State's International Cyber Office and other Team Telecom members.
- Lastly, get support from other national cybersecruity centers, namely DoD's Joint Task Force-Global Network Operations (JTF-GNO) and Joint Functional Component Command for Network Warfare (JFCC-NW), FBI's National Cyber Investigative Joint Task Force, the DNI's Intelligence Community-Incident Response Center and DoD's Defense Cyber Crime Center.

Steps to get International Government Support

- Seek initial support for the partnership from 5-EYES nations, i.e. Australia, Canada, New Zealand and United Kingdom.
- After 5-EYES nations approve, seek support from other nations' with major stakes in the success of cables, such as Brazil, China, Egypt, France, India, Italy, Japan, New Zealand, Pakistan, U.A.E.

- Announce the partnership during the two main government-only cyber conferences this year and invite other states to join:
  - The 6th Annual Meridian Conference in Taiwan in November 2010.
  - The International Watch and Warning Network (IWWN) annual conference, at which "15 countries collaborate on policy issues, and respond to cyber attacks."[135]

Steps to get Cable Company Support

- Seek support of senior management within major U.S. cable companies, namely Verizon, AT&T, Tyco, Hibernia Atlantic, Google, GlobeNet, Sprint and Columbus.
- Announce plans for partnership and seek corporate support at two major undersea cable company conferences:
  - The International Cable Protection Committee's 2010 conference in Mauritius. This conference will explicitly focus on government and company efforts to improve cable security.
  - SubOptic's 2010 conference in Yokohama, Japan.
- Seek the support of other cable organizations, namely NASCA and the UKCPC (see Appendix E).

[135] "A Focused Effort on Cybersecurity," Department of Homeland Security Leadership Journal. June 18, 2009. Accessed at http://www.dhs.gov/journal/leadership/labels/cybersecurity.html

CONSULTATIONS

Name	Organization
Mark Antholt	DHS Science and Technology, IGD Division
John Beaty	DHS ALERT Center/Northeastern University
Fiona Beck	Southern Cross Cable Network
Stephen Beckert	Telegeography
Shishir Belbase	Asian Development Bank
Libby Buckley	Porthcurno Telegraph Museum
Roger Callahan	Information Assurance Advisory, LLC
David Clark	Department of Defense (DoD), Office of the Secretary, Office of the Under Secretary for Intelligence
Richard Clarke	Good Harbor LLC
Erick Contag	GlobeNet
Kevin Coughlin	Commonwealth Fusion Center
Catherine Creese	U.S. Naval Seafloor Cable Protection Office
Don Diggs	DoD Office of Assistant Secretary of Defense (Networks Information and Integration)/Command and Control Division
Carl Foster	DHS National Communication Systems Office
Mick Green	International Cable Protection Committee
Pete Guevara	JPMorgan Chase
Bill Gunnels	DoD Office of Assistant Secretary of Defense (Networks Information and Integration)/Command and Control Division/National Security Policy Directorate
Mary Ellen Hynes	DHS Science and Technology, IGD Division
Calestous Juma	Harvard Kennedy School
Kim King	Department of Defense (DoD), Office of the Secretary, Office of the Under Secretary for Intelligence, Joint & Coalition Warfighter Support Division
Thomas Lehrman	Bolivien, LLC
David Lloyd	Hibernia Atlantic

Nicholas Lordi	Telcordia Technologies, Inc.
Anil Macwan	Bell Labs
Tim Malin	Formerly with Global Crossing
Maneck Master	Telcordia Technologies, Inc.
Tom Matthews	Department of Defense (DoD), Office of the Secretary, Office of the Under Secretary for Intelligence, Joint & Coalition Warfighter Support Division
John Marino	Davis Ross Group
Alan Mauldin	Telegeography
Hunter Newby	Allied Fiber
Fred Nichols	Office of Assistant Secretary of Defense (Networks Information and Integration)/Command and Control Division/National Security Policy Directorate
Karl Rauscher	IEEE, ROGUCCI Summit
Julian Rawles	Pioneer Consulting
Keith Schofield	Pioneer Consulting
Michael Silevitch	DHS ALERT Center/Northeastern University
Tom Sheahan	Northeastern University
Paul Stoddart	Australian Government, Attorney General's Department
Neil Tagare	BuySellBandwidth, Inc.
Mishac Yegian	Northeastern University
Albert Zhang	Harvard University, SEAS

BIBLIOGRAPHY

Connecting America: The National Broadband Plan, the Federal Communications Commission, March 16, 2010.

Cyberspace Policy Review, The White House, May 2009.

Department of Defense Instruction, "Critical Program Information (CPI) Protection Within the Department of Defense," July 16, 2009.

International Collaboration on Cyber Security Research and Development: Leveraging Global Partnerships for the Security of Free Nations and All Sector Preparedness and Response, NSTAC's Industry Executive Subcommittee's Research and Development Task Force, September 21-22, 2006.

National Strategy for Maritime Security: National Plan to Achieve Maritime Domain Awareness, The White House, September 2005

NSPD 54/HSPD 23 - *The Comprehensive National Cybersecurity Initiative,* The White House, March 2, 2010.

NSTAC: Cyber Collaboration Report, NSTAC May 21, 2009.

NSTAC Response to the Sixty-Day Cyber Study Group, NSTAC, March 12, 2009.

NSTAC Report to the President on International Communications, NSTAC, August 16, 2007.

NSTAC Report to the President on Emergency Communications and Interoperability, NSTAC, January 16, 2007.

NSTAC Global Infrastructure Resiliency Report, NSTAC, December 2006.

"C&W close to landing second multi-million dollar submarine cable," Telegeography.com, July 6, 2009.

"Hotter under the water: A look at the undersea Internet cable 'conspiracy' and the impact on global networks," February 07, 2008. www.networkperformancedaily.com/2008/02/hotter_under_the_water_a_look_1.html

"Meeting Minutes for July 19, 2007," Critical Infrastructure Partnership Advisory Council

James Bamford, “Big Brother Is Listening,” *The Atlantic Online*, April 2006.

Robert Bannon and Douglas Burnett, “Submarine Cable Infrastructure Defense Against Terrorist Aggression,” IEEE paper, 2005.

Ken Beauchamp, *The History of Telegraphy*, 2001.

Martin Brown, Alin Popescu, Todd Underwood, Earl Zmijewski, “Aftershocks from the Taiwan Earthquakes: Shaking Up Internet transit in Asia,” NANOG 42, February 2008.

Jos Chesnoy, *Undersea fiber communication systems*. Amsterdam; Boston: Academic Press, 2002.

Richard A. Clarke, *Breakpoint*, 2007

Lewis Coe, *The telegraph: a history of Morse's invention and its predecessors in the United States*. Jefferson, N.C. : McFarland, 1993

Gillian Cookson, *The Wire That Changed the World*, 2003

Mike Copeland, “Grande restores Waco cable service after limited disruption,” *Waco Tribune*, July 9, 2009.

Christopher Dickey, “The Surveillance-Industrial Complex,” *The New York Times*, January 11, 2009.

Andrew Donoghue, “Undersea cables extremely vulnerable say analysts,” ZDnet.co.uk, February 7, 2008

Doshea, “Telegeography: Trans-Atlantic bandwidth need increasing,” www.fiercetelecom.com June 22, 2009.

Nick Farrell, “Sharks ‘innocent’ of web cable attack,” vnunet.com, October 2, 2001.

Melody Flowers and Rob Knake, “Making Homeland Security Pay Dividends,” Harvard Kennedy School PAE, 2005.

R. K.T. Fong, “Global Submarine Cable Systems – Sustainable Growth or Stagnation,” IEEE.org, 2004.

Bill Glover, “History of the Atlantic Cable & Undersea Communications,” Atlantic-Cable.com

John Steele Gordon, *A Thread Across the Ocean: the heroic story of the transatlantic cable*, 2002

Daniel Headrick and Pascal Griset, “Submarine Telegraph Cables: Business and Politics, 1838-1939,” *The Business History Review*, Volume 75, No. 3., Autumn 2001, pages 543-578.

Chester G. Hearn, *Circuits in the Sea: The Men, the Ships and the Atlantic Cable*, 2004

Jeff Hecht, *City of light: the story of fiber optics*, 1999.

Stacey Higginbotham, “The Coming Trans-Atlantic Bandwidth Crunch,” June 22, 2009.

Gordon Housworth, “Submarine fiber optic cable breaks: a study in hysteria and ignorance against analysis,” Intellectual Capital Group, February 10, 2008.

Peter J. Hugill, *Global communications since 1844: geopolitics and technology*. Baltimore, Md.: Johns Hopkins University Press, 1999

Isabella Field Judson, *Cyrus W. Field, his life and work [1819-1892].* New York: Harper & Brothers, 1896.

Howard Kidorf, “Current Status of the Submarine Fiber Optics Market,” A presentation to NANOG45, Pioneer Consulting, January 27, 2008.

Howard Kidorf, “Submarine System Owner’s View,” A presentation to NANOG45, Pioneer Consulting, January 27, 2008.

Gary Kim, “Higher Trans-Atlantic Capacity Prices by 2014,” TMCnet.com, June 22, 2009.

Sylvie LaPerriere, “Taiwan Earthquake Fiber Cuts: a Service Provider View,” NANOG39, Febraury 5, 2007.

Grahame Lynch, “The new bandwidth barons: buying binge shifts global fiber assets from American to foreign ownership,” America’s Network, February 2005.

Linda Main, "The Global Information Infrastructure: Empowerment or Imperialism?" *Third World Quarterly*, Volume 22, No. 1 (Feb 2001), pages 83-97.

E.A. Marland, *Early electrical communication*, 1964.

Michael Morris, "The Incredible International Submarine Systems," Networkworld.com, April 19, 2009.

O'Reilly, "Cable cuts, conspiracies, and submarines…" O'Reilly Radar, February 4, 2008.

Petrony, "Verizon to sue organizers of cable attack that cut cable," *Ecommerce Journal*, April 20, 2009.

Alin Popescu, Todd Underwood, Earl Zmijewski, "Quaking Tables: The Taiwan Earthquakes and the Internet Routing Table," NANOG 39, February 2007

Ron Rapp, Mark Lawrence, Dick Borwick, Takuo Kuwabara, "Marine Survey and Cable Routing," Sub Optic 2004 Short Course, Submarine Cable Improvement Group, www.scig.net

Michael Ruddy, "An Overview of International Submarine Cable Markets," Executive Telecom Briefings, Boston University, December 12, 2006.

Michael Ruddy, "The Worldwide Submarine Cable Markets and the State of African Submarine Communications," Submarine Networks Africa, Johannesburg, November 27-28, 2007.

Robert Sabine, *The history and progress of the electric telegraph; with descriptions of some of the apparatus*, 1869.

Marcus Sachs and Jared Mauch, "Communications Sector and Information Technology Sector," Presentation to NANOG, June 15, 2009.

Mark Schneier, "Fourth Undersea Cable Failure in Middle East," Schneier on Security blog, February 5, 2008.

Keith Schofield, "Enabling Global Communication – From Risk to Reward: Why we must learn our own lessons before we change risk management behavior?" Pioneer Consulting, Sub Optic 2007 paper.

Seymour Shapiro, “Research & Security Applications of Submarine Technologies,” Tyco Telecommunications, Sup Optic 2007 paper.

Seiichi Shimura, *International submarine cable systems*. Tokyo, Japan: KDD Engineering and Consulting, 1984.

Su Shin, “Sandwich Isles Communications Unveils New Undersea Cable,” *Honolulu Advertiser.com*, June 26, 2009.

Dan Verton, BLACK ICE: THE INVISIBLE THREAT OF CYBER-TERRORISM, McGraw-Hill Osborne, 2003.

Graham White, “Telecoms Trade Disruption Insurance: A Different View on Revenue,” Submarine Telecom Forum.

Henry Daniel Wilkinson, *Submarine cable laying and repairing*, 1896.

Jonathan Reed Winkler, *Nexus: Strategic Communications and American security in World War I*. 2008

Appendix A: Definitions of Note

Undersea Communications Cable (commonly referred to as Submarine Cable)

These cables range in diameter from 17 millimeters to 69 millimeters[136]; that width places them between the size of a human thumb and a human wrist. Within 2,000 meters of a coastline, cables are typically armored, or even double-armored, and are buried upwards of 3 meters of seabed (see cable diagram below).[137] These measures protect the cable from fisherman trawling and ships anchoring around the shore. Outside of 2,000 meters, some cables may be buried in the seabed further, but they typically are unarmored in a Kevlar-coating.[138]

Many times though, the unarmored cable sits unprotected on the ocean floor. In this state, they can stretch for thousands of miles across the ocean floor, upwards of 12,000 kilometers in some cases, carry up to 10 terabytes per second of data and ensure traffic availability 99.999% of the time.[139] Cables

[136] See Kordje Bedourma, Memorandum to African Development Bank Regarding GHANA & NIGERIA: MAIN ONE SUBMARINE CABLE, January 6, 2009. Accessed at http://www.afdb.org/fileadmin/uploads/afdb/Documents/Environmental-and-Social-Assessments/30776237-EN-ESIA-REPORT-MAIN-ONE-SYSTEM-POSTING-JAN-09.PDF. Also see 2008 *Guardian (UK)* map, accessed at http://image.guardian.co.uk/sys-images/Technology/Pix/pictures/2008/02/01/SeaCableHi.jpg

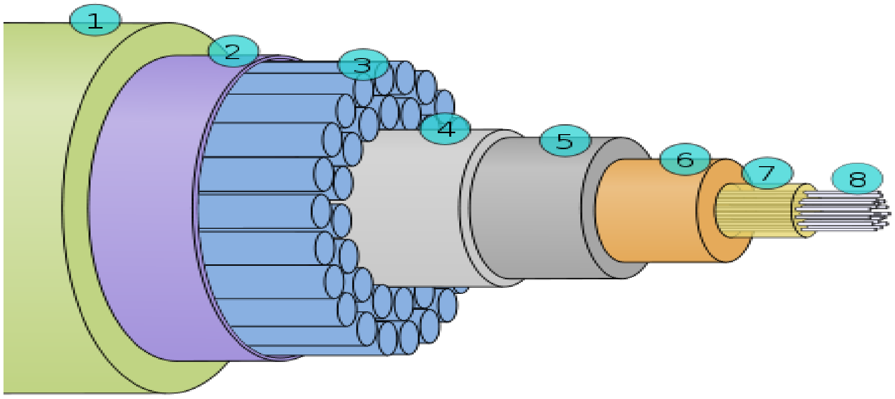
[137] "Framework for Burial Depth Specifications," Submarine Cable Improvement Group (SCIG). Accessed at http://www.scig.net/Section05.pdf

[138] Cathy Holding, "A global cable network of fragile links," *The Independent (UK)*, March 10, 2009. Accessed at http://www.independent.co.uk/news/business/sustainit/a-global-cable-network-of-fragile-links-1640448.html

[139] Laurie Doyle presentation, PTC 2007 conference.

can be laid to water depths of 8,000 meters and can withstand pressure of 10,000 psi.[140]

It can take at least 3-4 months to lay an undersea cable, depending on distance. But it can take a company or consortium of companies several years before it reaches the point to build. Drafting the construction and maintenance agreement and receiving the necessary permits from federal, state and local officials fills much of that time. Moreover, it costs generally $500 million to lay a new trans-oceanic cable system today.[141] See below for a cross-section of an undersea communications cable.[142]



Layers:

1. Polyethylene
2. "Mylar" tape
3. Stranded metal (steel) wires

[140] Maurice E. Kordahi, Seymour Shapiro, Gordon Lucas and Kelvin Moore, "International Standards For Undersea Cable System Testing," Submarine Cable Improvement Group (SCIG), http://www.scig.net/Section11b.pdf

[141] Resilient International Telecommunication Guidelines for the Financial Services Sector, Financial Services Sector Coordinating Council, August 2009. See page 13. Accessed at https://www.fsscc.org/fsscc/reports/2009/FSSCC-ResilientInternationalTelecommunicationsGuidelines_20090803-Version1_9-Final.pdf

[142] See picture from http://en.wikipedia.org/wiki/File:Submarine_cable_cross-section_3D_plain.svg

4. Aluminum water barrier
5. Polycarbonate
6. Copper or aluminum tube
7. Petroleum jelly
8. Optical fibers

Cable Outage

One recent report explains that “there exists no definition for what a cable outage is and there is currently no reporting standard on cable outages.”[143] Moreover, “no common methodology for capturing and characterizing the attributes of an outage” exists within the industry.[144] “Cable fault” or a “cable cut” is used interchangeably in many instances. The term cable outage is even “undefined in SCIG’s “Standard Definitions” webpage.”[145] As discussed earlier, cable cuts rarely occur; instead, cable is bent beyond its “bending radius”[146] causing the cable to fray or splice in one area, making it unusable.

Submarine Landing Terminal Equipment (SLTE)

SLTE is the necessary piece of equipment that connects the undersea (commonly referred to as “wet”) link with the land (commonly referred to as “dry”) links. It is housed within the cable landing station.

[143] Spilios Makris and Nick Lordi, “Analysis of Newsworthy Undersea Cable Infrastructure Outages (1999 – 2009),” Telcordia, Inc. Presentation delivered to ROGUCCI conference 2009. Also see Spilios Makris, “'Undersea Cable System Outages and Global Infrastructure Resiliency – A Discussion of Issues in Managing Third-Party Expectations,” Presentation delivered to IEEE. Accessed at http://www.ieee-cqr.org/2009/FINAL%20UPLOAD/DAY%203%20-%20THR/SPILIOS%20MAKRIS%20-%20Lordi_CQR2009_final.pdf

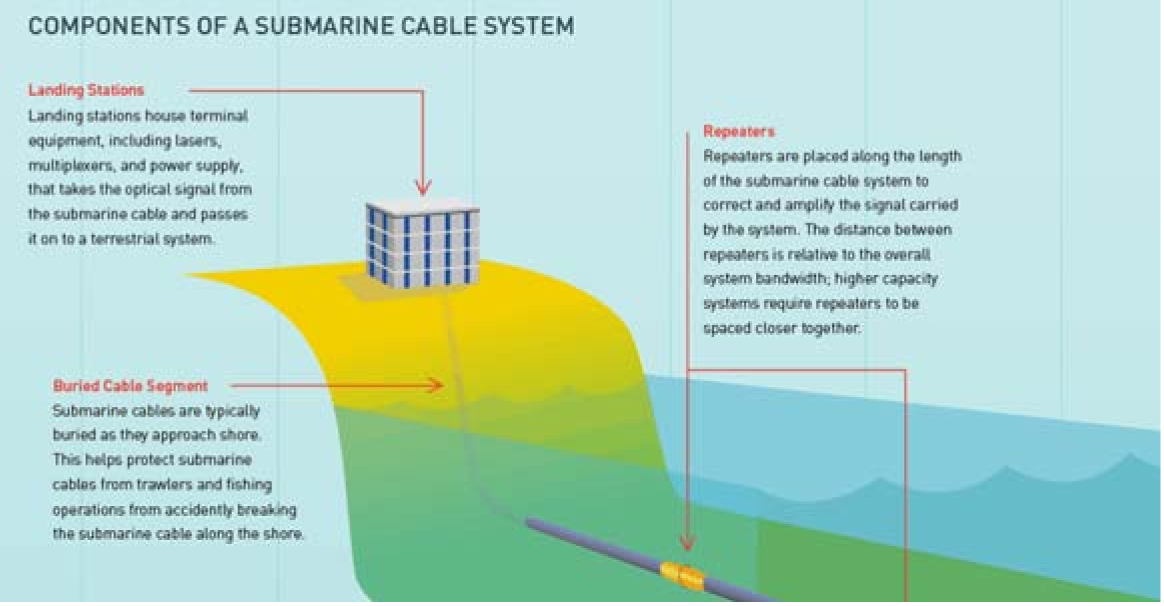
[144] Ibid.

[145] Ibid.

[146] Vivek Alwan, “Fiber-Optic Technologies,” Cisco Press, April 23, 2004. Accessed at http://www.ciscopress.com/articles/article.asp?p=170740&seqNum=10

Cable Landing Station

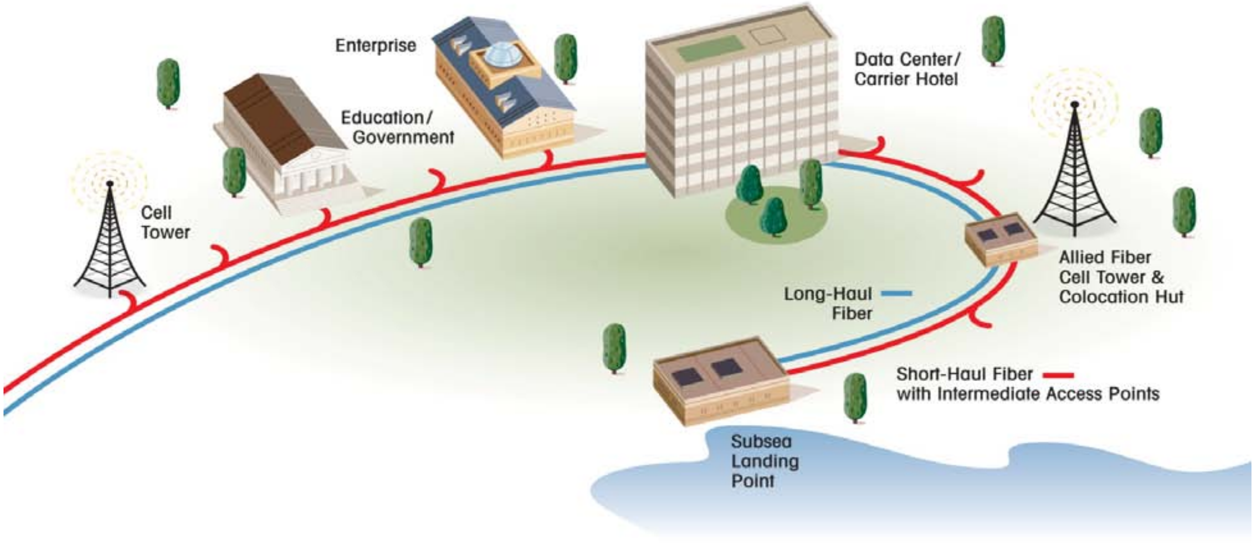
The cable landing station is the location where the undersea cable terminates before the signal is translated. Many times they come through the equivalent of a manhole cover to enter the facility through the ground. On average, 3-10 cable systems land in a typical landing station, making them highly significant parts of the undersea cable system.[147]


COMPONENTS OF A SUBMARINE CABLE SYSTEM
Landing Stations
Landing stations house terminal equipment, including lasers, multiplexers, and power supply, that takes the optical signal from the submarine cable and passes it on to a terrestrial system.
Repeaters
Repeaters are placed along the length of the submarine cable system to correct and amplify the signal carried by the system. The distance between repeaters is relative to the overall system bandwidth; higher capacity systems require repeaters to be spaced closer together.
Buried Cable Segment
Submarine cables are typically buried as they approach shore. This helps protect submarine cables from trawlers and fishing operations from accidently breaking the submarine cable along the shore.

Source: Components of a Submarine Cable System, Infranetlab.com[148]

[147] Remarks by Neil Tagare, "Wanted ASAP: A Global Mesh Disaster Recovery and Restoration Network," Presentation to PTC 2010 conference, January 19, 2010. Accessed at http://www.ptc.org/ptc10/program/images/papers/slides/Slides_Neil%20Tagare_Emg%20Com%20Wkshop.pdf

[148] Picture accessed at http://images.google.com/imgres?imgurl=http://infranetlab.org/blog/wp-content/uploads/2008/09/08_09_05_sub_cable_schematic.jpg&imgrefurl=http://infranetlab.org/blog/2008/09/rewiring-telegeography/&usg=__cMnCiVuzTz--E_hLFxi3Ij4gHXs=&h=300&w=580&sz=118&hl=en&start=116&um=1&tbnid=7EcGPeFpOmUwdM:&tbnh=69&tbnw=134&prev=/images%3Fq%3DSubmarine%2Bcables%2Bsystem%2Bnetwork%26ndsp%3D18%26hl%3Den%26rls%3DSNCA,SNCA:2009-46,SNCA:en%26sa%3DN%26start%3D108%26um%3D1


Enterprise
Data Center/ Carrier Hotel
Education/ Government
Cell Tower
Allied Fiber Cell Tower & Colocation Hut
Long-Haul Fiber
Short-Haul Fiber with Intermediate Access Points
Subsea Landing Point

Source: Allied Fiber, http://www.alliedfiber.com/images/AF_SystemModel_art1.jpg

Appendix B: Cable Topologies

Linear systems

In these systems, a single cable connects from one location to another. If the cable suffers an outage, all customers using just that cable for service will lose it entirely. Most cable systems were linear until the mid-1990s.

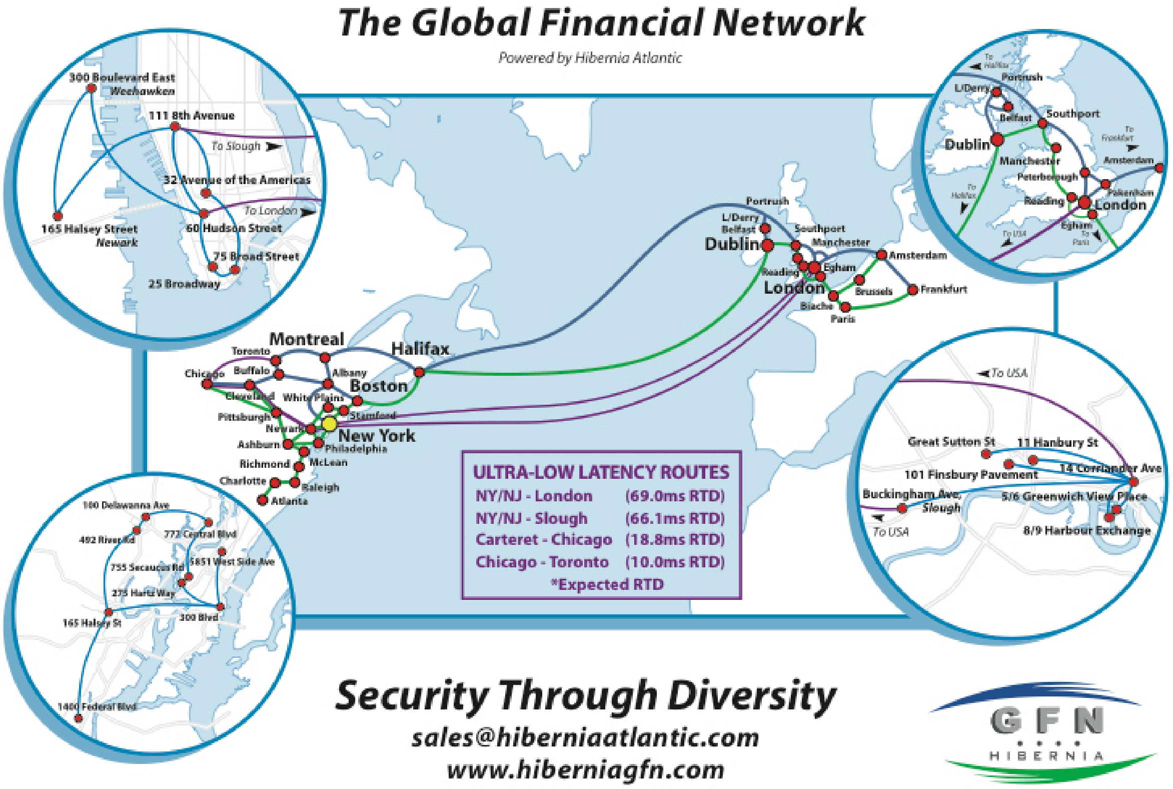
Ring systems

Most every cable system is created using a ring topology. A ring network provides redundant data traffic to the same location along two or more separate cable lines. Below is a diagram of Hibernia Atlantic's ring network across the Atlantic.[149] One half of the system extends from Boston to Halifax to Dublin, while the other half travels from Montreal to Halifax to Southport, UK. Boston and Montreal, as well as Dublin to Southport, are connected over terrestrial cable in order to restore connectivity instantly should one half of the cable go down. Thus the reason it is categorized as a ring.

To make the ring system work correctly, each cable line has a series of fiber optics inside, some of them with data communications running through them (called 'lit capacity') and other lines with no data traffic running through them (called 'dark' or 'unlit capacity'). When one half of the ring suffers an outage, the other system essentially "turns on" its 'dark capacity' to take on the downed system's 'lit capacity.' The process of turning on 'dark' or spare capacity on the other line can happen so fast that if you are on a telephone call and the cable goes down, it can get rerouted without the caller noticing a blip in the service. When the 'unlit' portion of a cable system takes on excess capacity, it can come close to maximum capacity in certain circumstances. Therefore, if both segments of the ring network suffer an outage, the

[149] Hibernia Atlantic's Global Financial Network, accessed via http://www.hiberniametro.com/images/GFNMap.jpg

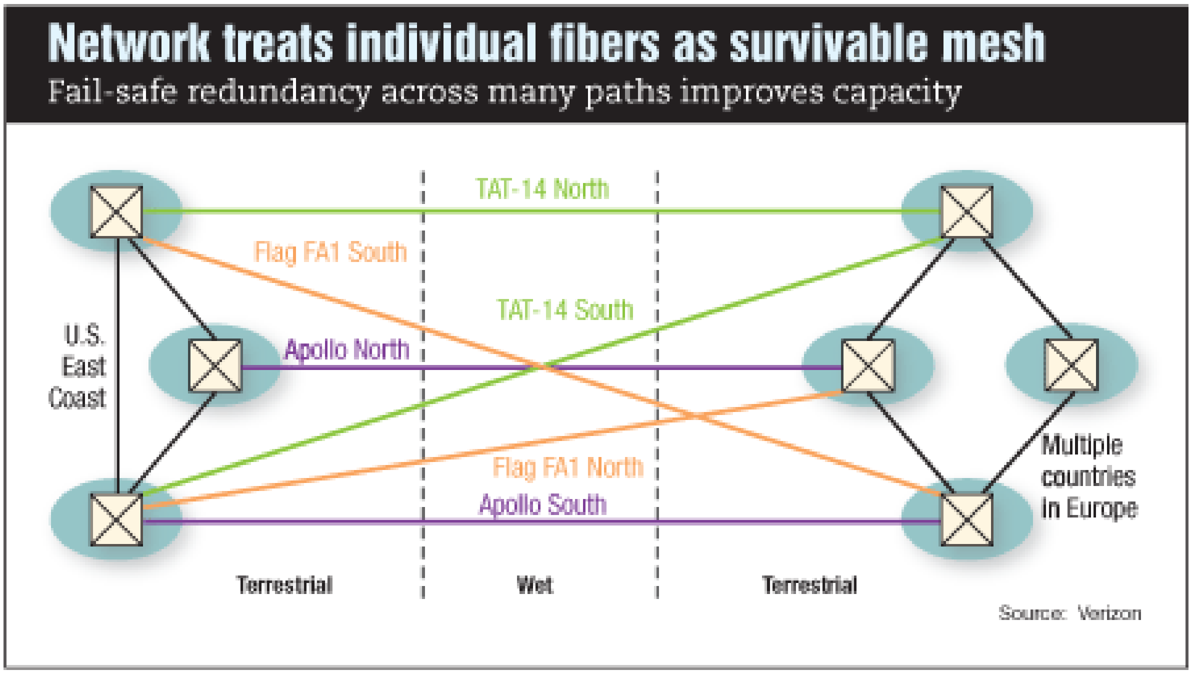
customers who use that cable for their traffic only will suffer a complete loss of service. Some customers, or network operators in charge of telecommunications service, have now switched to mesh networking to avoid the loss of a ring system.



Source: Hibernia Atlantic website,
http://www.hiberniametro.com/images/GFNMap.jpg

Mesh systems

Mesh networking allows for cable traffic to be routed over two or more fully redundant paths in order to reach its intended destination. Each cable landing station is connected to two or more undersea cables *and* to two or more terrestrial systems. Ciena Corp. (Linthicum, Md.), AT&T, Verizon Business, Internet 2 newbie Tata Teleservices (India) and more than 30 other carriers and service providers are switching from antiquated, point-to-point or ring networks to mesh topologies.[150] Verizon, for instance, can restore transpacific traffic in seven different ways should ring systems suffer complete outages. Two depictions of Verizon's mesh networking are found below.[151]


Network treats individual fibers as survivable mesh
Fail-safe redundancy across many paths improves capacity
TAT-14 North
Flag FA1 South
TAT-14 South
Apollo North
U.S. East Coast
Flag FA1 North
Apollo South
Multiple countries in Europe
Terrestrial
Wet
Terrestrial
Source: Verizon

Source: Dane Cooperson, "Undersea networks: Traffic growth and resiliency in the spotlight," 25 May 2007. Ovum report. Pages 6 and 8.

[150] R. Colin Johnson, "Self-healing mesh optical nets emerge," *EE Times*, April 25, 2008. Accessed at http://www.eetimes.com/showArticle.jhtml?articleID=207402005

[151] Accessed at http://www.eetimes.com/showArticle.jhtml?articleID=207402005 and http://www.ciena.com/files/Survivable_Submarine_Optical_Networks_A4_WP-wOvum_Foreword.pdf

Appendix C: Data on Cables Landing in the U.S.

The following analysis shows a total of 29 active cable systems land in the U.S. The specifics of each system are listed below. It is clear that many of the systems arrive in similar or nearby locations in many countries. In many instances, systems are owned by a consortium of companies, some of which are foreign-owned. Below shows the geographic locations of all cables systems entering the East and West Coast of the U.S. The map is somewhat dated[1], but the information is up-to-date. Thereafter, a summary of all active cable systems entering the U.S. is provided, including pertinent details about each line. All data has been personally compiled from Terabit Consulting's 2002 Undersea Cable Report, Teleography maps and Wikipedia entries on each cable system.

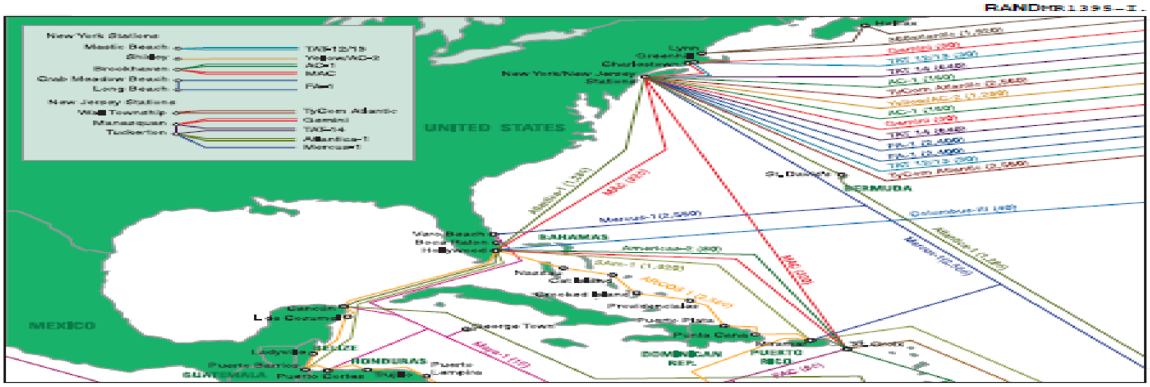


Figure I.5—Submarine Cables Terminating on the East Coast

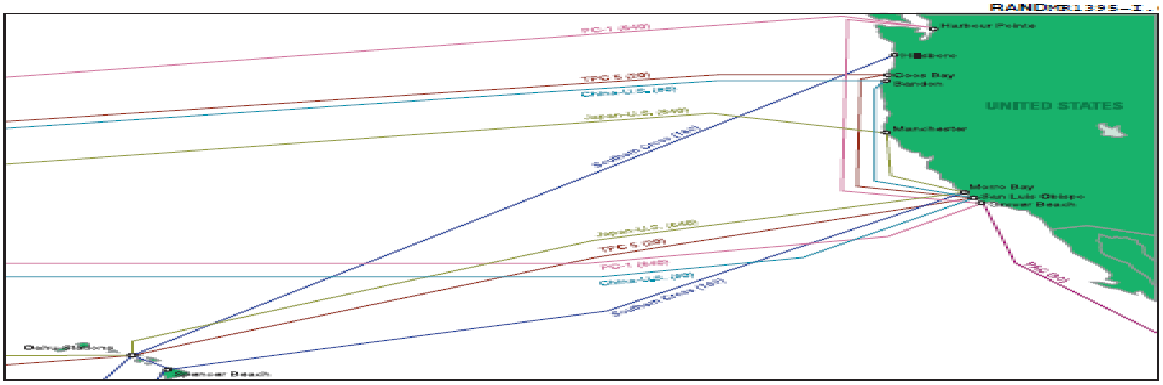


Figure I.6—Submarine Cables Terminating on the West Coast

Source: Frank Lacroix, et al., A Concept of Operations for a New Deep-Diving Submarine, Rand Corporation, 2003. Page 148.

EAST COAST CABLES*

System	Cost	Length	Owners	Years of service	Max Capacity	Landing Station
TAT-14	$1.5 bil.	15,000 km	50 carriers have owners	9 years	640 Gbps	Manasquan, NJ; Tuckertron, NJ; Blaabjerg, Denmark; St. Valey, France; Norden, Germany; Katwijk, Netherlands; Bude-Haven UK
Hibernia Atlantic	$880 mil	11, 700 km	Hibernia Atlantic	9 years	10.16 Tbps	Lynn, MA; Halifax, Nova Scotia; Dublin, Ireland; Southport, UK
Atlantic Crossing-1	$875 mil	14,000 km	Tyco/Global Telesystems Ltd	11 years	120 Gbps	Shirley, NY; Whitesand Bay, UK; Sylt, Germany; Beverwijk, Netherlands
Apollo	$1.2 bil	13,000 km	Apollo Submarine Cable System Ltd.	7 years	3.2 Tbps	Shirley, NY; Manasquan, NJ; Bude, UK; Lannion, France
VSNL Transatlantic	$800 mil	12,500 km	Videsh Sanchar Nigam Limited	9 years	5.12 Tbps	Wall Township, NJ; Brean, UK

System	Cost	Length	Owners	Years of service	Max Capacity	Landing Station
TAT 12/13	$750 mil	12,500 km	AT&T, BT; France Telecom; Cable and Wireless; Deutsche Telekom; Teleglobe; Telefonica; Marconi; Telecom India; Sprint; Worldcom and (64 other carriers)	15 years	20 Gbps	Shirley, NY; Greenhill, RI; Mastic Beach, NJ; Land's End, UK; Penmarch, France
FLAG Atlantic 1	$1.1 bil	12, 570 km	FLAG Telecom	9 years	2.4 Tbps	Crab Meadow, NY; Long Beach, NY; Cornwall, UK; Plerin, France
Yellow/Atlantic Crossing 2	$700 mil	N/A	Level 3 Communications; Global Crossing, Ltd.	10 years	640 Gbps	Bellport, NY; Bude, UK
Mid-Atlantic Crossing	$230 mil	7,500 km	Global Crossing	10 years	40 Gbps	Brookhaven, NY; Hollywood, FL; St. Croix, VI
360Americas	$1.183 bil	24,350 km	Brasil Telecom	10 years	1.28 Tbps	Tuckerton, NJ; Boca Raton, FL; St. David, Bermuda; Rio de Janeiro, Brazil; Fortaleza, Brazil; Maiquetia, Venezuela
Columbus III	$243 mil	10,000 km	30 owners	11 years	20 Gbps	Hollywood, FL; Azores Islands; Lisbon Portugal; Conil, Spain; Sicily, Italy

System	Cost	Length	Owners	Years of service	Max Capacity	Landing Station
Caribbean Crossing	$30 mil	557 km	Caribbean Crossings	9 years	960 Gbps	Boca Raton, FL; Hunters, Grand Bahama; Cave's Point, Bahamas; Eleuthera, Bahamas; Sandy Point, Bahamas;
ARCOS	$300 mil	8,400 km	20 companies	9 years	960 Gbps	North Miami, FL; Cancun, Mexico; Tulum, Mexico; Ladyville, Belize; Puerto Barrios, Guatemala; Puerto Cortes, Honduras; Trujillo, Hondorus; Puerto Cabezas, Nicaragua; Bluefields, Nicaragua; Puerto Limon, Costa Rica; Maria Chiquita, Panama; Ustopo, Panama; Cartagena, Colombia; Riohacha, Colombia; Punto Fijo, Venezuela; Willemstad, Curacao; San Juan, Puerto Rico; Punta Cana, Dominican Republic; Puerto Plata, Dominican Republic; Providenciales, Turks and Caicos; Crooked Island, Bahamas; Nassau, Bahamas

System	Cost	Length	Owners	Years of service	Max Capacity	Landing Station
Bahamas 2	$28 mil	473 km	AT&T, MCI, St. Thomas ad San Juan Telephone Company; Telefonica Larga Distancia de Puerto Rico	13 years	10 Gbps	Vero Beach, FL; Grand Island, Bahamas; Nassau, Bahamas
Maya 1	$207 mil	4,400 km	20 companies	10 years	20 Gbps	Hollywood, FL; Half Moon Bay, Cayman Islands; Tolu, Colombia; Puerto Limon, Costa Rica; Puerto Cortes, Mexico; Maria Chiquita, Panama
South America-1	N/A	22,000 km	Telefonica	10 years	1.92 Tbps	Boca Raton, Florida; Isla Verde, Puerto Rico; Fortaleza, Brazil; Salvador, Brazil; Rio de Janeiro, Brazil; Santos, Brazil; Las Toninas, Argentina; Valparaiso, Chile; Arica, Chile; Lurin, Peru; Puerto San José, Guatemala; and Puerto Barrios, Guatemala
Americas II	$375 mil	N/A	AT&T, MCI, Sprint and 27 other companies	12 years	2.5 Gbps	Hollywood, Florida, Fortaleza, Brazil; Cayenne, French Guyana; Chaguaramas, Trinidad; Camuri, Venezuela; Willemstad, Curacao; Le

						Lamentin, Martinique; St. Croix, USVI; and Miramar, Puerto, Rico[152]
Gemini-Bermuda[153]	$22 mil (upgraded)	1333 km	Verizon, Cedar Cable Ltd.	2 years	20 Gbps	Charleston, Rhode Island, Paget Bermuda

[152] Cable Landing License, FCC, November 10, 1998. Accessed at http://www.fcc.gov/Bureaus/International/Orders/1998/da982295.txt

[153] Information gathered from "Cable & Wireless Dish to be Replaced with Enhanced Cable System," Cable & Wirless press release, June 19, 2007 and Application for a Cable landing License, FCC, 2008. Accessed at http://licensing.fcc.gov/ibfsweb/ib.page.FetchAttachment?attachment_key=-148838

WEST COAST CABLES

System	**Cost**	**Length**	**Owners**	**Years of service**	**Max Capacity**	**Landing Station**
VSNL Transpacific	N/A	N/A	Videsh Sanchar Nigam Limited	8 years	9.6 Tbps	Hillsboro, OR; Los Angeles, CA; Piti, Guam; Emi, Japan; Toyohashi, Japan
Pacific Crossing 1	$1.3 bil	21,000 km	Global Crossing; Microsoft; Softbank; Goldman Sachs	9 years	640 Gbps	Grover Beach, CA; Harbour Pointe, WA; Ajigaura, Japan; Shima, Japan
Southern Cross	$1.1 bil	28,900 km	Southern Cross Cables Limited	10 years	1.2 Tbps	Nedonna, OR; Morro Bay, CA; Spencer Beach, HI; Kahe Point, HI; Suva, Fiji; Takapuna, New Zealand
China-US	$1.1 bil	27,000 km	Over 40 companies	10 years	80 Gbps	San Luis Obispo, CA; Bandon, OR; Pusan, Korea; Chongming, China; Fangshan, Taiwan; Shantou, China; Okinawa, Japan; Tanguisson, Guam
Japan-US	$1.15 bil	21, 000 km	At least 33 companies	9 years	1.28 Tbps	Makaha, HI; Manchester, CA; Morro Bay, CA; Maruyama, Japan; Kitaibaraki, Japan
TPC 5	$1.24 bil	22,560 km	AT&T, KDD and 78 others	13 years	20 Gbps	San Luis Obispo, CA; Keawaula, HI; Bandon, OR; Tumon Bay, Guam; Miyazaki, Japan; Ninomiya, Japan

System	Cost	Length	Owners	Years of service	Max Capacity	Landing Station
FLAG NGN	$1.5 bil	N/A	N/A	2 years	2.56 Tbps	Morro Bay, CA;Twin Rocks, Astoria or Brandon, OR; Wada, Japan
TPE	$500 mil	17,700 km	China Telecom; China Netcom; China Unicom; Chunghwa Telecom; Korea Telecom; Verizon Communications	2 years	5.12 Tbps	Nedonna Beach, CA; Tanshu, Taiwan; Qingdao, China; Chongming, China; Keoje, South Korea
Pan American Crossing (PAC)[154]	N/A	10,000 Km	Global Crossing	9 years	20 Gbps	Grover Beach, Calif., Tijuana, Mexico, Mazatlan, Mexico, Esterillos, Costa Rica, and Fort Amador, Panama
Asia America Gateway	$500 mil	20,000 km	17 companies	None	2.88 Tbps	Hawaii; Guam; Philippines; Hong Kong; Malaysia; Singapore; Thailand; Brunei; Vietnam
Telstra Endeavour	$275 mil	9,000km	Telstra	2 years	1.92 Tbps	Tamarama Beach, Sydney, Australia; Paddington, Sydney, Australia; Oahu, Hawaii

[154] Information collected from “Global Crossing Boosts Undersea Capacity to Meet Surging Latin America Demand,” Global Crossing press release, March 10, 2010. Accessed at http://www.nearshoreamericas.com/latin-america-undersea-fiberglobal-crossing/2872/ and “Global Crossing Completes Pan American Crossing Link,” Global Crossing press release, JANUARY 25, 2001. Accessed at http://www.convergedigest.com/Bandwidth/newnetworksarticle.asp?ID=3247

	SUMMARY					
TOTAL: 29 active systems (East Coast=18; West Coast=11)	**$19.08 billion** **(ave. cost = $763 mil.)**	**347,443 kms** **(average of 13,8974 km per system)**	**At least 67 different companies with some stake of ownership**	**247 years** **(average age is 8.5 years)**	**At least 52.85 Tbps capacity** **(East Coast = 27.53 Tbps; West Coast = 25.32 Tbps)**	**48 different countries** **(164 landings, including 55 in the U.S. in 32 distinct locations)**

***All information compiled from Terabit Consulting's 2002 Undersea Cable Report, Telegeography maps and Wikipedia entries for each system, unless otherwise noted.**

APPENDIX D: Recent Cable Breaks and Thefts

1. Algeria 2003

EVENT: On May 21, 2003, a 6.8 magnitude earthquake affected the Bourmerdes region, outside the coast of Algeria.[155] The earthquake occurred 7km offshore at a boundary between the European and Asian tectonic plates. A tsunami 2 meters high traveled across the Mediterranean Sea, turbidity currents generated extensive submarine landslides.

DAMAGE: The earthquake killed 2,266, injured 10,261 and caused extensive structural damage to the city of Bourmerdes and elsewhere in the country. The undersea landslides generated from the earthquake cut undersea cables approximately "45 km offshore from the epicentral area and disturbed the telecommunications link between Europe and several other countries in Asia and the Middle East."[156] Overall, undersea landslides damaged 5 telecommunications cables.[157]

IMPACT: It took 4 cable ships 6 weeks to fix all the cables.[158] One repair involved replacing a 120 km section of cable. All things considered, the earthquake caused an estimated US$100 million in damage.[159]

[155] A. AYADI, et. al., "Strong Algerian Earthquake Strikes Near Capital City," Eos, Vol. 84, No. 50, 16 December 2003. Accessed at http://atlas.cc.itu.edu.tr/~cakirz/papers/ayadi_etal_2003_EOS.pdf

[156] Ibid.

[157] ICPC, "Critical Infrastructure: Submarine Telecommunication Cables," Accessed at www.iscpc.org/publications/Critical_Infastructure_2009_V2.pps

[158] Ibid.

[159] Ibid.

2. Pakistan 2005

EVENT: On June 27, 2005, the only undersea communications cable connecting Pakistan with the rest of the world was disrupted. According to the repair company, the possible cause "was the fishing activity around the affected area," and "that an anchor of a fishing trawler had got entangled which ruptured the cable."[160] The disruption occurred 11-12 km from the port of Karachi.

DAMAGE: The breaks were significant. At the time, "Pakistan was the only country in the region that relies on a single cable. There were no backup cable, no disaster recovery strategy and no business continuity plan in place."[161]

Despite this plan, business suffered from the lost connection. As one airline director noted, "all our business including reservations, ticketing, check-ins and 500 agents all around the world are web-based and it was all affected badly. We had to switch to manual work and that was very difficult for us. Besides, we suffered severe damage to our market credibility."[162]

IMPACT: It took two cable repair ships over 11 days to fix the fault in the SEA-ME-WE-3 cable. According to an official from the Pakistani Internet service providers union, 10 million online subscribers in Pakistan went without internet service for more than a week because of the fault.[163] All e-services were affected, particularly the burgeoning Pakistani call center industry. As the President of the Call Centres

[160] "Submarine cable: IT ministry preparing load-sharing plan," Pak Tribune, February 14, 2006. Accessed at http://www.paktribune.com/news/index.shtml?134126

[161] Hayyan Faisal, "Task to detect major Fault in Pakistan's Internet cable Set Off," *Pakistan Times*, July 2005. Accessed at http://pakistantimes.net/2005/07/04/top1.htm

[162] "Bad weather obstructs Pakistan's Fiber Optic cable repair Work" *Pakistan Times Staff Report,* July 5, 2005. Accessed at http://pakistantimes.net/2005/07/05/top6.htm

[163] Faisal, Pakistan Times.

Association of Pakistan stated, "It has definitely caused millions of dollars in potential losses and a lot of intangible damage you cannot quantify."[164]

The loss of telecommunications in a country of size and scope of Pakistan reverberated with its trading partners. Several multinational IT and telecom contracts were cancelled, most notably a $10-$20 million investment by Indian call centers. The Indian companies "withdrew the offer as the lingering Internet blackout caused mistrust in India about Pakistan's Telecom infrastructure."[165] India could not outsource their work to Pakistan, fearing that their U.S.-based contracts would be unfulfilled.

RECOVERY: During that outage, 50% of internet subscribers and 20% of international phone callers received a connection via a back-up satellite plan provided by the Pakistani Telecommunications Cable Limited company. The PTCL implemented an ad-hoc tiered restoration structure, providing data access first to banks, airlines and the Pakistani stock exchange access first before all others.

[164] Ibid.

[165] Omair Rasheed, "Standby Net arrangements terminated in Pakistan," *Pakistan Times,* July 6, 2005. Accessed at http://pakistantimes.net/2005/07/06/top5.htm

3. Taiwan 2006

EVENT: On December 26, 2006, a seminal event occurred in the undersea cable industry. An earthquake of at least 6.7 magnitude triggered submarine landslide near the junction of the Eurasian and Philippine tectonic plates. Termed the Hengchun earthquake, the epicenter of the event landed directly in the middle of the heavily cabled Luzon Strait, off the coast of Taiwan. 10 aftershocks greater than 4.7 magnitude also hit the region.[166] From the timing of the breaks, a turbidity current averaging a speed of approximately 20km/hour traveled over 330 km.[167]

DAMAGE: Undersea landslides severed 9 out of 11 cables in the area, moving cables far away from their original routes. Only Asia Netcom's EAC and the Guam-Philippines cable were left online.[168] A total of 21 faults were discovered in the 9 damaged cable systems.[169] The damage extended to water depths of 4000 meters and covered many in tons of mud.[170] It took 11 cable ships (over 40% of the world's entire fleet) until February 15th – a total of 49 days or seven weeks to complete the cable repair work.[171]

[166] 2006 Hengchun earthquake, Wikipedia entry, accessed at http://en.wikipedia.org/wiki/2006_Hengchun_earthquake

[167] ICPC, "Critical Infrastructure: Submarine Telecommunication Cables," Accessed at www.iscpc.org/publications/Critical_Infastructure_2009_V2.pps

[168] Alin Popescu, Todd Underwood, Earl Zmijewski, "Quaking Tables: The Taiwan earthquakes and the Internet Routing Table," Rensys Corporation. Presentation delivered to APRICOT Bali, 2007. Accessed at http://www.renesys.com/tech/presentations/pdf/Plenary2-Underwood.pdf

[169] Ryan Singel, "Fiber Optic Cable Cuts Isolate Millions From Internet, Future Cuts Likely," *Wired Magazine*, January 31, 2008. Accessed at http://www.wired.com/threatlevel/2008/01/fiber-optic-cab/

[170] Ibid.

[171] Ibid.

IMPACT: The day after the earthquake, most people in Hong Kong were "just twiddling their thumbs."[172] Taiwan's international calling capacity to the U.S. was down to 40% its normal capacity.[173] 98% of Taiwan's communications with Malaysia, Singapore, Thailand and Hong Kong was also disrupted.[174] Internet access to China, Hong Kong, Vietnam, Taiwan, Singapore, Japan and the Philippines was seriously impaired. Banking, airline bookings, email & other services in many of these countries, particularly Taiwan and Singapore, were either stopped or delayed.[175]

Financial markets and general commerce were disrupted. A South Korean domestic bank reported that "trading of the Korean won has mostly halted due to the communication problem."[176] Other "securities traders in Hong Kong and Singapore were unable to obtain prices and complete orders… [and] dealers in the region said they have had difficulties accessing international news providers for

[172] Seth Mydans, "The Day the Pixels Froze: When a Digital World Was Stopped by a Natural Disaster," *The New York Times*, December 28, 2006. Accessed at http://www.nytimes.com/2006/12/28/business/28connect.html

[173] Sumner Lemon, "Earthquake disrupts Internet access in Asia," *Computer World Magazine*, December 27, 2006. Accessed at http://www.computerworld.com/s/article/9006819/Earthquake_disrupts_Internet_access_in_Asia?intsrc=news_ts_head

[174] Ibid.

[175] "Taiwan quake causes net blackout," *Reuters*. December 28, 2006. Accessed at http://www.smh.com.au/news/wireless--broadband/taiwan-quake-causes-net-blackout/2006/12/28/1166895395104.html

[176] "Asia communications hit by quake," *BBC News,* December 27, 2006. Accessed at http://news.bbc.co.uk/2/hi/asia-pacific/6211451.stm

information."[177] Customers also had trouble looking up various "stock prices online."[178]

RECOVERY: Some traffic that couldn't be carried on the two remaining undersea cable systems needed to find a different route in order to reach North and South America. One solution was to re-route traffic over terrestrial cables across Asia and through Europe. Despite these ad-hoc arrangements, some delay in internet traffic was still apparent even 2 months after the earthquake.

AFTERMATH: This event forced communication carriers to avoid cable-laying in seismically active areas. A new alliance of communication carriers, called the Pacific Partner Members Committee No. 2, was created after the crisis to deal with the aftermath of the event and how to prevent a future one.

4. Bangladesh 2007

Since connecting its first international undersea communications cable on May 21, 2006, Bangladesh has suffered numerous faults. In little over a year, 22 different faults were reported, either due to accidents, sabotage or thefts.

EVENTS: In November 2007, the Dhaka-Chittagong–Cox's Bazar portion of the SEA-ME-WE-4 submarine cable "was snapped at two points near Cox's Bazar and Feni" twice in one week.[179]

DAMAGE: All international communications to Bangladesh was disrupted for 15 hours during the second outage.

[177] Choe Sang-Hun and Wayne Arnold, "Asian Quake Disrupts Data Traffic," *The New York Times*, December 28, 2006. Accessed at http://www.nytimes.com/2006/12/28/business/worldbusiness/28quake.html?pagewanted=all

[178] Ibid.

[179] Sayeed Rahmna, "Bangladesh Submarine Cable link sabotaged again," Groundreport.com, November 13, 2007. Accessed at http://www.groundreport.com/Media_and_Tech/Bangladesh-Submarine-cable-link-sabotaged-again/2837950

IMPACT: Due to the cuts, the Bangladesh Telegraph and Telephone Board lost revenue on the order of $70,000 per hour.[180]

5. Middle East 2008

EVENT: Between January 23 and February 4th, 2008, "a total of five cables being operated by two submarine cable operators" were damaged in two locations each.[181] The cable SeaMeWe-4 (South East Asia-Middle East-Western Europe-4) near Penang, Malaysia, the FLAG Europe-Asia near Alexandria, the FLAG near the Dubai coast, the FALCON near Bandar Abbas in Iran and SeaMeWe-4, also near Alexandria, were all disrupted. Two ships, the MV Hounslow and the MT Ann, improperly dragged their anchors five miles north of Alexandria, Egypt, severing FLAG telecom and SEA-ME-WE-4.[182]

DAMAGE: Their anchors "severed the cables outside Alexandria after bad weather conditions forced ships to moor off the coast."[183] The first cut in the undersea Internet cable occurred on January 23, in the FALCON submarine cable which was not reported. It is unknown what caused the FALCON cable to break. The FLAG and

[180] Ibid.

[181] Asma Ali Zain, "Cable damage hits 1.7m Internet users in UAE," *Khaleej Times*, February 5, 2008. Accessed at http://www.khaleejtimes.com/DisplayArticle.asp?xfile=data/theuae/2008/February/theuae_February155.xml&section=theuae

[182] Lewis Page, "Dubai impounds cable slicing ships: Satellite images used to ID Gulf cable miscreants," *The Register (UK)*, April 14, 2008. Accessed at http://www.theregister.co.uk/2008/04/14/undersea_cable_cut_ships_nabbed/

[183] Malcolm Fried and Lars Klemming, "Severed Cables in Mediterranean Disrupt Communication (Update4)," *Bloomberg.com*, December 19, 2008. Accessed at http://www.bloomberg.com/apps/news?pid=20601085&sid=aBa0lTN.dcoQ

SEA-ME-WE-4 cables "have a capacity close to 620 gigabits per second,"[184] leaving only one cable connecting Europe with Egypt and the Middle East in operation. That cable, SEA-ME-WE-3, "has a capacity of 70 gigabits per second," and could not handle the large influx in traffic.[185]

IMPACT: The cuts "affected at least 60 million users in India, 12 million in Pakistan, 6 million in Egypt and 4.7 million in Saudi Arabia."[186]

In Egypt and Pakistan, "70 percent of its connection to the outside Internet and 30 percent of service to its call-center industry, which depended less on the lines," were lost.[187] Also, "50 and 60 percent of India's Net outbound connectivity was similarly lost on the westbound route critical to the nation's burgeoning outsourcing industry."[188] Between those three countries, 2500 networks went down during the outage period.

[184] John Borland, "Analyzing the Internet Collapse: Multiple fiber cuts to undersea cables show the fragility of the Internet at its choke points," *Technology Review (MIT)*, February 5, 2008. Accessed at http://www.technologyreview.com/web/20152/?a=f

[185] Ibid.

[186] Ali Zain, *Khaleej Times*, 2008.

[187] Borland, *Technology Review*, 2008.

[188] Ibid.

6. Mediterranean 2008

EVENT: 10 months later, it happened again. On December 19, 2008, three cable systems, SEA-ME-WE-4, SEA-ME-WE-3 and FLAG, "carrying close to 90 percent of all the data traffic between Europe and the Middle East" were cut.[189] The cables run from Alexandria in northern Egypt to Sicily in southern Italy, connecting the Middle East and South Asia with Europe. The cuts were caused along the Italy to Egypt route and a ship anchor or bad weather was likely to blame.

IMPACT: At one point as much as 55 percent of voice traffic in Saudi Arabia, 52 percent in Egypt and 82 percent in India was out of service, according to Orange.[190]

Again, these cuts caused massive outages; one article reported these significant outages:[191]

Saudi Arabia: 55% out of service; Djibouti: 71% out of service; Egypt: 52% out of service; United Arab Emirates: 68% out of service; India: 82% out of service; Lebanon: 16% out of service; Malaysia: 42% out of service; Maldives: 100% out of service; Pakistan: 51% out of service; Qatar: 73% out of service; Syria: 36% out of service; Taiwan: 39% out of service; Yemen: 38% out of service; Zambia: 62% out of service.

As mentioned in the opening story, DISA lost 60% of its international connectivity when these cables went down.

[189] Eric Krangel, "Egypt Goes Dark: Mediterranean Data Cables Toast," *Business Insider.com*, December 19, 2008. Accessed at http://www.businessinsider.com/2008/12/egypt-goes-dark-mediterranean-data-cables-toast

[190] Ibid.

[191] Arsalan Tariq Mir, "Three Undersea Cables Slashed," *AMMAR-3SIXTY! Blog*, Accessed at http://ammar360.com/2008/12/20/three-major-undersea-cables-slashed/

7. U.S. (California) 2009

EVENT: On April 4, 2009: "a total of ten fiber optic cables…were deliberately cut in three different locations in Southern California" within two hours.[192] One article notes that "a few vandals, equipped with pliers...cut fiber-optic cables in the San Francisco Bay area, paralyzing wireless, Internet, phone, and emergency communication for more than twelve hours."[193] The operation was easy; "whoever cut the fibers simply lifted the manhole cover, went down the ladder, and cut two cables."[194]

IMPACT: 1.5 million services were interrupted, including all ATM and credit card processing; 52,000 Verizon landlines lost service.[195] Although the case deals with a terrestrial cut, the situation makes the point that such a cut can happen on land.

8. West Africa 2009

EVENT: On July 30, 2009, SAT-3, the only cable connecting West Africa to other continents was severed.

IMPACT: Internet traffic was significantly disrupted to Benin, Togo, Niger and Nigeria. Nigeria appeared to be worst hit, as close to "70% of Nigeria's bandwidth

[192] Kevin Burton, Angela McGee, Jack Dibeler, "Who Turned Out the Light?" Burton Asset Management, 2009. Accessed at http://www.thinkbam.com/thinking/WebArticles/WhoTurnedOutTheLight.pdf

[193] Ibid.

[194] Margeurite Reardon, "How secure is the U.S. communications network?," *CNet News*, April 13, 2009. Accessed at http://news.cnet.com/8301-1035_3-10217550-94.html?part=rss&subj=news&tag=2547-1_3-0-20

[195] Burton, et al., Burton Asset Management report, 2009.

was cut, causing severe problems for its banking sector, government and mobile phone networks."[196]

9. Taiwan 2009

EVENT: On August 12, 2009, Typhoon Morakot, which triggered massive flooding in Taiwan, knocked out segment 7 of the Asia-Pacific Cable Network 2 (APCN2).[197] At that time, segment 1 of the same cable was being repaired. A week after the Typhoon, a 6.5 magnitude earthquake struck the region.[198] According to Verizon, "10 submarine cable systems in the Asia-Pacific region were damaged in more than 20 locations."[199] Near Taiwan alone, the APCN2, APCN, EAC and SMW3 cables were all impacted.[200]

IMPACT: Qatar and Singapore suffered the greatest communication failures. In addition, cable operators in Indonesia, the Philippines, South Korea and Japan all suffered disruptions to their networks.[201]

[196] "Cable fault cuts off West Africa," *BBC News*, July 30, 2009. Accessed at http://news.bbc.co.uk/2/hi/technology/8176014.stm

[197] Victoria Ho, "Typhoon knocks out Asia telecom cable," *CNet News*, August 13, 2009. Accessed at http://news.cnet.com/8301-1035_3-10308348-94.html

[198] Robert Clark, "After the typhoon, quake slows net access to a crawl," *Telecomasia.net*, August 19, 2009. Accessed at http://www.telecomasia.net/content/after-typhoon-quake-slows-net-access-crawl

[199] Verizon Business press release, "Verizon Business Global Mesh Network Investment Pays Big Dividends for Enterprise Customers During Multiple Submarine Cable System Disruptions in Asia-Pacific Region; All Restorable Customer Traffic Moved to New Routes Within Milliseconds," *M2 Newswire.com*, September 18, 2009. Accessed at http://www.highbeam.com/doc/1G1-208059844.html

[200] "BREAKING NEWS: Multiple cable cuts in Asia," *CommsDay International*, August 12th, 2009. Accessed at http://www.commsday.com/node/438

[201] Ek Heng, "Typhoon Morakot damages several subsea cable systems," *Telecomengine.com*, August 19, 2009. Accessed at http://www.telecomengine.com/article.asp?HH_ID=AR_5575

RECENT CABLE THEFTS

Acts of theft and sabotage are not new. The Vietnam case in 2007 can be considered both as it was designed to earn a profit by severing optical cable systems.

1. Vietnam 2007

In March 2007, a large undersea cable disruption in Vietnam occurred due to man-made activity, not natural disasters. In August 2006, the Vietnamese province of Ba Ria-Vung contracted "several companies to salvage undersea copper cable left over by the former government of South Vietnam..."[202]

Instead of recovering old cable, the companies and other fisherman started to pull up new ones. In the end, over 500km of cables was recovered from 5 illegal cable ring networks, with "roughly 43 km of fiber optic cable…belonging to a company in Singapore."[203]

More importantly, 11KM of Thailand-Vietnam-Hong Kong and 32 KM Asia Pacific Cable Network was taken, including housings that contained expensive equipment with long manufacturing lead times. The cable thefts forced Vietnam to rely on one submarine cable for 82% voice/data traffic.[204] Other traffic was pushed to terrestrial lines and satellite, creating internet delays for up to 3 months after the thefts.[205] To replace the 11 km section, Vietnam would have to pay $5.8 million. More than the money, Vietnam's credibility suffered as it sought to restore itself

[202] Matt Steinglass, "Undersea Cable Thieves Slow Vietnam's Internet Access," *VOA News.com*, June 1, 2007. Accessed at http://www1.voanews.com/english/news/a-13-2007-06-01-voa14-66777382.html

[203] Jacqui Cheng, "Phishing plumbs new depths: Vietnamese fishermen sever fiber optic lines," *Arstechnica.com*, June 8, 2007. Accessed at http://arstechnica.com/old/content/2007/06/phishing-plumbs-new-depths-vietnamese-fishermen-sever-fiber-optic-lines.ars

[204] "Critical Infrastructure: Submarine Telecommunication Cables," ICPC, Accessed at www.iscpc.org/publications/Critical_Infastructure_2009_V2.pps

[205] Ibid.

with the rest of the world.[206] The Prime Minister of Vietnam said the theft "directly affects Vietnam's socio-economic development, national security and the country's prestige in the region as well as in the world."[207]

So far, press reports of criminal prosecutions are available, but no official report has been published. Claims for compensation remain ongoing. The Prime Minister embarked on a campaign to educate the public on the significance of submarine cables so as to avoid anymore unwarranted cable theft.

2. Jamaica 2008

In Jamaica, "theft of copper cable was reported to have reached epidemic proportions, costing the UK telecoms giant Cable & Wireless Jamaica (C&WJ) over J$100m (£788,000) in losses and forcing them to offer J$1m (£7,880) for information leading to the arrest of the cable thieves."[208] The problem was out of control with reports stating thieves were stealing cable "at one end of a route while it was being replaced at the other."[209]

3. South Africa

Elsewhere, "South Africa's Telecom SA recently reported losses due to copper cable theft totaling almost 1bn rand – over [$100 million] – each year."[210]

[206] See Burnett, Douglas R. and Mick P. Green. "Security of International Submarine Cable Infrastructure: Time to Rethink?." *Legal Challenges in Maritime Security*. Eds. Ronán Long, John Norton Moore, Myron H. Nordquist and Rüdiger Wolfrum. Martinus Nijhoff Publishers, 2008.

[207] Ibid.

[208] Cathy Holding, "A global cable network of fragile links," *The Independent (UK)*, March 10, 2009. Accessed at http://www.independent.co.uk/news/business/sustainit/a-global-cable-network-of-fragile-links-1640448.html

[209] Ibid.

[210] Ibid.

Appendix E: Other International Cable Organizations

The North American Submarine Cable Association (NASCA)

NASCA is a non-profit organization of companies, formed in 2000, that own, install or maintain submarine telecommunications cables in the waters of North America. NASCA serves as a forum for its membership to provide and exchange information on technical, legal, and policy issues of common interest. These issues include standards and procedures for government approval of new cable installations; working relationships with other marine industries; and public education about such cables.[211]

KINGFISHER

KINGFISHER attempts "to reduce accidents, interaction has been established between fishermen and offshore operators to ensure mutual understanding of respective industries is established."[212] It also provides detailed maps of cable routes around the United Kingdom on the internet; more detailed maps are also sent to ship owners by requesting them on their website.

UK Cable Protection Committee (UKCPC)

The UKCPC is an "international forum of administrations and commercial companies which own, operate or service submarine cables in UK waters. The principal goals of the UKCPC are to promote the safeguarding of submarine cables and marine safety."[213] The UKCPC works closely with the KINGFISHER organization to protect cables by publishing charts.

[211] This information is accessed primarily from the NASCA website found here http://www.n-a-s-c-a.org/

[212] See "About KISCA," KISCA.org. Accessed at http://www.kisca.org.uk/about_kisca.htm

[213] "UKCPC," KINGFISHER charts, accessed at http://www.kisca.org.uk/ukcpc.htm