The Vulnerability of Subsea Infrastructure to Underwater Attack: Legal Shortcomings and the Way Forward

LAURENCE REZA WRATHALL*

TABLE OF CONTENTS

* J.D. and LL.M. in Taxation Candidate 2011, University of San Diego School of Law. I am sincerely grateful to co-workers at Systems Planning and Analysis, Inc. for their insight and professional mentorship, Professor Jorge Vargas for his support, the current editorial board of the *San Diego International Law Journal* for their corrections and suggestions, and friends and family—especially my wife Cheryl and daughter Caroline—for providing the relief and encouragement necessary to pursue my goals.

I. INTRODUCTION

Today's submarine pipelines and cables form modern sea lines of communication with important implications for global economic and maritime security.[1] This vital infrastructure is designed to be resilient; however, stability rests on international cooperation and law. Continued advances in international communications and energy exploration hinge on international legal standards that protect private investors (i.e., companies who build, maintain and operate underwater networks) from untoward acts.

A gap in legal protection for subsea pipelines and cables outside territorial waters could be exploited by undersea malfeasance. This is because trends in commercial undersea technologies are greatly expanding the size and sensitivity of the undersea "target set." As the economic significance of this critical infrastructure grows, so does the motivation to hold it at risk. This symbiotic evolution of technological capabilities and undersea targets grows more acute as offshore infrastructure moves into deeper and deeper water. And while legal regimes in place today afford some protection to infrastructure above the waterline, they fall short of protecting from ambiguous attack below.

This article explores the vulnerability of submarine pipelines and cables to underwater subterfuge beyond territorial waters, particularly with regards to the emerging threat posed by unmanned vehicles in executing such mal intent. Next, it describes the legal status of this critical infrastructure before identifying shortcomings in legal protection from underwater attack. Finally, potential solutions are offered for the way forward.

1. Scott Coffen-Smout & Glen J. Herbert, *Submarine Cables: A Challenge for Ocean Management*, 24 MARINE POL'Y 441, 442 (2000).

II. THE VULNERABILITY: CRITICAL UNDERSEA INFRASTRUCTURE

A. Oil and Natural Gas Pipelines

The world's biggest marine industry is offshore oil and natural gas—with oil production alone amounting to more than $300 billion per year.[2] Subsea[3] oil and gas markets have grown by more than 90% in the last five years and are projected to remain "very strong for the foreseeable future."[4] The commercial undersea energy infrastructure (UEI) that brings these energy resources to market includes: offshore rigs and platforms; floating storage, processing, and handling facilities; wells; and offshore handling terminals.

Subsea pipelines serve as the backbone for all this UEI.[5] They connect increasingly complex floating production networks as well as

---

2. *United Nations Convention on the Law of the Sea: Hearing on T. Doc. No. 103-39 Before the S. Comm. on Foreign Relations*, 108th Cong. (2003) (statement of Paul L. Kelly, Senior Vice President of Rowan Companies, Inc., on behalf of the American Petroleum Institute, the International Association of Drilling Contractors, and the National Ocean Industries Association), *available at* http://lugar.senate.gov/issues/foreign/pdf/sea/seareport.pdf at 117.

3. The term "subsea" is commonly used by the undersea oil and gas industry to identify assets and activities that utilize the sea floor. *See, e.g.*, *www.subsea.org.*

4. *Subsea Market to Remain Strong*, SUBSEA WORLD, Feb. 12, 2008, http://www.subseaworld.com/news (search "Subsea Market"; then select "Subsea Market to Remain Strong" hyperlink) (last visited June 6, 2010). Traditional oil producing basins have matured, particularly on land, and exploration and production companies have been forced to look for new reserves in ever more challenging deepwater environments off the Coast of Africa and beyond the Continental Shelf in the Gulf of Mexico to maintain production and profits. Between 2006 and April 2010, the number of deepwater rigs grew 43% in the Gulf of Mexico region. *See* Ben Casselman et al., *Blast Jolts Oil World*, WALL ST. J., Apr. 22, 2010, at A1, A4. Oil produced from these rigs has played an important role—the Gulf of Mexico produces 30% of the U.S. oil output and is an important source of revenue for oil majors like BP. *See id.* at A4. Worldwide, oil production at deepwater projects—those in waters at least 1,000 feet deep—grew 67%, or about 2.3 million barrels a day, between 2005 and 2008, which accounts for about 8% of global production. *See id.* In fact, so imperative is offshore drilling as a viable alternative to reliance on foreign oil imports, that the U.S. Export-Import Bank made a preliminary commitment of $2 billion in August 2009 to Petrobas of Brazil (at best, a lukewarm ally in the Americas) to finance the development of its Tupi fields. Review & Outlook, *Obama Underwrites Offshore Drilling*, WALL ST. J., Aug. 18, 2009, at A16.

5. Worldwide total offshore pipeline construction was 12,685 miles in 2008. Bruce Beaubouef, *Offshore Pipeline Construction Review*, PIPELINE & GAS TECH., Apr. 1, 2008, http://www.pipelineandgastechnology.com/Construction/ForecastsReviews/item55721.php (last visited June 6, 2010). In the North Sea alone, there are now more than 100,000 kilometers of pipeline. *See* Daniel Esser, *METS—The Tool for Pipeline Inspection*, SEA TECH., Apr. 2002, at 51. One 23.1-kilometer North Sea pipeline, the Tampen Link gas

vast subsea networks that directly feed ashore.[6] And ostensibly, they protect critical hardware from storms and terrorists too.[7]

All these new kilometers of piping coincide with the growing sensitivity of energy prices to supply disruption.[8] Factors mitigating the risk of untoward attack include robust pipeline construction with steel and concrete to withstand incidental impact from ship's anchors, frequent burial six to seven feet below the silt, and the increasingly interconnected

---

pipeline, exemplifies this increasingly indispensable role; it connects Norway's Statfjord oil and gas field to the United Kingdom (U.K.), which increases Norway's ability to export gas to the U.K. by 25 million cubic meters per day. *See* Nina Berglund, *New Pipeline Opens*, AFTENPOSTEN, Oct. 15, 2007, *available at* http://www.aftenposten.no/english/business/article2048659.ece.

The breadth and depth of UEI development in the Gulf of Mexico, where the lion's share of U.S. domestic crude oil supply is extracted, is also illustrative of worldwide trends. For example, the Gulfstream Natural Gas System pipeline runs 691 miles under the Gulf from Alabama to a growing consumer base in central Florida. Also, Thunder Horse oil field is located 125 miles offshore and in 6,000 feet of water. And now, drilling depths greater than 10,000 feet have become economically feasible as terrestrial supplies of oil and gas fail to satiate rising global demand. *See* Jad Mouawad, *Going Deep; The Gulf of Mexico Holds a Lot of Oil, but Recovering It Isn't Easy*, N.Y. TIMES, Nov. 8, 2006, at C1. *See also* Russell Gold, *BP's Big Oil Find Cements Gulf's Revival*, WALL ST. J., Sept. 3, 2009, at B1, B2 (many of these oil reserves are located in the Gulf's lower tertiary more than two miles below sea level and require expensive equipment to drill).

This ultra-deep water drilling, in turn, adds significant UEI inventory. Remotely Operated Vehicles assemble new seabed wells that then drill 30,000 feet below the seabed. *See* Amanda Griscom Little, *Pumped Up: Chevron Drills Down 30,000 Feet to Tap Oil-Rich Gulf of Mexico*, WIRED.COM, Aug. 21, 2007, http://www.wired.com/cars/energy/magazine/15-09/mf_jackrig (last visited June 6, 2010). Oil is then ported back from the 10,000-foot deep wellhead to floating storage, production, and offloading (FSPO) systems connected by networks of tiebacks, flowlines and risers—all pipelines. Similar FSPO operations off the coast of Brazil and West Africa tie as many as 40 to 55 subsea wells to one or two platforms using hundreds of kilometers of flow lines and risers.

Companies like BP, Marathon Oil, and Royal Dutch Shell increasingly rely on this method of subsea tiebacks to reuse old deepwater infrastructure and pump oil from smaller sized satellite fields. Russell Gold, *BP Drilling Platform Reaches Far Afield*, WALL ST. J., May 5, 2009 (Business Section), *available at* http://online.wsj.com/article/SB124155530486688737.html. By pumping oil from these far away deposits into already built platforms, they bypass the need to build additional rigs, which are expensive to construct and maintain. *See id.* Since the beginning of 2008, six new deepwater tiebacks have begun pumping, and an additional 23 tiebacks are in development and expected to be operational before the end of 2011. *See id.*

6. The Snøhvit development is the first on the Norwegian outer continental shelf with neither fixed *nor* floating units. It will pump from 140 kilometers offshore, in 250–354 meters of water, via pipelines to production facilities ashore. *See Facts about Snøhvit*, STATOIL.COM, http://www.statoil.com/en/OurOperations/ExplorationProd/ncs/snoehvit/Pages/default.aspx (last visited June 6, 2010). Likewise, technological advances in the Gulf of Mexico now enable wellheads far at sea to *directly* feed ashore. Piping larger proportions of total production in this manner further intensifies the breadth of undersea piping.

7. *See* Russell Gold & Ana Campoy, *Wells Take Voyage to Bottom of the Sea*, WALL ST. J., July 26, 2007, at B1, B6.

8. *See* INT'L ENERGY AGENCY, WORLD ENERGY OUTLOOK, 37–39 (2006).

nature of world energy markets.[9] These factors suggest that any attempt to disrupt pipeline operations would require a large, coordinated attack or precise insider knowledge of weak links, as well as the ability to absorb higher energy commodity prices.

B. Telecommunication Cables

Submarine telecommunication cables provide the "worldwide" part of the worldwide web and are the largest marine business after offshore energy extraction, global shipping, and naval expenditures.[10] Fiber optic cables were introduced in the 1980s,[11] and have since become indispensable arteries for the world's information lifeblood.[12] The heart of these cables is a set of six to twenty-four glass fibers, each the width of a human hair.[13] Lasers shoot pulses of light through these glass fibers, generating tens of thousands of communication circuits.[14] Even with additional shielding of copper, aluminum, polycarbonate, stranded steel wires, mylar, and polyethylene, cables typically span less than two inches in diameter.[15]

---

9. *See* Howie Doyle & Susan Troscinski, *Subsea Pipelines: From Survey to Start-Up New Technologies Conquer the Ocean Deep*, UNDERWATER MAG., Fall 1997, *available at* http://www.underwater.com/archives/arch/uw-fa97.02.htm. *See also* Magne Torhaug, *Petroleum Supply Vulnerability Due to Terrorism at North Sea Oil and Gas Infrastructures*, *in* PROTECTION OF CIVILIAN INFRASTRUCTURE FROM ACTS OF TERRORISM 77–78 (K.V. Frolov & G.B. Baecher eds., 2006).

10. Statement of Paul L. Kelly, *supra* note 2, at 1.

11. Coaxial cables were laid between 1950 and 1988; only a few are still used today. *See Fishing and Submarine Cables: Working Together*, INTERNATIONAL CABLE PROTECTION COMMITTEE [hereinafter ICPC] (2d ed.), Feb. 23, 2009, at 8, *available at* www.iscpc.org (select "Publications" tab, then select "Fishing and Cables").

12. *See Accession to the United Nations Convention on the Law of the Sea and Ratification of the 1994 Agreement Regarding Part XI of the Convention: Hearing Before the S. Comm. on Foreign Relations*, 110th Cong. (2007) (statement of Douglas R. Burnett, Int'l Cable Law Advisor and Partner, Holland & Knight LLP).

13. *Fishing and Submarine Cables*, *supra* note 11, at 9.

14. In 1958, Transatlantic Telephone [TAT] 1, the first transoceanic telephone cable, had 32 circuits. In 1979, TAT-7, the last analog cable, had 4200 circuits. Now, the Transpacific Express [TPE] cable system, a fiber optic undersea cable, has capacity equivalent to 62,000,000 circuits or simultaneous telephone conversations. *See* Statement of Douglas R. Burnett, *supra* note 12, at note 5.

15. *See Fishing and Submarine Cables*, *supra* note 11, at 9. See *Submarine Communications Cable*, WIKIPEDIA (July 26, 2010 3:51PM), http://en.wikipedia.org/wiki/Submarine_communications_cable, for a cross section of a submarine communications cable.

Owing to their lower cost and longer lifespan, submarine cables have surpassed satellites as the principal means of delivering international telecommunications traffic.[16] Swelling demand for bandwidth generated by the Internet and corporate data traffic, abetted by privatization of national telecommunication industries and private investment in submarine cables, has increased reliance on these undersea networks.[17] In fact, undersea cables carry over 95% of the world's (and 70% of U.S.) international voice, data, and video traffic, including almost 100% of transoceanic Internet ocean traffic.[18] There is insufficient satellite bandwidth to back up cable communications should they be lost.[19]

Despite the predominant use of fiber-optic cables for switched voice, private line services, and increasingly, the transmission of video signals, new scientific sources of demand for high-bandwidth global connectivity are also rising.[20] The high-energy physics research community has attempted to link scientists around the world to enable international collaboration on data-intensive projects.[21] Another emerging scientific

---

16. *See* Coffen-Smout & Herbert, *supra* note 1, at 441.

17. Two distinct technological convergences have caused the proliferation of fiber-optic cables: (1) the blurring of point-to-point communication and broadcasting; and (2) the convergence of telecommunications, computing, and entertainment into a common digital form. *See* Edward J. Malecki & Hu Wei, *A Wired World: The Evolving Geography of Submarine Cables and the Shift to Asia*, 99 ANNALS OF THE ASS'N OF AM. GEOGRAPHERS 360, 362 (2009). There are over 76 international cable networks of various sizes, owned by a consortium of private carriers. *See* James Jay Carafano & Alane Kochems, *Making the Sea Safer: A National Agenda for Maritime Security and Counterterrorism*, HERITAGE FOUND., Special Report No. 38 (Feb. 17, 2005), *available at* http://www.heritage.org/Research/Reports/2005/02/Making-the-Sea-Safer-A-NationalAgenda-for-Maritime-Security-and-Counterterrorism. *See also* Telegeography, http://www.telegeography.com/product-info/map_cable/index.php (last visited Nov. 3, 2010) for a submarine cable map of the world, and *infra* Attachment A (2009 variant of the map). Thirty of these cables land on the shores of ten U.S. coastal states: eleven in the Northeast (Rhode Island, Massachusetts, New York and New Jersey), eleven in Florida or Puerto Rico, and eight on the West Coast (California, Oregon, Alaska, Washington and Hawaii). Two new Pacific Ocean systems, each costing about half a billion dollars, will better connect the U.S. to Asia: the 10,800-mile TPE, discussed in the Statement of Douglas R. Burnett, *supra* note 12, connects the U.S. from Oregon to China, Korea and Taiwan; the 12,000-mile Asia-America Gateway cable system connects California, Hawaii, and Guam with Hong Kong, Malaysia, Thailand, Singapore, Vietnam, the Philippines and Brunei. Moreover, the BP Gulf of Mexico system, which will connect seven offshore production platforms, portends remote, continuous operations from control centers ashore, impervious to hurricanes. *See* Statement of Douglas R. Burnett, *supra* note 12.

18. *See About Submarine Telecommunication Cables*, ICPC, http://www.iscpc.org/publications/About_Cables_in_PDF_Format.pdf (last visited August 12, 2010).

19. *See* Carafano & Kochems, *supra* note 17, at 8.

20. *See* Malecki & Wei, *supra* note 17, at 364.

21. *See id.* For example, the authors mention the push to upgrade by the Standing Committee on Interregional Connectivity of the International Committee for Future Accelerators (ICFA-SCIC) at the European Organization for Nuclear Research (CERN).

application for submarine cables is undersea oceanographic research.[22] And the growing use of digital technologies in oil and gas exploration provides yet another market.[23]

While submarine fiber optic cables offer a number of security advantages over satellite communications (like less susceptibility to service disruptions during storms, greater barriers to eavesdropping, and more dependable installation and repair practices), they are nevertheless vulnerable to anthropogenic and natural disasters. Ship anchors and dredging fishing nets are two of the most common.[24] Earthquakes and shark bites—and hostile action—can also cut cables or bend them so severely that fibers crack and signals are lost.[25] Consequently, to improve their survivability, cables are often buried two to three feet in the seabed in water depths shallower than 2,000 meters.[26] And as fishing trawlers move into deeper waters, this burial may correspondingly increase.[27]

Intentional disruption of what has become the central nervous system of the global economy could cause significant harm to a wide range of international actors.[28] Impediments to the flow of real-time data for financial markets or to sensitive military communications that increasingly utilize the same infrastructure could spark widespread panic.[29] However,

---

22. *See id.* at 365. For example, the authors list the European Sea Floor Observatory Network (ESONET) and the North-East Pacific Time-integrated Undersea Networked Experiments (NEPTUNE).

23. *See id*. The authors describe how early three- and four-dimensional seismic visualization has greatly increased the success of drilling and exploration. Also, as offshore oil and gas fields are increasingly linked to onshore operations centers, "concerns about security from terrorist threats to oil facilities have pushed applications for remote access and control of high-resolution video, radar, and other surveillance systems beyond the capabilities of satellite communications."

24. *See* FRANK W. LACROIX ET AL., *Submarine Cable Infrastructure*, *in* A CONCEPT OF OPERATIONS FOR A NEW DEEP-DIVING SUBMARINE 140 (RAND Corp. 2001). *See also About Submarine Telecommunication Cables*, *supra* note 18.

25. In very deep water, cables are not necessarily armored, which reduces their weight and cost.

26. *See About Submarine Telecommunication Cables*, *supra* note 18.

27. *See id.*

28. *See* LACROIX, *supra* note 24, at 139–49. The threat of such disruption is as old as submarine cables themselves. A fisherman in 1850, thinking he had discovered a new species of seaweed, cut the first submarine telegraph cable (Dover to Calais) just a few days after it was inaugurated. *See* Coffen-Smout & Herbert, *supra* note 1, at 442.

29. *See, e.g.*, Richard Stiennon, *Richard Clarke on Recent Mideast Cable Outages*, THREAT CHAOS (Feb. 6, 2008), http://blogs.zdnet.com/threatchaos/?p=528 (interview with the chief counter-terrorism adviser on President Bill Clinton's U.S. National Security Council

as with undersea pipelines, self-deterrence is a significant factor militating against deliberate attack or sabotage on undersea cables. Because of the proliferation of civic services and interdependent functions that the Internet and telecommunications support around the world, it would be difficult for a saboteur to escape injury to their own organization or country.

C. Electricity Cables

Besides telecommunication cables, underwater power cables are becoming increasingly critical. For example, the Juan de Fuca Cable Project proposes to use an international electrical cable from Canada to Washington State.[30] There have been similar plans for a power cable from Canada to Boston and New York.[31] And now, with the anticipation of a green revolution in harvesting alternative energies, submarine electricity cables are likely to gain prominence as umbilical cords to future offshore energy parks.[32]

D. Collective Dim Mak Points[33]

Subsea pipelines, telecommunication, and power cables are critical, but vulnerable infrastructures.[34] They are targets for location-based

---

and author of BREAKPOINT, a fictional account about a series of attacks on U.S. infrastructure that start with simultaneous bombings of several beach heads for the main trans-Atlantic fiber cables and undersea cuttings of the same fibers).

30. *See* News Release, Sea Breeze Power Corp., Juan de Fuca Transmission Cable–Presidential Permit Application, (February 23, 2005), *available at* http://www.jdfcable.com/downloads/05-02-23.pdf (last visited June 6, 2010).

31. *See* Andrew Caffrey, *4,800 Megawatts Under the Sea? Jules Verne-esque Idea to Import Power*, WALL ST. J., May 23, 2001, at B1, B12.

32. *See* Emily Waltz, *Offshore Wind May Power the Future*, SCIENTIFIC AMERICAN.COM. (Oct. 20, 2008), http://www.scientificamerican.com/article.cfm?id=offshore-wind-may-power-the-future (describing proposed wind farm sixteen miles off the New Jersey shore). Long transmission lines would run from such deepwater farms.

33. *See generally* Victor Corpus, AMERICA'S DIM MAK POINTS: UNRESTRICTED WARFARE IN THE 21ST CENTURY (2009) (comparing vital yet vulnerable diplomatic, military and economic points to ancient Chinese acupuncture points called Dim Mak, which when hit in a specific way at certain times of the day, can cause paralysis or instant death).

34. Critical infrastructures are such that their function is vital for society; the vulnerability is the probability of system collapse. *See* Torbjorn Thedeen, S*etting the Stage: The Vulnerability of Critical Infrastructures*, *in* PROTECTION OF CIVILIAN INFRASTRUCTURE FROM ACTS OF TERRORISM 34 (K.V. Frolov & G.B. Baecher eds., 2006).

attacks[35] for reasons beyond their indispensable role in global markets. These reasons include:

- *Sensitive nodes*. UEI is increasingly centralized to minimize operating costs with multiple wells, often connected to a network of seabed pipelines, moving oil and gas to shore.[36] Meanwhile, telecommunication companies confront a paucity of adequate cable termination points that are isolated from heavy fishing and strong ocean currents.[37]
- *Concentrated routing and information chokepoints* (cables only). Consolidation and interdependence is even more acute beyond territorial waters.[38] At present, a large channel capacity in existing fiber optic lines provides re-routing capability. Now, telecommunication companies concentrate a large percentage of overall bandwidth in just a few major cable systems because new cable designs also incorporate such tremendous capacity.[39] Constraints on cable laying also result

35. *See* Michael Casey, *Communications Infrastructure Security*, *in* PROTECTION OF CIVILIAN INFRASTRUCTURE, *supra* note 34, at 233 (location-based attacks include the intentional severing of the backbone at a pre-determined site).

36. *See* Karl Hasslinger, *Vulnerabilities Await the U.S. on the Seabed*, DEFENSE NEWS, Jan. 14, 2008 (on file with author).

37. Termination points are repeatedly "stacked" to save the considerable cost of digging seabed trenches close to shore and then tunneling from the ocean bed up into a beach manhole. For example, all but one cable that terminates along the southern coast of the U.S. come ashore in three Florida cities. Of ten trans-Atlantic cable systems terminating along the Northeast corridor, eight terminate at two New Jersey cities, and two in Rhode Island. *See* LACROIX ET AL., *supra* note 24, at 144.

38. Until 1989, consortia dominated by monopoly telephone companies constructed international submarine cables, primarily to carry their own voice traffic. Telecommunication operators would sign a construction and maintenance agreement under which they agreed to contract, commission, operate, maintain, and own a cable system. These consortium cables remain common for very large or complicated systems, such as SEA-ME-WE 4, linking Southeast Asia, the Middle East, and Western Europe. By contrast, Fiber Link Around the Globe (FLAG) Telecom is a private cable system that uses an increasingly popular "sponsors approach," in which one or more private sponsors undertake the construction of the cable. Operators then purchase capacity, either through pre-sales or after final acceptance. The typical contract between a cable owner and a telecommunications operators use to be indefeasible rights-of-use (long-term rights, e.g., fifteen years or more, to use a specific amount of transmission capacity); increasingly, they are short-term, usually one-year leases. *See* Malecki & Wei, *supra* note 17, at 366–67.

39. *See* Carafano & Kochems, *supra* note 17, at 8.

in several cables being bundled together, offering a potentially lucrative, consolidated target for sabotage.[40]

- *Non-fungible facilities* (pipelines only). Pipelines that deliver oil and gas to markets ashore form tight linkages between at-sea facilities and nation-states. This would enable an aggressor to inflict disproportionate economic pain on nation-states that receive the piped fuel ashore, even though ripple effects might reverberate through the broader global energy market.
- *Dire environmental consequences* (pipelines only). Various oil and gas companies continuously monitor the internal condition of pipelines. However keen their pipeline integrity management and best practices, leaks are still possible from damage due to external objects.[41] Potential ecological and environmental disasters ensue from pipeline ruptures.[42]
- *Thin, expensive repair capacity*. Pipelines are lucrative targets because of high replacement costs and scarce and specialized repair and salvage capabilities.[43] Similarly for cables, low

---

40. Whereas, a single point attack on an undersea oil pipe might halt oil supply from one field (which is only a fraction of world oil supply, which, in turn, is only a fraction of total energy supply), a cable cut results in instant outage for all users upstream and downstream; no optical-electric equivalent of reserve production capacity exists when a bundle is entirely severed. Island nations are particularly susceptible. Rerouting capacity overland to cable termini in Canada and South America could mitigate the effects of an attack against U.S. subsea cables, but a single cut in 2000 to the SEA-WE-ME 3 network leading from Australia to Singapore caused Australia's largest Internet provider—Telstra— to lose up to 70% of its Internet capacity. *See* LACROIX, *supra* note 24, at 144. Similarly, Taiwan and Japan would be particularly vulnerable to undersea cable disruption, as evidenced by the severe communications disruption following an offshore earthquake in Taiwan in December 2006. *See* Chris Williams, *Taiwan Earthquake Shakes Internet*, REGISTER (U.K.) (Dec. 27, 2006), *available at* http://www.theregister.co.uk/2006/12/27 boxing_day_earthquake_taiwan/ (last visited June 6, 2010).

41. *See* Applied Tech. Workshop Abstract, Soc'y of Petroleum Eng'rs Int'l, Emergency Pipeline Repair Execution—Best Practices 3 (Jan. 12–14, 2009), *available at* http://www.spe.org/events/09adbi/documents/09ADBI_09AAD2.pdf.

42. Witness BP's struggle in the aftermath of the Deepwater Horizon drilling rig explosion on April 20, 2010. And as the United States and other Polar nations jockey for territorial rights in the increasingly accessible Arctic Ocean, an earlier oil spill on BP's hands became the impetus for the Arctic Oil Spill Research and Recovery Act (S. Bill 1561), which calls for more research to improve spill prevention and response in the Arctic. *See* Leonard Doyle, *Oil Gushes Into Arctic Ocean From BP Pipeline*, INDEP. (U.K.) (Mar. 21, 2006), *available at* http://www.independent.co.uk/environment/oil-gushes-into-arctic-ocean-from-bp-pipeline-470745.html.

43. There are only a few dozen large pipe-laying ships worldwide capable of welding together large pipeline sections and feeding them gently to the seafloor. The consortium of oil lessees operating on the Norwegian continental shelf relies instead on a small number of very advanced industrial robots (some weighing up to 100 tons), housed on a remote island near Stavanger, Norway. And five weeks into the environmental

market prices and high operating and maintenance costs have caused service fleets, the availability of trained crews, and worldwide spare part inventories to dwindle.[44]

- *Targeting data readily available in the public domain.* National Oceanographic and Atmospheric Agency (NOAA) nautical charts available on the Internet clearly depict platforms and connecting undersea pipelines.[45] Cable routes and landing stations are well-marked too.[46]
- *Security responsibility gaps*. Outside territorial waters, competing multinational corporations are free to route subsea pipelines provided they observe due care. However, unclear responsibilities beyond the boundaries of mining leaseholds generate little incentive for commercial companies to invest in common security systems. Moreover, cables span beyond the continental shelf, making them susceptible to surreptitious attack in the high seas. And as with undersea pipelines, governments have shifted much of the burden of cable defense to the private sector.[47] In response, private industry has adopted cost-effective practices to deal with incidental

---

disaster that followed the Deepwater Horizon drilling rig explosion of April 21, 2010, Coast Guard Admiral Thad Allen, national incident commander for the oil spill, admitted that "those (repair) technologies are not replicated inside the federal government." *PBS Newshour* (PBS television broadcast May 24, 2010), *transcript available at* http://www.pbs.org/newshour/bb/environment/jan-june10/thadallen_05-24.html.

44. *See* Carafano & Kochems, *supra* note 17, at 9.

45. *See generally* NOAA, Chart 11356, *available at* http://www.charts.noaa.gov/OnLineViewer/11356.shtml, and *infra* Attachment B (a close-up centered on 29º 07'N, 91º 15'W, approximately nine miles south of Point Au Fer Island, La.)

46. *See, e.g.*, *Submarine Telecommunications Cable*, GOV'T OF W. AUSTL. DEP'T OF TRANSP. (Dec. 6, 2007), http://www.dpi.wa.gov.au/imarine/19466.asp (SEA-ME-WE 3 submarine communications cable 51 nautical miles from Perth, Australia) (last visited June 6, 2010). *See also Eyebaling Transatlantic Cable Landings Eastern US*, CRYPTOME, http://cryptome.org/eyeball/cable/cable-eyeball.htm (U.S. transatlantic cable landings); *Eyeballing Transpacific Cable Landings Western US*, CRYPTOME, http://cryptome.org/eyeball/cablew/cablew-eyeball.htm (last visited June 6, 2010) (U.S. transpacifc cable landings).

47. In March 2002, at the 30th annual meeting of the National Ocean Industries Association, a panel of National Security agency representatives outlined some of the "precautionary steps companies should be taking to most efficiently *protect themselves*" (emphasis added). White House Office of Homeland Security representative Thomas DiNanno went on to say, "The assets are too diverse, and the challenges are too broad for the federal government to handle all of this." *See* Thomas J. Michels, *NOIA Annual Meeting—Safety and Security for Offshore Energy*, SEA TECH., Apr. 2002, at 47–49.

damage, but not necessarily to prevent purposeful damage.[48] The growing regionalization of cable systems further precludes coastal states' defenses.

III. THE THREAT: SUSCEPTIBILITY TO ATTACK FROM UNDER THE SEA

A. Undersea Concealment

Undersea systems—whether offensive, defensive, or commercial—share a fundamental set of attributes that derive from the nature of the domain in which they exist.

First, the undersea is opaque. What little sensory information is available is often distorted, incomplete, and ambiguous. Undersea systems are hard to detect without specialized equipment, and even then detection ranges are short and tracking information is murky. In contrast to a world of clear three-dimensional vision, precise radar images, and unconstrained line-of-sight communications at the speed of light, there are limits to data availability and transmission rates underwater.

Second, the demanding physical environment under water dramatically constrains one's range of motion. Pressure, salt water, and the absence of air and light make it technically challenging to operate undersea. This challenge grows dramatically as depth and time below the surface increase.

As a result of this opacity and these technological hurdles, the undersea domain remains an operational sanctuary for those who can afford to operate in it. In recent years, commercial submarines and remotely operated vehicles have facilitated access to this hostile environment. In turn, the impetus to drill in deeper and more isolated areas or to lay billion-dollar cables has increased as this technological capacity grows. These trends provide greater opportunities to use the sea for legitimate purposes, but they also enhance vulnerability to attack.

Why attack undersea pipelines and cables from under the sea? The short answer is stealth, which provides sanctuary from detection and prosecution.[49]

---

48. No organization monitors global networks for a concerted attack. Cable companies monitor their own cables and work with each other to repair outages quickly, but provide no feedback to governments. *See* Carafano & Kochems, *supra* note 17, at 9.

49. *See* Karl Hasslinger, *Undersea Warfare: The Hidden Threat*, ARMED FORCES J. (Mar. 2008), *available at* http://www.afji.com/2008/03/3463927.

> Unlike aviation stealth, which requires highly sophisticated and expensive aircraft, nearly any vehicle operating under the sea is extremely difficult to find. Whereas radars can scan thousands of square miles of air space and do so continuously, there is no equivalent system underwater. No one is watching the undersea approaches or checking the seabed along the continental shelf for nefarious activity. There is no undersea analogy to the no-fly zone designed to protect critical airspace.[50]

The stealth afforded by the sea—even for unsophisticated users—infers several advantages.[51] First and foremost is the ability to operate in proximity to an adversary's property without being observed.[52]

Surprise is a second major incentive because it enhances the ability to circumvent defensive measures.[53] A major advantage submarines enjoy is the ability to strike adversaries quickly and with surprise from close-in positions. Rogue actors may seek similar methods of asymmetric attack, for while attackers can easily locate targets of interest, the defender's task of detecting, classifying, and blocking undersea adversaries remains technologically and operationally challenging. High-frequency sonar systems or lasers can only *see* at short ranges, making large-area surveillance extremely difficult.[54]

Underwater concealment also maximizes economy of force.[55] "It allows a smaller number of operatives to place explosives in multiple locations over an extended time frame and later conduct coordinated, simultaneous strikes at a time of their choosing," making it harder for intelligence agencies to uncover.[56]

A final incentive is cost imposition due to ambiguity.[57] Just as post-9/11 air travel security measures instituted by the Transportation

---

50. *See id.*
51. *See id.*
52. Commercial security solutions for the Oil and Gas Industry include underwater surveillance to isolate and track underwater intruders. *See, e.g.*, *Security Solutions for the Oil & Gas Industry*, THALES GROUP, 4–5 *available at* http://www.thalesgroup.com/Workarea/DownloadAsset.aspx?id=2746&LangType=2057.
53. *See* Hasslinger, *supra* note 49.
54. Passive sonar is useful only to the extent undersea vehicles emit transient or continuous sound energy. Although some large passive sonar systems such as the Sound Surveillance System were effective in detecting older Soviet submarines at long range, newer submarines have such low sound signatures that they are extremely difficult to hear. *See id.*
55. *See id.*
56. *See id.*
57. *See id.*

Security Administration (TSA) have robbed millions of travelers of their time, increased the cost of air travel, and reduced overall productivity, one successful undersea attack could instill enormous anxiety and impose greater security costs.[58]

Ambiguity, coupled with our extreme reliance on undersea infrastructure, was on display in late January and early February 2008. Four undersea telecommunication cables were mysteriously cut within the course of two days, crippling Internet access across wide swaths of the Middle East and India.[59] Two cable breaks were in the Mediterranean—one near Alexandria, Egypt, and the other in the waters off Marseille, France.[60] The third break was thirty-five miles off the coast of Dubai and the fourth was along a cable linking the United Arab Emirates to Qatar.[61] Most telecommunication experts and operators deemed sabotage unlikely, believing instead that ship anchors had severed the cables when heavy storms swept through the region.[62] Nevertheless, the Egyptian Ministry of Communications refuted the presence of any ships near the Mediterranean cable cuts.[63] Moreover, the improbable incidence of four cuts in 48 hours fueled speculation about military involvement.[64] Sabotage theorists seized on reports of stifled Internet traffic through Iran,[65] while traffic to Israel, Lebanon and Iraq was apparently immune from chaos.[66] At the very least, this episode highlights how relatively small damage to undersea cables can instantly affect millions of people, and how a stealthy underwater attack—ambiguous and non-attributive in nature—could deal such a crippling blow.

---

58. *See id.*

59. *See* Heather Timmons, *Ruptures Call Safety of Internet Cables Into Question*, INT'L HERALD TRIB., 16 (Feb. 4, 2008), *available at* http://www.iht.com/articles/2008/02/04/technology/cables.php.

60. *See id.*

61. *See id*. *See also* Les Cottrell & Qasim Lone, *Effects of Fibre Outage through Mediterranean Seen by PingER*, SLAC (Jan. 30, 2008), http://www.slac.stanford.edu/grp/scs/net/talk08/med_fibre_cut_jan08.ppt.

62. *See* Timmons, *supra* note 59.

63. *See id.*

64. *See, e.g.*, Richard Sauder, *Middle East Undersea Cable Cutting A Zionist-NeoCon Covert Operation*?, RENSE.COM (Feb. 2, 2008), http://www.rense.com/general80/mid.htm (last visited Feb. 20, 2010).

65. *See id*. (citing http://www.internettrafficreport.com/asia.htm). Is it farfetched to believe state or non-state actors might tamper with submarine cables or pipelines to achieve desired effects? *See* SHERRY SONTAG & CHRISTOPHER DREW, BLIND MAN'S BLUFF: THE UNTOLD STORY OF AMERICAN SUBMARINE ESPIONAGE 237–57 (1998) (accounting U.S. submarine cable tapping operations during the Cold War).

66. *Internet Failure Hits Two Continents*, CNN.COM (Jan. 31, 2008), *available at* http://www.mindfully.org/Technology/2008/Internet-Cable-Failure31jan08.htm.

B. Unmanned Undersea Vehicles

Traditionally, there has been a high entry barrier to deep ocean areas. Only navies or state-sponsored research organizations could fund the vehicles needed to descend and work in such a hostile environment. However, today, an enemy could use a cheaply modified commercial or scientific vehicle combined with off-the-shelf sensors and explosives to attack undersea pipelines and cables.[67]

The most likely threat comes from Unmanned Undersea Vehicles (UUVs).[68] A UUV is defined as a "[s]elf-propelled submersible whose operation is either fully autonomous (pre-programmed or real-time adaptive mission control) or under minimal supervisory control and is untethered except, possibly, for data links such as a fiber optic cable."[69] The progress of resource extraction into deeper water has spurred the commercialization of UUVs in recent decades.[70]

Tethered variants were first used to recover underwater ordnance in the 1960s.[71] Today, researchers, salvagers, and undersea operators on ocean platforms or surface vessels continue to rely on their deep diving capability and their high degree of dexterity.[72] Virtual and augmented reality displays now fuse sensor inputs and further immerse shipboard operators in the vehicle's environment.[73]

---

67. *See* Carafano & Kochems, *supra* note 17, at 9 (citing CENTER FOR STRATEGIC AND BUDGETARY ASSESSMENTS, MARITIME FUTURES: THE UNDERSEA ENVIRONMENT 50 (Jan. 2003)).

68. UUV mirrors terminology utilized by the U.S. Navy. Elsewhere these vehicles have additional monikers, including Autonomous Underwater Vehicles (AUVs), Autonomous Marine Vehicles (AMVs), and Remotely Operated Vehicles (ROVs). *See* Andrew H. Henderson, *Murky Waters: The Legal Status of Unmanned Undersea Vehicles*, 53 NAVAL L. REV. 55, 56 (2006).

69. *See* U.S. DEP'T. OF NAVY, THE NAVY UNMANNED UNDERSEA VEHICLE (UUV) MASTER PLAN 4 (Nov. 9, 2004), *available at* http://auvac.org/research/publications/files/2004/uuvmasterplan.pdf.

70. *See* Bob Nugent, *The State of the Market: UUVs*, AMI INT'L., http://www.nwdefense.com/ami.pdf (last visited June 6, 2010).

71. *See* DELBERT C. SUMMEY ET AL., NAVAL SURFACE WARFARE CENTER, COASTAL SYSTEMS STATION, DAHLGREN DIVISION, CSS/TR-01/09, SHAPING THE FUTURE OF NAVAL WARFARE WITH UNMANNED SYSTEMS 3–7 (July 2001), *available at* http://handle.dtic.mil/100.2/ADA397057.

72. *See id. See also How Remotely Operated Vehicles Work in the Subsea*, BP.COM (May 4, 2010), http://www.bp.com/genericarticle.do?categoryId=9033657&contentId=7061733 (last visited June 6, 2010).

73. *See* A. Op den Bosch & J.C. Santamaria, *Monitoring Underwater Jobs Using Virtual Environments*, SEA TECH., Apr. 2002, at 17–25.

Untethered UUVs are also proliferating.[74] Those modified from commercial or scientific designs could provide an adversary what amount to guided torpedoes.[75] Though of limited range, UUVs can detonate at some prearranged time long after the delivery platform, submarine or surface vessel, has left.

Defending against such UUVs would require the operation of undersea point defense systems that can detect intruding vehicles and respond in a timely fashion.[76] Such measures would provide situational awareness of any limited entryways into areas of concern, and would also require significant investment. These efforts would probably impose a cost burden on states or alliances—not commercial entities. And such national-level investment would be unlikely to materialize unless undersea telecommunications, or the energy resources extracted from the defended fields, were solely bound for the states providing the defensive systems.

Alternatively, defenders could make efforts to create exclusion areas that prevent mother ship penetration in the first place. This limitation, or denial of passage, capitalizes on the existing weakness of both tethered and untethered variants of UUVs: both are tied to their delivery platform. The motive force for tethered vehicles is derived from the continuous electrical feed through their umbilical. Meanwhile, untethered variants are constrained by limited battery life. Their range, speed, and sensor capability is a function of their battery reserves. Thus, constricting the movement of potential delivery platforms is the surest defense against remote or autonomous UUVs they may harbor.

"A strong case can be made under U.S. law that UUVs are in fact vessels and, therefore, subject to all applicable rules for operation and navigation."[77] This is because most UUVs will either be considered components of their support ships, or be construed as vessels outright.[78]

---

74. *See* Nugent, *supra* note 70.

75. See Ronald O'Rourke, *Unmanned Vehicles for U.S. Naval Forces: Background and Issues for Congress*, *CONG. RESEARCH SERV.* (Oct. 25, 2006), *available at* http://fas.org/sgp/crs/weapons/RS21294.pdf, for a list of current U.S. Navy UUV missions and programs. *See also* Mathew Ritchey, *Unmanned Undersea Vehicles: An Asymmetric Tool for Sea Denial*, NAVAL WAR COLLEGE (May 21, 2008), *available at* http://*handle.dtic.mil/100.2/ADA484490* (student paper).

76. *See, e.g.*, UUV MASTER PLAN, *supra* note 69, at 35–40.

77. Henderson, *supra* note 68, at 72.

78. "If construed a submarine, like the largest UUVs might, they would be treated as such and be deemed vessels. If not, then under "component" criteria, UUVs would gain "vicarious" vessel status from the launching and/or controlling vessel, as the UUV would be both engaged in a maritime service and have some relation to navigation—or at least some connection with a vessel. Finally, [. . .] the fact that 'free-swimming' UUVs were

Far less regulatory or statutory guidance is available in the international arena.[79] If deemed vessels, UUVs may enjoy sovereign immunity as either warships or auxiliaries.[80] So, given the growing availability of UUVs to state and non-state actors around the world, the establishment of clear rules for their operation is crucial to nations with interests beyond territorial seas.[81]

IV. THE LEGAL STATUS OF SUBMARINE PIPELINES AND CABLES

States and private owners may assert claims or jurisdiction over undersea infrastructure on various grounds. States may assert claims on behalf of injured parties incorporated or present within their jurisdiction. Pipeline and cable owners, meanwhile, have direct recourse to traditional admiralty remedies in national courts that retain jurisdiction over the vessels and persons responsible for undersea depredations.[82] However, under international law, a corporate person whose property has been damaged possesses rights that are merely derivative of the rights of its state of nationality.[83] As a broad based source of international maritime rights and obligations, the 1982 Convention on the Law of the Sea (LOSC, or colloquially, the "Constitution of the Oceans")[84] currently

---

constructed for a purpose other than the transportation of persons or things does not preclude outright vessel status. As such, even the most autonomous UUVs could be deemed vessels in their own right." Henderson, *supra* note 68, at 66–67. However, it is conceivable that a UUV launched and operated from shore would have no support ship, nor would it technically be a means of transportation.

79. Henderson, *supra* note 68, at 72.

80. A well-established tenet of international law is that warships are extensions of their respective states, enjoying "sovereign immunity from interference by the authorities of nations other than the flag nation." U.S. DEP'T. OF NAVY, NWP 1-14M, THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS—ANNOT. SUPP. ¶ 2.1.2 (1997). Meanwhile, "[a]uxiliaries are vessels, other than warships, that are owned by or under the exclusive control of the armed forces. Because they are state owned or operated and used for the time being only on government noncommercial service, auxiliaries enjoy sovereign immunity." *Id.* ¶ 2.1.3.

81. *See* Henderson, *supra* note 68, at 72.

82. *See* Mark P. Green & Douglas R. Burnett, *Security of International Submarine Cable Infrastructure - Time to Rethink?*, *in* LEGAL CHALLENGES IN MARITIME SECURITY 557, 563 (Myron H. Nordquist et al. eds., 2008).

83. *See generally* Barcelona Traction, Light and Power Co. Ltd., (Belg. v. Spain), Judgment, 1970 I.C.J. 3. (Feb. 5, 1970), *available at* http://www.icj-cij.org/docket/files/50/5387.pdf.

84. *See* United Nations Convention on the Law of the Sea, Dec. 10, 1982, 1833 U.N.T.S. 397 [hereinafter LOSC].

contains the most robust provisions for claims asserted by either affected states or subsea proprietors.

The legal status of pipelines in waters beyond national jurisdiction has been associated with the status of submarine cables.[85] Without the LOSC, two operative treaties for international cables exist: the 1884 International Convention for Protection of Submarine Telegraph Cables (Cable Convention),[86] and the 1958 Geneva Convention on the High Seas.[87] These treaties deal with laying and repairing cables on the high seas—not in Exclusive Economic Zones (EEZ) and upon the continental shelf.[88] Moreover, they do not afford commercial owners significant deterrence against depredations.

Article 2 of the 1884 Cable Convention provides that "the breaking or injury of a submarine cable, done willfully or through culpable negligence, and resulting in total or partial interruption or embarrassment of telegraphic communication, shall be a punishable offence, but the punishment inflicted shall be no bar to a civil action for damages." Additionally, Article 10 allows a warship to obtain evidence of malfeasance.[89] However, unlike the LOSC, discussed below, no piracy provisions

---

85. *See* C. JOHN COLOMBOS, THE INT'L LAW OF THE SEA 382 (6th ed. 1967).

86. *See* Convention for the Protection of Sub-marine Cables, Mar. 14, 1884, 18 U.S.T. 380 [hereinafter Cable Convention].

87. *See* Geneva Convention on the High Seas, arts. 26, 27, Apr. 29, 1958, 450 U.N.T.S. 82.

88. The EEZ is defined as the area adjacent to and beyond territorial seas out to 200 nautical miles from the baselines from which territorial seas are measured. *See* LOSC, *supra* note 84, arts. 55, 57. The continental shelf comprises the seabed and subsoil of the submarine areas beyond the territorial sea to the outer edge of the continental margin, or to a distance of 200 nautical miles from the baseline, whichever is greater. *See id.* art. 76. The High Seas are all parts of the sea beyond the EEZ. *See id.* art. 86. *See generally* Douglas R. Burnett, *Maritime—Legal Jurisdiction Over International Submarine Cables*, *available at* www.iscpc.org/information/Legal_Regimes.PDF (two-slide presentation of Squire, Sanders & Dempsey L.L.P.), and *infra* Attachment C (amended first slide).

89. Evidence of violations of this convention may be obtained by all methods of securing proof that are allowed by the laws of the country of the court before which a case has been brought. When [commanding officers]… shall have reason to believe that an infraction of the measures provided by this Convention has been committed by a vessel other than a vessel of war, they may require the captain or master to exhibit the official documents furnishing evidence of the nationality of the said vessel…. Reports may, moreover, be prepared by the said officers, whatever may be the nationality of the inculpated vessel.

Cable Convention, *supra* note 86, art.10. This right was exercised in The *Novorossiisk*, when a warship boarded a Soviet fishing trawler on the high sea suspected of cutting transatlantic cables. See Press Release 211, *U.S. and U.S.S.R. Exchange Notes on Damage to Submarine Cables*, 40 DEP'T OF STATE BULL. 543, 555 (Apr. 20, 1959). The U.S. Government was satisfied that the evidence obtained raised a strong presumption that the master and crew of the trawler had violated Article 2 of the Cable Convention. *See id.*

provide for seizure of the offending vessel or universal jurisdiction over its crew. Also, the Cable Convention does not restrict breaking a belligerent state's cable during wartime.[90] In fact, during World War I, both Britain and Germany undertook offensive actions against each other's submarine cables.[91]

In its deliberations on the law of the sea, the International Law Commission (ILC) also considered the emerging issue of pipelines in the same context as submarine cables.[92] It confirmed that a state had the right to operate pipelines or cables beyond the territorial sea—through the high seas and on the continental shelf—provided such activity did not interfere with the coastal state's right to exploit its natural resources.[93] The ensuing 1958 Convention on the High Seas adopted the 1887 Cable Convention protection provisions, but simply confirmed the right to lay cables and pipelines outside the territorial sea.[94]

The LOSC, in contrast, provides a more robust legal regime for submarine cables and pipelines in ten specific articles.[95] One of the "freedoms of the high seas" is the right to lay and operate cables on the seabed.[96] This freedom now extends to territorial seas,[97] archipelagic waters,[98] the EEZ,[99] the continental shelf,[100] and "on the bed of the high seas beyond the continental shelf"[101]—which falls partly under national

90. *See* Cable Convention, *supra* note 86, art. 15.
91. *See* ROBERT K. MASSIE, CASTLES OF STEEL 77 (2003).
92. *See* Rep. of the Int'l Law Comm'n, *Commentary to the Articles Concerning the Law of the Sea*, 8th Sess, Apr. 23–July 4, 1956, arts. 61–5, U.N. Doc. A/3159; GAOR 11th Sess, Supp. No. 9 (1956), *reprinted in* [1956] 2 Y.B. Int'l L. Comm'n 293–94, U.N. Doc. A/CN.4/SER.A/1956/Add.1.
93. *See id.*, art. 70, at 298–99.
94. *See* Convention on the High Seas, *supra* note 87, arts. 26–28.
95. *See* LOSC, *supra* note 84, arts. 21, 51, 58, 79, 87, 112–15, and 297(1)(a).
96. *Id.* art. 87(1)(c). This freedom is subject to Part IV, pertaining to archipelagic states. *See id.* Although Article 87 phrases this freedom in the active tense (i.e., the freedom to *lay* rather than *maintain* cable systems), when read in the context of other LOSC articles concerning cables, it is obvious that the freedom to lay encompasses cable operation and repair. *See id.* arts. 58(1) and 79(5).
97. *Id.* art. 21(1).
98. *Id.* art. 51(2).
99. *Id.* art. 58(1).
100. *Id.* art. 79.
101. *Id.* art. 112.

jurisdiction if still in the EEZ,[102] but mostly under the responsibility of the International Sea-Bed Authority (in what is known as the *Area*).[103]

Though the LOSC does not consider the protection of submarine cables and pipelines in the EEZ, it does so in the context of the high seas.[104] With text that clearly draws from the 1884 Cable Convention, states have the obligation to pass laws and regulations to make the willful or culpably negligent breaking of a submarine cable or pipeline an offense.[105] Such offense can apply to ships flying the state's flag or to the state's nationals.[106]

The omission of submarine cable and pipeline protection in the EEZ can be explained by the nature of the right to lay a cable or pipeline.

> Apart from the restriction to have due regard for the coastal State's rights and advise it of a proposed route for a cable,[107] the right to lay a cable or pipeline through the EEZ is treated essentially as a high seas right. . . . This conclusion draws support from provisions concerning dispute resolution under the [LOSC], particularly [A]rticle 297, which indicates that while other EEZ rights need not be subject to compulsory dispute resolution, those attaching to high seas freedoms, [such as the laying of pipelines and cables, must be.][108]

This freedom to lay cables may, therefore, serve as a two-fold basis for bringing a claim for damages. First, according to ILC draft articles, state responsibility is triggered by an internationally wrongful act.[109] An internationally wrongful act is conduct consisting of an "action *or*

---

102. *Id.* art. 79(2).

103. *See* Burnett, *supra* note 88, and *infra* Attachment C (visual map of legal jurisdiction and regimes).

104. *See* LOSC, *supra* note 84, art. 113.

105. Every State shall adopt the laws and regulations necessary to provide that the breaking or injury by a ship flying its flag or by a person subject to its jurisdiction of a submarine cable beneath the high seas done wilfully or through culpable negligence, in such a manner as to be liable to interrupt or obstruct telegraphic or telephonic communications, and similarly the breaking or injury of a submarine pipeline or high-voltage power cable, shall be a punishable offence. This provision shall apply also to conduct calculated or likely to result in such breaking or injury. However, it shall not apply to any break or injury caused by persons who acted merely with the legitimate object of saving their lives or their ships, after having taken all necessary precautions to avoid such break or injuries.

Id. art. 113.

106. *Id.*

107. *Id.* art. 79(5).

108. Stuart Kaye, *International Measures to Protect Oil Platforms, Pipelines, and Submarine Cables from Attack*, 31 TUL. MAR. L.J. 377, 402–03 (2007).

109. *Responsibility of States for Internationally Wrongful Acts*, art. 1, [2001] 2 Y.B. INT'L L. COMM'N 32, U.N. Doc. A/CN.4/SER.A/2001/Add.1, *available at* http://untreaty.un.org/ilc/publications/yearbooks/Ybkvolumes(e)/ILC_2001_v2_p2_e.pdf.

omission" in breach of an international obligation of that state.[110] Conduct is attributable to the state if an individual or group of individuals act "on the instructions of" or "under the direction or control of" that state.[111] Second, since the LOSC calls for the application of flag state laws and regulations for the protection of cables and pipelines in the high seas,[112] a state could also be held liable for shirking "jurisdictional control" over ships flying its flag in respect of "administrative, technical and social matters."[113]

Moreover, while LOSC provides that the high seas shall be reserved for peaceful purposes,[114] it is not intended to be the sole source of law in relation to the high seas or EEZ.[115] The LOSC is *lex generalis*, which must be viewed in the context of *lex specialis* dealing with the use of force at international law.[116] The legitimate use of force under the U.N. Charter, either in self-defense or pursuant to a Security Council resolution, should be permissible in all maritime areas. Such an interpretation is explicitly supported in Article 301 of the LOSC.[117]

V. SHORTCOMINGS IN THE LEGAL PROTECTION OF SUBMARINE PIPELINES AND CABLES

The LOSC provisions are for essential security protection within territorial seas.[118] Any threat or use of force or weapons, any act prejudicial

110. *Id.* draft art. 2.
111. *Id*. draft art. 8.
112. *See* LOSC, *supra* note 84, art. 94(7).
113. *Id.* art. 94(1).
114. *Id.* art. 88.
115. *Id*. art. 87(1).
116. Stuart Kaye, *Freedom of Navigation in a Post 9/11 World: Security and Creeping Jurisdiction*, *in* THE LAW OF THE SEA: PROGRESS AND PROSPECTS 353 (David Freestone et al. eds., 2006).
117. In exercising their rights and performing their duties under this Convention, state parties shall refrain from any threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the principles of international law embodied in the Charter of the United Nations.

LOSC, *supra* note 84, art. 301.
118. The coastal State, may, without discrimination in form or in fact among foreign ships, suspend temporarily in specified areas of its territorial sea the innocent passage of foreign ships if such suspension is essential for the protection of its security, including weapons exercises. Such suspension shall take effect only after being duly published.

Id. art. 25(3).

to good order or security, or any launching of a military craft, is considered inconsistent with the right of innocent passage in the territorial seas.[119]

Meanwhile, the freedoms of the high seas are described as being subject to the conditions set in the LOSC and "other rules of international law."[120] However, in light of the vulnerability of undersea cables and pipelines to underwater subterfuge, the breadth of international law that provides protection beyond territorial seas is limited, even under the LOSC.

A. Lack of Domestic Legislation to Enforce Article 113 of the LOSC

The degree of protection under the LOSC would improve if parties were to adopt domestic legislation with teeth.[121] In spite of directing states to enact domestic legislation making malfeasance a punishable offense,[122] regulatory deficiencies persist. U.S. submarine cable law is exemplary in the way it frustrates cable owners' protection and recovery efforts. In typical cases of damage by vessels, cable repair and restoration of telecommunication services can cost cable owners up to $2 million in expenses and lost revenue.[123] Nevertheless, the U.S. federal statute for submarine cable protection imposes a paltry maximum penalty of only $5,000 for willful injury to cables.[124] This inconsequential fine underscores the feeble enforcing mechanism LOSC signatories utilize to ensure other states domesticate any legislative deterrent.

The following account of one LOSC signatory is illustrative of this anemic enforcement. In May 2007, it was reported that the Vietnamese military had recovered a significant amount of undersea cable and related equipment on Vietnamese soil, which was later confirmed as belonging to commercial carriers.[125] It was also reported that numerous vessels had been outfitted with special equipment to cut these cables and that cable coordinates were being sold illicitly.[126] Then, in June, it was reported that over 500 kilometers of telecom cable, including an eleven kilometer segment of the SEA-ME-WE 3 cable system, were seized by

---

119. *See id.* arts. 19(1), (2)(a)–2(c), 2(f).
120. *See id.* art. 87(1).
121. *See* Eric Wagner, *Submarine Cables and Protections Provided by the Law of the Sea*, 19 MARINE POL'Y 127 (1995).
122. *See* LOSC, *supra* note 84, art. 113.
123. *See* Coffen-Smout & Herbert, *supra* note 1, at 444.
124. 47 U.S.C. § 21 (2006).
125. *See* Green & Burnett, *supra* note 82, at 561.
126. *See id.*

Vietnamese police.[127] It subsequently came to light that local authorities had been complicit in the removal and theft of some undersea cables. The local authorities permitted fisherman to salvage, remove, and sell lengths of copper cable pinpointed as having been deployed before 1975, but did not anticipate that the fishermen would take this authorization as carte blanche to abscond with all types of cables.[128] In this instance, not only was there a paltry penalty for cable depredations, but as the reporting suggests, the cable thefts could also be traced to the flag government of the culprit vessels.[129]

B. Lack of Physical Manifestation Means Less Protection

The physical manifestation of offshore installations such as oil and gas platforms affords them a legal status—and concomitant protection—unavailable to underwater infrastructure. For cables and pipelines, there is no equivalent to the Protocol for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation (SUA Protocol)[130] or its 2005 Amendment.[131]

Specific concerns about maritime terrorism against offshore oil and gas installations led to the SUA Protocol in 1988. This protocol applies to "fixed platforms" on the continental shelf, but not the territorial sea, which include artificial islands, installations, and structures engaged in exploration or exploitation of the seabed or some other economic seabed.[132] Offenses under the SUA Protocol are very similar to those under the SUA Convention.[133] These include seizure by force, threat, or

127. *See id*.
128. *See id*. at 561–63.
129. *See id.* at 561.
130. *See* Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf, Mar. 10, 1988, 1678 U.N.T.S. 304 [hereinafter SUA Protocol].
131. *See* International Maritime Organization [IMO], *Protocol of 2005 to the Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf*, IMO Doc. LEG/CONF. 15/22 (Nov. 1, 2005) [hereinafter 2005 SUA Protocol Amendments].
132. SUA Protocol, *supra* note 130, art. 1.
133. *See* Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, Mar. 10, 1988, 1678 U.N.T.S. 201 [hereinafter SUA Convention]. The SUA Convention was negotiated as a direct result of the ACHILLE LAURO hijacking in 1985. *See* Kaye, *supra* note 108, at 389. The lack of international consensus on whether the Palestine Liberation Front's seizure of this Italian cruise liner satisfied the "private" ends requirement for piracy drew attention to the need for international agreement. *Id*. The

intimidation; destruction or damage threatening the safety of the platform; or placement of a device designed to damage, destroy, or endanger platform safety.[134] Similarly, jurisdictional reach is as wide as under the SUA Convention. A coastal state exercises jurisdiction over fixed platforms on its continental shelf as well as over foreign nationals or stateless individuals who coerce the state.[135]

While states were slow to adopt the SUA Convention and Protocol, 9/11 renewed attention to international security risks and precipitated amendments to both. The principal focus of the 2005 SUA Convention Amendments[136] is on the nonproliferation of weapons of mass destruction (WMD), and the use of a ship for terrorist activities or for transporting a violator of the SUA Convention is designated as an offense.[137]

Meanwhile, the 2005 SUA Protocol Amendments for fixed platforms are less wide-ranging, but follow a similar trend. New offenses are created where an individual uses explosive, biological, or radioactive material to cause damage to an installation, death, or serious injury.[138] The threat to undertake such an offense is an offense itself,[139] as is participation in the preparation and organization of such offenses.[140] Moreover, much of the SUA Convention and 2005 amendments relating to extradition, cooperation in acquiring data and evidence, and creation of domestic offenses are applied by the 2005 SUA Protocol *mutatis mutandis* in the context of the new offenses.[141]

In light of these fixed platform protections in the SUA Protocol and the ensuing 2005 Amendments, it has been proposed that a pipeline associated with an installation on the continental shelf might be regarded as a structure[142] and afforded equal protection. However, a pipeline

---

SUA Convention provided for protection against certain acts against shipping, including seizing a ship, performing acts of violence against individuals on a ship, damaging a ship or its cargo in a way that endangers its safe navigation, endangering the safety of a ship by interfering with maritime navigational facilities, or sending a false signal. *Id*. at 389–90.

134. *Id*. art. 2.

135. *Id*. art. 3.

136. IMO, *Protocol of 2005 to the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation*, IMO Doc. LEG/CONF. 15/21 (Nov. 1, 2005) [hereinafter 2005 SUA Convention Amendments].

137. *See id.* arts. 3bis(1)(a)(3), 3ter.

138. *See* 2005 SUA Protocol Amendments, *supra* note 131, art. 2bis(a).

139. *See id*. art. 2bis(c).

140. *See id*. art. 2ter.

141. *See id*. art. 2.

142. *See* IMO, *Invitation To Consider the Legal Questions Associated with CO2 Sequestration in Geological Formations Under the London Convention and Protocol*, I.M.O. Doc. LC.2/Circ.439 (Mar. 31, 2005), *reprinted in* http://www.imo.org/includes/blastDataOnly.asp/data_id%3D12076/439.pdf.

cannot be regarded as a structure for the purposes of the LOSC.[143] Given the LOSC's explicit language when dealing with submarine cables and pipelines, it seems unlikely that a generic term would be used to encompass pipelines in this context.[144] And while the ILC in 1956 considered the issue of safety zones around pipelines,[145] such buffers would effectively sever large ocean areas from international navigation. This was not the intent of the LOSC delegates who espoused freedom of navigation, and it is even inconsistent with earlier work of the ILC.[146]

In fact, in the context of safety zones, the International Maritime Organization (IMO) has mandated that states mark pipeline locations on publicly available charts[147] and disseminate details of pipeline work to ensure navigation safety.[148] But such markings further publicize sensitive location information—perhaps the sole protection in the absence of safety zones afforded to fixed platforms offshore.

C. No Protection Under Article 101 (Piracy) of the LOSC

Since the present system of enforcement based on nationality is unsatisfactory to cope with undersea malfeasance, another potential mechanism to assert jurisdiction over terrorists launching or fleeing an attack might be to equate such acts to piracy, which attracts universal jurisdiction under the LOSC.[149] This would avoid jurisdictional entanglements and give any state—not merely coastal states—lawful recourse.

However, there are several difficulties with such a formulation: first, the LOSC definition of piracy, that a piratical act should be for private gain, not political purpose;[150] and second, the status of an installation in

143. *See* LOSC, *supra* note 84, art. 60 (dealing strictly with artificial islands, installations and structures).
144. *See* Kaye, *supra* note 108, at 403.
145. *See* Special Rapporteur, *Regime of the High Seas and Regime of the Territorial Sea*, Int'l Law Comm'n, U.N. Doc. A/CN.4/97 (Jan. 27, 1956) (by J.P.A. François), *reprinted in* [1956] 2 Y.B. INT'L L. COMM'N 12, U.N. Doc. A/CN.4/SER.A/1956/Add.1.
146. *See* Kaye, *supra* note 108, at 403.
147. *See* IMO, *Safety Zones and Safety of Navigation around Offshore Installations and Structures*, IMO Assemb. Res. A. 671(16) (Oct. 19, 1989) (*replacing* IMO Assemb. Res. A. 621(15), IMO Assemb. Res. A. 379(X) and IMO Assemb. Res. A. 341(IX)).
148. *See id*. annex ¶ 4.24.
149. *See* LOSC, *supra* note 84, art. 110.
150. *See* LOSC, *supra* note 84, art. 101.

international law.[151] Traditional approaches to define piracy have focused exclusively on ships,[152] and while there have been debates as to whether an installation could, under certain circumstances, be treated as a ship,[153] it is apparent in the context of the LOSC that installations are treated distinctly from vessels.[154]

In this regard, both fixed platforms and undersea infrastructure face an uphill battle in gaining "vessel" status under the LOSC. Like international shipping, submarine cables span thousands of miles and are susceptible to attack from *hostes humani generis*,[155] but the visible presence of fixed platforms affords them a stronger textual argument for being subject to piratical acts. And yet even these fixed platforms and their attendant piping fall short of vessel status since they are deemed within reach of coastal state defenses.[156] In sum, application of the LOSC's protection is limited where terrorists take hostile actions for political, non-pecuniary ends against fixed platforms and, especially, cables and pipelines that are out of sight.

In total, there are substantial limitations on the legal regimes for the protection of submarine pipelines and cables beyond territorial seas. While some progress has been made in the context of installations with the SUA Protocol and subsequent amendments, it is apparent that neither the LOSC nor any other international instrument were drafted with the possibility of an attack on pipelines or cables in mind, let alone an underwater attack. The jurisdictional limitations on the United States and other coastal states to protect this critical infrastructure need to be addressed.

VI. PROPOSALS AND RECOMMENDATIONS

A. Ratify the LOSC (United States specific)

Even if the LOSC fails to classify subsea attack as piracy with full recourse to the convention's robust remedies, it does proscribe depredations against cables and pipelines under the high seas and the

151. *See* Kaye, *supra* note 108, at 415.
152. *See* Colombos, *supra* note 85, at 443–57 (discussing historical development of the law pertaining to piracy).
153. *See* Green & Burnett, *supra* note 82, at 578 (advocating how defining cable depredations as piracy within the meaning of art. 101 will facilitate a meaningful political and legal response).
154. Kaye, *supra* note 108, at 415.
155. *See* Le Louis, (1817) 2 DODS. 210 (P.C.) 229, 165 Eng. Rep. 1464, 1467 (U.K.).
156. *See* Kaye, *supra* note 108, at 416.

EEZ. As discussed above, the traditional rights of U.S. cable owners outside of territorial waters have been victimized by a dearth of enforcing legislation. By delaying the ratification of the LOSC, this lack of effective prosecution persists.[157]

World telecom companies rightly believe that the LOSC facilitates more confident investments than simply operating under the bare aegis of customary international law.[158] Simply defending against customary law encroachments does not deter underwater attack, but with U.S. ratification, U.S. telecom and energy companies as well as the U.S. Navy could seek greater government assistance in enforcing property rights and undersea infrastructure security outside of territorial seas.[159] Moreover, all U.S. stakeholders would have a firmer basis in holding other states responsible for their loss.[160]

As a condition for ratifying LOSC, the United States could take the helm in updating the convention to meet new military and commercial paradigms since it was first drafted three decades ago. Such revisions may include one or more of the following proposals.

B. Adapt the 2005 SUA Protocol and Amendments

The LOSC provides a starting point: the high seas shall be reserved for peaceful purposes.[161] However, it is not intended to be the sole source of law in relation to the high seas or EEZ.[162] In order to more

157. Douglas R. Burnett, *The Importance of UNCLOS to the U.S. Cable Industry*, TELECOMM. NEWSL. (Holland & Knight, U.S.), 1Q 2006, *available at* http://www.hklaw.com/id24660/PublicationId2291/ReturnId31/contentid49626/.

158. Statement of Douglas R. Burnett, *supra* note 12.

159. An expert legal panel, convened in 2006 to assess trends in global legal order and their impact on maritime strategy, warned that the instability of the 1982 UNCLOS regime is exacerbated by the failure of the United States to accede to the convention. *See* Craig H. Allen, *Moderator's Report: Legal Experts' Workshop on the Future Global Legal Order*, 60 NAVAL WAR COLLEGE REV. 73, 90 (2007).

160. Each State shall cause an inquiry to be held by or before a suitably qualified person or persons into every marine casualty or incident of navigation on the high seas involving a ship flying its flag and casing loss of life or serious injury to nationals of another State or serious damage to ships or installations of another State or to the marine environment. The flag State and the other State shall cooperate in the conduct of any inquiry held by that other State into any such marine casualty or incident of navigation.

LOSC, *supra* note 84, art. 94(7).

161. *See id.* art. 88.

162. *See id*. art. 87(1).

clearly delineate areas of responsibility and permissible jurisdiction over critical undersea infrastructure, the IMO could adapt the SUA Protocol and Amendments to this end. Such *lex specialis* would give states a stronger basis for marshaling naval forces to surveil and patrol threatened cables and pipelines, and if necessary, to board mother ships suspected of launching surreptitious attacks.

The spine of this new Undersea Infrastructure Protocol could be a mandatory system of cable and pipeline registration, which would give the state of registration a limited ability to enforce laws that protect it from interference.[163] The state would therefore have a right to protect pipelines or cables analogous to its right to protect vessels flying its flag.

The drag on this new Protocol (or amended SUA Protocol) remains the opacity of the seas and the impunity with which underwater craft, once launched, can inflict damage. The fact that the threat lurks below the waterline, masked by stealth, and largely immune from detection and classification, renders most any response untimely, stifling the efficacy of any *lex specialis*.

C. Issue Declaratory Policies (United States specific)

In light of the sensitivity of global economies to subsea infrastructure attack, the shortcomings in legal protection under the LOSC (even assuming U.S. Senate ratification), and the improbable effect of any SUA Protocol adaptation or amendment, the United States may look to the sheer deterrence of a powerful declaration. This may take the shape of a presidential proclamation that declares the sovereignty of all undersea infrastructure which is U.S. owned or services U.S. consumers, and provides for retaliatory response if it is besieged. Such declaration would comport with a rich tradition of U.S. presidential proclamations concerning jurisdictional boundaries at sea, which include: President Truman's proclamation on the Continental Shelf;[164] President Reagan's proclamation on sovereign rights and jurisdiction within the EEZ,[165] and extension of the territorial sea to twelve nautical miles;[166] and President

163. *See* Kaye, *supra* note 108, at 423.

164. *See* Policy of the United States With Respect to the Natural Resources of the Subsoil and Sea Bed of the Continental Shelf, Proclamation No. 2667, 10 Fed. Reg. 12,303 (Sep. 28, 1945).

165. *See* Exclusive Economic Zone of the United States of America, Proclamation No. 5030, 48 Fed. Reg. 10,605 (Mar. 14, 1983).

166. *See* Territorial Sea of the United States of America, Proclamation No. 5928, 54 Fed. Reg. 777 (Jan. 9, 1989).

Clinton's proclamation extending the Contiguous Zone to twenty-four nautical miles.[167]

A proclamation of undersea infrastructure sovereignty would anchor to the doctrine of self-defense—proportionate use of force against actors who threaten the security of undersea pipelines or cables. Since freedom of navigation on the high seas and the EEZ is circumscribed by the notion of "due regard" for the rights of others,[168] a surreptitious attack would first be classified as a violation of long-held customary international law, and, therefore, a legitimate basis for sanction.

However, constraints similar to those limiting the efficacy of Protocol amendments arise. Coastal and non-coastal states must characterize suspicious behavior as an affront to which they may respond. Proof of deliberate attack could be difficult to muster, tainting the legitimacy of any retaliatory act in the name of self-defense.

A second basis for presidential proclamation might be the doctrine of necessity, either environmental or commercial, in the face of imminent peril. The environmental necessity argument could be predicated on the ecological disaster that would ensue from an oil pipeline rupture. However, jurisdiction based on environmental protection would not apply to telecommunication cables. Moreover, the peril necessitating preemptive action would be difficult to prove in advance of any disaster. And though the LOSC permits coastal states to take enforcement actions against foreign ships in its territorial sea,[169] any unilateral enforcement in the EEZ or on the high seas would be decried as creeping jurisdiction.

Commercial necessity would incorporate telecommunication cables since their integrity is critical to global commerce. But again, the evidentiary requirement for either preemptive action or retaliatory response could prove disruptive to international commerce and antithetical to freedom

---

167. *See* Contiguous Zone of the United States, Proclamation 7219, 35 WEEKLY COMP. PRES. DOC. 1684 (Sept. 2, 1999).

168. *See* LOSC, *supra* note 84, arts. 87(2), 58(1).

169. Where there are clear grounds for believing that a vessel navigating in the territorial sea of a state has, during its passage therein, violated laws and regulations of that state adopted in accordance with this convention or applicable international rules and standards for the prevention, reduction and control of pollution from vessels, that state, without prejudice to the application of the relevant provisions of Part II, section 3 [i.e. innocent passage] may undertake physical inspection of the vessel relating to the violation and may, where the evidence so warrants, institute proceedings, including detention of the vessel.

Id. art. 220(2).

of navigation. Furthermore, any proclamation might only serve to highlight the vulnerability to attack, and its deterrent effect may not inhibit politically motivated, non-state actors.

D. Establish a Single Point of Contact to Monitor Threatening Behavior

International associations and consortiums like the International Cable Protection Committee (ICPC)[170], the North American Submarine Cable Association (NASCA),[171] and the Submarine Cable Improvement Group (SCIG),[172] all have a strong interest in being able to maintain and protect their cables. However, a strong, central monitoring authority—one that monitors all cable and pipeline disruptions and is connected to defense ministries around the world—is acutely lacking.

In the United States, "the fundamental orientation of the Homeland Security Act regarding protection of this infrastructure is a voluntary one of cooperation among all levels of government and private owners and

---

170. The ICPC has 106 Members from over 50 countries who are major owners or operators of submarine cables. The purpose of the ICPC is to help safeguard the submarine cable portions of power and telecommunications networks from human and natural hazards. This is achieved by sharing expert knowledge and promoting ideas that are beneficial to the protection of submarine cable systems worldwide.

About the ICPC, ICPC, http://www.iscpc.org/information/About_ICPC.htm (last visited July 24, 2010).

171. NASCA is a non-profit association of submarine cable owners, submarine cable maintenance authorities, and prime contractors for submarine cable systems. *See* NASCA, http://www.n-a-s-c-a.org (last visited July 24, 2010). NASCA's members include: Alaska United Fiber System Partnership; Alcatel-Lucent Submarine Networks; Apollo Submarine Cable System Ltd.; AT&T Corp.; Brasil Telecom of America, Inc./GlobeNet; Global Crossing Ltd.; Columbia Ventures Corporation; Columbus Networks, Inc.; Global Marine Systems Ltd.; Hibernia Atlantic; Level (3) Communications, LLC; New World Network, USA, Inc.; Southern Cross Cable Network; Sprint Nextel Corp.; Tyco Telecommunications (US) Inc; Verizon Communications, Inc.; and VSNL International, Inc. *See NASCA Member Companies*, NASCA, http://www.n-a-s-c-a-.org/member-companies-1 (last visited Aug. 15, 2010).

172. [SCIG] was formed in 1995 by four industry leaders: Alcatel Submarine Networks, Global Marine Systems Ltd, Kokusai Cable Ship Co., Ltd. and Tyco Telecommunications (U.S.) Inc., 'to develop cost-effective approaches and solutions to improve cable reliability and to communicate these to relevant international parties.' Collectively, the four companies and their predecessors have led the undersea cable industry for over a century. The SCIG has developed and distributed guidelines for cable engineering, cable burial depths and for the burial of cable in deepwater. In addition, the Group has published several papers on cable faults and other topics.

SUBOPTIC, http://www.suboptic.org/About-SubOptic/Industry-Affiliations.aspx (last visited Sept. 15, 2010).

operators of infrastructure."[173] Under the current approach, private entities have to be willing to share information regarding their vulnerabilities and security measures with government, which turns on their trust that such sensitive information will not be divulged or used against them.[174] The main obstacles to forming an effective authority in the United States and abroad thus become cost and information sharing. A strong, viable international authority necessitates costly policing and significant access to proprietary and sensitive information, both of which require a collective mandate.

Recent U.S. government action on cyber-space security provides a blueprint for germinating such centralized authority. First, order a security review on the vulnerability of critical undersea infrastructure to undersea attack, just as President Barack Obama ordered a sixty day cyber-space policy review in February 2009. Second, use the review team's recommendations to signal new policy imperatives. President Obama did precisely this when, as recommended, he appointed a cyber-security official and a new office to coordinate the nation's cyber-security policy. Third, envelope these new policy imperatives in a public awareness campaign to invoke a collective call to action while simultaneously signaling to perpetrators that any covert attack will be tracked, unmasked, and met with proportionate retaliation. The White House cyber report said:

> the nation must get serious and coordinate action to secure the government's vulnerable computer infrastructure, and calls upon state, local and tribal governments to elevate cyber-security as an issue . . . [It] also suggests updating the national strategy for cyber-security and incident response, implementing a national education campaign about cyber-threats, and building an identity management vision for the country, among several other goals.[175]

Fourth, vest the new authority with meaningful police power. The White House cyber review, for example, was accompanied by the introduction of the Cybersecurity Act in the U.S. Senate,[176] which:

---

173. James W. Conrad, Jr., *Information Protection*, *in* HOMELAND SECURITY 95, 118–19 (Joe D. Whitley & Lynne K Zusman eds., 2009).

174. *See id*. (author cites the Critical Infrastructure Information Act of 2002 (CIIA) as a step to encourage such sharing within the United States). *See also* 6 U.S.C. §§ 131–134 (2009).

175. Matt Williams, *National Cyber-Security Report Is a Call to Action*, GOV'T TECH., *available at* http://www.govtech.com/gt/articles/691709 (last visited June 6, 2010).

176. *See* S. 773, 111th Cong. (2009).

> would establish a new Cybersecurity Advisory Panel within the White House and streamline the cybersecurity effort through all levels of government. The bill also calls on the Department of Commerce to establish and maintain a clearinghouse on information related to cybsecurity threat and vulnerability information to public and private infrastructure deemed "critical" by the President. The Secretary of Commerce would be given access to this information "without regard to any provision of law, regulation, rule, or policy restricting such access." The bill would also give the President new authority to "declare a cybersecurity emergency and order the limitation or shutdown of Internet traffic to and from any compromised Federal Government or United States critical infrastructure information system or network.[177]

The mandate for greater vigilance and protection of U.S. cyber assets was initiated by the President's review, and culminated in proposals for more centralized control. There is no reason why a similar directive cannot be issued for the cables through which cyber pulses traverse.

E. Establish Safety Zones

Professor Stuart Kaye has proffered the following compromise solutions:

> In the context of pipelines and cables, it may be appropriate to revisit the proposal originally considered by the ILC in the 1950s, and permit the creation of prohibited areas for anchoring. These would not restrict navigation, but would prevent vessels from loitering in the immediate vicinity of a pipeline or cable. The width of such a zone could be relatively modest, and probably be no more than 500 meters at best. [However,] States were reluctant to accept such a concept in 1958, and it is likely that they would still be reluctant over fears of harm to freedom of navigation. . . .
>
> . . . .
>
> If widening a safety zone is not an option, then widening the zone for certain purposes might produce a more acceptable balance of interests. A zone of three nautical miles width acting as a warning zone, rather than a navigation exclusion zone, might present a way forward. Vessels without sovereign immunity could be advised to avoid such zones, and upon entry render themselves obliged to report detailed information concerning their intentions, cargo, and destination. Failure to report would render the vessel liable to be boarded. The non-application of this to sovereign immune vessels, principally warships, might help allay concerns over freedom of navigation.[178]

The Australian Communications and Media Authority appears to have already acted on this proposal by declaring a protection zone off Perth, Western Australia for the SEA-ME-WE 3 submarine communications

---

177. *S.773: Cyber Security Act of 2009*, OPENCONGRESS, http://www.opencongress.org/bill/111-s773/show (last visited June 6, 2010).

178. Kaye, *supra* note 108, at 421–22.

cable.[179] Activities that could damage the cable, such as trawling or anchoring, are restricted or prohibited within one nautical mile of the cable to a depth of 2,000 meters, fifty-one nautical miles from shore.[180] Interestingly, the Australian Authority has also stiffened the penalty for contravening this restriction: $66,000 (AUS) and/or ten years imprisonment.

The recurring dilemma here is one of competing interests: security of critical infrastructure versus freedom of navigation and maintaining precise locations secret. Restricting transit or loitering within a prescribed distance from charted cables and pipelines (e.g., 2,000 yards) might ease the burden of attributing mal intent. UUVs entering the secure zone could be detected with passive sensors and possibly disabled. More consequentially, impeding mother ships from maneuvering in close proximity to undersea infrastructure would force attackers to rely on the more dubious control and endurance of long-range, untethered UUVs to execute any underwater nefariousness.

Nevertheless, publicizing the location of undersea cables and pipelines may only serve to inform attackers. As prevalent as this locating information appears in the public domain, many precise coordinates remain sheathed in corporate secrecy. And without doubt, restrictions on the freedoms of navigation that undergird the LOSC will be politically unsavory.

Perhaps, in spite of these drawbacks, critical undersea infrastructure, like cyber security, is so vital as to necessitate amending the LOSC's emphasis on freedom of navigation. This reasoning comports with the Obama administration's renewed emphasis on cyber security, yet runs counter to its open defense of unfettered internet access around the globe. Ongoing international cyber security debates engender a classic trade-off between individual liberties and collective security,[181]

---

179. *See Submarine Telecommunications Cable*, *supra* note 46. *See also* Australian Communications and Media Authority (ACMA), WA Protection Zone, http://www.acma.gov.au/WEB/STANDARD/pc=PC_100868 (select "Map–Perth Protection Zone" link) (last visited Nov. 3, 2010), *infra* Attachment D.

180. *See id*.

181. *See, e.g.*, Mark Landler & Edward Wong, *China Rebuffs Clinton on Internet Warning*, N.Y. TIMES, Jan. 22, 2010, at A4, *available at* http://www.nytimes.com/2010/01/23/world/asia/23china.html:

> The Obama administration . . . repeated its demand that Beijing provide a more detailed response to Google's allegations that its computer network had been infiltrated by hackers based in China. But the United States held off lodging a

like notions of buffering undersea pipelines and cables from untoward encroachment.

F. Clarification of Piracy Under the LOSC

Finally, there is temporal ripeness to treat undersea pirates as *hostes humani generis*. Critical infrastructure below the waterline is often beyond national jurisdiction and remote from the state of affiliation. Therefore, it should be unambiguously incorporated into the LOSC definition of piracy along with ocean platforms. The *two-vessel* requirement and the *private ends* limitation should be eliminated to deter signatory states and their inhabitants from looting and possibly inciting economic and environmental shock at the margins of antiquated definitions.

As in several recommendations above, the United States can take the lead in updating the LOSC to account for technology trends and the changing dynamics of modern threats and defenses. The United States can drive this discourse by ratifying the LOSC. Further, it can condition ratification on the incorporation of security amendments, including an updated definition of piracy.

The modification of this one definition may not assist in attributing a surreptitious attack to its culprits, but could be the foundation for a more coordinated and enforceable response in the global commons. As in declaring safety zones around pipeline and cable routes, the aim would not be to thwart the possibility of attacks as much as to deter attacks through the specter of tough international sanctions. And if international responses are still deemed too tepid and ginger in punishing pirates, then a revised definition could at least provide affected flag states with a recognized prerogative to prosecute offenders akin to a coastal state's sovereignty within its territorial waters.

> formal diplomatic protest, suggesting that administration officials were still uncertain about how hard to push China on the matter. . . . Beijing and Washington both initially tried to treat the Google case as mainly a commercial dispute. But [a Secretary of State speech on Internet freedom], with its cold war undertones, has catapulted the dispute from the realm of technology and cybersecurity to one of fundamental freedoms.

VII. CONCLUSION

Submarine cables and pipelines are vulnerable assets in the global commons.[182] Their protection from undersea attack is a real prescriptive and enforcement challenge because of our extreme reliance on this critical infrastructure; its multi-jurisdictional span beyond territorial seas; the availability of precise locational coordinates; the opaque environment below the waterline; and the accessibility to commercial-grade vehicles that can exploit this environment and inflict disproportionate harm.

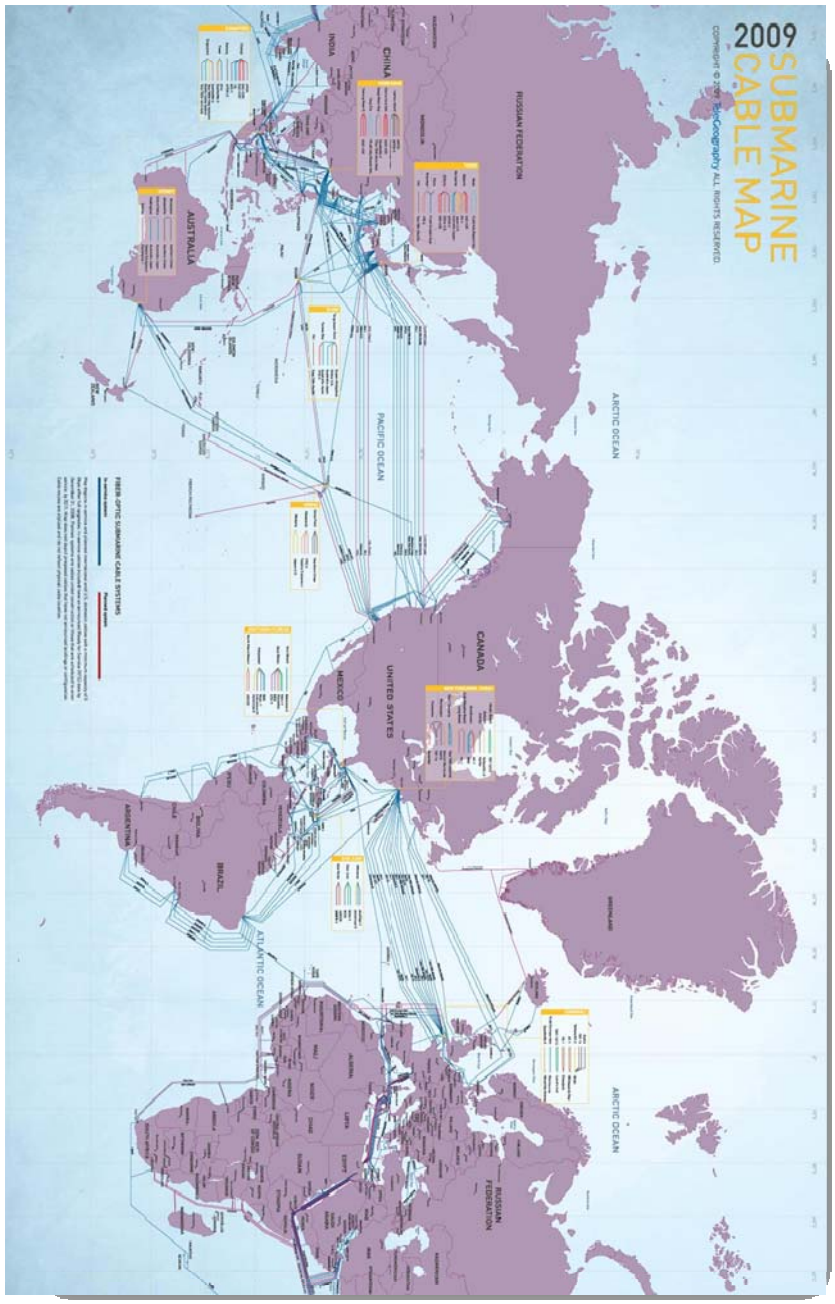
The opaque environment and the accessibility to UUVs set this challenge apart from challenges above the water's surface to flagged vessels and platforms. As with cyber threats, this necessitates an effective deterrence policy to compensate for an inability to pinpoint suspected culprits. Not only do legal shortcomings in jurisdiction and security enforcement float above the surface, but arguably more sinister shortcomings lurk below. These threats also require an even more delicate balance between disclosure and secrecy, and between freedom of navigation and reasonable restraints for collective security.

In the end, whatever vigor is applied towards cyber security, and whatever balance is struck for internet freedoms should be matched by securing the very cables that transport this life-blood of commerce. Likewise, investment in energy independence should correspond to the security of the very arteries that enable and spur offshore energy exploration.

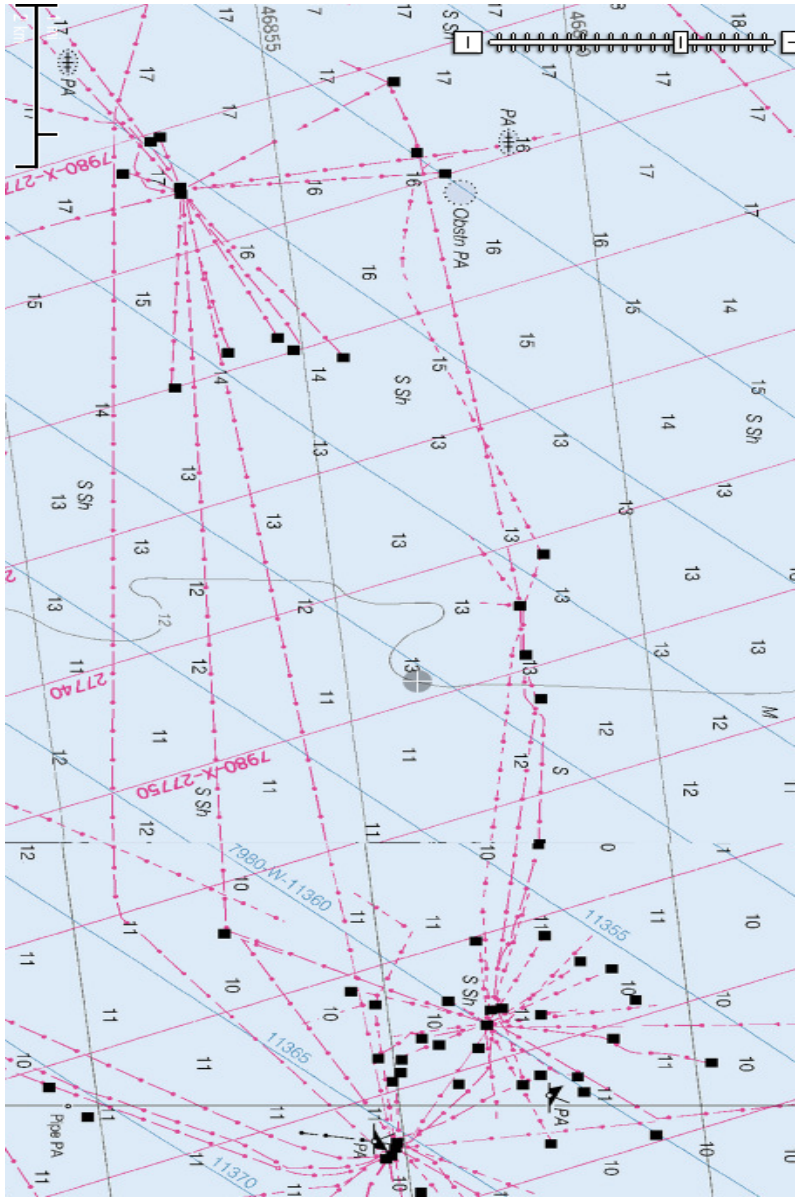
The underwater environment may be opaque and the potential international solutions may be equally murky, but on account of this confluence of vulnerabilities, threats and legal shortcomings, it is imperative to address this unique challenge and devise solutions with sufficiently deliberate haste so as to deter attacks and provide for redress if deterrence proves ineffective.

182. *See* Stuart Kaye, *Threats From the Global Commons: Problems of Jurisdiction and Enforcement*, 83 INT'L LAW STUDIES 69, 73 (2007).

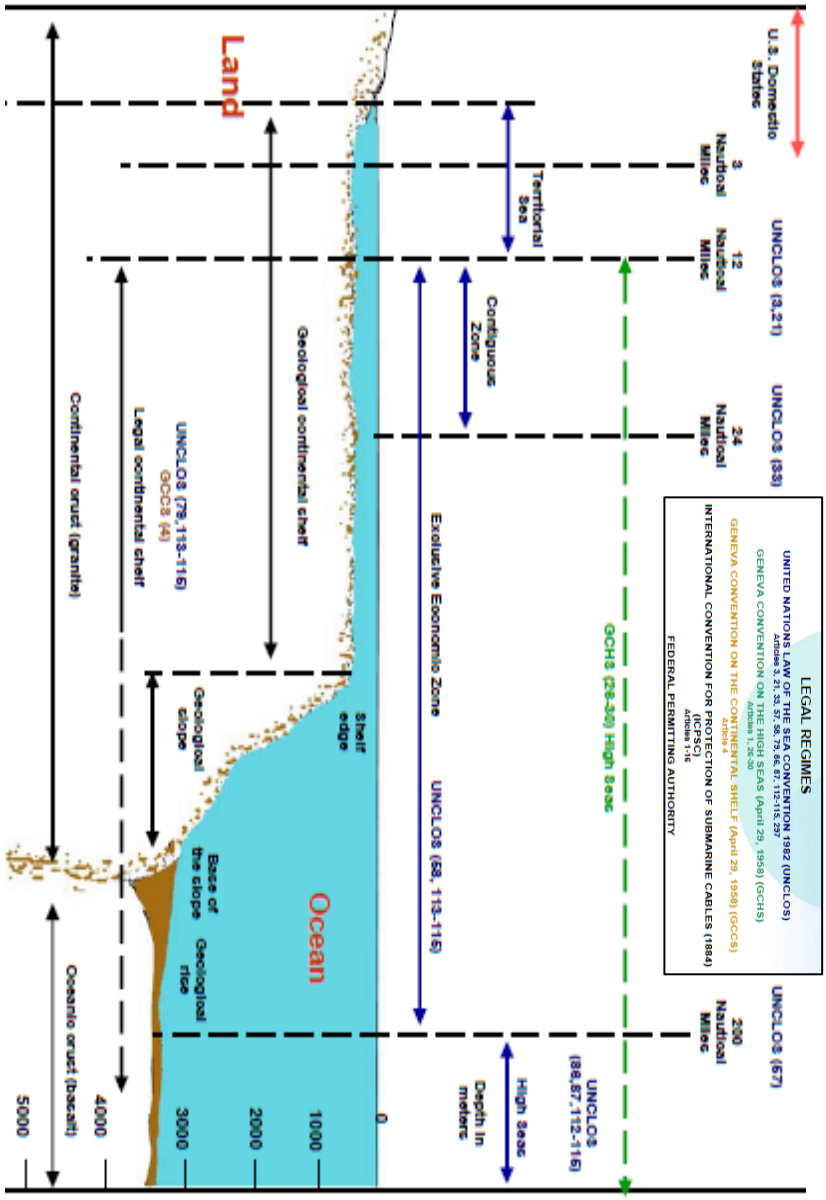
ATTACHMENT A



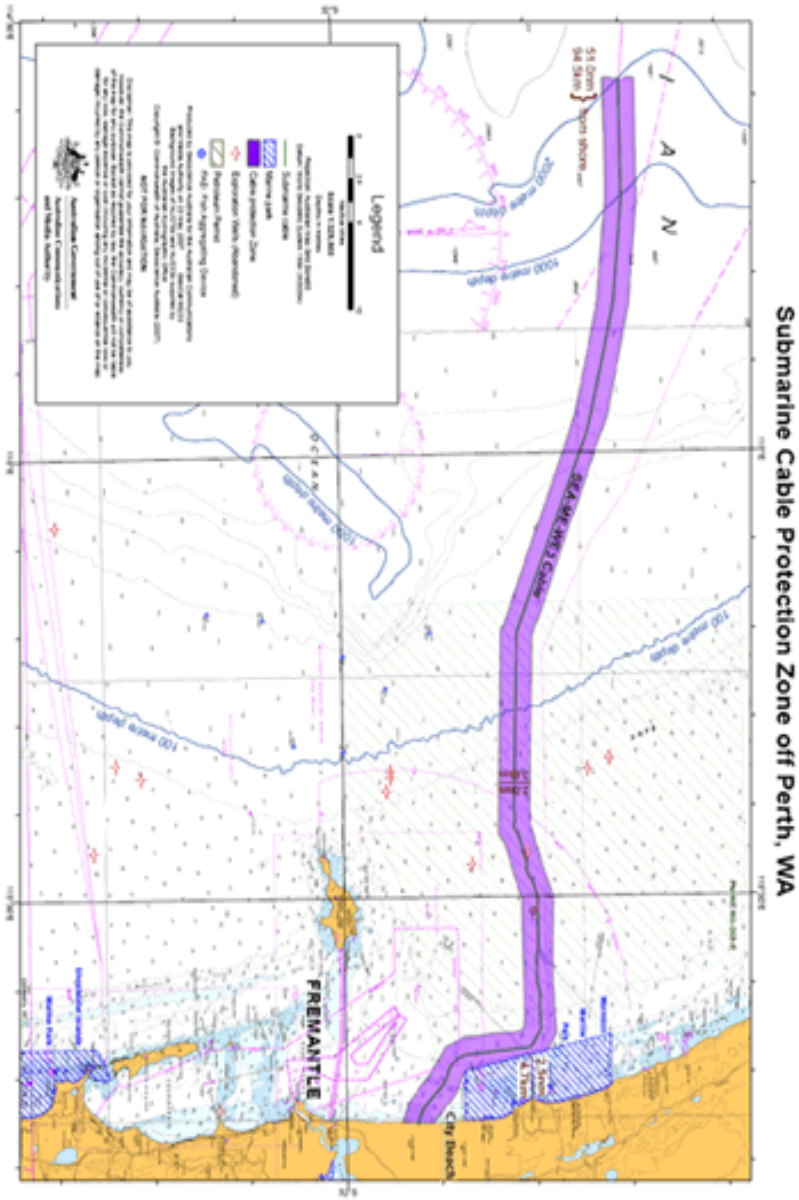
ATTACHMENT B



ATTACHMENT C



ATTACHMENT D



Submarine Cable Protection Zone off Perth, WA