

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](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 Amendments¹³⁶ 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 structure¹⁴² 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 charts¹⁴⁷ 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 causing 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.

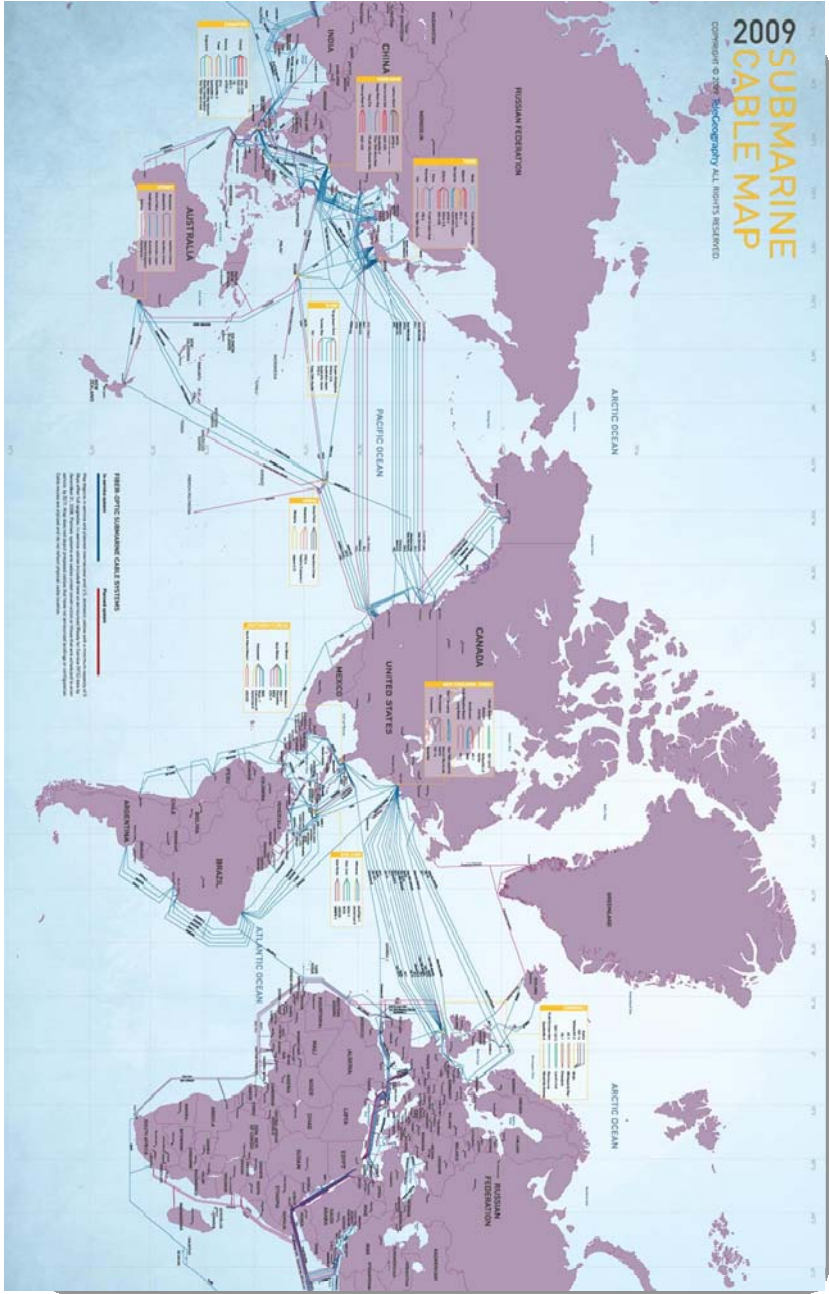
The opaque environment and the accessibility to UUVs set this challenge apart from challenges above the water's surface to flagged vessels and platforms. As with cyber threats, this necessitates an effective deterrence policy to compensate for an inability to pinpoint suspected culprits. Not only do 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.

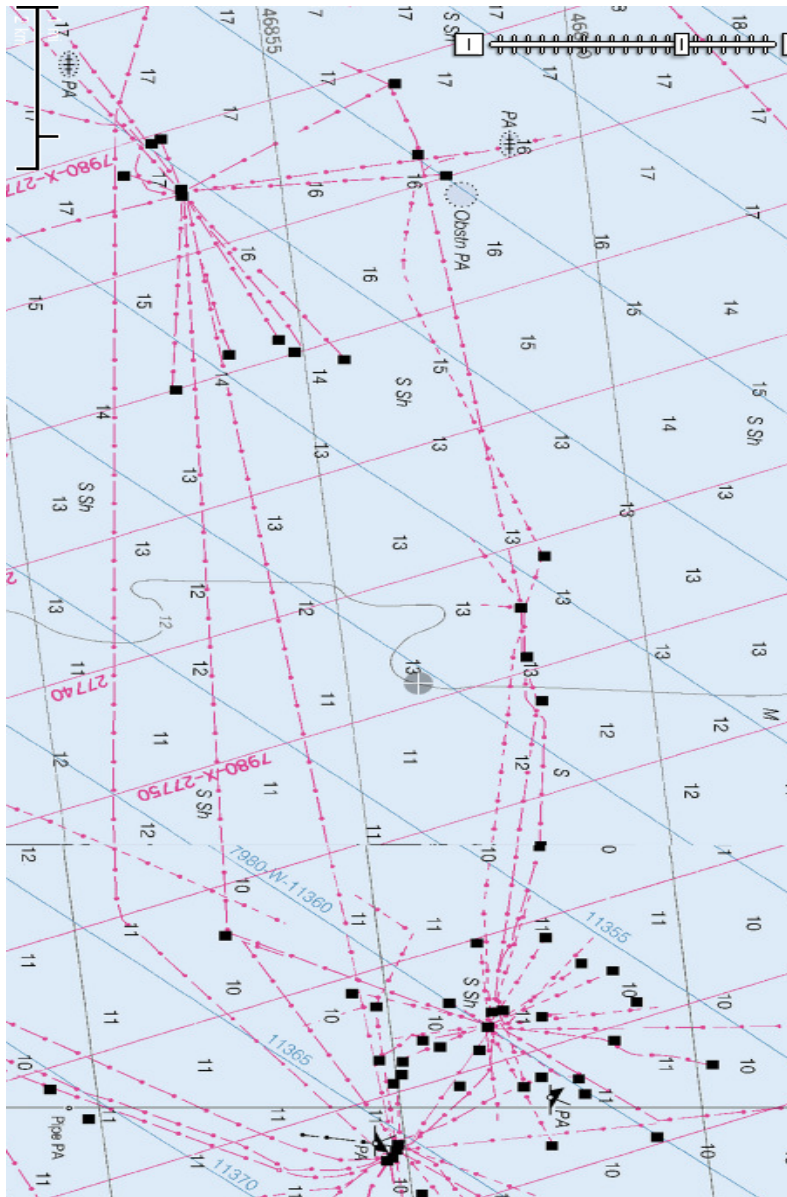
The underwater environment may be opaque and the potential international solutions may be equally murky, but on account of this confluence of vulnerabilities, threats and legal shortcomings, it is imperative to address this unique challenge and devise solutions with sufficiently deliberate haste so as 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).

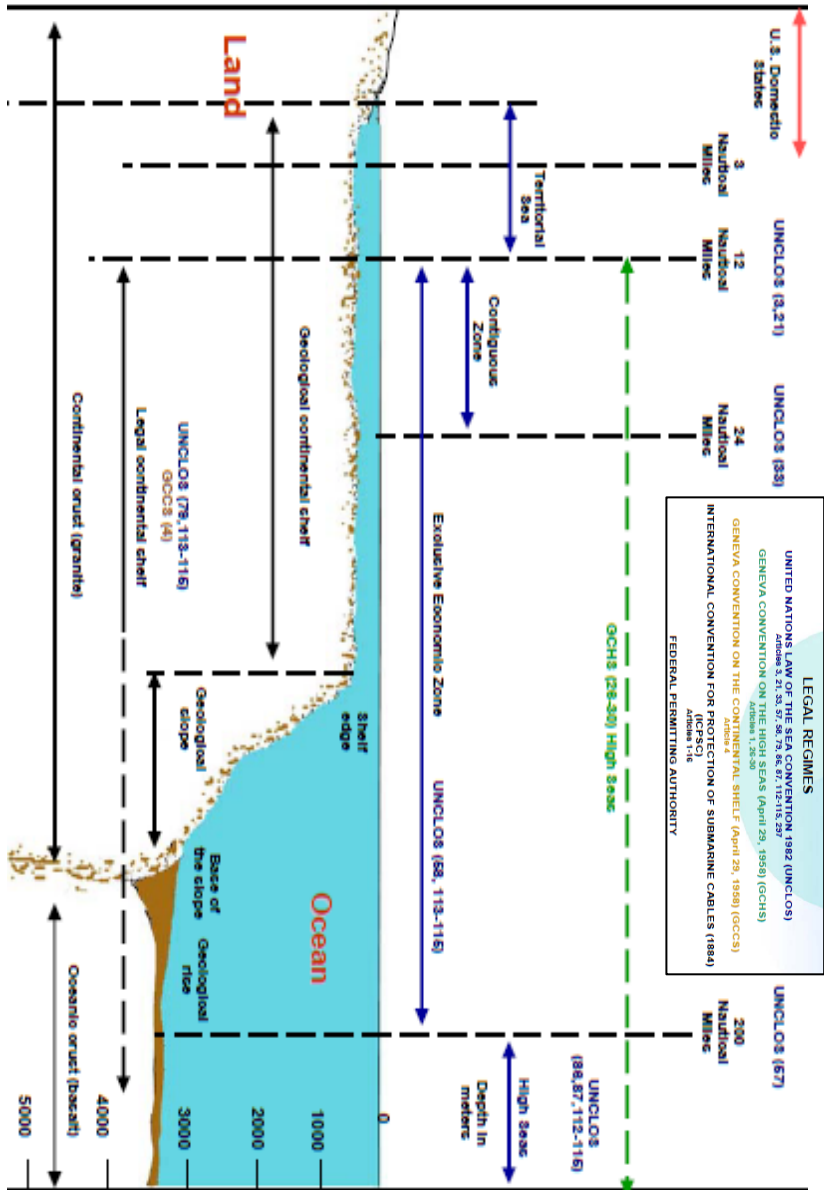
ATTACHMENT A



ATTACHMENT B



ATTACHMENT C



ATTACHMENT D

