CHARACTERISTICS AND COMMON VULNERABILITIES INFRASTRUCTURE CATEGORY: CABLE LANDING STATIONS

Protective Security Division
Department of Homeland Security

DRAFT - Version 1, January 15, 2004

Preventing terrorism and reducing the nation's vulnerability to terrorist acts requires understanding the common vulnerabilities of critical infrastructures, identifying site-specific vulnerabilities, understanding the types of terrorist activities that likely would be successful in exploiting those vulnerabilities, and taking preemptive and protective actions to mitigate vulnerabilities so that terrorists are no longer able to exploit them. This report characterizes and discusses the common vulnerabilities of United States cable landing stations, which are the terrestrial gateway facilities between domestic telecommunications (voice/data) networks and underwater cable systems.

CABLE LANDING STATION CHARACTERISTICS

Characterization of the Industry

Underwater cables carry telecommunications traffic (voice and data) under bodies of water (e.g., lakes and seas). These cables carry about 95% of all intercontinental telecommunications traffic. International banking and finance transactions are highly dependent on underwater (also known as submarine) communications cables. Some military communications traffic is carried via underwater cables. Most underwater communications cables in service are fiber-optic cables. New systems are almost always equipped with fiber-optic cables (rather than older technology coaxial cables). Underwater cable systems have expanded in recent years due to increased demand, changes in technology, and reduction in costs. This paper focuses on the gateway point to underwater cable systems, the cable landing station, including the fiber run from the station to shore where the fiber enters the water. Additional detail on the underwater portion of fiber cabling can be found in *Characteristics and Common Vulnerabilities, Infrastructure Category: Underwater Cables* (Draft, December 15, 2003).

The longest underwater telecommunications cable systems connect continents. Shorter systems are laid along coastlines to avoid problems of siting terrestrial systems. Alternative routes are often installed to increase system reliability.

The first underwater cable, a telegraph cable, was laid in 1850 between England and France. Like most early cables, it failed quickly. Including that first cable, 950 underwater cables have been installed worldwide through 2003. The first fiber-optic cable, TAT-8, was put into service in 1988. Since then, 178 cables have been laid.

Submarine cables enter the Continental United States (U.S.), Hawaii, and Alaska at various locations as shown in Figure 1. Each of the cable landing locations has a number of redundant and diverse backhaul routes. These routes provide connectivity on both regional and local levels between the cable landings and the domestic network. Table 1 lists 52 cable landing stations in the U.S. The majority of these landing sites use fiber optics.

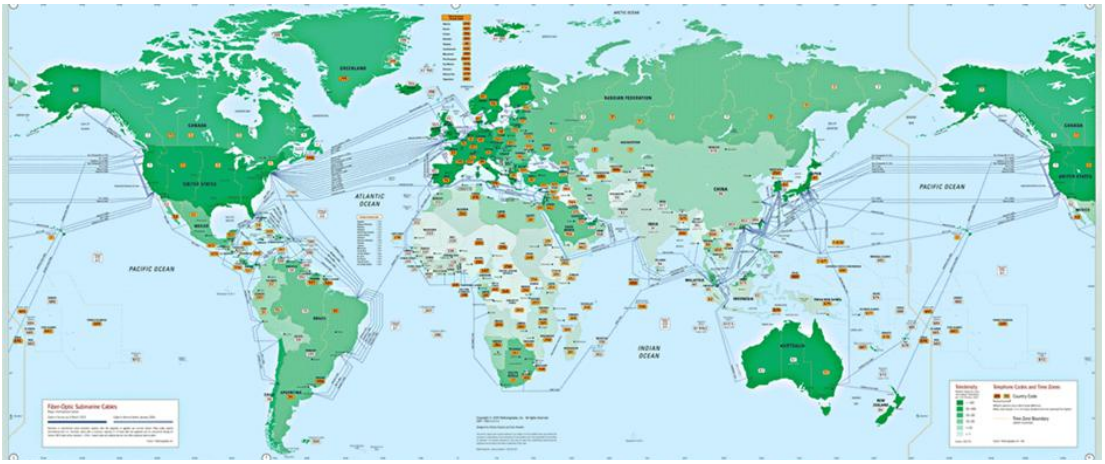

Figure 1 Underwater Cables

Table 1 U.S. Cable Landing Locations

City	State	City	State	City	State
Lynn	MA	Seward	AK	Moss Landing North	CA
Green Hill	RI	Juneau	AK	Moss Landing South	CA
Shirley	NY	Whittier	AK	San Luis Obispo	CA
Brookhaven	NY	Valdez	AK	Grover Beach	CA
New York City	NY	Harbour Pointe	WA	Hermosa Beach	CA
Far Rockaway	NY	Seattle	WA	Kahe Point	HA
Arverne	NY	Lynnwood	WA	Lualualei	HA
Manhattan Beach	NY	Nedonna Beach	OR	Makaha	HA
Mastic Beach	NY	Coos Bay	OR	Lihue	HA
Crab Meadow Beach	NY	Pacific City	OR	Keawaula	HA
Long Beach	NY	Bandon	OR	Spencer Beach	HA
Manahawkin	NJ	Twin Rocks	OR	Ko Olina	HA
Manasquan	NJ	Hillsboro	OR	Koko Head	HA
Tuckerton	NJ	Manchester	CA	Kihei	HA
Wall Township	NJ	Point Arena	CA	Kawaihae	HA
Boca Raton	FL	Morro Bay	CA	Sandy Beach	HA
Hollywood	FL	Monterey Bay	CA	Manele Bay	HA
North Miami Beach	FL				

Although there are a number of locations and cables and the data flow can usually be dynamically re-routed in the event of secondary single path losses, the usage or capacity is not evenly distributed. Figure 2 shows that the largest data pipes are currently between New York and the United Kingdom.

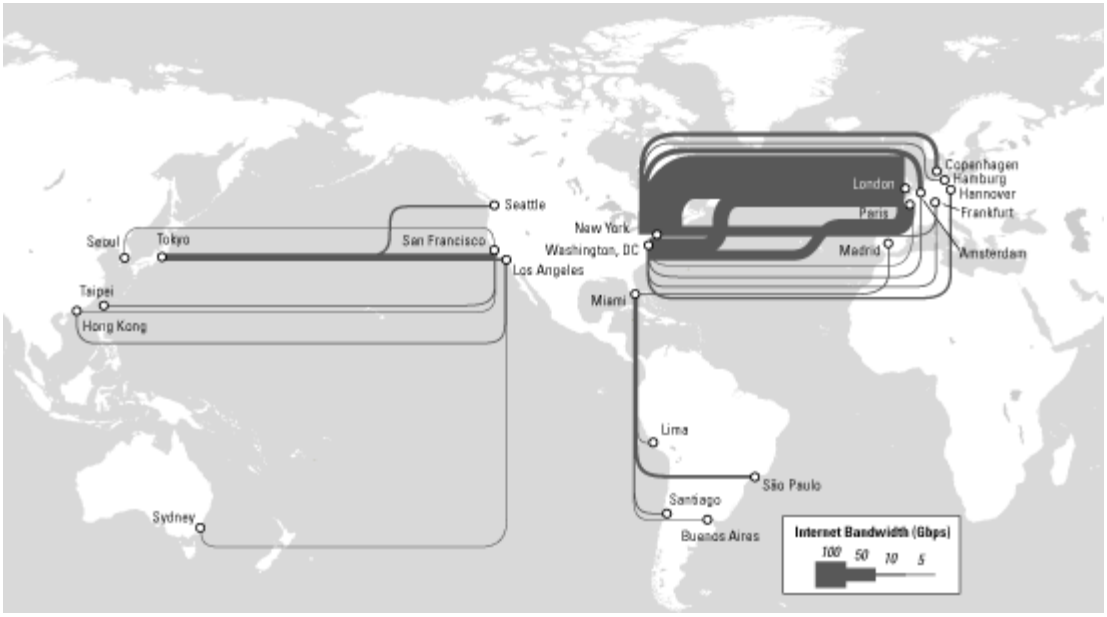

Figure 2 Map of Major Interregional Internet Routes, 2003

Common Facility Components

International traffic is routed through various switching centers located throughout the U.S. The general switching architecture is shown in Figure 3. In most cases, the domestic network is connected to multiple international switches, and each international switch connects to multiple cable landing locations. In some configurations, an alternate cable completes a SONET ring, which is provisioned to handle the entire traffic load and enables instant restoration capabilities. In other configurations, the alternate cable serves as a backup in case the primary cable fails; however, the backup cable may not have enough capacity to handle the increased traffic load. If both cables were to fail or the alternate cable could not handle the entire traffic load, a satellite link[1] would be often used as a secondary backup. This fully redundant architecture is typical for many providers and can sustain multiple points of failure without the loss of connectivity.

Figure 4 shows an end-to-end schematic for an underwater telecommunications cable. One or more landing stations are associated with each end of a cable. Landing stations comprise the "dry plant," and a cable and its components comprise the "wet plant" for a cable system. Communications traffic flows between landing stations.

[1] Although these satellite links are available, they have limited capacity and are not engineered to handle the same levels of traffic as typical wireline architectures.

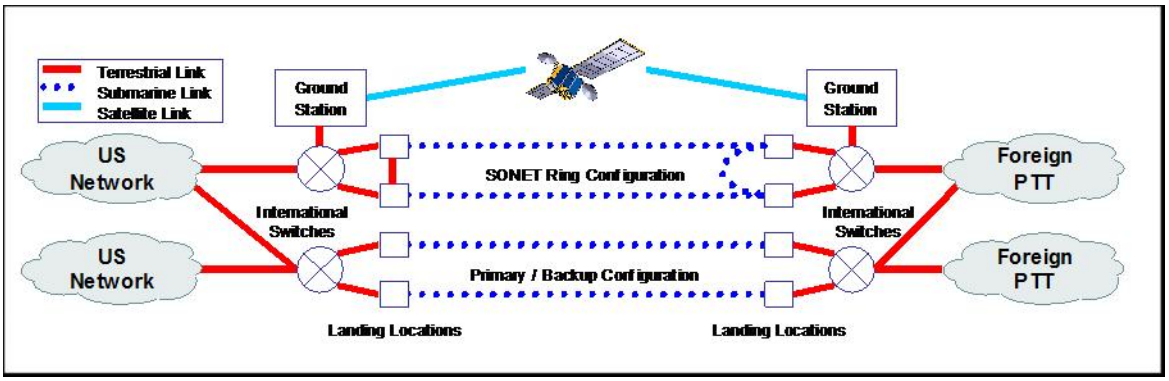

Figure 3 Typical Switching Architecture

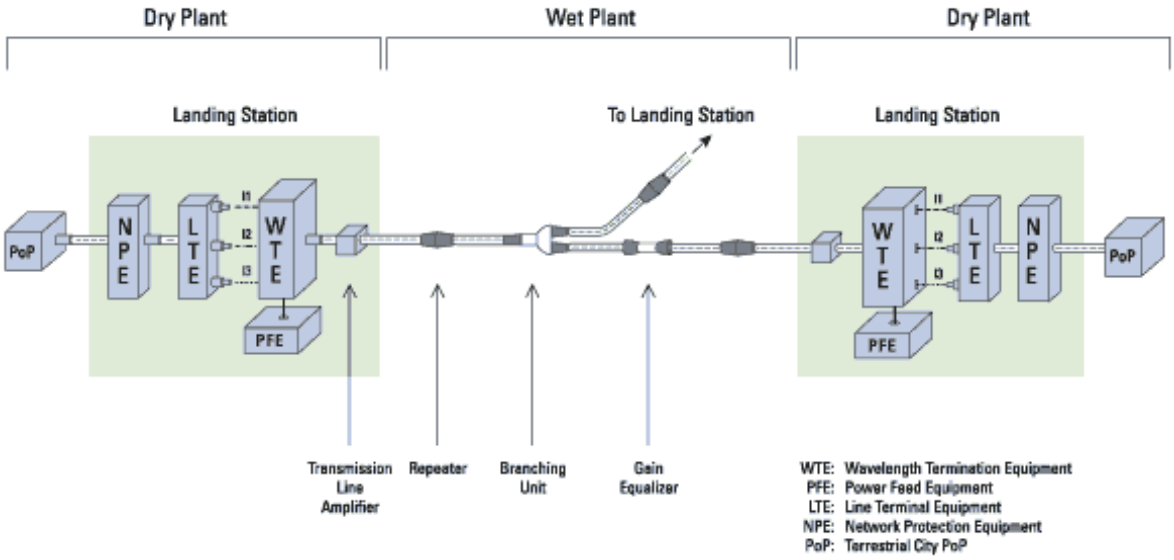

Figure 4 End-to-End Schematic for an Underwater Telecommunications Cable

As shown in Figure 5, a typical cable landing station, or dry plant, consists of a single building that contains:

- Telecommunications equipment
- Power generator
- Battery plant
- One or more control rooms

Cable landing stations are located in areas with a high level of activity such as Manhattan, as well as in somewhat remote areas such as Nedonna Beach, Oregon. Most are located at or near an oceanic shoreline. Connections to the facility include intercontinental fiber, domestic fiber/copper, and power. Telecommunications equipment is typically located in fire-suppression-protected rooms, which are environmentally controlled.

Telecommunications Equipment

Power Generator

Battery Plant

Control Room

Figure 5 Typical Cable Landing Station Equipment

The telecommunications portion of the dry plant typically includes the following components:

- Network protection equipment (NPE),
- Line terminal equipment (LTE),
- Wavelength termination equipment,
- Transmission line amplifiers,
- Circuitry for supervisory functions (cable performance, fault detection, and location), and
- Terrestrial city point-of-presence – a site with a collection of telecommunications equipment (usually modems, digital leased lines, and multi-protocol routers).

At the cable landing station, terminal equipment (NPE, LTE) is installed and connected to the land-side (domestic) communications network. The intercontinental fiber is brought on-shore and is typically trenched (as shown in Figure 6) or routed along ROWs (rights-of-way), such as along bridges and railways.

Figure 6 Cable Trench

Common threats to cable landing stations can take many forms from sabotage to external attack. Attacks can target the fiber, the switching/network control equipment, and/or the power equipment. The primary protection against basic attacks lies in the self-healing ability of networks to reroute traffic around damaged nodes and paths. The primary form of protection against catastrophic attack lies, to a great extent, in the ability to recover from any attack, which may include the reconstruction or relocation of facilities.
Localized damage to fiber-optic cable is relatively easy to repair, unless an entire area is contaminated or unreachable. Furthermore, because of the capability of rerouting, most fiber

breaks do not cause long-term loss of communication unless multiple simultaneous attacks occurred on primary fiber paths. Fiber-optic cable is, however, quite vulnerable, as it is not practical to guard the entire length of every fiber. Because some runs of fiber are easily accessible to the public, they can be readily accessed without detection. Runs of fiber-optic cable from the beach presence to the cable landing station are particularly vulnerable where they are visible aboveground (e.g., along ROWs), or readily accessible belowground (below a manhole cover).

Damage to the landing station itself can be indirect (interruption of power), direct (physical attack on the building), or internal sabotage (fire, physical damage, computer virus).

Power interruptions (e.g., damaging a nearby power substation) are a possible but unlikely target due to the availability of battery backup and integrated power generators. An attack on the power system would more likely take the form of a regional attack that disrupts considerably more than a landing station.

Because equipment is concentrated in a small area and limited physical barriers, landing stations are vulnerable to physical attack by a variety of means, including bombs or armed assault, as damage does not need to be inflicted over a large area to be effective and because such damage can be accomplished quickly.

CONSEQUENCE OF EVENT

Underwater cables form the backbone of international voice and data communications, which include portions of the Internet. International banking, finance, and commerce are highly dependent on these cables. Underwater cables also carry military communications traffic and signals from hydrophones (scientific research and ship guidance). When viewed as a system, these cables comprise a highly sophisticated and robust web of communications channels that has no single point of failure. Telecommunications traffic can be quickly rerouted over alternative channels to bypass failed components. Traffic flow would not be appreciably affected unless several cables or primary landing stations were incapacitated.

In general, cable cuts near the shoreline can be repaired relatively quickly because the cables are more accessible. Conversely, cable cuts that occur in the deep sea may take a few weeks or longer to repair, depending on the location of the cable cut and the position of the closest repair ship. With publicly available information on submarine cable route positions, terrorists could potentially cut many submarine cables along the coast in a short period of time with no attribution. This type of attack, if successfully executed, would effectively disable a large percentage of international connectivity and take several weeks from which to recover. Although satellite backups are available, they may not be able to handle the traffic volume if several of the major submarine cables were cut.

Despite numerous and frequent individual cable cuts, the U.S. has suffered little disruption of international service. A worst-case scenario that completely disrupts all international telecommunications would have to involve simultaneous damage to both the submarine cable infrastructure and the satellite infrastructure in various U.S. locations. While such an event is highly unlikely for the U.S., this type of worst-case scenario actually occurred for Algeria on

May 23, 2003, as a result of an earthquake. This event damaged several submarine cables in the Mediterranean Sea and satellite ground stations in Algeria, leaving little international connectivity for Algerian telecommunications.[2] Although international connectivity was quickly restored through other terrestrial channels, repairs to the submarine cables were not completed until June 21, 2003, partly because of instability resulting from recurring aftershocks caused by the earthquake.[3]

[2] http://quickstart.clari.net/qs_se/webnews/wed/bi/Qalgeria-quake-telecoms.RxjR_DyN.html
[3] http://www.dailymailnews.com/200306/22/news/city02.html

COMMON VULNERABILITIES

Critical infrastructures and key assets vary in many characteristics and practices relevant to specifying vulnerabilities. There is no universal list of vulnerabilities that applies to all assets of a particular type within an infrastructure category. Instead, a list of common vulnerabilities has been prepared, based on experience and observation. These vulnerabilities should be interpreted as possible vulnerabilities and not as applying to each and every individual facility or asset.

The following is a list of common vulnerabilities found at cable landing stations and along the routes of underwater cables.

Exhibit 1 Economic and Institutional Vulnerabilities	
Economic and institutional vulnerabilities are those that would have extensive national, regional, and industry-wide consequences if exploited by a terrorist attack.	
1	Underwater cables carry 95% of international business, banking, and commerce transactions. Damage to a single cable is unlikely to cause much disruption. Destruction of a cable landing station, particularly one that is a point of presence for more than one cable, is potentially more serious. In most instances, there is enough capacity in the entire system to avoid serious disruptions to business, though a multi-location attack may result in long-term damage, albeit predominantly economic.
2	Almost all intercontinental Internet traffic is carried on underwater cables.
3	Coastal U.S. underwater cables avoid congested terrestrial telecommunications corridors. Because of the existence of terrestrial and other communications channels, disruption of one of these coastal underwater cables is not likely to have a significant impact on business, banking, and commerce transactions and Internet traffic.
4	A distinguishing vulnerability of intercontinental underwater cables is attributable to the fact that the other end of a cable lands in a foreign country. Although cable systems are usually constructed and maintained through cooperative ventures between domestic and foreign companies, financial and political conditions may result in changes of the cable's control. Such changes could pose a threat to the planned operation of a cable. A point of fact is the recent bankruptcy of Global Crossing, a major cable system operator. The disposition of this company and its cable systems is of concern to the U.S.
5	Because of the threats posed by mariners, information on underwater cable routes through lakes, rivers, and coastal shores is made widely available through NOAA, the Coast Guard, and other sources.

Exhibit 2 Site-Related Vulnerabilities

Site-related vulnerabilities are conditions or situations existing at a particular site or facility that could be exploited by a terrorist or terrorist group to do economic, physical, or bodily harm, or to disable or disrupt facility operations or other critical infrastructures.

Access and Access Control	
1	Public roads are in close proximity to cable landing stations.
2	Cable landing stations may not have perimeter fencing. If they have perimeter security, it may only have chain-link fences and remote cameras.
3	Public roads or rail lines pass over or next to cable landing stations.
4	Cables may pass under/along side other structures (e.g., bridges).
5	Cars and trucks may be parked near a cable landing station.
6	Uncontrolled waterways may provide access above underwater cables.
7	Approach structures [piers] may be accessible to foot and vehicle traffic.
8	Cable landing stations may not have security guard forces.
9	Signs to deter vehicles, boats, or pedestrians from approaching underwater cable routes or cable landing stations may not be posted, though ironically may facilitate an attack if posted.
10	Video surveillance may not be in place at cable landing stations.
11	Lighting may be inadequate in certain parts of the landing stations (e.g., too little, poorly spaced, or improperly directed).
12	Vegetation may provide adequate cover for potential adversaries.
13	Cable landing stations may be accessed via private access roads.
14	Cable landing stations may be vulnerable to attack from the air.
15	Due to the length and location of underwater cables, countermeasures may not be practical to install.
16	Submarine cable routes may not be patrolled on a regular basis.
17	The cabling conduit from the ocean may be accessible from the street via standard manholes.
Operational Security	
18	Technical and operational specifications may be publicly available.
19	Local operating procedures may be widely known and easily obtained.
20	Websites may provide detailed information on critical assets, maps, and other operational data.
Emergency Planning and Preparedness	
21	Uncontrolled access to private industry security information shared by various agencies may compromise the effectiveness of asset protection (CIP Act of 2002).
22	Coordination with local, state, and federal agencies on roles/responsibilities may be inadequate.
	(Continued on next page.)

23	Interoperability of communications systems (LEA, EMT, NGB, FEMA, Hazmat Response) may be limited.
24	Nontraditional fires/explosions may cause additional challenges to first responders.
25	There is electrical current around cable landing station infrastructure. Emergency personnel must make sure that a station employee verifies that power has been cut off before attempting any response efforts near any underwater cable landing station.
26	Contingency plans may not always be adequately formalized or exercised.
27	Cable cuts that occur in the deep sea may take a few weeks or longer to repair, depending on the location of the cable cut and the position of the closest repair ship. Mutual aid agreements are in place to expedite repair.

Exhibit 3 Interdependent Vulnerabilities

Interdependency is the relationship between two or more infrastructures by which the condition or functionality of each infrastructure is affected by the condition or functionality of each other. Interdependencies can be physical, geographic, logical, or information-based.

General	
1	Cable landing stations are critical nodes in intercontinental telecommunications systems. International banking, finance, and commercial transactions depend heavily on underwater cables.
2	Internet traffic, including scientific research, depends heavily on underwater cables.
Electric Power	
3	Cable landing stations rely on electric power grids to operate auxiliary equipment and power repeater systems, though this risk is most effectively mitigated with on-site battery backup and generators.

OTHER INFORMATION

Concentration of International Switching Facilities

While the landing points of submarine cables are fairly diverse, many of the facilities that handle a significant portion of international switching are located in the same general vicinities (e.g., Manhattan). This is even more the case in other countries such as the United Kingdom and Australia where virtually all international switching is concentrated in one or two areas. Within the U.S., the telecommunications industry can diversify international switching functions to other facilities along the backhaul fiber infrastructure connected to the submarine cables. This backhaul fiber infrastructure is diverse and not concentrated in any one particular location.

Availability of Information

Due to the free flow of information and government regulation, researching the cable landing locations as well as their "target value" based on the volume/type of traffic, is possible through research online and through various companies such as telegeography. Further, some organizations document these locations with photographs and assessments, and make this information readily available for free, or conveniently on CD for a modest fee (http://cryptome.org).The value of attacking a cable landing station has also been discussed online at http://asksollog.com/2002/0801.shtml.

Landing Locations

In general, terrorists could potentially sabotage submarine cables and cable landing locations with minimal expertise and funding. Increasing security at all submarine cable landing locations in the U.S. to buffer against terrorist attacks may be prohibitively expensive. Also, submarine cable operators may not be willing to invest large amounts to further secure these locations. Furthermore, without strong international agreements, the U.S. has little to no ability to influence protection of the corresponding submarine cable landing locations that reside on foreign soil.

USEFUL REFERENCE MATERIAL

1. The White House, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, Feb. 2003 [http://www.whitehouse.gov/pcipb/physical.html], accessed Aug. 11, 2003.
2. Federal Communications Commission, *Cable Landing License Act (*47 USC §§ 34-39*)* [http://www.fcc.gov/ib/pd/pf/clla.html], accessed Aug. 11, 2003.
3. U.S. Environmental Protection Agency, *Federal Register Environmental Documents: Review of Commission Consideration of Applications Under the Cable Landing License Act* [http://www.epa.gov/fedrgstr/EPA-IMPACT/2002/January/Day-14/i789.htm], accessed Aug. 13, 2003.
4. United Nations, *Regulatory Aspects of Underwater Cable Protection*, by Kuwazuru, Masakuni, and R. Hoshina.
5. Yamamoto, S., *The Law of the Sea* (in Japanese).
6. Wagner, E.S., B. Belkin, and D.R. Burnett, "International Legal Aspects in Submarine Cable Protection," *Proceedings of SubOptic '93*, Versailles, France, pp. 491–496.
7. E.S. Wagner, "Submarine Cables and Protections Provided by the Law of the Sea," *Marine Policy*, **19**(2):127–136, 1995.
8. Shapiro, S., J.G., Murray, R.F. Gleason, S.R. Barnes, B.A. Eales, and P.R. Woodward, "Threats to Submarine Cables," *SubOptic '97* [http://www.scig.net/Section07b.pdf], accessed Aug. 12, 2003.
9. Williams, D.O., *An Oversimplified Overview of Undersea Cable Systems* [http://davidw.home.cern.ch/davidw/public/SubCables.html], accessed Aug. 13, 2003.
10. Institute for Security Technology Studies at Dartmouth College, *Information and Telecommunications Sector Vulnerabilities and Threats*, Sept. 2002.
11. Federal Energy Regulatory Commission, *FERC Approves Process for Lake Erie Link: Project Meets Significant Regulatory Milestone* [http://www.electricityforum.com/et/issue0302/i03_ferc.htm], accessed Aug. 12, 2003.
12. Panepento, P., "Underwater Cables Would Link Canada to U.S. Power Grids," *Erie Times*, Dec. 10, 2001 [http://www.greatlakesdirectory.org/pa/1210cable.htm], accessed Aug. 13, 2003.
13. *History of the Atlantic Cable & Submarine Telegraphy* [http://www.atlantic-cable.com/], accessed Aug. 13, 2003.
14. Bill Glover's chronological record of every known submarine communication cable [http://www.atlantic-cable.com/Cables/CableTimeLine/index.htm], accessed Aug. 11, 2003.
15. NOAA's Office of Coast Survey provides nautical charts showing the routes of underwater electric and telecommunications cable, as well as underwater pipelines [http://www.nauticalcharts.noaa.gov], accessed Aug. 12, 2003.

RELATED WEBSITES

1. U.S. Department of Homeland Security [http://www.dhs.gov/dhspublic/index.jsp], accessed Aug. 11, 2003.
2. Federal Bureau of Investigation [http://www.fbi.gov/], accessed Aug. 14, 2003.
3. U.S. Environmental Protection Agency [http://www.epa.gov/], accessed Aug. 11, 2003.
4. U.S. Department of State [http://www.state.gov/], accessed Aug. 13, 2003.
5. Federal Energy Regulatory Commission [http://www.ferc.gov], accessed Aug. 14, 2003.
6. United Nations [http://www.un.org/], accessed Aug. 13, 2003.
7. Oregon Fishermen's Cable Committee [http://www.ofcc.com], accessed Aug. 11, 2003.
8. The International Cable Protection Committee [http://www.iscpc.org], accessed Aug. 14, 2003.
9. Global Marine Systems [http://www.globalmarinesystems.com], accessed Aug. 11, 2003.
10. KDDI-SCI [http://www.kddiscs.co.jp/e/business/02.html], accessed Aug. 11, 2003.
11. Makai Ocean Engineering Inc. [http://www.makai.com], accessed Aug. 11, 2003.
12. Global Crossing [http://www.globalcrossing.com], accessed Aug. 11, 2003.
13. Neptune Regional Electrical Transmission System [http://www.neptunerts.com], accessed Aug. 11, 2003.
14. The International Cable Protection Committee [http://www.iscpc.org], accessed Aug. 13, 2003.
15. Federal Energy Regulatory Commission [http://www.ferc.gov], accessed Aug. 14, 2003.
16. John Young's Eyeballing Series [http://cryptome.org/cable-eyeball.htm], accessed Aug. 14, 2003.
17. Compagnie Financière Alcatel [http://www.alcatel.com/submarine/index.htm], accessed Aug. 11, 2003.
18. Telegeography [http://www.telegeography.com], accessed Aug. 12, 2003.
19. "Ask Sollog" (discussion of Cable Landing Site takeover) [http://www.asksollog.com/2002/0801.shtml], accessed Jan. 14, 2004.