
SUBMARINE CABLE INFRASTRUCTURE

INTRODUCTION

The backbone of the nation's—and indeed, of the world's—information infrastructure is now preponderantly composed of fiber optic cables. A critical element of that backbone is the world's ever-expanding network of submarine fiber optic cables. The importance of those cables could conceivably make them a potential target or targets for other states or terrorists. This appendix briefly documents the importance of the fiber optic cable network to the United States, potential vulnerabilities in the network, and the possible ramifications for the United States of a widespread network failure brought about by an act of sabotage.

Over the past decade, the increased demand for bandwidth driven by the Internet, as well as the continuing international trend of privatization of national telecommunications industries, has outstripped by far the resources offered by satellite transmission of voice and data (Petit, 1999). Instead, the fraction of transoceanic voice and data transmitted over undersea cables has grown in the past 12 years from 2 percent to as high as 80 percent in 2000 (Mandell, 2000). As demand has grown, so have the numbers of cables on the seabed.

While experts differ on whether the world's fiber optic network faces a capacity “glut” or “crunch,”¹ it is certain that demand for higher

¹For pieces bullish on bandwidth, see Williamson (2000), McClelland (2000), and Rowley and Ling (2000). One article suggesting a future glut is Behr (2000).

bandwidth will continue to grow, and with it, the capacity of cables—those currently existing and those soon to be laid—to grow hand in hand. Due to be completed this year, for instance, is the Southern Cross cable network, offering a quantum leap in carrying capacity in the Southern Pacific (up to 160 gigabytes per second) in a three-tiered ring totaling some 29,000 kilometers. Similarly advanced systems are due to come on-line in the North Atlantic as well, increasing the total transatlantic carrying capacity to more than 1,000 gigabytes per second, enough capacity for the contents of 200 compact discs to be transmitted every second (McClelland, 2000).

VULNERABILITIES?

These fiber optic networks offer a number of security advantages over satellite communications. Fiber optic cables are thought to be much harder to “eavesdrop” (Mandell, 2000) on than satellites and have more dependable installation and repair practices (Mandell, 2000).

However, those fiber optic cables are in many ways significantly more vulnerable than is commonly thought. Submarine cables already face many man-made and natural dangers. Anchors dropped from ships and dredging fishing nets are two of the most common (McClelland, 2000; ICPC, 1996). The occasionally volatile nature of the seabed can expose a previously buried segment of cable (ICPC, 1996). Between 1985 and 1987, AT&T found that its first deep-sea submarine fiber optic cable (laid between the Canary Islands, Grand Canaria and Tenerife) suffered periodic outages because of frequent attacks of the *Pseudocarcharias kamoharai*, or crocodile shark, on the cables.² In deep ocean, the cables often lie unprotected on the ocean floor; cables in areas closer to the shore, where seabed activity might include fishing, are usually both armored and buried some two to three feet deep in the ocean floor (ICPC, 1996). The cables need only be bent to suffer significant damage (ICPC, 1996).³

²The electric fields of which, it was thought, duplicated that of the shark’s prey under attack (Martin, 2001).

³“Any sharp bend will cause [fibers] to crack and signals to be lost” (ICPC, 1996). Even a slight bend may cause the cables to suffer significant drop-off in the strength of the signal (Held, 1999).

Security is an important issue, because these cables are an increasingly vital element of the global economy. As one analyst has noted, “the increase in demand is being driven primarily from data traffic from Web-enabled applications . . . undersea cables are becoming an integral part of the everyday telecommunications infrastructure in a world that has no boundaries” (Carlson, 2000). In short, an intentional systemwide disruption of fiber optic cables could cause significant commercial damage.

In particular, the ability of overseas firms to get reliable, real-time data regarding U.S. markets—and vice versa—could be substantially curtailed, potentially sparking a panic. In addition, an increasing amount of U.S. military communications occurs over these commercial networks. Disruption could significantly impede these communications. In all cases, of course, action would be taken to shift transmissions from the disrupted networks to other cables and satellite transmissions. But, as discussed above, the current satellite capacity is far exceeded by bandwidth demand. As we will see below, this problem becomes even more marked when examining the case of an island, such as Taiwan.

Potential Vulnerabilities

In recent years, wiring companies have focused on redundancy as an important aspect of the cable network. While early fiber optic cables were “point-to-point” systems, modern systems are configured as loops, connecting two landing stations—at least 100 kilometers away from one another—in one country to two in another. Because it would be unlikely for an isolated nautical event—a sudden shift in the seabed on which the cables rest, for instance, or an inadvertent break caused by a fishing net or a ship’s anchor—to affect both cables, the systems are thought of as secure (Williams, 2000).

However, the desire for security against inadvertent nautical events may have been counterproductive. When seeking adequate termination points for cables, companies have faced a relative paucity of suitable sites (relatively isolated from heavy fishing activity and strong ocean currents), particularly on the East Coast (see Table I.1). Because of this lack of sites, and given the considerable effort in digging a trench on the seabed for the last kilometers of the cable, then

Table I.1
Submarine Cables Terminating in the Northeast United States

Cable Name	Capacity	Termination Points (U.S.)	2d Termination Point
TAT-8	280 MB/s	Tuckerton, N.J.	
BUS-1	2.5 GB/s	Tuckerton, N.J.	
PTAT-1	420 MB/s	Manasquan, N.J.	
CANUS-1	2.5 GB/s	Manasquan, N.J.	
Gemini	2 × 15 GB/s	Manasquan, N.J.	Charlestown, R.I.
TAT-14 (planned)	16 × 10 GB/s	Manasquan, N.J.	Tuckerton, N.J.
TAT-9	560 MB/s	Manahawkin, N.J.	
TAT-11	560 MB/s	Manahawkin, N.J.	
TAT-10	560 MB/s	Green Hill, R.I.	
TAT 12/13	2 × 5 GB/s	Green Hill, R.I.	Shirley, N.Y.

tunneling from the ocean bed up into a beach manhole, to bring the cable ashore, cable companies have, again, especially on the East Coast, repeatedly placed cable termination points on the same shore (Chave, 2000).⁴

The results of this “stacking” can be seen in Table I.1. Of 10 cable systems with a total capacity of about 206 gigabytes per second (assuming that TAT 14 begins operations as planned in 2001), six terminate in only one of the same three cities, Tuckerton, Manasquan, and Manahawkin, New Jersey. One—a self-healing loop—terminates in both Tuckerton and Manasquan. A sixth terminates in both Manasquan and Charlestown, Rhode Island. Theoretically, an attack on two or three of these sites—at the point where the cables come together in the undersea trench before coming ashore—could cause enormous damage to the entire system. For instance, a successful attack on trenches in Tuckerton and Manasquan and Charlestown would eliminate all but 11 gigabytes per second of carrying capacity in that region—a 95 percent cut.

Similarly, all submarine cables but one terminating in the south of the United States terminate at one of three points in Florida: Vero Beach, Palm Beach, and Hollywood.

⁴The authors are indebted to Doctor Chave for his patient description of this process.

Of course, it is important not to overstate the potential problem. After all, the United States is not isolated—some transmissions could be rerouted through systems in Canada and South and Central America. However, given that the vast majority of transatlantic and transpacific cables terminate in the United States, the prospect of a concerted attack on these cables is troubling.

Moreover, this point yields an interesting counterexample: that of Taiwan. Unlike the United States, Taiwan would be unable to depend on a vast overland information infrastructure beyond its borders in the event of damage to its fiber optic lifelines. A recent example of the chaos potentially caused by communications outages is that of Australia. One cut cable in the SEA-WE-ME-3 network leading from Australia to Singapore caused Australia's largest Internet provider—Telstra—to lose up to 70 percent of its Internet capacity (Miller, 2000; LaCanna, 2000; Park, 2000a and 2000b).

As seen in Table I.2, a recent survey of the number of international submarine cables reaching Taiwan is particularly disconcerting. Four out of five undersea fiber optic cables reaching Taiwan do so at either Fangshan or Toucheng (the fifth, a “self-healing loop” reaches Taiwan at both, meaning that both cables would have to be damaged for Taiwan to be cut off). Two more planned cables have landing

Table I.2
Submarine Cables Reaching Taiwan

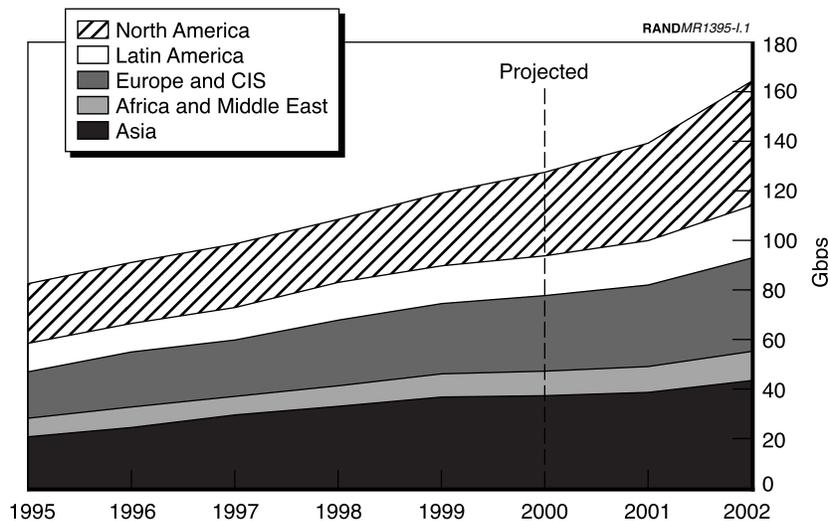
Cable	Capacity	Termination Points (Taiwan)
GPT	280 MB/s	Fangshan
Hon-Tai 2	420 MB/s	Fangshan
APC	2–3 × 560 MB/s	Toucheng
APCN	5 GB/s	Toucheng
SEA-ME-WE-3	2.5 GB/s	Toucheng and Fangshan
China-U.S. (Planned)	4 × 20 GB/s	Fangshan
APCN2 (Planned)	2fp × 8d × 10 GB/s	Tanshui
H-P-T (Planned)	4fp × 2d × 10 GB/s	Fangshan

SOURCE: Charts on the Web site of the ICPC, available at <http://www.iscpc.org/cabledb>.

areas at Fangshan. Only one planned cable is due not to land at either Fangshan or Toucheng. In short, Taiwan's ability to send and receive data over submarine cables might be significantly impaired by an attack on cables leading into either landing area. A well-orchestrated set of undersea attacks on the cable "trenches" at both locations might well have a sudden and calamitous effect on Taiwan's ability to communicate with the outside world. This information may well have increased relevance in light of China's renewed emphasis on information warfare.

Conclusion

By 1969, analysts had perceived vast potential military and economic benefits in cable's exploitation (IISS, 1969). With the explosion in importance of fiber optic networks (see figures I.1, I.2, I.3, and I.4 to



SOURCE: Euroconsult.

NOTE: Chart assumes that a pair of 36-MHz equivalent transponders will yield approximately 40 Mbps transmission capacity. Transponder inventory refers to available capacity in orbit (minus satellites retired) or already under construction at the end of March 2000.

Figure I.1—Growth in Satellite Communication

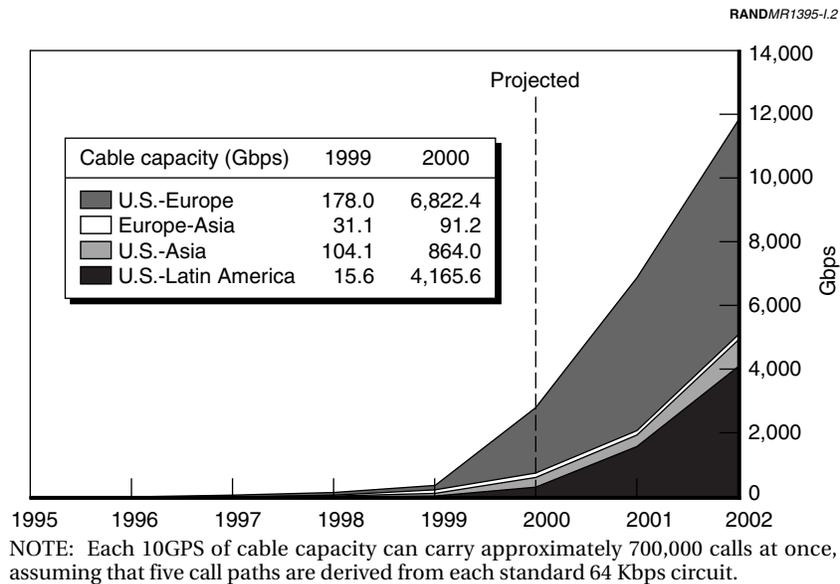
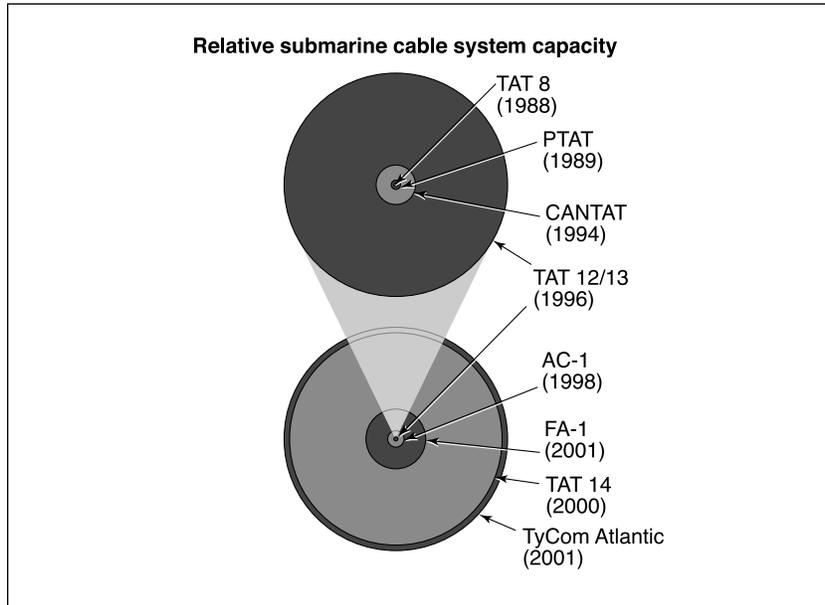


Figure I.2—Growth in Cable Communications

compare the growths of satellite communications, cable, communications, and submarine cable bandwidth), this potential has been realized and will continue to grow; at the same time, however, so will the attendant vulnerability. The submarine fiber optic cable network is of great importance to the United States (see Figures I.5 and I.6 for a glance at the cables terminating on each coast). Moreover, constraints on cable laying mean that several cables are likely to be bundled together, offering a potentially lucrative target for sabotage.

In most industry publications, however, little attention is given to the possibility of deliberate attack on the fiber optic network. Indeed, one of the few discussions of the possibility says simply that “while undersea cables could be cut, the practice of burying the in-shore segments makes this difficult; the mid-ocean portions are hard to find without a map and help from shore-based monitoring stations” (Mandell, 2000).

RANDMR1359-I.3



NOTE: Cables are scaled to announced maximum upgradable capacity.

Figure I.3—Growth in Submarine Cable Bandwidth

Given the above, however, it is clear that more attention should be paid to the potential for deliberate attacks on the global fiber optic cable network (see figures I.7 and I.8 for a look at some of the cables terminating in Asia and Europe). Currently, for instance, shore authorities have positioned radars and occasionally scheduled flyovers for areas in New Jersey that might be targeted (Chave, 2000). The NR-2 with the capacity to maneuver and search on the seabed may be the most valuable asset of all in monitoring the status and security of cables terminating in the United States and on the shores of our allies.

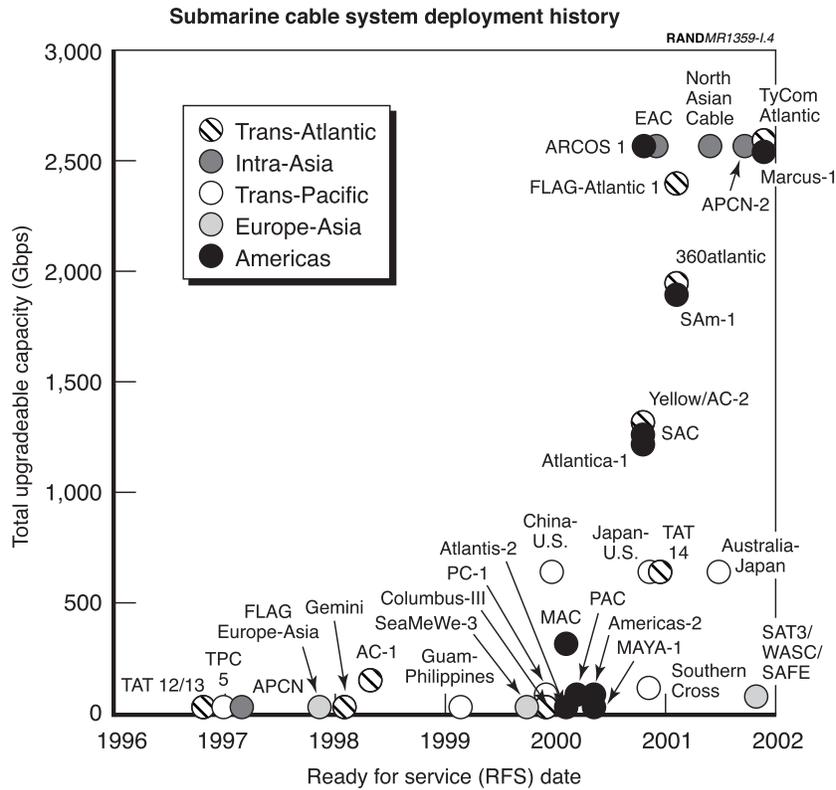


Figure I.4—Historic Growth of Submarine Cable Capacity

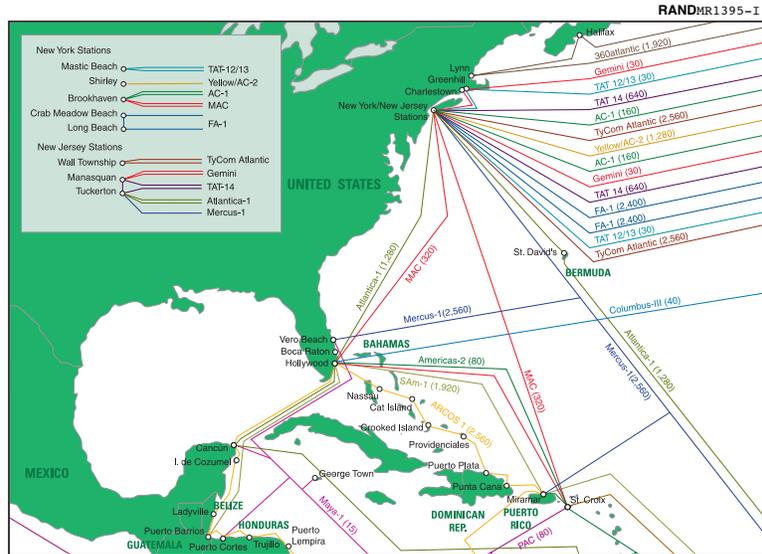


Figure I.5—Submarine Cables Terminating on the East Coast

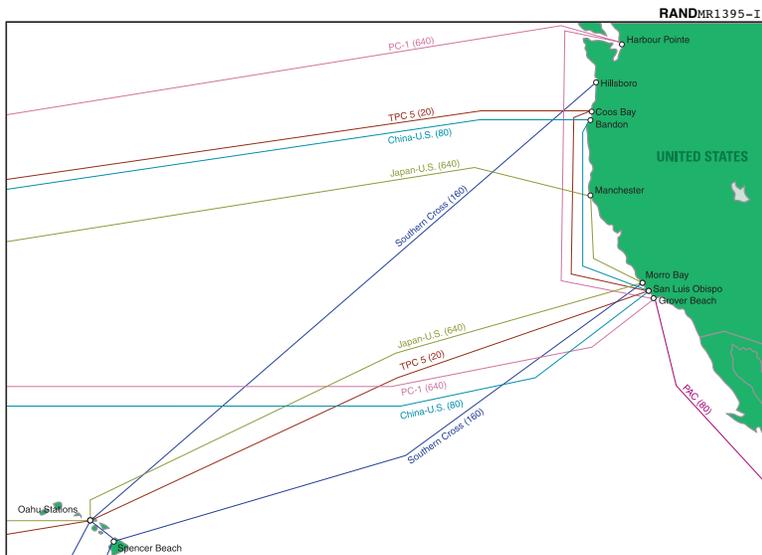


Figure I.6—Submarine Cables Terminating on the West Coast

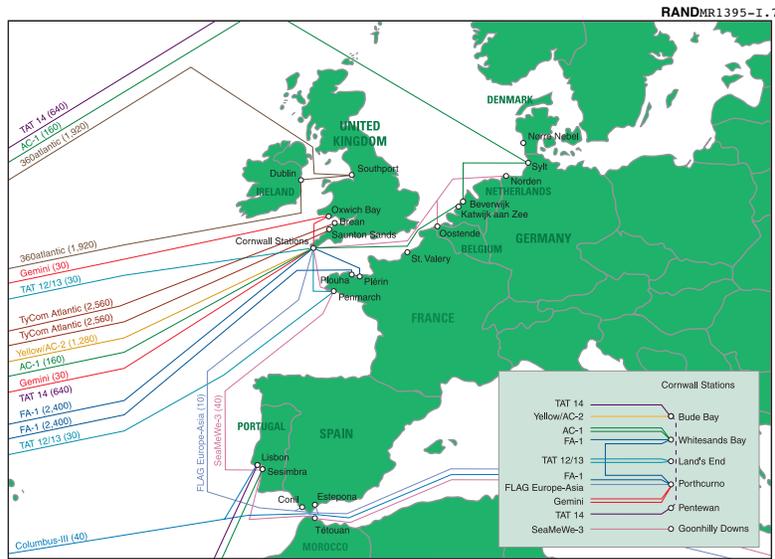


Figure I.7—Submarine Cables Terminating in Europe

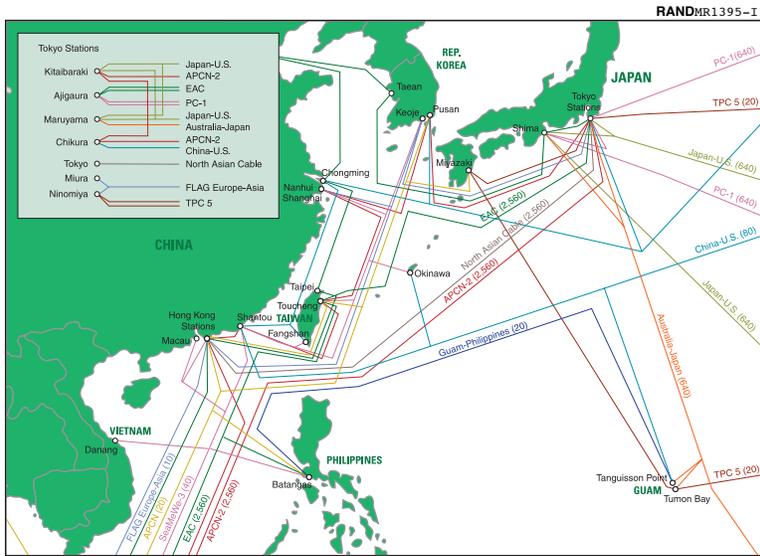


Figure I.8—Submarine Cables Terminating in East Asia