29 DEC 2016 NEWS FEATURE

All At Sea

Danny Bradbury Contributing Writer
Follow @dannybradbury

When you watch Netflix, deal with your email or make a Skype call, the traffic travels along a relatively small number of routes to its destination. Like most of the world's internet traffic, it travels via submarine cables, typically the width of a garden hose. Today, there are 356 of these cables spread across the world. How safe are they from attack or disruption?

These cables run between continents, channelling terabits of information down a single fibre-optic link. They are incredibly expensive to build, with a transatlantic link costing around $500 million, and only a handful of firms have the ability to lay them.

Laying the cables is a tricky business. Out in deep ocean waters, there are few threats to the integrity of a cable, and cable-laying ships will simply let them fall unprotected to the sea floor. As the cables get closer to the shore, though, the ocean bed becomes shallower, and more threatening. Wayward anchors can easily sever a cable. Consequently, for several miles before they come ashore they're protected by strong metal sheathing. When they hit land, they'll typically connect to land-based fibre cables in trenches protected by manhole covers or in anonymous-looking concrete shacks.

There are two kinds of potential attack on the submarine cable system. The first involves denial of service by disruption.

Information about cable locations is documented by several organizations including the National Oceanographic Data Center (DMA/NOAA) in the US and the UK's Admiralty Hydrographic Office. If a cable's ingress point is relatively unprotected, then wouldn't a determined adversary be able to disrupt internet service – and therefore key parts of the critical national infrastructure – by simply blowing one up?

Why Not Watch?

4 OCT 2016

Yahoo! A Breach Too Far or the Reality of Consumer Privacy

5 MAR 2015

How to Build a generation Sec Programme

It's a risk, admits Tim Stronge, vice president of research at telecommunications research firm TeleGeography. In the deep sea, attackers are effectively targeting a piece of garden hose. "At the beach, it might be a little harder but a determined adversary could damage where the cable comes in or they could damage or blow up a facility where the traffic is exchanged," he says.

There are a handful of cases in which cables have been cut intentionally. In 2007, fishing trawlers near Vietnam did just that, pilfering 61 miles of undersea cables for copper content, taking out cables in southeast Asia for several months in the process.

The answer to these risks is safety in numbers, argues Stronge. In many developed countries, multiple cables land in different parts of the country. If one cable were to be disrupted, then there would be others that could take up the slack.

"The fact that the cable breaks a lot and Americans and Europeans hardly hear about it is because there is so much failover," he says.

Some undersea cables are also structured with their own redundancy, Stronge points out. The Southern Cross cable that connects the US with Australia was laid in a built-in redundant ring formation that can fail over in the event of a break, he says.

Keith Schofield, general manager of the International Cable Protection Committee, adds that many submarine cables have far more capacity, thanks to technologies that make the capacity upgradable by enhancing equipment at either end.

"It's rare for those cables to be full on day one", he says. So if one cable is cut, another can take up the slack.

How many cables would an attacker have to sever to bring down a country's internet? It depends on the region. Southeast Asia in particular is constrained by two things. First, it faces a lack of diversity. Lots of licensees want the same routes to minimise latency, resulting in high concentrations of traffic, and the cables are clustered into choke points. A 2016 Verizon report identified historically proven single points of failure in this region and across the north and eastern coast of Africa.

The second constraint in the Indian ocean concerns national policy. There are a finite number of repair ships that can hoist cable from the sea floor and repair it using splicing equipment. In some regions, such as Indonesia, a 'cabotage' policy that favours locally-owned vessels can hold up repairs. That is gradually changing, says Schofield.

"Now, nations are beginning to realise that it's not in their citizen's interest to restrict access to the Internet," he says.

More generally, situations have arisen where it has taken time for a vessel to become available and get to the repair point. The more outages that happen at once, the greater the overhead on the repair assets. A concerted attack could theoretically cause significant problems.

Submarine snooping

The second kind of attack is more covert: tapping the cables directly to snoop on information. This has been done domestically, says Telegeography's Stronge, because the Snowden files tell us so. BLARNEY and FAIRVIEW were all data gathering projects which involved "collection of communications on fiber cables and infrastructure as data flows past," according to a leaked NSA document. These could just as easily be harvested with the operators' collaboration, which has happened on several occasions.

What about foreign governments snooping on a nation state's cable operation? Would it be possible to splice the cable using the same equipment used to repair it? It would be difficult, argues ICPC's Schofield, because operators would sense differences in signals on a tapped line. However, the US has equipped military vessels such as the SS Jimmy Carter with cable splicing mechanisms in the past.

Need for international governance

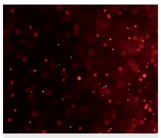
We shouldn't overcook the risks associated with undersea cable, warn experts, but they are there. This is why the ICPC earlier this year identified several security gaps that should be filled. It wants tighter laws to punish intentional cable destruction in international waters, because currently, few if any penalties exist. Penalties for destroying cables inside national waters are also woefully mild, Schofield adds.

Nations should cut through the red tape, getting rid of "cabotage" and other restrictions, to

in 2016?

5 DEC 2012

Malware Update - sponsored by FireEye



26 MAR 2015

Insights into Incident Respo
A View from th
Front Lines

Related to This Story

Cable modem hacker convicted of defraudin
firms out of $1 million

Ransomware Economics: Why the Threat is H
Stay

Edward Snowden: The Internet Is Not Our En
and Encryption Can Protect It

The EU Sees Itself as an Honest Broker for Int
Governance

#BHUSA Kaminsky Highlights Flaws of Lead
Internet

What's Hot on Infosecurity Magazine?

Read | Shared | Watched | Editor's Ch

1 29 DEC 2016 NEWS FEATURE
All At Sea

2 28 DEC 2016 BLOG
The Non-Refundable Fundamen
Estimating the Cost of a Data Br

3 28 AUG 2013 NEWS
Password Cracker Cracks 55 Cha
Passwords

4 23 DEC 2016 NEWS
Researchers Discover New Lean
Mean ATM Malware

5 29 DEC 2016 MAGAZINE FEATURE
Ransomware Economics: Why th
Threat is Here to Stay

6 23 DEC 2016 NEWS
VPN Firms Set for a Great 2017 T
to Snoopers' Charter

expedite the repair process, he added.

Finally, co-ordination is key, he warns. He wants desktop-style exercises between the ICPC and multiple states to play out procedures for repairing cables. At a national level, he wants countries including the US to overcome the 'too many cooks' problem. Several government agencies have jurisdiction over some element of submarine cables, but there is no one agency with total oversight. That impedes co-ordinated protection of the cable ecosystem, he warns, adding that Australia and Singapore have rationalized submarine cable control with effective results.

It would take a concerted attack on the cable infrastructure to make a dent in it. After all, the internet itself was designed to route itself around damage. But the risks are there. While the authorities work slowly to improve its resilience, some countries are taking ownership themselves. Facebook and Microsoft are both laying their own cable, and Google's is already live. That represents yet another layer of vertical integration for these hyperscale firms – and just a little more peace of mind.

The Magazine
About Infosecurity
Subscription
Meet the Team
Contact Us

Advertisers
Media Pack

Contributors
Forward Features
Op-ed

Subscribe to Infosecurity Magazine

Terms and Conditions Privacy Policy Use of Cookies Sitemap