Submarine Cables and Internet Resiliency

The IIJ Innovation Institute is engaged in research that helps to improve the resiliency of the global Internet through measurement and analysis. In this chapter, we report on research that aims to improve resiliency by understanding the submarine cables that underpin the Internet. This is a summary of a paper presented at ACM HotNets 2018[*1].

3.1 Introduction

Ninety-nine percent of all international data is carried by submarine cables[*2]. Deployments of the submarine network date back to the mid-19th century, and total capacity of this undersea infrastructure is now growing at an exponential rate. Today, a complex mesh of hundreds of cables stretching over one million kilometers[*3] connects nearly every region in the world (Figure 1). It comprises both the operation backbone of major corporations' global services and cables that ensure connectivity to regions with limited terrestrial connectivity[*4*5].

Yet, despite the impressive scale and criticality of the submarine cable network, past studies have either treated it as a black box or focused on specific events and their impact on particular links, and its role in the global Internet is not well understood.

Here, we describe the growth and state of the submarine cable network based on publicly available information and put forward an approach for examining the impact of submarine cable disruptions on the global network based on observational data.

3.2 Background to the Submarine Cable Networks

The first commercial submarine cable was laid across the English Channel in 1850. Early cables were made of stranded copper wires and used for telegraphy. Fiber-optic cables were developed in the 1980s and the first fiber-optic transatlantic cable (TAT-8) was put into operation in 1988. Today nearly all cables are fiber-optic cables. In modern cables, the core optical fibers are protected by multiple layers, depending on the cable depth, including a copper tube, an aluminum water barrier, stranded steel wires, and a polyethylene shield (Figure 2). Cables vary in thickness from 10cm in diameter, weighing around 40t/km for shore-end cable, to 2cm in diameter, weighing about 1.5t/km, for deep-sea cable.

Most submarine cables have been constructed and are managed by consortia, and shared by multiple network operators. TAT-8, for instance, had 35 participants including most major international carriers at the time (including

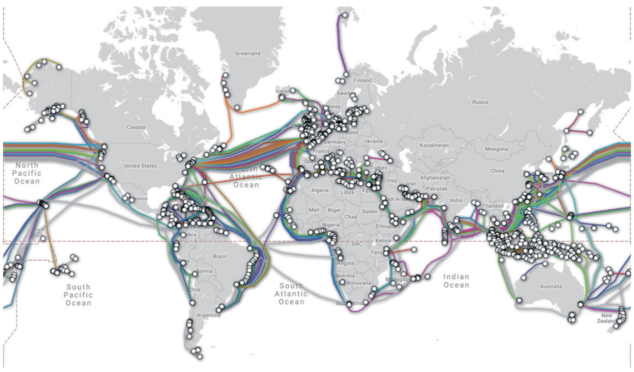

Figure 1: TeleGeography's Submarine Cable Map (June 2018)[*6]

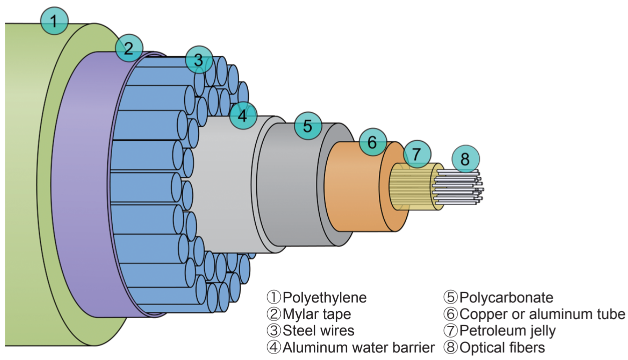

Figure 2: Cross Section of Submarine Cable with Multilayer Protection

*1 Zachary S. Bischof, Romain Fontugne, Fábian E. Bustamante. Untangling the world-wide mesh of undersea cables. In Proc. of HotNets, November 2018.

*2 P. Edwards. A map of all the underwater cables that connect the Internet, 2015 (https://bit.ly/2Ep19i4).

*3 The various threats to subsea cables. Ultramap (https://bit.ly/2Ld9LKW).

*4 NEC begins construction of submarine cable links to the islands of Palau,Yap and Chuuk. NEC, May 2017 (https://bit.ly/2JqQQaE).

*5 Z. S. Bischof, J. P. Rula, and F. E. Bustamante. In and out of Cuba: Characterizing Cuba's connectivity. In Proc. Of IMC, October 2015.

*6 TeleGeography. Submarine cable map (https://www.submarinecablemap.com/).

AT&T, British Telecom, and France Telecom)[*7]. The latest construction boom, however, seems to be driven by content providers, such Google, Facebook, Microsoft, and Amazon. According to TeleGeography, the amount of capacity deployed by content providers rose 10-fold between 2013 and 2017, outpacing all other customers[*8].

3.2.1 Problems Related to Submarine Cables

As the total length of submarine cables continues to expand rapidly, so too does the chance of network disruptions due to cable problems. The natural environment poses a number of risks for starters, from large-scale disasters like earthquakes and tsunamis, to undersea landslides and ocean currents that can scrape cables across the rocky surfaces and shark attacks on some cables.

Even more than natural forces, human actions—intentional or not—are the biggest threat to cables, with approximately 70% of disruptions being caused by fishing trawlers and ship anchors[*3], as well as growing concern over intentional attacks on vulnerable cables. For instance, US Navy officials have stated concern upon observing Russian submarines and spy ships operating near important submarine cables[*9*10].

While the high degree of connectivity available in certain areas may limit the consequence of cable disruptions, other regions appear to be particularly vulnerable[*11*12*13]. The Asia America Gateway cable (AAG), notorious for frequent breakdowns, connects Southeast Asia and the US, handling over 60% of Vietnam's international Internet traffic. In 2017 alone, the AAG suffered at least five technical errors[*14].

In another incident, divers off the coast of Egypt were arrested for cutting the SE-WE-ME-4 submarine cable, leading to a 60% drop in Internet speeds[*11*15]. Other incidents have resulted in entire countries being taken offline due to a single submarine cable cut, such as Mauritania in April 2018[*12].

To understand these risks, it is necessary to clarify the role of the submarine network as a component of the global network. Routes that appear to be distinct paths at the network layer may rely on the same cable at the physical layer.

For particularly critical routes (e.g., transpacific or transatlantic), large network operators often utilize multiple cables. Yet even with full details on the Layer 3 topology, the lack of visibility as to which routes and submarine cables networks are connected by makes it difficult for third parties to quantify the dependence of Internet connections on particular submarine cables.

3.2.2 The World's Submarine Cables

Data on submarine cables are publicly available on a number of websites. Here, we use data collected from two sites—TeleGeography's Submarine Cable Map[*6] and Greg (Mahlknecth)'s Cable Map[*16]—to describe the growth and current state of submarine network infrastructure in terms of the number and capacity of the cables. Both sites present a global map of hundreds of submarine cables with details on each cable. While there is a large overlap between them, we find significantly more cables in TeleGeogaphy's Map than in Greg's.

A caveat is that both resources only list details on publicly announced cables[*17]. TeleGeography estimates that by early 2018 there were approximately 448 submarine cables in service globally[*18], 90% of which were publicly announced. Most of the remaining privately owned and unannounced cables belong to content provider networks—such as Facebook and Google—who have made significant

*7 N. Starosielski. The Undersea Network. Duke University Press.
*8 A. Mauldin. A complete list of content providers' submarine cable holdings.
*9 M. Birnbaum. Russian submarines are prowling around vital undersea cables. It's making NATO nervous. The Washington Post, December 2017 (https://wapo.st/2NW71QP).
*10 D. E. Sanger and E. Schmitt. Russian ships near data cables are too close for US comfort. The New York Times, October 2015 (https://nyti.ms/2uqCnXh).
*11 C. Arthur. Undersea internet cables off Egypt disrupted as navy arrests three. The Guardian, March 2013 (https://bit.ly/2mlluZK).
*12 C. Baynes. Entire country taken offline for two days after undersea Internet cable cut. Independent, April 2018 (https://ind.pn/2L0zIOn).
*13 R. Noordally, X. Nicolay, P. Anelli, R. Lorion, and P. U. Tournoux. Analysis of Internet latency: The Reunion Island case. In Proc. Of AINTEC, 2016.
*14 B. Anh. Vietnam Internet returns to normal after AAG repairs. Submarine Telecom Forum, June 2018.
*15 A. Chang. Why undersea Internet cables are more vulnerable than you think. Wired, April 2013 (https://bit.ly/2KYFP5Y).
*16 G. Mahlknecht. Greg's cable map (https://www.cablemap.info/).
*17 A. Mauldin. A complete list of content providers' submarine cable holdings. Telegeography blog, November 2017 (https://bit.ly/2Lw7DLm).
*18 Telegeography. Submarine Cable 101 (https://bit.ly/2qcGSTc).

investments in undersea cables as part of their inter-datacenter networks[*17]. Although we focus here on those cables that are part of the public Internet, understanding the relation between the public and private submarine cable network is an open research question.

Each site lists the name of the cable, a list of its landing points, an approximate cable length, a ready-for-service date, and for some cables, links to external websites. Figure 3 shows an example of the data made available by TeleGeography, including cable length, owners, and landing points.

3.2.3 Growth and State of the Network

The submarine network has seen consistent linear growth in number of cables since the late 1980s. Using the data collected from the TeleGeography site, Figure 4 plots the number of cables currently in use based on ready-for-service dates (includes cables slated to go into operation by the end of 2020). As Figure 4 (left axis) shows, over the last thirty years there has been, on average, a new cable activation per month. Note that this data set is missing cables that were decommissioned. For example, TAT-8 (constructed in 1988) was the first fiber-optic cable in the Transatlantic Telephone (TAT) series of cables, but it was decommissioned in 2002 and is not part of TeleGeography's current dataset. The currently active TAT-14 cable began operating in 2001. Thus, the graph shows a lower bound on the total number of cables active each year.

The submarine network has grown not just in number of cables but also in the length of these cables. Figure 4 also plots the total length of currently active cables per year (right axis). By 2018, the total length of currently active cables had grown to over 1.2 million km.

The graph shows an interesting spike in lengths starting around 2015. The only period with faster growth corresponds with the dot-com boom (1997–2001).

Today, the global submarine infrastructure is capable of transferring over 1 Pbps of traffic, with total capacity growing multiple orders of magnitude in the last few decades. Using the bandwidth capacities from Greg's Cable Map, we plotted the total global bandwidth for currently active submarine cables, shown in Figure 5. A comparison with Figure 4 indicates that recently constructed cables are responsible for carrying a large portion of Internet traffic. Figure 6 shows the average bandwidth capacity of new cables from Figure 5 and Figure 4. Despite some noise in the early 1990s, we see that the average bandwidth capacity of cables grew by 2–3 orders of magnitude through around 2015. While average cable capacity remained relatively consistent between 1995 and 2010, capacity has spiked again in recent years.

These data represent conservative estimate as the sources do not include decommissioned cables and are restricted to publicly announced cables.

Asia-America Gateway (AAG) Cable System
Email link

RFS: November 2009
Cable Length: 20,000 km
Owners: Telekom Malaysia, AT&T, Starhub, PLDT, CAT Telecom Public Company Limited, Airtel (Bharti), Telstra, Telkom Indonesia, BT, Eastern Telecom, PT Indonesia Satellite Corp., Spark New Zealand, Viettel Corporation, Saigon Postel Corporation, Vietnam Telecom International, Brunei International Gateway, BayanTel, Ezecom
URL: http://www.asia-america-gateway.com

Landing Points

Changi North, Singapore
Keawaula, Hawaii, United States
La Union, Philippines
Lantau Island, Hong Kong, China
Mersing, Malaysia
San Luis Obispo, California, United States
Sri Racha, Thailand
Tanguisson Point, Guam
Tungku, Brunei
Vung Tau, Vietnam

Figure 3: Example of TeleGeography's Data

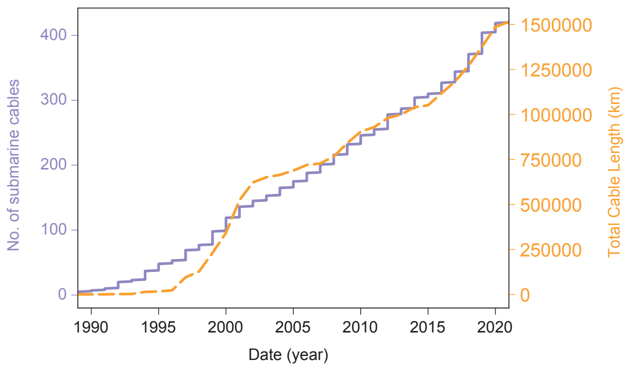

Figure 4: Number of Cables and Total Cable Length

3.3 Submarine cables and the Internet

We discuss the relationship between these submarine cables and the Internet. We set out three high-level tasks here: (1) creating an abstract graph of the submarine cable network, characterizing connectivity and identifying regions that are particularly susceptible to cable disconnections; (2) inferring the relationship between network-level resources and specific submarine cables in order to connect observations at the physical and network layers, and (3) exploring the consequences of submarine cable failures for Internet users.

3.3.1 Graphing Submarine Cable Connections

The first task is to derive an abstract graph of the submarine network. While seemingly simple, mapping cables, each with multiple landing points in different countries and land masses, on a single plot is no easy task.

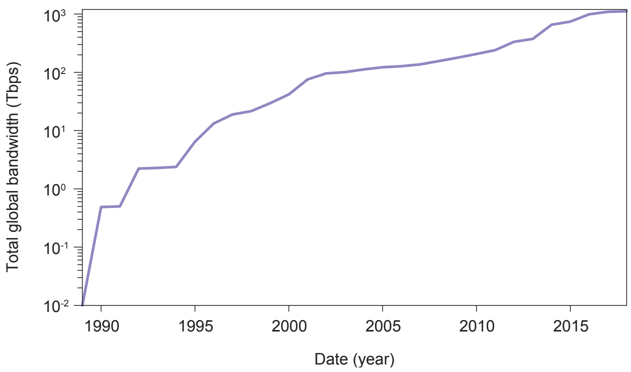

Figure 5: Time Series of Total Bandwidth of Currently Active Cables (per Greg's Cable Map)

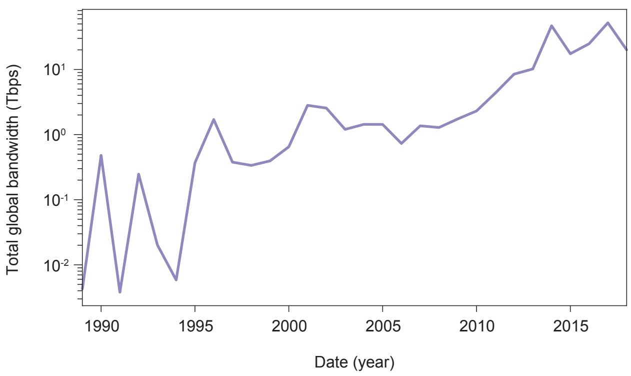

Figure 6: Time Series of Average Bandwidth of New Cables (per Greg's Cable Map)

In a first approximation, one could group cities connected by terrestrial network infrastructure into edges on the graph, using the submarine links between them as vertices. Take, for example, the Greenland Connect cable, shown in Figure 7, which connects Canada with two landing points in Greenland and one in Iceland. This approach will group the two Greenland points as having a land-based connection, with submarine connections between Canada and Greenland and between Greenland and Iceland*19. But a continuous landmass does not necessarily imply a terrestrial network connection. For example, although Panama and Colombia are contiguous neighbors, the lack of any transit infrastructure across the Darién Gap means that for connectivity purposes, these are essentially separate regions. We are currently using map data from Google Maps and Open Street Map to aid in identifying these disconnected regions.

A more difficult problem appears when landing points are close by. Consider the ACE (Africa Coast to Europe) cable, shown in Figure 8, and the Jasuka cable from Telkom Indonesia, in Figure 9. Unlike the Greenland example, ACE has 22 landing points connecting tens of countries on the west coast of Africa to two locations in continental Europe (Portugal and France). Even if one could imagine grouping the European points into a single vertex, it is unclear how to best group the west Africa points. The Jasuka cable, connecting 11 points around the island of Sumatra, further complicates matters—here, the exact definition of landing points is not even clear.

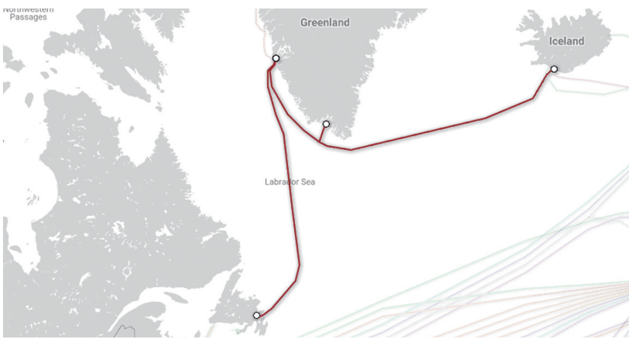

Figure 7: Greenland Connect (per TeleGeography Cable Map)

*19 In reality, even this "simple" example is not so straightforward; despite being on the same landmass, we need to treat the landing points in Greenland as separate due to the lack of infrastructure connecting the cities.

We plan to apply a variation of our basic approach, using other publicly available records, while building a common repository for the inferred view. Using this abstraction of the submarine cable network will help us to study the dependability of geographical areas to physical cables and identify high-risk links from a connectivity perspective.

3.3.2 Mapping onto the Internet

Most studies on Internet topology rely solely on measurements at the network layer. Inferring network reliability from such analysis has limits, as traffic that appears to be traveling via separate network paths could potentially be relying on the same physical resource. Besides shared infrastructure such as datacenters, submarine cables are commonly co-owned or leased by multiple network operators (e.g., TAT-14 is co-owned by over 30 network operators).

Figure 8: ACE (Africa Coast to Europe) (per TeleGeography Cable Map)

Understanding the relationship between network-level measurements and the underlying cables is key to accurately assessing the resiliency of the Internet[*20] Toward that understanding, we envision a service that, given a traceroute, can annotate the appropriate hops with the submarine physical links traversed.

We have started to explore this possibility using the RIPE Atlas[*21] topology data to identify submarine cable hops. RIPE Atlas is an Internet measurement project run by RIPE NCC, connecting traceroutes and other data from users around the globe. Using over 500 million traceroutes collected by the RIPE Atlas project between January and April 2018, we estimated the latency between routers at each hop using a method that we developed for estimating RTTs[*22]. Here, we use pairs of router IP addresses that appeared adjacently in traceroutes with summary statistics of their differential RTT. There is a large disparity among separate RTT data sources, but statistical processing of large quantities of data can lead to greater precision.

We then use RIPE's geolocation service[*23] to get an approximate location for each router IP address. For each IP pair for which we were able to geolocate both IPs, we then compared the geographical distance and differential RTT between them to determine whether it is possible for the path between them to traverse any of the submarine cables. Specifically, we assume the path traverses a particular

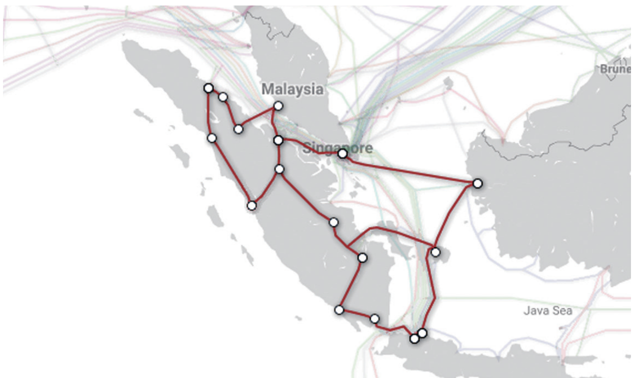

Figure 9: Telkom Indonesia's Juska (per TeleGeography Cable Map)

*20 R. Durairajan, P. Barford, J. Sommers, and W. Willinger. Intertubes: A study of the US long-haul fiber-optic infrastructure. In Proc. of ACM SIGCOMM, August 2015.

*21 RIPE NCC. RIPE Atlas (http://atlas.ripe.net).

*22 R. Fontugne, C. Pelsser, E. Aben, and R. Bush. Pinpointing delay and forwarding anomalies using large-scale traceroute measurements. In Proc. of IMC, November 2017.

*23 M. Candela. Multi-approach infrastructure geolocation. Presentation at RIPE 75, October 2017.

submarine cable and calculate the distance between the IPs through a pair of the cable's landing points. We compare this value with the distance found using the differential RTT and the speed of light in a fiber cable to assess the possibility of that particular submarine cable having been used.

After running this analysis for each pair of IPs in our RIPE Atlas dataset, we identified 3,429 unique IP pairs that could have possibly traversed a submarine cable.

While promising as a starting point, we face a number of challenges with this approach. For starters, we are unable to obtain a location for some of these routers (e.g., because data needed to get an accurate location estimate do not exist). Also, 90% of IP pairs mapped to two or more possible cables. This is not surprising given that multiple cables share similar landing points and co-location facilities, and that limits on accuracy are inherent in RTT-based analysis.

We are working on adding other methods to improve accuracy. For example, using information about which operators use each cable should help to narrow down the set of cables that could possibly be used by the AS to which IP addresses belong.

Another approach we are investigating is the use of cable outage information for cable identification. Submarine cable outages, due to maintenance or faults, are frequent. Such service outages are often reported by the news or by individuals or research groups on Twitter. Relationships can be inferred from the correlation between service outages and RTTs.

A report by Palmer-Felgate and Booi[*24] used data on over 1,000 submarine cable faults between 2008 and 2014 to create a model of cable outages and repairs. The results indicated that cables had at most two nines of availability, with the majority having outages for 9 or more days per year. By viewing historical traceroute data and comparing with reports of cable outages, we can identify IP pairs that disappear in sync with cable faults.

3.3.3 Quantifying Cable Failure Aftermaths

Mapping router IP addresses to specific physical cables will allow us to study the impact of submarine cable outages on Internet users.

Using traceroutes from RIPE Atlas, we studied the impact of a number of cable cuts in recent months. While collecting reports of submarine cable damage, we observed a number of recent outages and repairs in Southeast Asia. While these issues did not result in any major network outages, we did notice a significant impact on latency.

One of these events is damage to the SEA-ME-WE-3 cable on May 10, 2018. SEA-ME-WE-3 is one of the longest cables in the world, reaching from western Australia to western Europe via the Middle East. Once this cable was

*24 A. Palmer-Felgate and P. Booi. How resilient is the global submarine cable network? SubOptic, 2016 (https://bit.ly/2L5JHST).

damaged, certain traffic had to be rerouted via longer alternative routes, resulting in increased latency. Figure 10 shows latency measurements between Australia and Singapore before and after the cut. We see that RTTs more than tripled, from 97ms to over 320 ms. This latency spike continued for days after the cable break, as repairs to submarine cables can take weeks.

Another possible source of performance degradations is submarine network misconfiguration or maintenance.

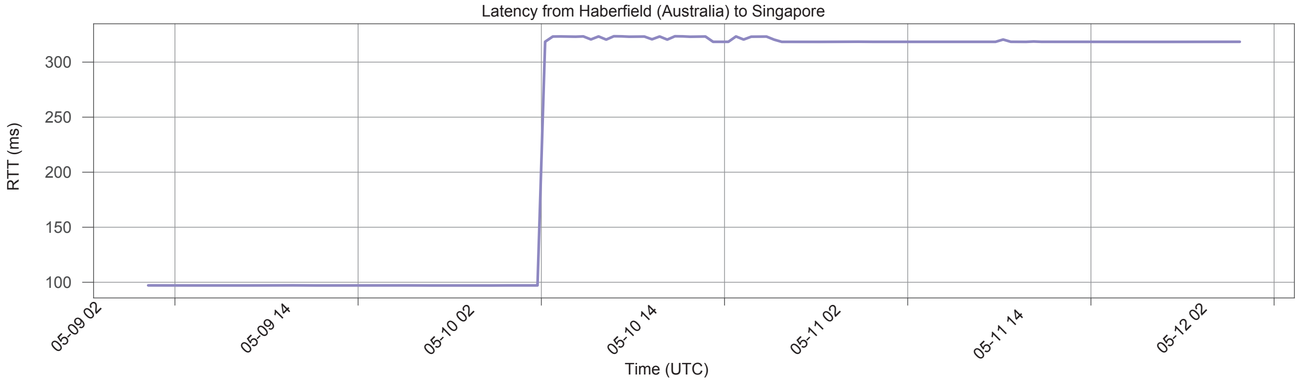

Figure 10: South-East Asia - Middle East - Western Europe 3 (SEA-ME-WE-3) undersea cable break and latency between Australia and Singapore (May 10, 2018)

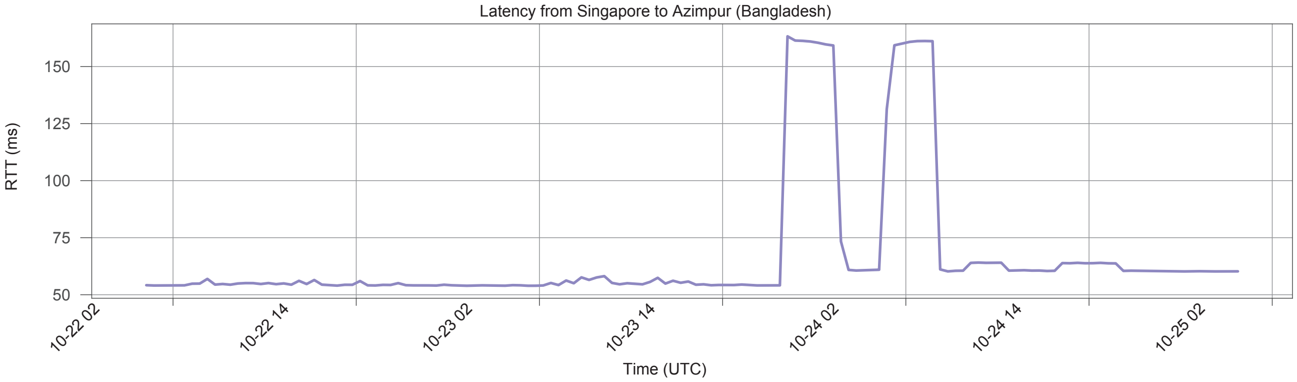

Figure 11: South-East Asia - Middle East - Western Europe 4 (SEA-ME-WE 4) cable reconfiguration (October 2017)

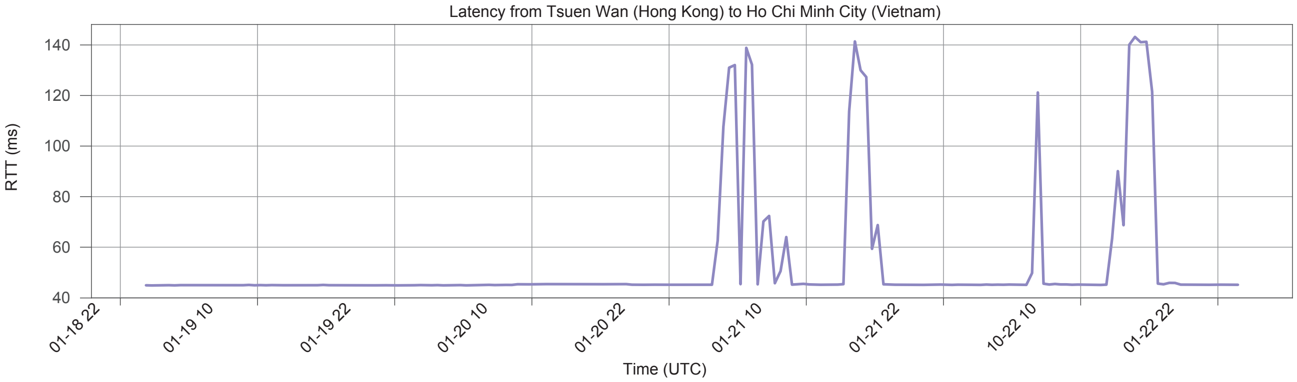

Figure 12: Latency between Hong Kong and Vietnam during Asia-America Gateway (AAG) cable reconfiguration (January 2018)

Figure 11 shows a latency increase due to reconfigurations on the SEA-ME-WE 4 submarine cable[*25]. We observed an almost tripling of latency between Singapore and Bangladesh over a period of about 12 hours.

Similarly, we observed an increase in latency between Hong Kong and Vietnam, coinciding with the reconfiguration of the Asia-America Gateway (AAG) cable starting on January 21, 2018, as shown in Figure 12.

Annotating intercontinental traceroutes with the submarine cables traversed along the path will help in diagnosing the cause of spikes such as these. Cables disappearing from traceroutes could signify a cable cut or change in routing behavior. Correlating this information will aid in understanding the underlying cause of performance anomalies.

The IP paths to submarine cables mapping can also assist network operators in understanding the dependence on a network to submarine cables. This information is important for planning future expansions of network infrastructure. For example, an operator looking to add a new upstream ISP to improve resiliency could select an ISP that uses different submarine cables from its existing providers.

Furthermore, tracking cables that appear in traceroutes would also help identify cables that are heavily utilized in a given region. Such cables could have a significant impact on performance and routing if damaged. Durairajan et. al conducted a similar study of the terrestrial long-haul fiber-optic infrastructure in the US,*20 identifying high-risk links and making suggestions for deploying new links in specific regions to reduce both risk and latency. We plan to conduct a similar analysis on the submarine network.

3.4 Conclusion

As we continue to invest on the defense of the virtual network, our limited understanding of the physical network that enables it will become its most serious vulnerability. We have put forward an approach for combining information on cables and measurements on the network layer to explore the state of the submarine cable network using publicly available data. Taking connectivity risks to physical routes into account, we believe this approach can be used to assess Internet redundancy and resiliency.

Acknowledgments
This work was funded in part by the JSPS fellowship program and NSF CNS award 1619317.

Zachary Bischof
Visiting Researcher, IIJ Innovation Institute
Zachary conducts experimental research on networks and large-scale distributed systems.
He aims to characterize broadband networks through DNS and traffic analysis.

Romain Fontugne
Senior Researcher, IIJ Innovation Institute
Fabián E. Bustamante
Professor at Northwestern University, United States

*25 T. D. Star. Internet to be slow for next 4 days (https://bit.ly/2LmlNSn).