Untangling the world-wide mesh of undersea cables

Zachary S. Bischof
IIJ Research Lab
bischof@iij.ad.jp

Romain Fontugne
IIJ Research Lab
romain@iij.ad.jp

Fabián E. Bustamante
Northwestern University
fabianb@cs.northwestern.edu

ABSTRACT

The growth of global Internet traffic has driven an exponential expansion of the submarine cable network, both in terms of the sheer number of links and its total capacity. Today, a complex mesh of hundreds of cables, stretching over 1 million kilometers, connects nearly every corner of the earth and is instrumental in closing the remaining connectivity gaps. Despite the scale and critical role of the submarine network for both business and society at large, our community has mostly ignored it, treating it as a black box in most Internet studies, from connectivity to inter-domain traffic and reliability. We make the case for a new research agenda focused on characterizing the global submarine network and the critical role it plays as a basic component of any inter-continental end-to-end connection.

1 INTRODUCTION

Ninety-nine percent of all international data is carried by a mesh cable network at the bottom of the ocean [20]. While initial deployments of the submarine network date back to the mid-19th century [12], the recent explosion on Internet traffic has driven an exponential growth of the total capacity of this undersea infrastructure [33].

Today, a complex mesh of hundreds of cables stretching over 1 million kilometers [2] connects nearly every region in the world (Figure 1). It constitutes at once both the operation backbone of global services like those of Google, Facebook and Microsoft, and a critical piece in closing the remaining connectivity and under-connectivity gaps [3, 10].

Yet, despite the impressive scale and criticality of the submarine cable network, we lack a clear understanding of its role in the global Internet. Past studies have either treated it as a black box or focused on specific events and their impact on particular links [9, 14, 35].

We make the case for a new research agenda focused on characterizing the global submarine network and the critical
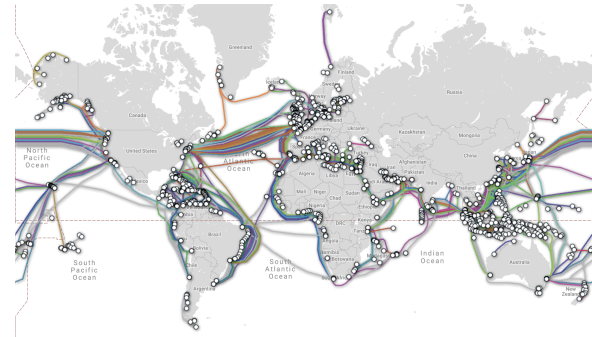
Figure 1: State of TeleGeography's Submarine Cable Map, July 2018. Source: [44].

role it plays as an essential component of any inter-continental end-to-end connection.

The submarine network's role as mainstay of the world's economy, security and well-being, provides clear motivation for such an agenda. Beyond this, from an intellectual perspective, the network's scale, management complexity, and opaque architecture pose significant research challenges.

Criticality and scale interact in unexpected ways. As the total length of submarine cables continues to expand rapidly, so too does the chance of network disruptions due to cable problems. For starters, there is a number of potential risks stemming from their natural environment — from large-scale disasters like earthquakes and tsunamis [9], to undersea landslides and ocean currents that can scrape cables across the rocky surfaces on the ocean floor, to even sea-life attacks on less protected cables [27, 34].

Even more than natural forces, human actions – intentional or not – are considered the biggest threat to cables, with approximately 70% of disruptions being caused by fishing trawlers and ship anchors [2], 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 [8, 40].

While the high degree of connectivity available in certain areas may limit the consequence of these problems [30], other regions appear to be particularly vulnerable [5, 6, 36]. The $560-million 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 has suffered at least five technical errors [4].

In another incident, divers off the coast of Egypt were arrested for cutting the SE-WE-ME-4 submarine cable [5], leading to a 60% drop in Internet speeds [15]. Other incidents have resulted in entire countries being taken offline due to a single submarine cable cut, such as Mauritania in April 2018 [6].

Researchers trying to characterize the submarine network and its role as a component of the global network face a number of challenges. For starters, submarine cables are commonly managed by consortia and shared by multiple network operators. As a result, routes that appear to be distinct paths at the network layer may rely on the same cable at the physical layer.

Furthermore, for particularly critical routes (e.g., transpacific or transatlantic) large network operators often utilize multiple cables. Thus, even with the full details on the underlying topology, our lack of visibility below Layer 3 makes it difficult to map specific network routes to their underlying conduits and quantify the dependence of Internet connections on particular submarine cables.

We start by summarizing the state of the Internet's submarine cable infrastructure and describe its growth over the years. In making the case for a research agenda focused on characterizing the global submarine network, we outline steps for improving our understanding of its topology and discuss the frequency and impact of submarine cable reliability issues.

2 BACKGROUND

While submarine cables date back to the 1840s, with the first commercial cable being laid across the English Channel in 1850, early cables made of multi-stranded copper wires had very limited capacity and were used primarily for telegraphy. Today nearly all cables are fiber-optic cables. Fiber-optic cables were developed in the 1980s and the first transatlantic cable (TAT-8) was put in operation in 1988. 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 thick polyethylene shield (Figure 2). Cables vary in thickness from four and a half inches in diameter, weighing approximately 60 tons per mile for shore end cable, to one inch in diameter, weighing about 2.5 tons per mile, for deep-sea cable which comprise the majority of the run.

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 AT&T, British Telecom and France Telecom).[1] The latest construction boom, however, seems to be driven by content providers, such Google, Facebook, Microsoft, and Amazon. According to Telegeography's Research Director Alan Mauldin, the amount of capacity deployed by content providers has risen 10-fold between 2013 and 2017, outpacing all other customers
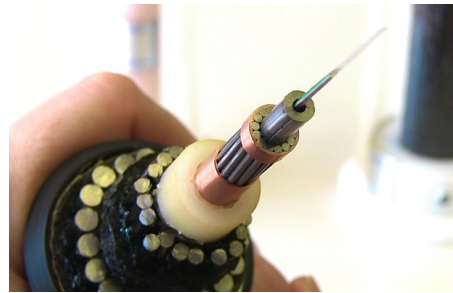

Figure 2: Cutaway of a submarine cable that shows the layers of protection. Photo by Tim Hornyak. Source: [25].

of international bandwidth [31]. Today, 99% of the data traffic crossing oceans is carried by undersea cables [42].

Considering the importance and high costs of these cables (a typical multi-terabit transoceanic cable costs several hundred million dollars to construct) [23], they are highly valued by the corporations building and operating them, as well as by national governments that consider them "vital to the national economy" [17, 29].

2.1 Datasets

To capture the growth and current state of the global submarine network we rely on two, somewhat complementary, datasets that are publicly available: TeleGeography's Submarine Cable Map [44] and Greg (Mahlknecth)'s Cable Map [28]. Throughout this section, we use the data collected from both sites to describe the growth and current state of submarine network infrastructure in terms of the number, extent 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 ($n = 405$) than in Greg's ($n = 265$).[2]

A caveat is that both resources only list details on publicly announced cables [32]. TeleGeography estimates that by early 2018 there were approximately 448 submarine cables in service globally [43], 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 investments in undersea cables as part of their inter-data-center networks [32]. 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.

In their descriptions, each site lists the name of the cable, a list of its landing points, an approximate cable length, a ready for service date or RFS (the date at which the cable becomes operational) and for some cables, links to external websites with more details about them. Figure 3 shows an example of

---

[1]http://atlantic-cable.com//Cables/CableTimeLine/index1951.htm

[2]Further complicating things, many cables appear with different names (e.g., "Yellow" on one and "Atlantic Crossing-2 (AC-2)" in the other) and some cables listed in one set appeared to have been decommissioned.

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: An example of the data made available by Tele-Geography. Source: [44].
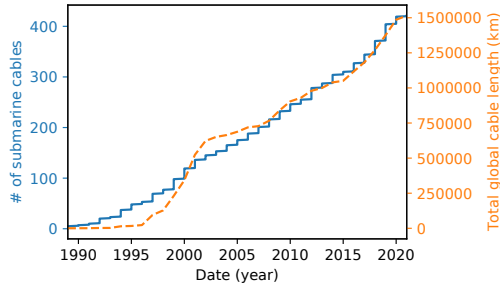

Figure 4: Number of active submarine cables based on their ready for service dates (RFS) (left axis). Total length of currently active submarine cables by year (right axis). Includes planned cables for future activations through 2020.

the data made available by TeleGeography, including RFS (Ready For Service), cable length, owners, and landing points. There are also some fields unique to each website. The Tele-Geography's data includes a list of owners for some of the cables, while Greg's Cable Map provides a bandwidth capacity of the cable as well as a description of the accuracy of the cable's actual path as displayed.

We collected the descriptions of each cable from the Tele-Geography and Greg's Cable Map websites using the Selenium web testing driver [1]. Due to the larger number of cables included, in most cases we use the TeleGeography dataset. However, some parts of the overview require data only available from Greg's Cable Map. We note when this is the case.

2.2 Growth and State of the Network

The submarine cable network has seen a consistent linear growth, in number of cables, since the late 1980s. Using the data collected from the TeleGeography site, we plotted
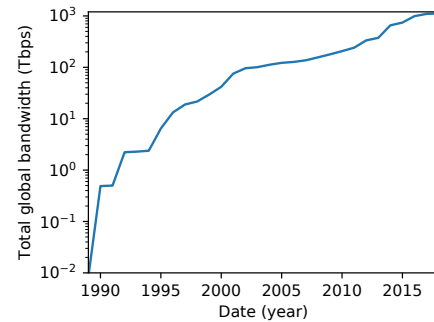

Figure 5: Time series of the total bandwidth of currently active cables according to RFS date. Data sourced from Greg's Cable Map.
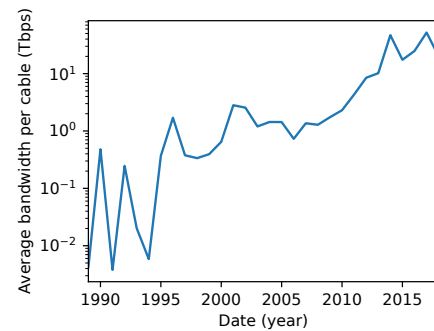

Figure 6: Time series of the average bandwidth of cables constructed according to the RFS date. Data sourced from Greg's Cable Map.

the RFS (Ready For Service) dates of currently active fiber cables. As Figure 4 (left axis) shows, over the last thirty years there has been, on average, a new cable activation per month. Note, in addition, that this data set misses cables that were decommissioned and subsequently removed from (or never included) in TeleGeography's dataset. For example, TAT-8 (constructed in 1988) was the first fiber-optic cable in the Transatlantic Telephone (TAT) series of cables. This cable was subsequently decommissioned in 2002 and is not part of TeleGeography's current dataset. A series of additional cables were built (with overlapping periods of service), with the latest iteration, TAT-14, beginning operation 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 in the length of these cables. This can be seen in Figure 4 which also plots the total length of currently active cables per year (right axis). By 2018, the total length of currently active cables has 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 and bust (1997-2001).

Today, the global submarine infrastructure is cable of transferring over 1 Pbps of traffic, with total capacity growing

multiple orders of magnitude in the last few decades. Using the bandwidth capacities listed in the data from Greg's Cable Map, we plotted the total global bandwidth for currently active submarine cables according to each cable's RFS date, shown in Figure 5. By combining these results with the linear growth shown in Figure 4, a relatively small number of conduits (i.e., a few hundred) are responsible for carrying a large portion of Internet traffic. Along this line, Figure 6 shows the average bandwidth capacity of the cables introduced each year. Despite some noise in the early 1990s, we see that the average bandwidth capacity of cables has grown by 2-3 orders of magnitude. We found that there have been multiple jumps in bandwidth capacity. And while average cable capacity remained relatively consistent between 1995 and 2010, capacity has spiked again in recent years.

It is worth noting that, while impressive, these trends in number, length and capacity of submarine cables are a conservative estimate as these data sources do not include cables that were built and subsequently decommissioned, and are logically restricted to publicly announced cables.

3 RESEARCH AGENDA

In this section, we discuss our thoughts on a research agenda focused on characterizing the global submarine network and the critical role it plays as a basic component of any intercontinental end-to-end connection.

We outline this agenda around three high-level tasks (1) creating an abstract graph of the submarine cable network, characterizing connectivity and identifying regions that are particularly susceptible to disconnections from cable damage; (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 dependence of Internet resources on submarine cables and the performance consequences of cable failures on Internet users. We now describe each of these steps in more detail.

3.1 Characterizing the network

A first task then is to derive an abstract graph of the submarine network to understand its basic connectivity risks. While seemingly simple, early analysis shows the challenges with mapping cables, each with multiple landing points in different countries and land masses, into a set of edges and common vertices.

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. This approach will map a cable such as Greenland Connect (with a landing point in Canada, two in Greenland and one in Iceland) into three vertices and two edges connecting these countries.[3]

One challenge with this approach is the need for data on terrestrial infrastructure between landing points. 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 trying to apply this approach to the range of submarine cables that make the submarine network. Considered, for instance, the ACE (Africa Coast to Europe) and the Jasuka cable from Telkom Indonesia. Unlike the Greenland Connect example, ACE has 22 landing points connecting tens of countries in 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 abstract the landing points on west Africa for analysis. To further complicate matters, the exact definition of *landing points* may not be as clear as we first imagined, when considering the Jasuka cable and 11 of its landing points linked through the island of Sumatra.

We plan to apply a variation of our basic approach, using other publicly available records, while building a common repository and front-end 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 solely from a connectivity perspective.

3.2 Mapping down the stack

Most studies on Internet topology rely solely on measurements at the network layer to identify Internet paths. Inferring network reliability from such analysis is at best risky, 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 collocation facilities, submarine cables are commonly co-owned or leased by multiple network operators (e.g., TAT-14 is co-owned by over 30 network operators).

Understanding the relationship between network-level measurements and the underlying physical infrastructure is key to accurately assessing the resiliency of the Internet [19]. 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 in this context within the global, if limited, perspective of RIPE Atlas. Using over 500 million traceroutes collected by the RIPE Atlas project [38] between January and April 2018, we are applying the methodology in Fontugne et al. [21] to estimate the latency added at each hop. The resulting dataset is then comprised of pairs of router IP addresses that appeared adjacently in traceroutes with summary statistics of their differential RTT.

We then use RIPE's geolocation service [13] to get an approximate location for each router IP address. While the geolocation service provides multiple data sources (e.g., crowdsourcing), we only use the single-radius measurement, which

---

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

estimates an IP's location using speed-of-light calculations based on RTTs from RIPE Atlas probes.

For each adjacent IP pair for which we were able to geolocate both IPs, we then use the calculated differential RTT between them to determine whether or not it is physically possible for the path between them to traverse any of the known submarine cables. Specifically, we do this by calculating the distance of the shortest possible path between those IPs that also traverses a pair of submarine cable landings. For example, for a pair of IPs (ip_1, ip_2) and a pair of landings (x_i, x_j) that belong to a single cable X, we calculate the total distances of the paths $[ip_1, x_i, x_j, ip_2]$ and $[ip_1, x_j, x_i, ip_2]$, selecting the path with the shortest distance. This is repeated for each pair of landings for each submarine cable.

Then, using 1.4696 as an estimate of the refractive index for the speed of light in a fiber cable, we calculate if it is possible for this path to be traversed within the previously calculated differential RTT. After running this analysis for each pair of IPs in our 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 an approximate location for some of these routers (e.g., no Atlas probes are able to measure a low enough RTT to get an accurate location estimate). Another issue is that over 90% of IP pairs mapped to 2 or more possible cables. This is not surprisingly given that multiple cables share similar landing points and co-location facilities, and that issues such as persistent congestion complicate a latency-based analysis.

We are working on adding other methods for obtaining an accurate estimate of a router's location. We are also exploring several techniques to reduce the number of IP-level to submarine cable matches, collecting information about the network operators that sharing ownership of a cable. Details about the business relationships of each cable, combined with the AS information of each IP in the pair should help us narrow down the set of possible cables.

Another approach we are investigating is the use of cable outage information for cable identification. Submarine cables frequently undergo maintenance, often due to irrecoverable outages. Such cable cuts are often reported by the news [5, 6, 18, 45] or by individuals or research groups on Twitter.[4]

In a report by Palmer-Felgate and Booi [37], the authors used data on more than 1,000 submarine cable faults between 2008 and 2014 to create a model of cable outages and repairs. In their results, cables had at most two nines of availability. The majority of simulated cables had outages for 9 or more days per year. We believe that cable outages are frequent enough to aid in mapping network-level measurements to their respective physical paths. By viewing historical traceroute data and comparing with reports of cable outages, we can
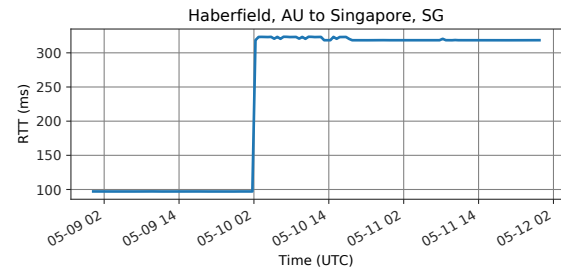

Figure 7: South-East Asia - Middle East - Western Europe 3 (SEA-ME-WE-3) undersea cable break on May 10th, 2018 between Australia and Singapore.

identify IP pairs that disappear and re-appear in sync with cable faults and repairs.

This set of challenges is in no way exhaustive. Identification is further complicated by technologies such as Multiprotocol Label Switching (MPLS) tunneling. This can obfuscate large sections of the path in traceroutes. For example, in our dataset, we identified instances where a single hop in traceroute would need to be traversing multiple submarine cables, such as in paths involving the Caribbean and Oceania. In such instances, a single hop appearing and disappearing from traceroute measurements could correlate with outages of multiple cables.

3.3 Quantifying cable failure aftermaths

Mapping router IP addresses to specific physical cables will also allow us to study the dependence on Internet resources to submarine cables and 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 country-level network outages, we did notice that it had a significant impact on latency.

One of these event is damage to the SEA-ME-WE-3 cable on May 10th, 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 damaged, certain traffic had to be rerouted via longer alternate routes, resulting in increased latency. Figure 7 shows latency measurements between Australia and Singapore before and after the cut. We see that RTTs more than tripled, from 97 ms to over 320 ms. This latency spike continued for days after the cable break, as repairs to submarine cables can take weeks to schedule and complete.

Another under-studied possible source of performance degradations is submarine network misconfiguration or maintenance. Figure 8 shows a latency increase due to reconfigurations on the SEA-ME-WE 4 submarine cable [41]. We found that RTTs spiked for probes from Singapore to Bangladesh.
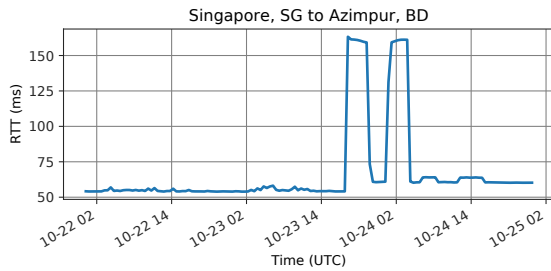
---

[4]Some examples include posts on the accounts of:
https://twitter.com/philBE2 and
https://twitter.com/InternetIntel.

Figure 8: South East Asia - Middle East - Western Europe 4 (SEA-ME-WE 4) cable reconfiguration on October 2017.
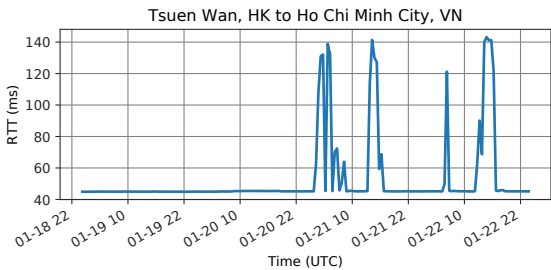

Figure 9: Asia-America Gateway (AAG) cable reconfiguration for the section S1 to Vietnam on January 2018.

Over approximately a 12 hour period, latencies fluctuated significantly, almost tripling for an extended period.

We also observed a reconfiguration of the Asia-America Gateway (AAG) cable starting on January 21, 2018 [22]. Figure 9 shows the latency between Tsuen Wan, Hong Kong and Ho Chi Minh City, Vietnam. Latencies consistently hovered just below 45 ms before the event. Once the reconfiguration started, latency frequently spiked to well over 100 ms, in some cases reaching over three times higher than the previous period.

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 these trends with latency measurements will aid network operators and researchers 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. Using traceroutes from multiple vantage points towards a certain network would reveal the submarine cables typically used to reach this network. This enables operators to monitor their network dependence on submarine cables beyond the border of their own infrastructure, which is important for planning future infrastructure deployment. For example, an operator seeking resiliency for its customers may select a new upstream ISP by comparing the ISP's submarine cables to the ones used by its current providers.

Furthermore, tracking cables that appear in traceroutes would also help identify cables that are heavily utilized in a given region. Applying heuristics works such as Sanchez et. al's [39] to estimate the volume of traffic carried by these cables would aid in identifying critical infrastructure. Cables that are more heavily utilized with high capacity 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[19], 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.

4 RELATED WORK

A number of works have focused on the specific engineering challenges of deploying submarine cables in marine environments. Choi et. al looked to address some of the difficulties of the cable-laying process itself by improving automation [16]. While Huang et. al focused on methods to improve seafloor mapping and obstacle detection, improving route selection [26]. Others have focused on improving the technology in the cables themselves, such as the application of multiplexing in long-haul transmission to increase bandwidth [7] or evaluating the properties of submarine cable materials [11].

Beyond submarine networks, others have focused on studying the characteristics and management of fiber optic networks in general. However, most of these works look at either the network on the whole or focus on a terrestrial backbone, ignoring the particularities of submarine links in the network. A series of papers looked at Microsoft's fiber-optic infrastructure. One work analyzed the features of outages focused on Microsoft's backbone [24] while another looked for efficient ways to improve bandwidth capacity [24].

5 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 made a case for a research agenda aimed at characterizing the global submarine network and its critical role in the public Internet. We used available data to explore the evolution and current state of the undersea infrastructure and discussed possible lines of exploration, from the challenges with understanding basic connectivity risks, to the need for connecting measurements at the network-layer with the underlying physical paths and the implications it has on Internet redundancy and resiliency.

ACKNOWLEDGMENTS

REFERENCES

[1] Selenium. https://www.seleniumhq.org.

[2] The various threats to subsea cables. Ultramap. https://bit.ly/2Ld9LKW.

[3] NEC begins construction of submarine cable links to the islands of Palau, Yap and Chuuk. NEC, May 2017. https://bit.ly/2JqQQaE.

[4] B. Anh. Vietnam Internet returns to normal after AAG repairs. Submarine Telecom Forum, June 2018.

[5] C. Arthur. Undersea internet cables off Egypt disrupted as navy arrests three. The Guardian, March 2013. https://bit.ly/2mlluZK.

[6] C. Baynes. Entire country taken offline for two days after undersea Internet cable cut. Independent, April 2018. https://ind.pn/2L0zIOn.

[7] N. S. Bergano and C. R. Davidson. Wavelength division multiplexing in long-haul transmission systems. *Journal of Lightwave Technology*, 14(6):1299–1308, June 1996.

[8] M. Birnbaum. Russian submarines are prowling around vital undersea cables. it's making NATO nervous. The Washington Post, December 2017. https://wapo.st/2NW71QP.

[9] Z. S. Bischof, J. S. Otto, and F. E. Bustamante. Distributed Systems and Natural Disasters: BitTorrent As a Global Witness. In *Proc. of CoNEXT Special Workshop on Internet and Disasters*, 2011.

[10] 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.

[11] S. Boggs, D. H. Damon, J. Hjerrild, J. T. Holboll, and M. Henriksen. Effect of insulation properties on the field grading of solid dielectric DC cable. *IEEE Transactions on Power Delivery*, 16(4):456–461, October 2001.

[12] B. Burns. Cyrus w. field. History of the Atlantic Cable and Undersea Communications, 2011. http://atlantic-cable.com/Field/.

[13] M. Candela. Multi-approach infrastructure geolocation. Presentation at RIPE 75, October 2017.

[14] E. W. W. Chan, X. Luo, W. W. T. Fok, W. Li, and R. K. C. Chang. Non-cooperative diagnosis of submarine cable faults. In *Proc. of PAM*, 2011.

[15] A. Chang. Why undersea Internet cables are more vulnerable than you think. Wired, April 2013. https://bit.ly/2KYFP5Y.

[16] J.-K. Choi, T. Yokobiki, and K. Kawaguchi. Rov-based automated cable-laying system: Application to donet2 installation. 43(3), July 2018.

[17] A. Communications and M. Authority. Report on the operation of the submarine cable protection regime.

[18] C. Duncan. Lightning knocks out Internet. Cayman Compass, February 2016. https://bit.ly/2A0ploC.

[19] 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.

[20] P. Edwards. A map of all the underwater cables that connect the Internet. https://bit.ly/2Ep19i4, 2015.

[21] 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.

[22] S. T. Forum. Vietnam Internet connectivity fully restored. https://subtelforum.com/vietnam-internet-fully-restored/.

[23] B. Gardiner. Google's submarine cable plans get official.

[24] M. Ghobadi and R. Mahajan. Optical layer failures in a large backbone. In *Proc. of IMC*, November 2016.

[25] T. Hornyak. 9 things you didn't know about Google's undersea cable. ComputerWorld, July 2015. https://bit.ly/2JWo8mV.

[26] S. W. Huang, E. Chen, and J. Guo. Efficient seafloor classification and submarine cable route design using an autonomous underwater vehicle. *IEEE Journal of Oceanic Engineering*, 43(1), January 2018.

[27] D. Kravets. It's official: Sharks no longer a threat to subsea Internet cables. Arstechnica, July 2015. https://bit.ly/2uD8qCM.

[28] G. Mahlknecht. Greg's cable map. https://www.cablemap.info/.

[29] R. Martinage. Under the sea: the vulnerability of the commons. 94.1.

[30] L. Matsakis. What would really happen if Russia attacked undersea Internet cables. Wired, January 2018. https://bit.ly/2F4Yqqb.

[31] A. Mauldin. A complete list of content providers' submarine cable holdings.

[32] A. Mauldin. A complete list of content providers' submarine cable holdings. Telegeography blog, November 2017. https://bit.ly/2Lw7DLm.

[33] A. Mauldin. Content, capacity, and the great, growing demand for international bandwidth. Telegeography, May 2018. https://bit.ly/2JsduPK.

[34] R. McMillan. Sharks want to bite Google's undersea cables. Wired, August 2014. https://bit.ly/2NTyfHG.

[35] X. Nicolay, R. Noordally, and P. Anelli. Where is my next hop? The case of Indian Ocean islands. In *Proc. of the Global Information Infrastructure and Networking Symposium*, 2017.

[36] R. Noordally, X. Nicolay, P. Anelli, R. Lorion, and P. U. Tournoux. Analysis of Internet latency: The Reunion Islan case. In *Proc. of AINTEC*, 2016.

[37] A. Palmer-Felgate and P. Booi. How resilent is the global submarine cable network. SubOptic, 2016. https://bit.ly/2L5JHST.

[38] RIPE NCC. RIPE atlas. http://atlas.ripe.net.

[39] M. A. Sanchez, F. E. Bustamante, B. Krishnamurthy, W. Willinger, G. Smaragdakis, and J. Erman. Inter-domain traffic estimation for the outsider. In *Proc. of IMC*, November 2014.

[40] 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.

[41] T. D. Star. Internet to be slow for next 4 days. https://bit.ly/2LmlNSn.

[42] N. Starosielski. *The Undersea Network*. Duke University Press.

[43] Telegeography. Submarine cable 101. https://bit.ly/2qcGSTc.

[44] TeleGeography. Submarine cable map. https://www.submarinecablemap.com/.

[45] K. Zetter. Undersea cables cut; 14 countries lose web. Wired, December 2008. https://bit.ly/2Lm6B7L.