Out of Sight, Not Out of Mind - A User-View on the Criticality of the Submarine Cable Network

Shucheng Liu
Northwestern University

Zachary S. Bischof
IIJ Research Lab

Ishaan Madan
Northwestern University

Peter K. Chan
Northwestern University

Fabián E. Bustamante
Northwestern University

ABSTRACT

Nearly all international data is carried by a mesh of submarine cables connecting virtually every region in the world. It is generally assumed that Internet services rely on this submarine cable network (SCN) for backend traffic, but that most users do not directly depend on it, as popular resources are either local or cached nearby. In this paper, we study the criticality of the SCN from the perspective of end users. We present a general methodology for analyzing the reliance on the SCN for a given region, and apply it to the most popular web resources accessed by users in 63 countries from every inhabited continent, collectively capturing ≈80% of the global Internet population. We find that as many as 64.33% of all web resources accessed from a specific country rely on the SCN. Despite the explosive growth of data center and CDN infrastructure around the world, at least 28.22% of the CDN-hosted resources traverse a submarine cable.

ACM Reference Format:

Shucheng Liu, Zachary S. Bischof, Ishaan Madan, Peter K. Chan, and Fabián E. Bustamante. 2020. Out of Sight, Not Out of Mind - A User-View on the Criticality of the Submarine Cable Network. In *ACM Internet Measurement Conference (IMC '20), October 27–29, 2020, Virtual Event, USA.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3419394.3423633

1 INTRODUCTION

Ninety-nine percent of all international data is carried by a mesh of submarine cables at the bottom of the ocean [34], connecting nearly every region in the world. While initial deployments of the submarine network date back to the mid-19th century [22], the recent explosion of Internet traffic has driven an exponential proliferation on the total capacity required of this infrastructure [30].

Today, the submarine cable network (SCN) is recognized as vitally important to the global economy and as an enabler of sustainable growth in developing regions [7, 21]. For instance, it is estimated that if the ≈40 cables connecting the US to the rest of the world were cut, only 7% of the total US traffic volume could be carried by satellite [28]. At the same time, new cable deployments increase international capacity and add competition at the backhaul level, triggering drops on wholesale and connectivity prices, thus helping expand Internet access previously limited by cost [18].

Despite its obvious importance, we lack a clear understanding of the criticality of the SCN in the global Internet. While it is generally understood that Internet services rely on the SCN for backend traffic, the common assumption is that most Internet users do not directly depend on it, as popular resources are either local or cached by nearby CDN servers [19]. The reoccurrence of country-wide disconnections or performance issues as a result of submarine cable cuts casts doubt on this assumption [26].

In this work, we study the criticality of the SCN from the perspective of Internet end users. We present a general methodology for analyzing the reliance on the SCN of a given region (§3). We apply this methodology to the most popular web resources accessed by users in over 60 countries, covering every inhabited continent in the world and collectively capturing ≈80% of the global Internet population (§4). We show (§5) that as many as 64.33% of all resources accessed from an island country and 43.18% accessed from a non-island country rely on the SCN. Even from landlocked countries – those without direct access to an ocean – 16.25% of all web requests, on average, depend on the SCN. Despite the explosive growth of datacenter and CDN infrastructure around the world, we find that on average, at least 28.22% of the CDN-hosted resources hit a submarine cable, with that figure as high as 65.1% for some countries.

To encourage further research on the criticality of the SCN, we make our measurement framework, dataset, and analysis

IMC '20, October 27–29, 2020, Virtual Event, USA

ACM ISBN 978-1-4503-8138-3/20/10…$15.00
https://doi.org/10.1145/3419394.3423633

code publicly available at https://github.com/NU-AquaLab/Criticality-SCN.

2 MOTIVATION

Today's SCN includes over 400 cables across more than 1 million kilometers, and transfers over 1 Pbps of traffic [20]. The majority of these cables have been constructed and managed by consortia, and are 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) [35]. However, the latest construction boom has been largely driven by content providers such as Google, Facebook, Microsoft, and Amazon [29]. According to TeleGeography, the amount of capacity deployed by content providers has risen tenfold between 2013 and 2017, outpacing all other customers of international bandwidth [29].

Damage to submarine cables can cause wide-spread network issues impacting Internet services and end users, especially when multiple such events occur in a short time period [26]. One particularly severe example was the 2008 submarine cable disruption [36], wherein a series of cable cuts within a two week period resulted in 14 countries having connectivity issues that ranged from complete disconnections to severely limited bandwidth. In early 2013, divers off the coast of Egypt attempting to cut the cable SEA-WE-ME-4 caused a 60% drop in Internet speed, which took about 20 hours to recover from [17]. As recently as January 2020, cable cuts to FALCON, SAT3/WASC and WACS resulted in major outages and degraded Internet performance in parts of the Middle East and throughout much of Africa [16, 32].

Despite the continued investments in the SCN over the last three decades, increased caching infrastructure (e.g., CDNs) around the globe, and data centers moving closer to the network edge, major events such as these seem to occur with some regularity, directly impacting not only backend traffic, but resource retrieval for end users as well.

Previous works have demonstrated how changes in SCN infrastructure can affect network traffic at a general level (e.g., performance and reachability) [21, 25]. Our goal is to understand, empirically, the degree to which the SCN is critical for end users. To this end, we need to start with a clear, quantifiable definition of criticality.

2.1 Defining Criticality

Critical infrastructure generally refers to an asset that is essential to the functioning of a society, its economy, public health, or safety. In this work, we focus on the SCN infrastructure, looking at its criticality from the perspective of the individual, rather than from the perspective of society as a whole.

For our analysis, we use the top Alexa sites for each country as a proxy for identifying Internet resources that are important to users in that region. We thus define the criticality of the SCN as the percentage of resources for these top sites retrieved via SCN infrastructure, as revealed by our analysis. We use this to calculate a *SCN hit rate* of a region.

In considering criticality, we focus on the impact of SCN failures on reachability, and leave the potential impact on performance – as networks route around failures via potentially less optimal paths [5, 6] – for future work.

In addition to web browsing, other categories of network applications such as personalized live streaming, video conferencing and IP telephony could serve as viable proxies for evaluating the criticality of the SCN, potentially requiring a different methodology and yielding different results. This is another promising direction for future research.

3 METHODOLOGY

In this section, we describe the methodology developed for this work. At a high level, for a given country, we look to determine the degree of criticality of the SCN from the perspective of Internet users in that country by: (1) identifying a set of popular Internet resources (e.g., resources used by top x Alexa sites for the country, popular video hosting/streaming services, etc.), (2) geographically locating the servers hosting those resources and a sufficient fraction of the routers along the path, and (3) identifying the use of SCN links on the path to the aforementioned servers. The following paragraphs expand on this.

3.1 Popular Internet Resources

As a first step in our methodology, we identify a set of popular Internet resources for a given country. For this, we consider the Alexa country/region rankings to identify those resources relied on by the most popular sites for a given country. While other definitions of popularity are plausible, we argue that resources from top Alexa sites are a good proxy, considering that web browsing is one of the most common Internet activities.

3.2 Resource Paths Geolocation

After identifying the set of popular Internet resources, we geolocate both the servers hosting them and a large subset of the routers in the path. To this end, we first launch traceroute measurements from RIPE Atlas nodes [31] in each country/region towards the identified hosting servers. With the collected traceroute measurements, we employ the RIPE Atlas IPMap [3] active IP geolocation method to geolocate hosting servers and routers. We also extract geolocation hints from the host names of routers and server infrastructures obtained from reverse DNS and HLOC [33]. As some of the hosting servers can be part of existing cloud or CDN deployments, we use publicly available datasets [1, 2] for major cloud service providers (Amazon and Microsoft Azure) to map their infrastructure to publicly announced server locations.[1] We cross validate our geolocations using the results from different geolocation techniques. We then leverage online CDN detection tools to tag CDN-hosted resources.[2]

3.3 Detecting Submarine Cable Links

In the last step, we tag resources that use SCN links on the path to their hosting servers. We rely on several heuristics for this, building on our previous work [20]. We first employ a simple heuristic to identify possible routes relying on the SCN. Previous work [24] has shown that a significant fraction of all the long-haul physical links in the US are co-located with roadway infrastructure and railroad. Based on this observation, we rely on a heuristic we refer to as *drivability* which can be summed up as follows – *if there is no drivable route (avoiding ferries) between each end of a given data path, there must not be a continuous landmass connecting them. This would suggest that some part of the path relies on a submarine cable*. Since a small fraction of these routes may instead use a satellite link [21], we use the difference in round trip time (RTT) between each hop to discard satellite links by checking that the difference is greater than 476 ms (minimum RTT for satellite communication) [21].

Note, however, that even if there is a drivable route, it is still possible that the resource is accessed via a submarine cable. For instance, previous work has shown that network traffic from South Africa to Angola uses the WACS cable [25]. Our heuristic would discard any SCN path as a possible candidate since there is a drivable route between these two endpoints. Thus, our analysis yields a conservative estimate of the criticality of the SCN for particular countries.

Finally, to determine a list of candidate submarine cables capable of carrying network routes, we rely on a second heuristic based on *speed of light (SoL)* estimations. For each traceroute, we iterate through a list of submarine cables, testing if it is possible for a signal to traverse from source to destination, via the landing site of a given cable, within the minimum measured time. Listing 1 describes this test.

Listing 1: Pseudocode for *SoL* testing of SCN usage

```
Define:
 S: Location of the source VP for the traceroute
 D: Location of the hosting server
 L1: Cable landing site near source VP
 L2: Cable landing site near hosting server

begin
 foreach cable C in the mapped set
    foreach pair of landing sites (L1, L2) for this cable
        calculate the geographic distance of the full path for S − L1 − L2 − D
        set time limit to half of the minimum RTT
        if the signal could traverse the path at the speed of signal (2/3 speed of light)
              within the time limit
           then add cable C to candidates
end
```

Region	Countries	Class			Region	World
		Other	LL	ISL	%	%
Asia	15	10	0	5	91.1	45.8
N. America	2	2	0	0	99.9	7.6
C. America	2	2	0	0	81.9	2
S. America	4	4	0	0	77.1	5.2
Africa	2	2	0	0	15.1	1.7
Europe	34	22	9	3	83.5	13.3
Mid. East	2	2	0	0	13.3	0.5
Oceania	2	1	0	1	91	0.5
Total	63	45	9	9	-	77.6

Table 1: Summary of coverage per region. Last columns are the percentage of users in the region, and the percentage of the world's users covered by our dataset. (LL: Landlocked countries; ISL: Island countries.)

4 DATA COLLECTION

The following paragraphs present the data collection process and describe the dataset used in our analysis. We select a list of countries per region that, together, capture a significant portion of Internet users for (most) regions and the world [11]. We use the top sites ranking provided by Alexa, which consists of the most popular sites visited by users in each country/region, and various VPN services to identify the resources served by these sites to users in those countries. We then launch traceroutes to the hosting resources from RIPE Atlas nodes within those same countries. For submarine cable detection, we rely on the SCN dataset made publicly available by TeleGeography [35]. We ran this data collection process twice between April and September of 2020, with the same list of countries and websites.

4.1 Countries and Regions

For data collection, we focus on countries that (1) host servers with available VPNs with DNS servers within the country, (2) have good coverage of RIPE Atlas probes [31], and (3) for which Alexa Top Sites [8] data exists. Our set includes 63 countries covering every sub-region in the world, including the Americas, Europe, Asia, Oceania[3], Middle East and Africa.

[1] For others, such as Google, we use RDNS hints as they show very consistent naming patterns.

[2] We rely on publicly available tools [4] and [23] that use CDN CNAME record with database matching to determine the CDN service used.

[3] We treat Australia as an island country based on our definition.

While the SCN interconnects almost every country in the world, we expect the criticality of this network to vary widely depending on features such as sub-region, geography and Internet penetration. For example, we would expect an island-country like Japan to rely on the SCN more heavily than a landlocked country like Switzerland would. Thus we classify each country [12, 13] as *Island, Landlocked* or *Other*. An *Island* country is defined as one without land borders with other countries/regions, while a *Landlocked* country is defined as one with only land borders. The remaining countries are classified as *Other*. Table 1 lists, for each sub-region, the number of countries included per class, and the percentages of Internet users in both the sub-region and the world. For instance, in Europe, our dataset includes 34 countries, 9 of which are Landlocked countries and 3 of which are Island countries. Together, they capture 83.5% of the Internet user population of Europe and 13.3% of the world's Internet population. The percentage of the Internet population covered is computed as the fraction contributed by the sub-region times the percentage of the sub-region's Internet population captured by our dataset. For most sub-regions, we have included enough countries so as to cover > 75% of the Internet user population in that sub-region. Two exceptions are in the Middle East and Africa, together contributing 15.4% of the world Internet population, where we could not find sufficient vantage points, particularly from VPN services.

4.2 Web Page Resources Dataset

For the selected countries, we use the local Alexa Top-50 sites as a proxy for the most popular Internet resources users in those countries rely on (with a total of 1864 websites). While some popular sites may be similar across countries (≈1% of sites are shared by ≈50% of the countries), the set of resources those sites rely on and the servers hosting those resources are likely to be different. To capture the actual resources users in specific countries rely on, we employ servers hosted by the Nord [14], Cyberghost [9], HideMyAss [10] and Transocks [15] VPN services as web vantage points when crawling these sites. For each VPN connection, we use a Selenium-controlled Chrome web browser instance to crawl the sites.

Since a single server could host multiple resources, we maintain a map matching resources requested to server IP address. On average, each country is mapped to 848 unique IP addresses hosting web resources. We then use the designed IP geolocation pipeline to geolocate all the unique resource server IP addresses. On average, we were able to geolocate 61.24% of the server IP addresses, which corresponds to an average of 66.28% of all resources geolocated for all countries/regions. As a last step, we use a publicly available tool for tagging resources with CDNs [4, 23].

4.3 Traceroutes and Country Level Routes

With the collected set of resources and their corresponding hosting servers identified, we launch traceroute measurements to the different hosting servers from RIPE Atlas probes in the respective countries. We thus collect 53,419 traceroute measurements for our analysis. To better understand the criticality of the SCN for landlocked countries, we derive a country-level path from the collected traceroutes by geolocating each router on the path.

4.4 Submarine Cable Data

We collect information on submarine cables, including landing sites and their geographic coordinates, countries, and cable length, using the dataset made publicly available by TeleGeography [35]. The overall dataset consists of the main information for all submarine cables currently deployed or under construction around the world. We iterate through all submarine cables listed on the TeleGeography public dataset, and use all pairs of landing points that are connected by each submarine cable to create a table of key-value pairs. We use the countries of the two landing sites as keys, with the values being the sets of submarine cables that connect the two countries.

4.5 Summary of the Dataset

In summary, our dataset includes an average of 12,199 unique resources per country, for 63 countries around the world. These resources are hosted by the Alexa Top-50 sites for each country, with a total of 1864 unique websites. We resolve each resource URL to get the IP address of the server hosting the resource. On average, we observe 848 unique IP addresses for the selected countries. For each pair of country and IP address hosting resources for content accessed from that country, we launch traceroute measurements using an in-country RIPE probe towards the IP address. In total we generate 53,419 traceroute measurements for our analysis. All dataset and VPN configurations are publicly available.

5 RESULTS AND ANALYSIS

We now present results from our analysis of the criticality of the SCN infrastructure for different countries around the world, focusing both on individual Internet resources and full websites. We look at the benefits of CDNs and frame our results in terms of the Internet population impacted.

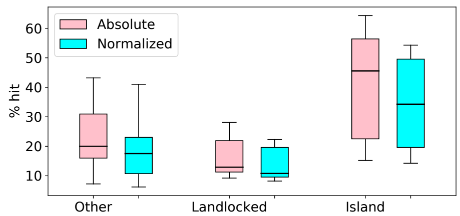

Figure 1: SCN path hit rates for countries in each geographic category, both absolute and normalized by Internet penetration per country.

5.1 Criticality

We first look at the criticality of the SCN, separating countries based on their geographic categories (i.e., Landlocked, Island, and Other). Figure 1 shows the distribution of SCN hit rates per geographic category. As a reminder, we define criticality (§2) in terms of the fraction of "popular" Internet resources hosted on the other side of a submarine cable.

As one would expect, Island countries are the most dependent on the SCN, with an average SCN hit rate of 42.7% and a maximum hit rate at 64.33% (Cyprus).[4] For regions classified as "Other" (neither landlocked nor islands), we find a lower yet significant reliance on the SCN infrastructure, with nearly a quarter of all resources (22.98%), on average, hosted on the other side of a submarine cable (maximum is 43.62%, South Africa).

Perhaps most surprisingly, we find that Landlocked countries, despite not having any part of their territory connected to an ocean or sea, still have an average of 16.25% reliance on the SCN.

To better understand how Landlocked countries access the SCN, we obtain a country-level route (§3) for the SCN paths to popular resources from these countries. Figure 2 shows a Sankey diagram summarizing how Landlocked countries in our dataset rely on neighboring countries to reach the SCN. On average, these countries use 4 neighboring countries (with the exception of Belarus, which routes traffic via 7 different countries), and do so with a clearly preferred neighbor (> 40% of their SCN paths). Of the countries in this subset (all of them in Europe), Germany, the United Kingdom, France and the Netherlands are the most frequently chosen countries for routing. These four countries are also host to some of the largest European IXPs – DE-CIX, AMS-IX, LINX and France-IX.

Thus far, our analysis has focused on the criticality of the SCN on a per-country basis. The degree of criticality when focusing on end users, however, is in part a function of the fraction of its Internet population. For example, while Indonesia and Taiwan have similar SCN path hit rates (53.73% and 50.77%, respectively), Indonesia has a 62.6% Internet penetration rate, much lower than Taiwan's 92.6%.

[4]The minimum hit rate is 15.19% corresponding to Japan.

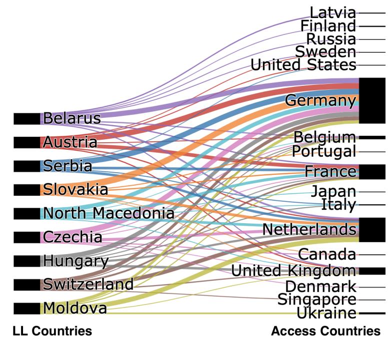

Figure 2: Neighbor countries (right) used by landlocked countries (left) to access the SCN.

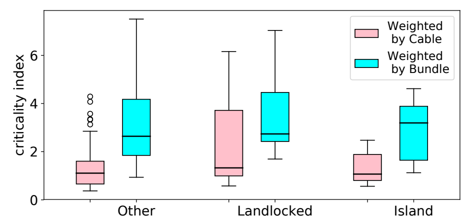

Figure 3: SCN path hit rates for countries in each geographic category, weighted by cable/bundle.

To account for this, the second set of boxes in Fig. 1 shows the percentage of SCN path hits weighted by the respective country's *Internet penetration*. In the previous example, the reliance on the SCN is adjusted to 33.64% for Indonesia and 47.02% for Taiwan.

Our initial analysis of criticality also ignores the degree of redundancy in the SCN infrastructure available to a given country. While two countries may show comparable reliance on the SCN, one with greater redundancy should be less affected by any single cable failure. To account for this, we weight the percentage of popular resources retrieved via the SCN by the number of cables and by the set of bundles available, yielding two values of *criticality index*. Figure 3 presents box plots for each country category. Using the number of cables as weight can be seen as a *best case* analysis, as it assumes that all cables are interchangeable. Weighting by bundles, on the other hand, offers a more realistic view of criticality, considering that only cables in the same bundle, as determined by the *SoL test* (Listing 1), provide redundancy. The criticality index ranges between 0 and 100, with 100 meaning that the country retrieves all resources over the SCN and has only one cable or bundle connecting it. The largest observed criticality index corresponds to Argentina, with a 30.02% hit ratio and reliance on 7 cables and 4 bundles.

It is interesting to compare Figs. 1 and 3; while Landlocked countries are expected to be less dependent on the SCN than Island countries, they also tend to have less redundancy. As such, their weighted criticalities are comparable.

5.2 Benefit of CDN

One would assume that the potential added delay incurred by traversing a submarine cable would motivate content providers and CDNs to host resources (in particular, popular ones) on nearby servers, and in the process avoid the potential risks of SCN failures. To understand the extent to which this holds, we look at the fraction of CDN resources hosted in replicas reached via submarine cables.

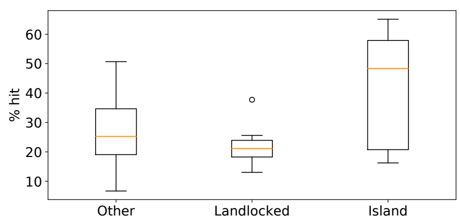

Figure 4: SCN path hit rates for CDN-hosted resources for each geographic category.

For the CDNs detected in our dataset,[5] Fig. 4 summarizes the SCN path hit ratios of CDN-hosted resources for countries in each geographic class. Across all countries in our dataset, an average of 28.22% of requests to CDN-hosted resources hit a SCN path. In some instances (Cyprus), we find as many as 65.1% of all requests for CDN-ized content relying on the SCN!

Of the three classes of countries, the group most clearly benefiting from nearby CDN replicas is the Landlocked group, with an average SCN path hit ratio of 21.95% (as a point of reference, the average SCN path hit ratio for its non CDN-hosted content is 8.48%). North Macedonia is the outlier in this class, with its SCN hit rate for CDN-ized content reaching 37.73%. While this hit rate for CDN-hosted content is lower than those of countries in the other two categories, it is still significant.

This finding challenges our own assumptions that the expansion of CDN deployments could reduce the criticality of the SCN for end users. There are a number of plausible explanations for this, including the fact that although they have large and growing infrastructures, the majority of CDNs adopt a *bringing-ISPs-home* type of deployment [27], implying longer routes to content and higher chances of traversing a submarine cable.

[5] The CDN detection tool used may not capture all CDN-hosted resources. There may be more resources hosted on CDN's in our dataset.

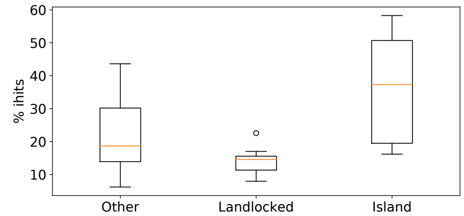

Figure 5: Fraction of websites with index page request relying on the SCN.

5.3 Landing Pages Across the Ocean

The ability to retrieve a website's landing page (index), the first resource to be requested when visiting a web page – and to do so in a timely manner – is critical when browsing the web. If a site's landing page is hosted across the SCN, then an end user's ability to load the page would be directly affected by any SCN disruption.

Figure 5 shows the percentage of sites for which the landing page was retrieved via a SCN path for each geographic class. Surprisingly, an average 22.85% of websites for all countries in our dataset hit a SCN path during retrieval (≈37%, 14%, and 22%, on average, for Island, Landlocked and Other countries, respectively).

6 CONCLUSIONS

While the submarine cable network is generally recognized as critical infrastructure, we lack a clear understanding of the extent of its criticality from the perspective of end users. We presented a general methodology for analyzing the reliance on the SCN of a given region, and applied it to 63 countries from every continent, focusing on the most popular web resources accessed by users in those regions. Our results show that, contrary to popular belief, users rely on the SCN to access a significant fraction of popular web resources, across countries. Despite the explosive growth of data center and CDN infrastructure around the world, we found that on average, at least 28.22% of the CDN-hosted resources hit a submarine cable, with that figure as high as 65.1% for some countries. These findings make the case for further analysis of the criticality of this network infrastructure for end users.

ACKNOWLEDGMENTS

We would like to thank our shepherd Alberto Dainotti and the anonymous reviewers for their helpful feedback. This project was in part supported by NSF grant CNS-1619317. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of any funding agencies.

REFERENCES

[1] [n. d.]. AWS IP address ranges. ([n. d.]). https://docs.aws.amazon.com/general/latest/gr/aws-ip-ranges.html
[2] [n. d.]. Microsoft Azure Datacenter IP Ranges. ([n. d.]). https://www.microsoft.com/en-us/download/details.aspx?id=56519
[3] [n. d.]. RIPE IPmap. ([n. d.]). https://ipmap.ripe.net
[4] [n. d.]. What's My CDN? ([n. d.]). https://www.whatsmycdn.com/
[5] 2015. Impact of Provider Failures on the Traffic at a University Campus. In *Proc. IFIP Networking*.
[6] 2017. Detecting Peering Infrastructure Outages in the Wild. In *Proc. of ACM SIGCOMM*.
[7] 2017. NEC begins Construction of Submarine Cable Links to the Islands of Palau, Yap and Chuuk. NEC. (May 2017). https://bit.ly/2JqQQaE.
[8] 2020. Alexa Top Sites by Country. (May 2020). https://www.alexa.com/topsites/countries
[9] 2020. CyberGhost VPN. (2020). https://www.cyberghostvpn.com/
[10] 2020. HideMyAss VPN. (2020). https://www.hidemyass.com/en-us/index
[11] 2020. Internet World Stats. (May 2020). https://www.internetworldstats.com
[12] 2020. Landlocked country. (May 2020). https://en.wikipedia.org/wiki/Landlocked_country
[13] 2020. List of island countries. (May 2020). https://en.wikipedia.org/wiki/List_of_island_countries
[14] 2020. NordVPN. (2020). https://nordvpn.com/
[15] 2020. Transocks. (2020). https://www.transocks.com/
[16] Africanews. 2020. Internet slows across Africa as major undersea cables falter. (January 2020). https://www.africanews.com/2020/01/17/africa-internet-outage-after-cable-issue/
[17] Al-Masry Al-Youm. 2013. Internet saboteur caught, says Telecom Egypt CEO. (March 2013). https://www.egyptindependent.com/internet-saboteur-caught-says-telecom-egypt-ceo/.
[18] Alliance for Affordable Internet. 2020. 2019 Affordability Report. (2020). https://a4ai.org/affordability-report/report/2019/.
[19] APEC Policy Support Unit. 2013. Economic Impact of Submarine Cable Disruptions. (February 2013). https://www.apec.org/Publications/2013/02/Economic-Impact-of-Submarine-Cable-Disruptions
[20] Zachary S Bischof, Romain Fontugne, and Fabián E Bustamante. 2018. Untangling the world-wide mesh of undersea cables. In *Proceedings of the 17th ACM Workshop on Hot Topics in Networks*. 78–84.
[21] Zachary S. Bischof, John P. Rula, and Fabian E. Bustamante. 2015. In and Out of Cuba: Characterizing Cuba's Connectivity. In *Proc. of IMC*.
[22] Bill Burns. 2011. Cyrus W. Field. History of the Atlantic Cable and Undersea Communications. (2011). http://atlantic-cable.com/Field/.
[23] CDNPlanet. [n. d.]. CDN Finder Tool. ([n. d.]). https://www.cdnplanet.com/tools/cdnfinder
[24] Ramakrishnan Durairajan, Paul Barford, Joel Sommers, and Walter Willinger. 2015. InterTubes: A study of the US long-haul fiber-optic infrastructure. In *Proc. of ACM SIGCOMM*.
[25] Rodérick Fanou, Bradley Huffaker, Ricky Mok, and KC Claffy. 2020. Unintended Consequences: Effects of Submarine Cable Deployment on Internet Routing. In *Proc. of PAM*.
[26] Submarine Telecoms Forum. 2020. Outage Archives. (April 2020). https://subtelforum.com/tag/outage/.
[27] Cheng Huang, Angela Wang, Jin Li, and Keith W. Ross. 2008. Understanding Hybrid CDN-P2P: Why Limelight Needs Its Own Red Swoosh. In *Proc. of NOSSDAV*.
[28] International Cable Protection Committee. 2016. Submarine cables and the BBNJ. *Submission to the Preparatory Committee established by UN General Assembly resolution* (2016).
[29] Alan Mauldin. 2017. A Complete List of Content Providers' Submarine Cable Holdings. Telegeography blog. (November 2017). https://bit.ly/2Lw7DLm.
[30] Alan Mauldin. 2018. Content, Capacity, and the Great, Growing Demand for International Bandwidth. Telegeography. (May 2018). https://bit.ly/2JsduPK.
[31] RIPE NCC. 2020. RIPE Atlas Probes. (2020). https://atlas.ripe.net/probes
[32] Lily Hay Newman. 2020. Cut Undersea Cable Plunges Yemen Into Days-Long Internet Outage. (January 2020). https://www.wired.com/story/yemen-internet-blackout-undersea-cable/
[33] Quirin Scheitle, Oliver Gasser, Patrick Sattler, and Georg Carle. 2017. HLOC: Hints-based geolocation leveraging multiple measurement frameworks.
[34] STF Analytics. 2020. Submarine Telecoms Industry Report. (2020). https://subtelforum.com/submarine-telecoms-industry-report-web-edition/
[35] TeleGeography. 2020. Submarine Cable Map. (2020). https://www.submarinecablemap.com/
[36] Kim Zetter. 2008. Undersea cables cut; 14 countries lose web. Wired. (December 2008). https://bit.ly/2Lm6B7L.