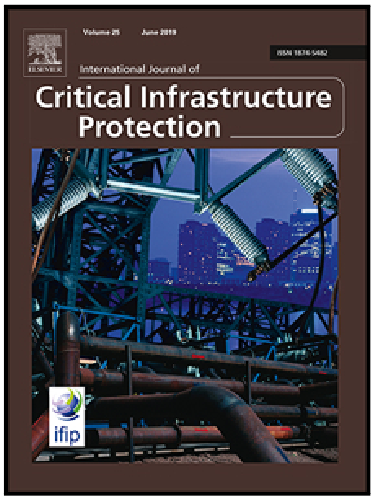
Journal Pre-proof



nThe Digital Divide in State Vulnerability to Submarine Communications Cable Failure

Jonas Franken

PII: S1874-5482(22)00013-0
DOI: https://doi.org/10.1016/j.ijcip.2022.100522
Reference: IJCIP 100522

To appear in: *International Journal of Critical Infrastructure Protection*

Received date: 29 March 2021
Revised date: 21 January 2022
Accepted date: 26 February 2022

Please cite this article as: Jonas Franken , nThe Digital Divide in State Vulnerability to Submarine Communications Cable Failure, *International Journal of Critical Infrastructure Protection* (2022), doi: https://doi.org/10.1016/j.ijcip.2022.100522

Highlights

- Little academic attention is paid to the subsea fiber cable network in its entirety
- Public cable data and network analysis tools allow modeling the internet backbone
- Submarine communication cable links are unevenly distributed at global scale
- On average, developing economies have lower levels of backbone redundancy
- Internet outage risk due to subsea cable failure is higher in least developed areas

The Digital Divide in State Vulnerability to Submarine Communications Cable Failure

Authors

(anonymized)

Abstract

The backbone network of submarine communication cables (SCC) carries 98% of international internet traffic. Coastal and island states strongly depend on this physical internet infrastructure to provide internet connectivity. Although about 100 SCC breakdowns of human or natural origin occur at yearly average, a literature review reveals that there is no global comparison that assesses individual state vulnerability to SCC failure in global comparison. In this article, the global SCC network is modeled based on publicly available data. Besides the analysis of the global network properties, a focus is put on remaining bandwidth capacities in three different failure scenario simulations of SCC breakdowns. As a result, this study identifies 15 highly vulnerable states and overseas territories, and another 28 territories that are classified as partially vulnerable to SCC failures. Since economic market decisions shape the structure of the SCC network, an uneven distribution of redundancies and the resulting vulnerability of disadvantaged economies can be confirmed. Therefore, the study's findings may contribute to a better assessment of the necessity of preventive protection measures of critical telecommunication infrastructures in states and territories characterized by high and medium vulnerability.

Keywords

Submarine Cable Network, Internet Backbone Infrastructure, Global Network Analysis, Internet Blackout Vulnerability, Global Digital Divide

Introduction

With over four billion users, the internet is the dominant medium of communication of present times [1]. Although no general and uniform definition of critical infrastructure on the international level has yet emerged [2], the communication sector is typically part of the core classifications in most countries and international bodies [3]. The United Nations Office for Disaster Risk Reduction (UNDRR) defines critical infrastructures as "*[t]he physical structures, facilities, networks and other assets which provide services that are essential to the social and economic functioning of a community or society*" [4]. Internet is ubiquitous, at least in most parts of the world, and modern societies and economies are highly dependent on its provision. Therefore, the physical internet providing infrastructures can be considered critical infrastructures [5,6].

The internet is based on a multitude of different physical transmission structures that are essential for its operation, the most important being land-based fiber optic communication cables (LCC) and submarine fiber optic communication cables (SCC). For the transmission of global data traffic, the latter is by far most important: More than 98% of international online communication is handled via fiber optic cables laid in the world's oceans [6,7]. Therefore, the global backbone network of SCCs is indispensable for the worldwide operation of online data exchange [8]. Currently, over 80% of the 1.3 million kilometers of active submarine fiber optic cables are located in inaccessible deep sea below 1500 m depth [9], which makes it impossible for authorities or private companies to ensure continuous surveillance and physical protection of it [10]. Hence, fiber optic cables are regularly exposed to factors that potentially impair their function. According to Mauldin [11], most of the incidents originate from unintended human activity at sea, such as fishing (38%) and drag anchoring (25%), followed by environmental hazards (14%) like seaquakes or underwater currents. Considering over 100 failures of SCCs on yearly average [11], it appears obvious that the functionality of the global internet cannot be taken for granted. Although many cable failures can be compensated by longer and slower alternative routes, these are not available in all geographical regions [12]. The alternative technology of satellite-based internet, which can, in theory, be accessed worldwide, is far from being able to transmit the necessary amount of data to compensate for an SCC [7]. Low earth orbit technologies like SpaceX's Starlink or OneWeb do not yet provide the bandwidth currently needed by whole societies, as they are still in trial phase [13].

The following example of a cable failure that led to the complete loss of broadband connectivity for an entire territory illustrates the consequences of internet outages: On the archipelago of the Northern Marianas, the only available submarine cable ruptured in 2015 due to underwater currents, completely cutting off the island from broadband traffic for several days [14]. Cascading effects caused internet, telephone communication, and air traffic to collapse, along with disruptions in the health, tourism, and education sectors. The U.S. overseas territory with 50,000 inhabitants suffered damage amounting to 21 million USD. Small island developing states (SIDS) hardly offer any possibility to operate a cable economically due to their characteristics, such as their remote location, small number of citizens, and below-average GDP, resulting in lower internet usage [15]. Consequently, if any, internet connectivity is usually available only via one or two submarine cables [16]. Here, the state's dependency on the functioning of an SCC is apparent. Nevertheless, cable ruptures in the past also triggered consequences for countries with multiple alternative cables [17,18]. In order to generate a broader picture and not reduce the consequences of a cable break to the, according to literature, most vulnerable group of SIDS alone [16,19], a global focus is chosen for this paper.

The research question underlying the work will therefore be:

Which states and overseas territories are vulnerable regarding the loss of functionality of adjacent submarine communication cables in global comparison in mid-2020?

To approach this question, we divided this paper into six sections. After the introduction (Sec. 1), we provide an overview of the related work (Sec. 2). Subsequently, we proceed with the method section, where core definitions, network analysis tools, and the data compilation are presented (Sec. 3). We continue with the data analysis, including calculating the network indices, forming groups of vulnerability levels, and checking for statistical correlations with development status (Sec. 4). The paper closes with a discussion of our findings (Sec. 5) and concluding remarks (Sec. 6).

Related Work and Research Gap

The degree of dependency on critical communication infrastructure is unevenly distributed across the globe. Already since the early 2000s, research on shortcomings and imbalances in the provision of internet access and the unequal exploitation of economic gains for societies was developed within the framework of the digital divide theory. In the early phase of broadband deployment from 1995 to 2005, the digital divide was explained by the presence and quality of physical access to the internet [20], followed by increased research on the micro-level of digital skills and usage from 2002 onwards. In the third and nascent phase, attention is paid to outcome aspects and path dependencies of internet use [21]. In the following study, we want to combine features of the purely physical focus of the early research with the outcome side of increasing societal and economic dependency on the internet on global level. The growing demand for internet bandwidth throughout the COVID-19 pandemic has further raised awareness on these dependencies in 2020 and beyond [22,23].

In the current academic research on the vulnerability of the submarine fiber optic network, several contributions approach the subject from the perspectives of diverse scientific disciplines (see Table 1). Various types of empirical academic case studies on specific countries [24,25], continents [26], and regions [15,27–30] are presented, each with a distinct understanding of vulnerability. The studies of national focus incorporate a wide range of local proponents like geographic, geopolitical, and environmental context but do not offer definitions of vulnerability measurable through empirical means. In contrast to that, Cariolle defines digital vulnerability in his study on sub-Saharan Africa *"as the risk for a country and its population of its access to telecommunication services being hindered by failures in its telecommunication networks"* [26], taking into account internal digital divides of the 46 countries he analyzes. Whereas Cariolle considers the local perspective of countries as a single reference unit, Omer et al. evaluate the vulnerability of the global network *"by identifying the links in the network that would lead to greater damage than others when disrupted"* [31], putting more emphasis on the critical links than on the nodes. A similar edge-bound perspective is taken in the study of Palmer-Felgate and Booi on different SCC system designs. Here, vulnerability is understood in a broader sense as the absence of resilience, with the latter being statistically modeled through the availability of alternative routes, short repair times, and reliability of an SCC [32,33]. Their study focuses on the edges of the submarine network, not the consequences of failure for the nodes. Furthermore, the routes used in their simulation omit several extensive sections of coastline, such as Australia, Oceania, Central America, and Sub-Saharan Africa [32]. Within our work, however, we put focus on the vulnerability in terms of internet access security from the perspective of redundancy availability in each territory. We only consider the meta-structures of the whole network to familiarize the reader with the global SCC network.

Study	***Perspective***	***Unit***	***Academic Discipline***
O'Malley, 2019 [24]	National	State	Security studies
Muneez et al., 2017 [25]	National	State	Environmental studies
Hummelholm, 2019 [29]	Regional	Cities	Cyber security studies
Sutherland, 2009 [15]	Regional	States	Economics

ITU, 2018 [30]	Regional	Islands states and overseas territories	Economics, development studies
Cariolle, 2019 [26]	Intra-continental	States	Development studies
Palmer-Felgate & Booi, 2016 [32]	(Partly) Global	Cable routes	Engineering
Omer, 2009 [31]	Global	Continents	Engineering
Research gap	Global	States and overseas territories	Critical infrastructure research

Table 1: Overview of empirical academic studies analyzing the consequences of submarine cable failures.

With the exception of the contribution by Omer et al. [31], the studies presented above have not reached the perspective of a global comparative analysis of the statistical population. As the exponentially increasing development of SCC numbers, bandwidths, global cable length, and internet traffic demand has continued since the years of data collection (2006, 2008) and publication (2009) of Omer's work, it is worthwhile to look at the present status of the submarine cable network more than a decade later. In addition, the capacities of the relevant statistical programs have further developed over the past decade, which allows a more detailed global view of the backbone structures than a rough comparison of the world regions.

Although Bischof et al. [8] also take a global perspective, they focus on the consequences of higher latency in data traffic rather than on the total loss of internet connectivity in a country when an SCC is lost. The shortest possible latency can be crucial for certain sectors of the economy, such as high-frequency trading in modern finance. However, latency plays a minor role when viewed from the perspective of national internet supply vulnerability.

Consequently, there is a research gap in the global analysis of internet supply security, which considers all coastal and island territories as the central unit of analysis at the same time. To assess the necessity of preventive protection measures, it is important for legislators and authorities to compare the global internet infrastructure redundancies. Hence, the first goal of this work is to provide an up-to-date picture of the global internet supply security situation through SCCs for each autonomously regulated territory. The second goal is to examine whether the global digital divide is also reflected in SCC fault vulnerability.

Method

To approach both goals in a methodologically thorough way, we first find suitable definitions for the core concepts of this work (3.1). We then introduce the network analysis method and discuss the applicability of various centrality measures to the SCC network (3.2). Afterward, the specific scenario formation for the vulnerability estimation for the territories (3.3) is described. Subsequently, we present the availability (3.4) and compilation of the data sets (3.5) and discuss the network analysis software (3.6).

Definitions

The concept of vulnerability is a matter of considerable controversy in risk research. It is variously defined, depending on the context of use and the application of the psychological, social, or technical perspective [23]. Therefore, this concept, which is central to the following work, needs to be discussed. Simply put by the Society of Risk Analysis, the core of most vulnerability definitions is "the degree to which a system is affected by a risk source or agent" [24]. On the other hand, the UNDRR, in its own definition of vulnerability, specifies the context variables that influence the degree of vulnerability: "The conditions determined by physical, social, economic and environmental factors or processes which increase the susceptibility of an individual, a community, assets or systems to the impacts of hazards." [4]. The latter definition is adopted in the following as it provides a comprehensive understanding of possible influencing factors. In this work, we will limit ourselves to the referent object of the community, which is located within the territorial boundaries of a state or an overseas territory. The influencing factors are primarily physical, as the connection to physical infrastructure is examined. It is worth noting that the UNDRR's definition of vulnerability considers individual, communal, and systemic levels of analysis as a reference object. This study applies the definition to states since they represent an applicable and appropriate level of analysis in a global comparison. In this perspective, a state fulfills two roles: First, it is an object of risk that is threatened by the impairment or loss of data traffic; secondly, by taking preventive measures and exercising its regulatory competence in terms of internet governance, it also influences the quality of a threat. Although overseas territories, in some cases, do not own full autonomy in terms of these competencies, they will be considered at an equal level, as it would not make sense in this context to consider them as part of their respective mainland. For example, it would contradict the purpose of the study to add the SCC connections and bandwidth of Martinique, Mayotte, and French Guiana to France, because all units are located in different geographical contexts. Consequently, for the purpose of this study, the geographical location is more important than the state affiliation of a particular region. Fortunately, the International Telecommunication Union (ITU) offers databases for each member state as well as overseas territories (see 3.5.2). The fact that internal inequalities regarding digital vulnerability within states and societies exist is hence ignored in favor of a globally quantifiable unit of analysis.

This study is based on the hypothesis that the number of cable connections in a territory and their transmission capacity (bandwidth) measures the extent to which a country depends on an SCC's functioning. A low number of links to the global fiber optic network then indicates high vulnerability. Conversely, following the hypothesis, a comparatively high number of connections to the physical backbone infrastructure suggests many redundancies and thus low vulnerability. For this study, we define redundancy as an alternative, secondary infrastructure which provides the same or similar service as a potentially failed primary infrastructure. If multiple infrastructures provide this option, the plural form 'redundancies' is applied.

Network Analysis

The global internet backbone constitutes a complex network of relationships between a large number of coastal states and territories, whose connectivity is characterized by their position in it. Consequently, the fiber optic network can be analyzed not only as a physical network of fiber optic cables but also as an abstract network from which characteristics of its components can be deduced. With the method of network analysis, graph theory offers a tool that considers multidimensional group contexts and allows conclusions to be drawn from the position of nodes in the network and the connections (edges) between the nodes [34]. Quantitative network analysis deals with the relationship of nodes by assigning quantifiable values. The presence of a communication cable (binary) as an edge and a metrically scaled property (e.g., their bandwidth) between two states or overseas territories are both quantifiable and can therefore be modeled using quantitative network analysis.

In the following, we will explain the conceptualization of the graph since certain features may limit the choice of centrality measures [35]. First, the edges will be undirected because the SCCs send data in two directions. Second, as there is the possibility of multiple SCCs connecting the same nodes, the network will be modeled as a multigraph. Replacing multiple edges with the cumulated weight in a single edge between two nodes is not possible, as we consider the bandwidth of the cables as the weight of the individual edges. Third, loops will not be formed because this would contradict the requirement to exclusively include *inter*national SCCs. The network is constructed through the graph G

$$G = (V, E, r) \qquad \textbf{Eq. 1}$$

with the nodes V, the edges E and the incidence function r defined as

$$r : E \rightarrow \{\{v, w\} : v, w \in V, v \neq w\} \qquad \textbf{Eq. 2}$$

with v and w as distinct nodes potentially connected through multiple edges.

In general, network analysis offers measurements to assess the general network properties, demonstrating topological characteristics as well as different types of measures for centrality and efficiency of transmission. To familiarize the reader with the network, we have chosen $|V|$, $|E|$, largest component, maximum degree, edge density, mean distance, diameter, and largest clique as measures for an overview (see 0).

A wide array of global and local centrality measures can be applied to determine the positions of nodes – either in the global network or locally within their closest neighborhood [36,37]. Since the network has a moderate size, the global network measures can be calculated for the graph. With a view to the second goal of this study, we want to form groups of highly vulnerable nodes. In this regard, those located in the peripheries of the global network, far from high values of centrality, are of particular interest. Most studies on networks fall under the paradigm of criticality, where highly connected central nodes are presumed to be of higher importance for the functioning of a network as a whole [35]. Considering the position of the weakest connected nodes is a somewhat atypical perspective.

The most frequently applied measures are degree centrality, betweenness centrality, and closeness centrality. For weighted graphs, strength and local efficiency are also often considered.

First, degree centrality $Deg(v)$ measures the number of connections to a node v, irrespective of their weight. It is a local measure, as the global network does not need to be known; it only counts the number of edges to adjacent nodes w. This is given through an adjacency matrix a_{vw}, whose elements take the value 0 if v and w are not connected by an edge and otherwise the value 1. The maximum degree of G is denoted as $\Delta(G)$.

Eq. 3

$$Deg(v) = \sum_{w} a_{vw}$$

As the analysis is aimed at the availability of redundancies, degree centrality seems to be the obvious measure to apply. Firstly, it counts the edges, which is the class of components we identified as the independent variable. Secondly, as a local measure, it offers a simply calculated yet granular level of analysis. However, degree centrality does not consider the weights of the edges.

To account for weighted graphs like G, Barrat et al. extended degree centrality to vertex strength $Str(v)$ [38], as the sum of the weights of the local edges of a node. In our model, this corresponds to the local sum of the SCC bandwidths b adjacent to any given node v.

Eq. 4

$$Str(v) = \sum_{w=1}^{V} a_{vw} b_{vw}$$

A third measure, closeness centrality $Cls(v)$ is determined by the average of the shortest paths δ of a node v with every other node of the network. High values of closeness centrality mean close relationships with many nodes.

Eq. 5

$$Cls(v) = \frac{1}{\sum_{w \in G} \delta\,(v, w)}$$

Based on the closeness centrality, Hao et al. found that balancing node traffic in network design can enhance robustness regarding cascading failures [39,40].

Fourth, another measure based on shortest paths is betweenness centrality $Btw(v)$. It reveals the frequency of node v being a transmitter of information in the network. This is achieved by dividing the number of all shortest paths of any other nodes in G in which node v is present with all geodesic distances δ in G. For example, betweenness has been applied by Nguyen et al. on attack strategies on networks to identify those nodes, which removal would lead to longer δ, making information exchange more costly [41].

Eq. 6

$$Btw(v) = \sum_{u \neq v \neq w} \frac{\delta_{u,w}(v)}{\delta_{u,w}}$$

Finally, the local efficiency $Eff_{loc}(v)$ measure first introduced by Latora & Marchiori [42] for small-world networks was later modified to extend its application to complex networks with weighted and multiple edges [43]. It quantifies the fault tolerance of the immediate neighborhood of v to cope with the removal of v. Therefore, G_v denotes the subgraph of the neighborhood of v without v itself and $Eff(G) = 1/V(V-1)\sum_{v \neq w \in G} 1/\delta(v,w)$.

Eq. 7

$$Eff_{loc}(v) = \frac{1}{V}\sum_{v \in G} Eff(G_v)$$

We are not modeling global internet outages but the consequences of single, double, or triple cable failure on a territorial level. Hence, we limited the choice of centrality measures to those offering benefits in the perspective of edge removal in G (see 3.2). For the SCC network, it must be considered that single nodes may be connected to only one other node but by several parallel edges. If measures have the shortest path as the basis of their calculation, removing an edge does not change the values if a parallel edge connecting the same nodes replaces it. Consequently, closeness and betweenness centrality are not producing meaningful results with multigraphs. Therefore, we rejected closeness and betweenness centrality as suitable measures for redundancy analysis. Local efficiency works with the simulation of a node failure, which contradicts the idea of measuring SCCs as edge failures. Nagurney and Qiang modified local efficiency into a network performance measure to be applied to both components of a graph (edges and nodes), but only for directed graphs [44]. As G is undirected, the modified local efficiency is not further considered.

To support the decision for an adequate redundancy metric, a basic assumption for state backbone access needs to be kept in mind. The total available bandwidth of node v (B_v) is the sum of edge bandwidths b from the available points of access to external networks, be it through SCCs or LCCs:

Eq. 8

$$B_v = b_{SCC\,v} + b_{LCC\,v}$$

Applied to an SCC network, degree centrality and strength as redundancy measures both have a key disadvantage. Degree alone does not consider the highly diverse bandwidths of SCCs, ranging from 1 GB/s to 250 TB/s. On the other hand, the strength measure can only be applied for SCCs, as there is no available data for cross-border LCC bandwidths. Satellite communication is, due to its low bandwidth and low prevalence in the population – rooted in high prices and long latency time – not considered an equivalent redundancy and is therefore omitted from the analysis. To overcome the problem of only partially available bandwidth data, we have decided to perform a two-step calculation. The first step is to cluster groups based on the number of backbone accesses and is intended to identify potentially vulnerable units. SCCs and LCCs are treated equally in the failure scenarios applied for the formation of groups (see 3.2). In the second step of analysis, the share of individual local SCC in the total SCC bandwidth (strength) of a node is measured. This is necessary to account for the large spectrum of bandwidths of globally installed SCC. The local proportion p of the weight of an edge y to the $Str(v)$ can be modeled accordingly as percentage:

$$p_{b_y}(v) = \frac{b_y}{Str(v)} \times 100 \quad \textbf{Eq. 9}$$

The higher $p_{b_y}(v)$, the more vulnerable a node is to the loss of edge b_y. A value of $p_{b_y} = 100$ would mean that cable y is the only access to international networks. Vice versa, the closer the value approaches 0, the less the contribution of a cable to the connectivity of a territory is to be rated, which is why the state's vulnerability is also reduced for the potential loss of this individual cable. The local weight of all adjacent SCCs is being calculated for each territory. Subsequently, the cables can be arranged by their locally weighted capacity input, enabling the application of worst-case scenarios.

Scenarios and Group Formation

Information and communication technology (ICT) infrastructures are subject to different influencing factors during times of peace, crisis, or conflict [45]. We applied the classification of Aceto et al. [17] on various SCC disruption events which we then formed into corresponding scenarios (see Figure 1). To simulate local SCC disruption scenarios, the consequences of removing the edges with the highest bandwidth in the overall strength of the node under consideration are examined. Therefore, we apply three scenarios, in which each state is simulated to lose its first ($S1$), the top two ($S2$), and the top three ($S3$) data-carrying edges.

With an average of 100 yearly incidents, single SCC disruptions are common [11], making the occurrence of $S1$ by far the most probable. Unintended human incidents like anchoring and fishing accidents triggering cable rupture typically led to the single SCC loss scenario $S1$. A variety of situations exist that can potentially result in the simultaneous loss of several cable connections, e.g., a seaquake and subsequent underwater landslides. This kind of cascading incident has led to multiple cable breaks in various regions in the past [33]. There have been cases of multiple cable losses parallel in time, as in the Egyptian incident of 2008 and Taiwan’s situation in December 2006 [10,18]. With $S2$, we intend to model these incidents of parallel small-scale SCC disruptions. Meanwhile, there are no criminal, terrorist, or military interference records with SCCs or cable landing stations (CLS). However, targeted attacks like sabotage bear the potential for multiple simultaneous cable connection losses if conducted with accurate timing [46,47]. As sabotage, terrorism, and criminally motivated actions will likely target the edges of the highest bandwidth, we hold $S3$ to be an appropriate reflection of a multiple-loss scenario with coordinated targeting of the top edges. By reducing our focus exclusively to physical disruptions, we do not consider those outages triggered by governmental interference with internet traffic or the different types of cyber weapons [48,49]. Since the cables themselves do not contain any software components, it is more appropriate to model these types of disruptions with the removal of other, land-bound nodes.

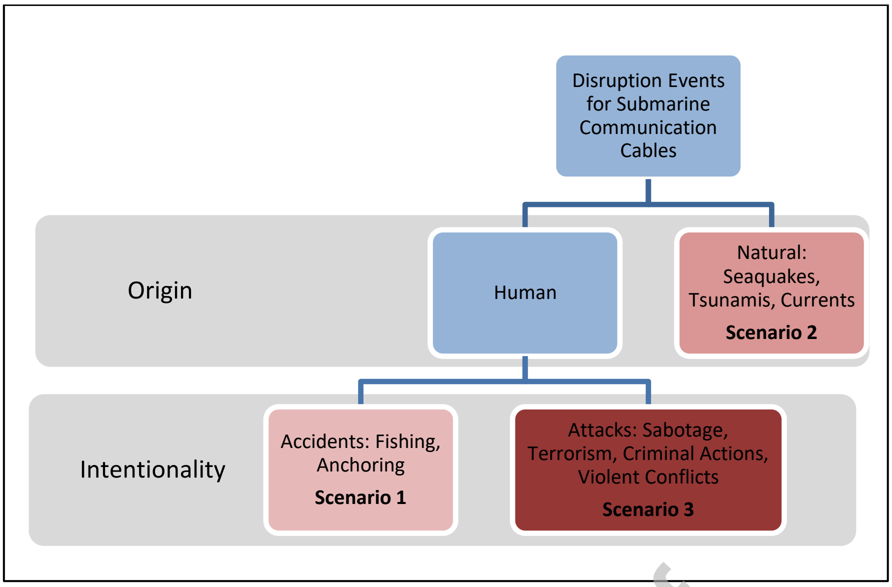


Figure 1: Classification of disruption events and corresponding scenarios for submarine communication cables (Own representation based on the category system of [17]).

The local scenario $S1$ for node v is being modeled as

$$S1_v = \frac{b_{\max(y)}}{Str(v)} \times 100 \qquad \textbf{Eq. 10}$$

where $b_{\max y}$ is the SCC with the locally highest bandwidth in v. This allows us to calculate the proportion of criticality for the strongest SCC. The scenarios $S2$ and $S3$ are modeled accordingly:

$$S2_v = \frac{b_{\max(y)} + b_{\max(n-1)y}}{Str(v)} \times 100\,; \qquad \textbf{Eq. 11}$$

$$S3_v = \frac{B_{\max(y)} + B_{\max(n-1)y} + B_{\max(n-2)y}}{Str(v)} \times 100. \qquad \textbf{Eq. 12}$$

The units are divided into three groups according to the scenarios: Units that have no redundancies, meaning their broadband connection depends entirely on the operation of one SCC, are assigned to Group 1. Units that encounter a complete failure of their broadband connection within the given scenarios $S2$ or $S3$ are assigned to Group 2. All other nodes – having connections to more than four SCCs or LCCs in sum – are assigned to Group 3. Within the groups, rankings are identified according to specific group characteristics (see 4.2).

Availability of Data Sets

There are three comprehensive compilations of the worldwide SCC paths regarding the data sets. While both data sets provide information on cable names, approximate cable runs, adjacent CLS, length, and operational status, they differ in terms of additional information and the number of cables listed. First, the *Submarine Cable Almanac* (*SCA*) of the Submarine Telecoms Forum [50] provides a list of global cable routes (n=301), supplemented with information on the transmission capacity of the cables. The report is updated quarterly with publicly available data from the submarine cable industry. Second, more detailed map material (n=480) is provided by the *Submarine Cable Map* of the online platform TeleGeography, where the owner and operator companies are also listed [51]. Still, the bandwidths of the cables are not specified [51]. Third, the *Infrastructure Map* of the online capacity marketplace Infrapedia also offers detailed SCC capacity data submitted by experts and constantly validated [52]. In the rare cases of conflicting information on the properties of an SCC, we incorporated the information from the *SCA* to prevent potential entry errors of the *Infrastructure Map*, which has only been in operation since 2019. Regional data sets, such as the map of the African Network Startup Resource Center [53], were used to verify the information. The validation of the bandwidth data can be done for cables that are in operation until 2016 with data from *Greg's Cable Map* [54]. ITU's *Interactive Transmission Map* [55] was used and validated with data from the *Infrastructure Map* for data on the quantity of cross-border LCCs. The information of the maps mentioned above is publicly available for non-commercial use, and the *SCA* is accessible online and free of charge [50–54].

The ITU surveys the international broadband traffic for each member state, with the information given directly by governments through yearly questionnaires. The data is provided in the *World Telecommunication/ICT Indicators Database*, which is updated every six months. It contains 180 measures of 200 countries, including "*International internet bandwidth, in Mbit/s*", "*Lit/equipped international bandwidth capacity*", and "*International bandwidth usage*" [56]. The database also contains information on various internet usage indicators in the population [56]. The *World Telecommunication/ICT Indicators Database* is only available on payment basis.

Data Compilation

Since the intention is to assign properties to edges and nodes in a network, two data sets required to create the model are introduced in this section. On the one hand, the edge list is crucial, because the connections between the units and their properties are listed there. On the other hand, the node list describes specific properties of the connected units, the states and overseas territories.

Compilation of the Edge List

Three categories of submarine cables were excluded from the data set and thus omitted in the model. Firstly, cables whose CLS are located within the same territory were not included because they do not contribute to the international data traffic of a state/overseas territory. Examples are *ADONES*, the domestic Angolan submarine cable network and the *JaKa2DeLeMa* intra-Indonesia cable system [50]. The second exclusion category consists of cables only intended for data use at sea, such as oil drilling platforms or shipping. An example of an offshore system is the *TampNet* system installed in the North Sea [50]. Lastly, SCCs that connect military bases and do not contribute to the local connectivity are also excluded from the sample. The only two occurrences in the SCA are the *GTMO-1* and *GTMP-PR*, connecting Guantanamo Bay US Naval Base with Florida and Puerto Rico.

This leaves 197 active cable systems out of 301 cables listed in the SCA, which are modeled over 605 edges between territories. We omitted those nodes adjacent only to excluded SCC. While the majority of these SCCs have two CLS, more complex cable systems also exist. With 33 connected units, *SEA-ME-WE 3* has the highest global connectivity for a single cable system. Cable systems like these are represented in the model by individual edges between territories, as in the case of *SEA-ME-WE 3* by 32 individual edges.

Numerous variables are integrated into the edge list. Essential variables are the states and overseas territories where an SCC is landing. In addition, there is the bandwidth as a measure of the weight of the cable, which is coded in terabytes per second (TB/s). In public data sets, the design capacity is usually given as the maximum capacity of a communication cable expected at the time of design. However, older cables can be used far beyond their original design capacity by applying new technologies like wavelength-division multiplexing [57]. If there is an upgrade for the capacity of a cable that exceeds the design capacity, the upgrade capacity is applied.

Other variables include the location of the CLS, the years of commissioning and expected end of operation, length in km, ownership, and construction costs. These are not necessarily used in the model but have been integrated into the data set for advanced data visualization or subsequent research projects.

Compilation of the Node List

In the node list, the specific data on coastal states and overseas territories are combined. The node list only includes states and territories considered in the edge list. This leaves coastal and island units without qualified SCC connections out of the analysis, for example, East Timor, Poland, or Slovenia. This limitation leads to a reduced sample, including 169 states and overseas territories for the following analysis. This figure may change in the future as more territories are connected to the submarine cable network. For example, with the completion of *Southern Cross NEXT,* Kiribati and Tokelau will be connected by submarine cable for the first time [58].

For the node list, essential variables for the analysis can also be distinguished from auxiliary variables for better visualization. Essential variables are the name of the respective state or territory, the number of cable accesses (credit), the sum of the bandwidth of the SCC connections to a unit (strength), and the number of alternative internet resources. The latter is composed of the number of adjacent cross-border fiber optic LCCs that were counted on the basis of the ITU Interactive Transmission Map [55].

Other variables that serve to visualize the data are the geographic data of the territories. We used the geographical center (centroid) of units for simplicity, which we took from the *rworldmap* expansion program in *R* [59]. To be able to test the hypothesis of the digital divide, the socio-economic development status of the states and overseas territories from the M49 Standard of the UN Statistics Division is included for every unit [60].

Statistical Analysis Program

The network analysis is performed with *R (Version 4.0.0)*. With the packages *igraph* and *sna*, two libraries are available to execute a social network analysis [61–63]. Since *igraph* offers more functions than *sna* and performs faster for networks with over 150 nodes [61], we modeled the network with *igraph (Version 1.2.6)*. Another argument in favor of the *igraph* package is that interactive visualization can be carried out using an *RShiny* web application via the extension package *igraphinshiny* [64].

Findings

A purely visual analysis of the global network offers limited advantages due to the quantity of nodes and edges, as the network model overlaid on a world map in Figure 2 illustrates. Therefore, a resort to mathematical network parameters to identify the structures in the network is necessary (Table 2). The modeled graph consists of 169 units (states/territories) connected by 613 edges (submarine cables and cable system branches). Each node is part of the largest component so that there is at least one possible path between each node in G through which information can be exchanged, making G a connected graph.

The edge density of the model is 4.31%. This indicates the ratio of the actual edges to the number of possible edges. Thus, the submarine fiber optic network is relatively loose. The mean distance between two nodes is 4.44 edges, while the network's longest possible distance (*diameter*) consists of nine edges. A *clique* is a group of several nodes in which each member has at least one direct edge to every other member. In G, the largest clique of five members exists between the Southeast Asian states of Thailand, Indonesia, Hong Kong, Malaysia, and Singapore. A dense network of submarine cables connects these territories. In addition, there are another 18 cliques of four units each, in East Asia, the MENA region, Southern Europe, and the Caribbean.

Measure	***Value***
$\vert\boldsymbol{V}\vert$	169
$\vert\boldsymbol{E}\vert$	613
Largest component	169 (all nodes)
$\boldsymbol{\Delta(G)}$	58
Edge density	0.0431
mean distance	4.44
diameter	9 edges
largest clique	5 nodes

Table 2: General properties of the network model.

After this short overview on the properties of the network as a whole, this section continues with node-specific evaluations through the identification of central nodes (4.1), the formation of groups of redundancy levels (4.2), and the testing of the hypothesis of the Global Digital Divide (4.3). Subsection 4.4 summarizes the findings of the previous sections and merges them into the overall result.

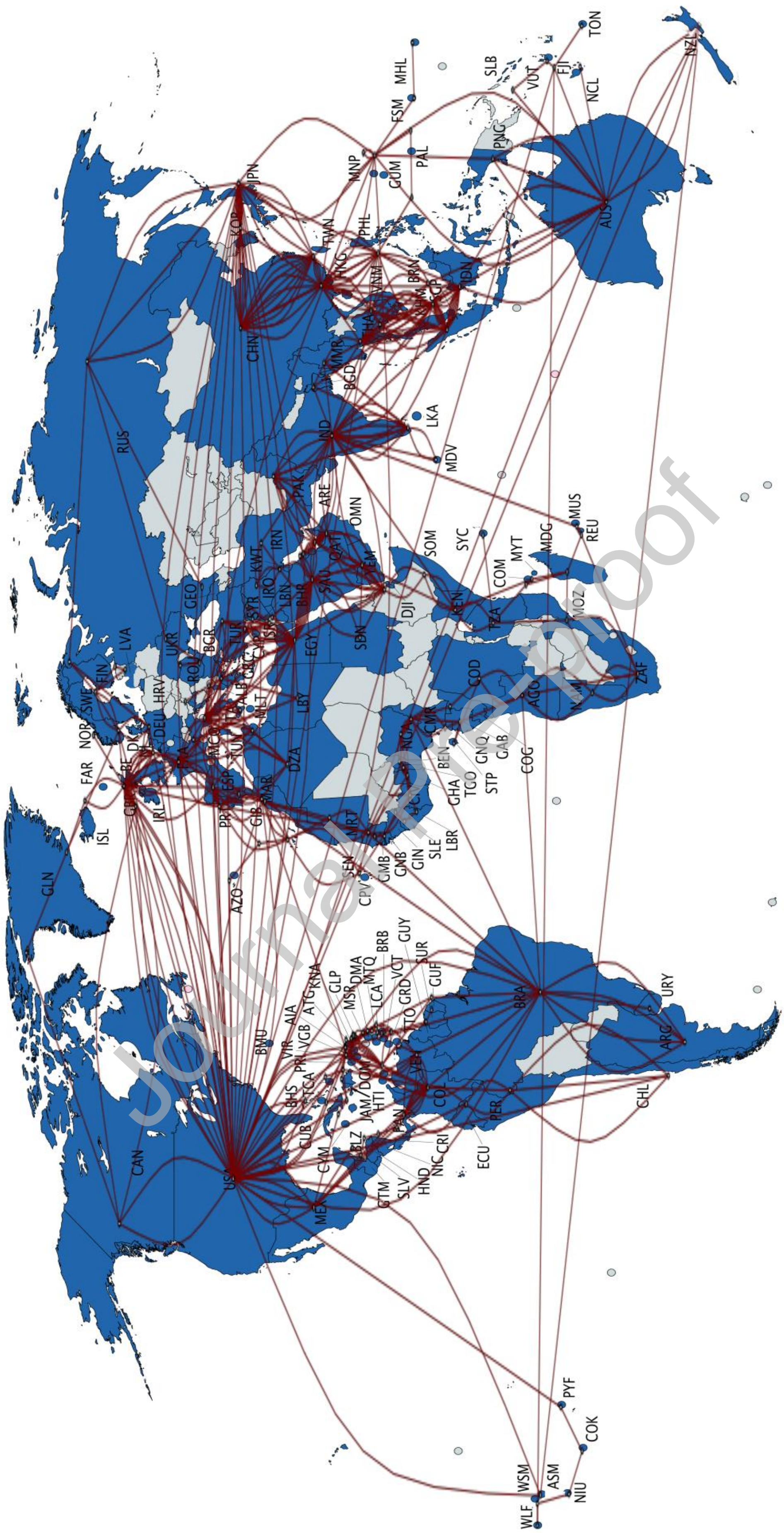


Figure 2: Visualization of the global SCC network (red) between all qualified units (blue), named with their ISO3 country code (Own representation through igraph [63] and mapchart).

Identification of Central Nodes through Centrality Indices

When examining individual nodes, the centrality measures offer a way of identifying particularly central and marginal nodes [65]. The most straightforward measure of centrality is *degree* centrality. For this purpose, each territory is examined locally for the number of its adjacent edges. With 58 adjacent SCCs, the USA clearly leads the ranking, while the United Kingdom and Japan dominate their regions with a degree centrality of over 30. Egypt's high value can be explained by its role as a transit country for SCCs. Since the shortest sea connection between Europe and East Asia leads through the Suez Canal, a large number of SCCs – parallel to shipping routes – run through the Egyptian mainland. The high values of Italy and Saudi Arabia also reflect this effect, as both countries are often the next CLS after the Egyptian bottleneck. With Hong Kong, Singapore, and Malaysia, there are also three East Asian trade and technology centers in the top ten of degree centrality. At the lower end of the scale, 15 units are connected to only one SCC. At first glance, these can be divided into two categories: On the one hand, Northern and Eastern European countries may be provided with sufficient bandwidth through fiber optic land connections to allied states (e.g., Croatia, Lithuania, and Romania). On the other hand, there are island states and territories that are connected to the submarine fiber optic network without redundancy due to their geographical isolation, e.g., the Marshall Islands, Palau, and the Seychelles. Furthermore, 28 territories can be identified with only one redundancy, i.e., two SCC in sum.

Assessing State Vulnerability to SCC Loss through Fault Scenarios

To account for different levels of redundancy, the units are classified according to the group formation as described in section 0. For each of the three groups, a short introduction is followed by an exemplary case study to facilitate the interpretation of data. We chose a distinct visualization of single critical SCC sections (group 1) or the simulations of failure scenarios (group 2 and 3) for each group.

Group 1: No Redundancy

The first group includes units without redundancy in case of failure of their single SCC – neither SCC nor LCC. Figure 3 lists these 15 units along with the SCC through which they are being supplied. Included are territories that are connected by a short cable system branch, such as Gibraltar. The distance from the T-junction of the *Europe India Gateway* system to the CLS in Gibraltar amounts to only 15 km, where the worst case of a complete loss of bandwidth can occur. On the other hand, New Caledonia is dependent on a single cable – rather than a multi-station system – to connect with Australia. The distance over which damage to the cable named *Godwana-1* would be critical to New Caledonia amounts to 2150 km.

The exemplary case study concerns the Seychelles, a state whose access to the global network depends on a single SCC, the *Seychelles to East Africa System*, linking the capital Victoria on the main island Mahé with Dar es Salaam in Tanzania. Island states and island territories in group 1 cannot obtain LCC access, which implies that S1 already leads to a 100% loss of potential broadband connectivity. The critical cable distance of an SCC failure that would amount to full connectivity loss is approximately 1811 km. The *Seychelles to East Africa System* was commissioned in 2012 with a total capacity of 320 GB/s. This potential bandwidth exceeds the actual demand for bandwidth (2018: 4.2 GB/s) by a multiple, which is partly due to the medium level of internet usage among the population (2017: 58.11%) [56] and the relative novelty of the cable, which means that its end-of-service date is not planned until 2037 [52]. To remain commercially viable for a quarter of a century, the design bandwidth capacity of modern cables usually far exceeds the demand of a unit in the ready-for-service year. In the case of Seychelles, a projected second backbone connection is planned through a branch of the *Pakistan & East Africa Connecting Europe (PEACE)* cable system in 2021. This development can be assessed as positive from the perspective of the Seychelles. Yet, the PEACE cables system as a whole is also the subject of geopolitical debate due to the involvement of Chinese companies in its construction [66].

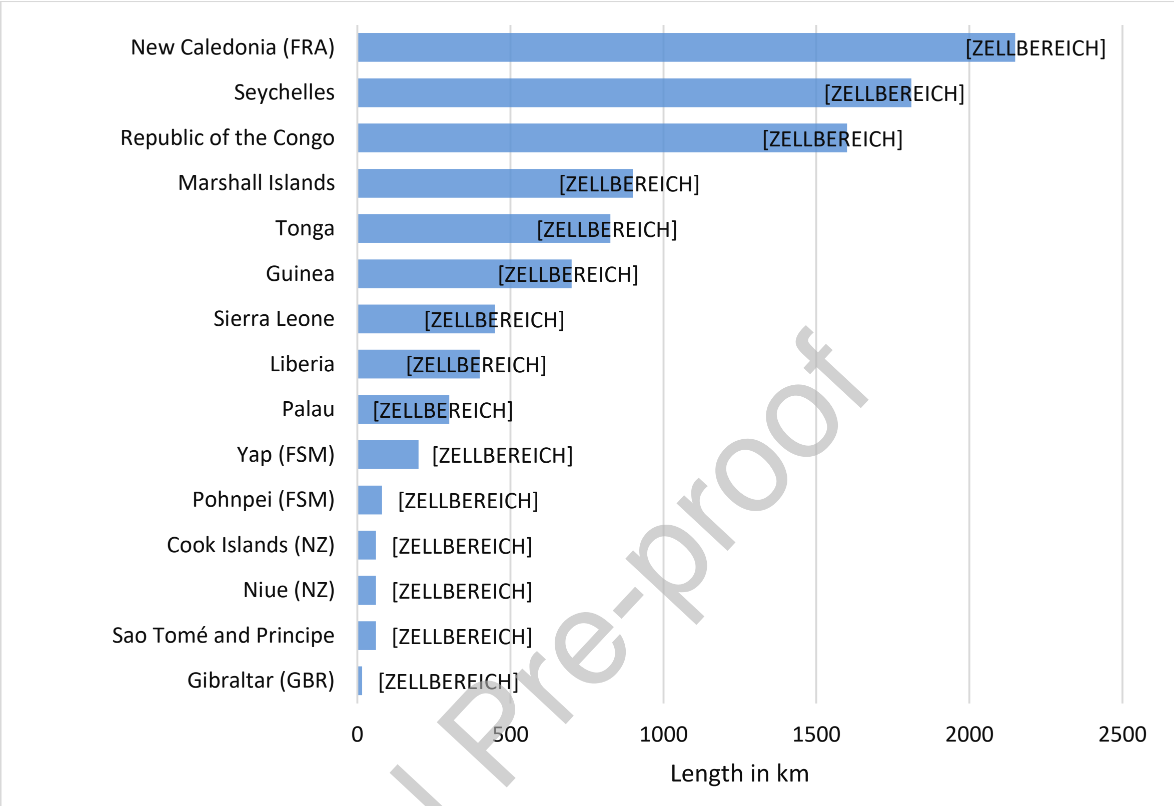


Figure 3: Length of critical cable sections of units with single SCC connection and missing LCC redundancy (Group 1) with the adjacent SCC system or connected territory (own figure).

Group 2: Low Redundancies with Balanced and Imbalanced Fallback Levels

The units that suffer 100% connection failure in S2 or S3, i.e., units with a maximum of three SCC connections, are classified as the second group of units in this study (Figure 4). To additionally take the potential of redundancy through LCC connections of coastal states into account, only units with less than three cross-border LCCs are considered to belong to this group. It is advantageous for this group of 19 units to have a balanced fallback bandwidth ratio to maintain connectivity and minimize risks if the widest and second widest cables fail. Iceland can be considered a good example in this respect. Despite its insular situation, the unit is served by three different cables, all transmitting a fairly similar amount. Even with the removal of the widest cable (*Greenland Connect*), 58.73% of the bandwidth is maintained by the capacity of the other two cables (*Farice-1* and *Danice*).

In contrast, the ratio of Uruguay's cables is rather unbalanced. There, the elimination of the *Tannat* SCC would result in a relative bandwidth loss of 95.74%, with only 2 TB/s weighted design capacity remaining for the whole of Uruguay through the *Antel* cable. As a case study, Samoa is chosen, which has connections to two cable systems: The *Manatua One* and *TUI Samoa.* Both SCCs deliver a combined weighted capacity of 8.5 TB, with 6 TB/s accounted for by Manatua One and 2.5 TB/s by TUI Samoa. This results in a 70.59% to 29.41% ratio of potential bandwidth capacity. Although the fallbacks are not ideally balanced (50%/50%), a sufficiently balanced redundancy level can be assumed, especially considering the equipped international bandwidth capacity of only 4 GB/s (ITU 2017). This leads to a problem arising from the similar CLS in Samoa's capital Apia, which means that the main island has a single point of failure despite its SCC redundancies.

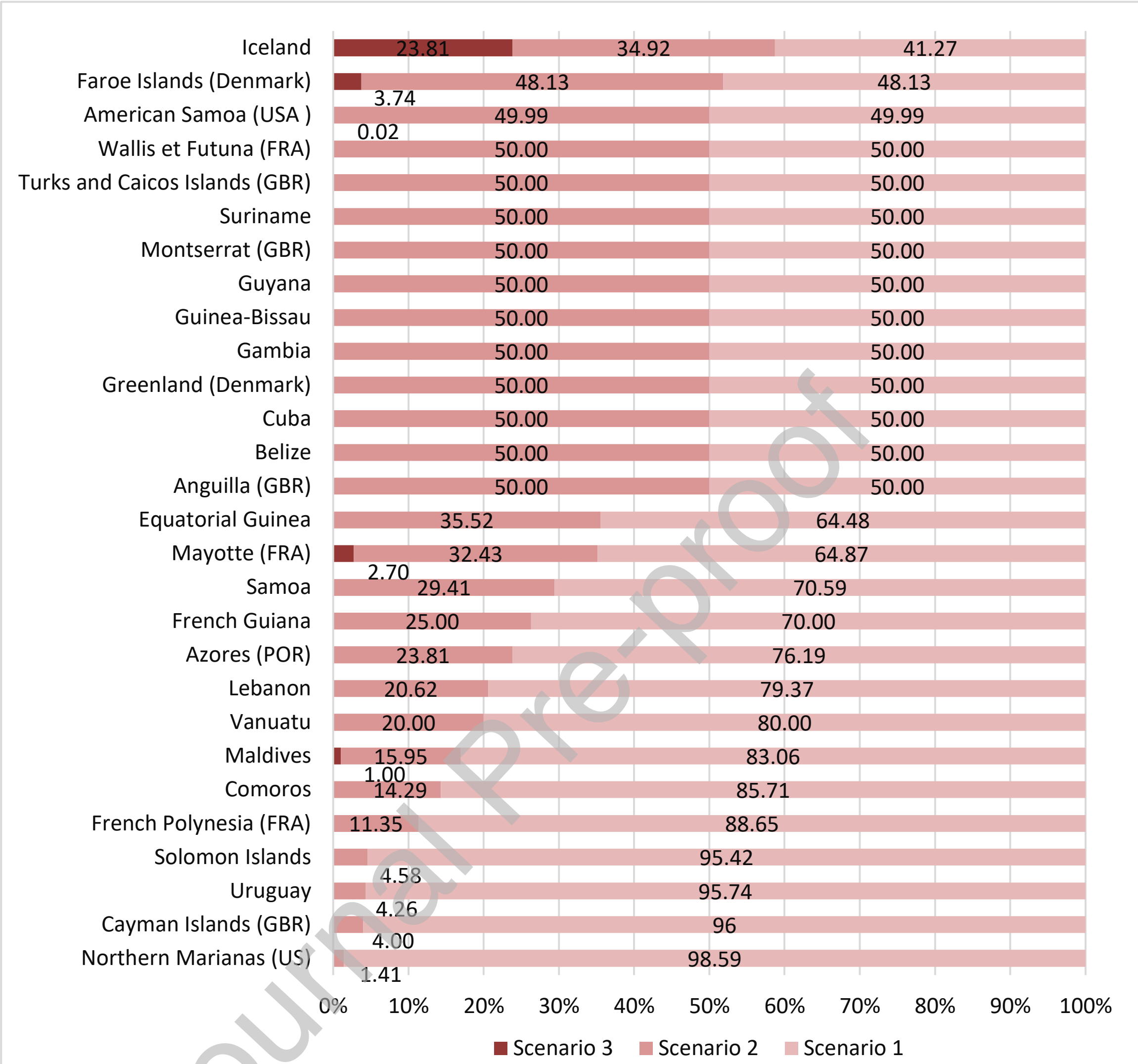


Figure 4: Scenarios of SCC failures for units with low redundancy in relation to their overall SCC connectivity, in the order of relative connectivity loss severity in S1 (own figure).

Group 3: High Redundancy

The remaining 126 units are assigned to group 3. This includes all units equipped with three or more redundancies, regardless of whether they are SCCs or LCCs. These units may suffer from a reduction in the data flow, for instance, due to reduced capacities. However, a complete territory-wide failure of the critical telecommunications infrastructure is unlikely. Further differences can be identified within this group, such as the sum of SCC and LCC connections. As point of reference, Figure 5 depicts the scenarios for the G20 member states. The USA is leading in terms of the availability of redundancy after the application of S3. Saudi Arabia holds the lead in S1, Japan in S2, while the USA remains among the top 3 of the G20 in both latter scenarios. Regarding the USA, excellent availability of redundancy can therefore be determined. The USA is leading the ranking of incident edges in the model with $\Delta(G) = 58$. Thus, the USA is considered a representative case for the group of states with high SCC redundancies.

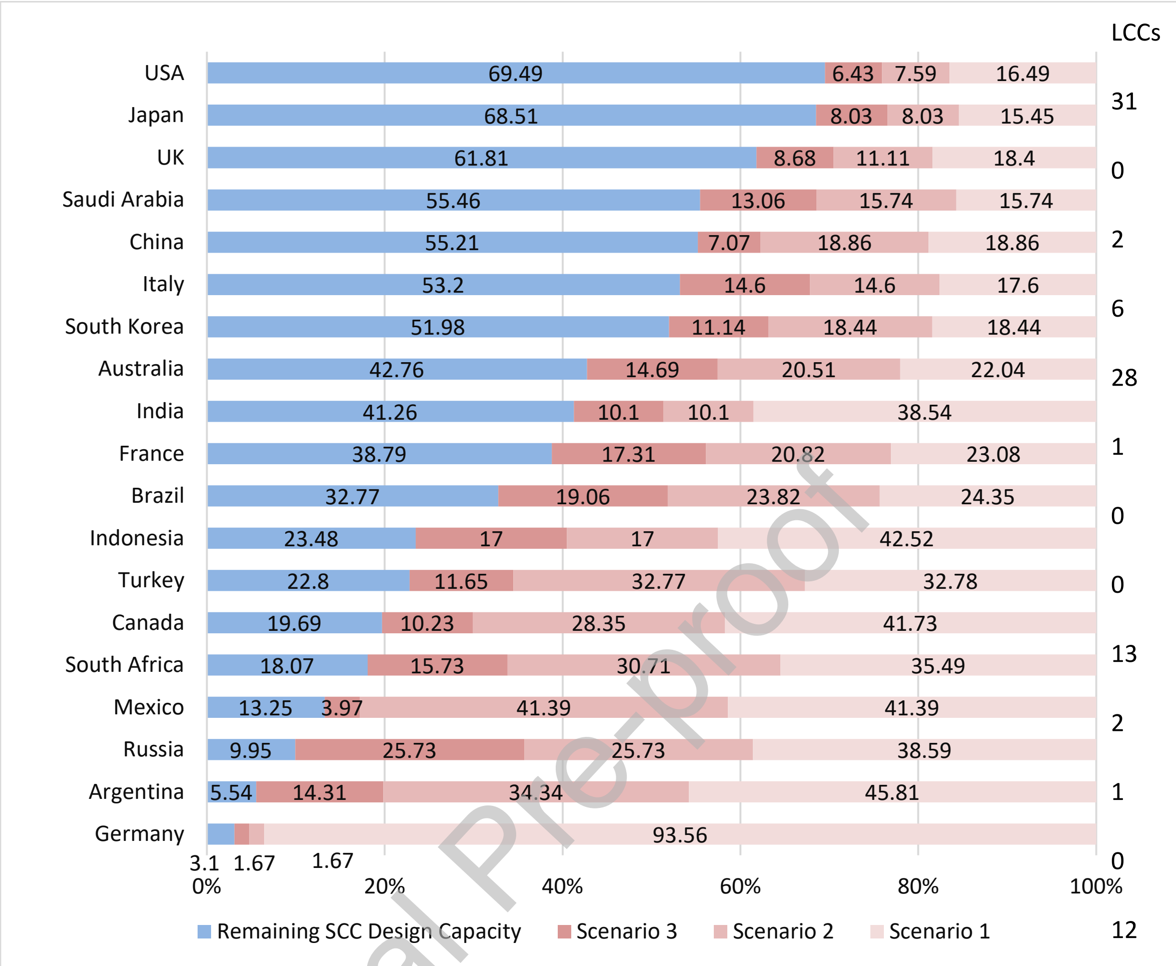


Figure 5: Scenarios of SCC failures for the G20 members in relation to their overall SCC connectivity. The European Union was omitted due to its status as an association of states. The number of LCC connections providing additional redundancies is specified in the right column. (own figure)

The potential international SCC bandwidth for the USA is estimated at 606.4 TB/s. The application of scenario 1, the connection loss of *MAREA*, results in a reduction of the potential SCC bandwidth by 100 TB/s. In relative terms, the failure of the widest cables would therefore amount to a 16.5% reduction of the overall potential SCC bandwidth. In scenario 2, in which the cable *BRUSA* additionally fails, the USA is missing 146.5 TB/s, respectively 24.1% of the potential SCC bandwidth. The loss of the three strongest cables in scenario 3 translates into a potential loss of 185 TB/s. Thus, even in the worst-case scenario simulated in this study, the USA would still have a potential remaining bandwidth of 421 TB/s. A comparison with the actual bandwidth needs of the USA (2017: 36 TB/s, estimated 2020: 42 TB/s) reveals conclusively that the USA's access to the global network will be maintained even under severe failures. In addition to its maritime connections, the USA is also equipped with LCC-Connections to Canada (n=22) and Mexico (n=9) and a vast access to the internet provided by satellites [67,68]. Figure 6 visually sums up the group classifications on a world map while including the different types of omitted units as well.

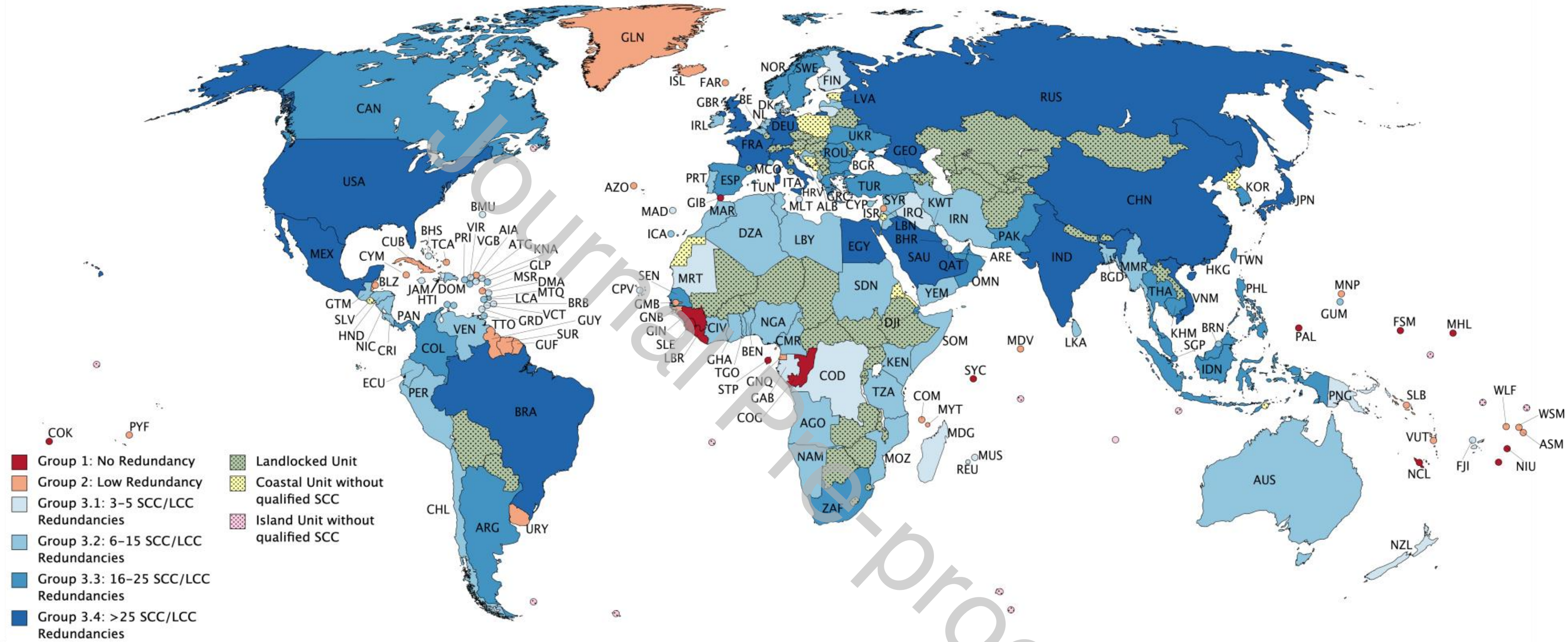


Figure 6: World map depicting classification of units into groups of high (blue) to low (red) redundancy through SCCs and LCCs. Landlocked units (green), units of coastal and island location without qualified SCC connection (yellow, pink) were omitted from the model. (own figure, created with mapchart)

Socio-Economic Development and Redundancy Levels

To test for the digital divide phenomenon, we combined our classifications of the analyzed territories with their respective socio-economic development status in Table 3 below. In the case of statistical independence between the socio-economic development status and the level of redundancy, the actual shares of redundancy groups within the UN M49 Standard subsamples would be close to the expected proportions derived from all territories in the second column of Table 3. However, we found large variation in group proportions within the socio-economic subsamples:

Of 39 units that we identified as developed countries, we assigned 34 (84.61%) to the highest redundancy group 3, four units (10.26%) to the medium redundancy group 2 and only one (2.56%) unit (Gibraltar) to the low redundancy group 1. Due to its geographical location and size, Gibraltar is an exceptional case. It has redundancy from the Spanish mobile network, at least in certain areas close to the border. Foreign mobile networks were not categorized as sufficient redundancy in the analysis, which consequently leaves the individual case of Gibraltar in group 1. Based on the data, we concluded that the geographic distribution of SCC connections in the Global North is reasonably good. This results in a very low probability of internet failure due to SCC outages in the aggregate, even in locations with multiple simultaneous outages (S3), by rerouting traffic through the available alternative routes.

Meanwhile, parts of the Global South are more at risk of experiencing a loss of broadband connectivity due to SCC losses. Accordingly, among the 106 developing countries that were not categorized as least developed countries (LDCs), 77 units (72.64%) were placed in group 3, 19 units (17.92%) were assigned to group 2, and ten units (9.43%) were listed in group 1. Among the total 24 LDC units, we allocated four units to group 1 (16.17%), which is a comparatively high proportion. In addition, five units (20.83%) are assigned to group 2 and 15 (62.50%) to group 3. Based on this matrix, the χ^2 value is 6.1015 with 4 degrees of freedom. As this study analyzes the statistical population of all coastal and island states and territories fitting into the pre-defined limits and no random sample has been taken in the process of analysis, no p-value is determined. With a value of Cramér's V = 0.27, it can thus be assumed that there is a moderately strong correlation between redundancy level and socio-economic development. Thus, the hypothesis of the Global Digital Divide can be confirmed for the availability of redundancies in developing countries and especially for LDCs.

			Socio-Economic Development Status (UN M49 Standard)					
Redundancy Level	***All Territories***		***Developed Countries***		***Developing Countries***		***Least Developed Countries***	
No Redundancy	15	8.88%	1	2.56%	10	9.43%	4	16.17%
Low Redundancy	28	16.57%	4	10.26%	19	17.92%	5	20.83%
High Redundancy	126	74.56%	34	87.18%	77	72.64%	15	62.50%

Sum	**169**	**100%**	**39**	**100%**	**106**	**100%**	**24**	**100%**

Table 3: Group classification in absolute and relative values and assigned to their socio-economic development status.

Summary of the Findings

In subsection 4.1., we revealed an imbalance with regard to the overall network structure. There is a wide variation in the different centrality measures. Yet, it is mainly the same – often developed – units topping the rankings in the positive sense in the indicators of node importance. Vice versa, some countries appear at the lower end of various centrality rankings in different centrality measures. This result is partly due to certain overlaps in the calculation of the centrality measures, yet the tendency of an unbalanced network can nevertheless be concluded from it. While this is not an original new finding, it represents a central role as confirmation of the propositions of older studies [26,27] that the imbalance in the internet backbone still applies in the global context for the chosen time of analysis in mid-2020.

Keeping this fundamental observation in mind, subsection 4.2. aimed to precisely identify those units that, due to their position in the internet backbone, suffer total bandwidth losses (group 1, n = 15) or a significantly increased risk thereof (group 2, n = 28) due to an SCC failure. For group 2, it can also be noted that limitations in data traffic speed may also occur, especially in the territories with an unbalanced level of redundancy. On a positive note, the large majority of the units examined (n = 126) were assigned to group 3, thus assuming a sufficient level of redundancy for them.

Based on the group classifications we developed, we then determined the correlation of socio-economic development status with the level of redundancy in subsection 4.3. Among LDCs, there is a clear overbalance in terms of the group 1 status redundancy. At the same time, developed countries are more likely to be members of group 3 than the expected frequencies would predict. The hypothesis of the Global Digital Divide can thus be validated for LDCs and developed countries. Regarding the non-LDC Developing Countries, which make up the center group of the development status variable in the present study, we assigned some units to the lower redundancy levels. However, their occurrences are close to the expected frequencies or proportions of those within their development status group; see the fourth column of Table 3. These differences within the respective groups could best be explained by the inclusion of further variables but cannot be explained by our model.

Discussion

Both central variables chosen for analysis, grouping into three redundancy levels and United Nations Statistics Division (UNSD) socio-economic development status, can be discussed. First, classification based on fault scenarios provides the opportunity to make clear divisions into internally homogeneous and comparable groups. A metric measure would have hindered a concise intra-group representation of the relevant vulnerable units. Second, while widely used for academic studies with a global focus, the UNSD socio-economic development status has not been immune to criticism. The rather crude subdivision into developed, developing, and least developed regions creates very broad categories that are highly heterogeneous within. We chose this indicator anyway because it makes an objective classification of overseas territories possible. This puts it ahead of other indicators of socio-economic development such as the Human Development Index. The fact that the UN uses the ternary variable in reporting of the Sustainable Development Goals underscores its lasting relevance.

Due to the global focus, we decided to work with two ordinal variables in this study. Therefore, an analysis of the SCC backbone structure with applications of variables on ratio scale is advised for analyses of smaller scope, such as regional approaches or case studies.

The findings of this study must be seen in light of some limitations: First, states and territories are treated as a black box in this study, which masks local differences and discrepancies in failure resilience, for example, between rural and urban contexts, prosperous and poor communities, or household and corporate customers. This is rooted in the global focus of the study. An overly detailed level of analysis would have been at the expense of the clarity of the results. Second, we did not include landlocked states in the study. This can be explained by the lack of data on the design capacity bandwidth of LCCs. Moreover, by definition, landlocked states can only access the submarine fiber optic internet backbone passively via the transit of an adjacent coastal state. Consequently, landlocked states depend less on the functioning of an SCC than on the function of their LCCs and the willingness of their neighbors to forward internet traffic. However, a specific study on the status of landlocked states would be conceivable, and the study of Liu et al. [69] already offers a good starting point for further exploration.

Third, the actual usage of a cable (lit capacity) is rarely made public, creating a data gap. This study takes the perspective of supply security, therefore rendering this point irrelevant. Nevertheless, the analysis of the maximum (design) capacities is not suitable for telecommunication market analyses, as they do not provide any information on the share of cable utilization through leasing by telecommunications providers. This point is not so much a limitation of the analysis itself but rather a reminder to interpret the data with appropriate caution. Fourth, the model disregards the varying risk of cable failure by applying the same scenarios to each country. Palmer and Booi discovered significant differences in the likelihood of cable failure depending on its geographic location [32]. Correspondingly, high traffic volumes from fishing and cargo shipping, shallow waters, and tectonic activity in a maritime area raise the risk of SCC failure accordingly. Figure 3 should therefore be interpreted with caution since it has not been determined how dangerous the geographic contexts of the respective cable sections are. Future studies may combine our results with failure probabilities to provide an even more realistic estimation of a state's vulnerability towards SCC failure.

Recalling the vulnerability definition of the UNDRR, it has to be kept in mind that the vulnerability of a reference object to a threat is not determined solely by the presence or absence of one aspect like redundancy. Instead, states can influence their individual vulnerability in the internet backbone cable system by preventive action like declaring cable protection zones. While these solely protect against accidental cable damage by establishing fishing boundaries and anchoring prohibitions, they do not protect against natural hazards. Avoiding geologically active zones on the seabed along the cable route is required to prevent destruction by natural hazards, particularly those triggered by tectonic activity. Regulative bodies may advocate this in negotiations with SCC installing and operating companies. Additionally, developing comprehensive reaction plans based on failure scenarios, the close-by stationing of repair resources (material, technicians, and vessels), as well as satellite internet receiving devices, would further lead to enhanced resilience against SCC failures. This study's results can thus help assess the redundancy level and, if necessary, justify the need for preventive measures.

Another aspect that needs to be investigated to better limit vulnerability is the consequence side of internet blackouts after SCC incidents and what measures have proven helpful in the event of damage. An index that globally compares the criticality of internet connectivity on the social, economic, or administrative levels does not yet exist. However, quantification of interactions between different critical infrastructures utilizing dependency risk graphs allows a better estimate of the consequences of a failure. By modeling potential cascading effects of critical infrastructures along dependency risk chains, cost-efficient mitigation strategies can be pursued [70]. With ongoing digitalization efforts in critical infrastructure sectors such as food, health and water, a growing complexity of these risk chains is likely [71–73].

Moreover, van Eeten et al. have found that energy and telecommunications infrastructures represent the overwhelming majority of initiators of cascading effects between critical infrastructures [74]. However, empirical risk approaches like dependency risk graphs require data from previous outages to determine probabilities and negative consequences. With the cases of the Northern Marianas [14] and, more recently, Tonga in 2019 [19,75] and 2022 [76,77], there are only a few incidents of internet downtime after single SCC failures for whole territories, making it hard to develop best practices. In the exemplary case of the Northern Marianas, few emergency connections could be established via satellite phones [78]. Territories characterized by even higher shares of internet-dependent economic sectors such as finance and digital services or extensively digitized public administration are exposed to higher costs in the event of an internet blackout. Regarding these sectors, specific requirements could be introduced that oblige, e.g., banks, larger online businesses, or authorities to enhance redundancy through satellite internet capacities to maintain essential services. In this light, the increasing diversification of the backbone through the ongoing installation of further SCCs and broadband satellite internet technologies can be considered a positive development for the global internet backbone resilience.

Conclusion

This paper has analyzed the vulnerability of states and overseas territories by modeling the international submarine fiber optic communication network. For the vast majority (n = 126) of the territories examined, there is only a low probability of an internet outage after SCC failure. Nevertheless, academia and governments should not dismiss this situation altogether, especially if an intentional and concerted (military or terrorist) attack on the SCC network is kept in mind. As a result, however, 43 units were identified with an increased risk of cable failure, 15 of which did not even have one sufficient SCC as redundancy. In addition, we found a positive correlation between a lower redundancy level and a low socio-economic development status (developing country or least developed country). Therefore, states and territories in the Global South are more likely to be highly vulnerable to SCC faults. At the same time, they often do not offer economic incentives to implement additional SCCs.

The present study is the first to provide redundancy analysis for the SCC backbone network that has approached a worldwide perspective since 2009 [31], thus allowing a global investigation of 169 territorial units as of mid-2020. On the one hand, we followed the approach of Omer et al. in its global scope. On the other hand, we conducted our analysis with territorial entities as units, since it is at the national level that governments can take decisions for redundancy promoting measures most effectively. Thus, we followed the majority of the literature on particular continents and world regions in their national comparisons without excluding overseas territories by considering their typical insular situation.

As internet coverage continues to be built for the current 3.8 billion people not using the internet yet, there will continue to be vulnerabilities due to a lack of redundancies in developing and least developed countries. The most vulnerable territories must be identified to minimize the likelihood of such critical telecommunication infrastructure failures on the national level. For this purpose, this paper offers an initial approach based on redundancy analysis. In future research, we will pursue the inclusion of measures to assess the dependency on internet connectivity of the society and economy of a territory. Also, investigating the future impact of emerging internet-providing technologies like low-earth-orbit satellite internet and their adoption in contexts that we rated as vulnerable in this study might prove important. The satellite mega-constellations could reach the threshold for providing sufficient broadband connectivity in some time without requiring the construction of fiber optic cables. From the perspective of developing countries without any backbone connection or with low redundancy levels, a crucial question will also be whether the pricing of these services will lead to a further intensification of the Global Digital Divide.

Acknowledgments

(anonymized)

References

[1] International Telecommunication Union, Measuring digital development Facts and figures 2020, ITU Publ. (2020). https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2020.pdf.

[2] C.M. Newbill, Defining Critical Infrastructure for a Global Application, Ind. J. Glob. Leg. Stud. 26 (2019) 761–779. https://www.repository.law.indiana.edu/ijgls/vol26/iss2/11.

[3] M. Hollick, S. Katzenbeisser, Resilient Critical Infrastructures, in: C. Reuter (Ed.), Inf. Technol. Peace Secur., Springer Fachmedien Wiesbaden, Wiesbaden, 2019: pp. 305–318. https://doi.org/10.1007/978-3-658-25652-4_14.

[4] United Nations Office for Disaster Risk Reduction (UNDRR), Report of the open-ended intergovernmental expert working group on indicators and terminology relating to disaster risk reduction, Geneva, 2017. https://undocs.org/en/A/71/644.

[5] L. DeNardis, Hidden Levers of Internet Control, Information, Commun. Soc. 15 (2012) 720–738. https://doi.org/10.1080/1369118X.2012.659199.

[6] NATO Cooperative Cyber Defence Centre of Excellence, Strategic importance of, and dependence on, undersea cables, Tallinn, 2019. https://ccdcoe.org/uploads/2019/11/Undersea-cables-Final-NOV-2019.pdf.

[7] D. Winseck, The Geopolitical Economy of the Global Internet Infrastructure, J. Inf. Policy. 7 (2017) 228–267. https://doi.org/10.5325/jinfopoli.7.2017.0228.

[8] Z.S. Bischof, R. Fontugne, F.E. Bustamante, Untangling the World-Wide Mesh of Undersea Cables, in: Proc. 17th ACM Work. Hot Top. Networks, Association for Computing Machinery, New York, NY, USA, 2018: pp. 78–84. https://doi.org/10.1145/3286062.3286074.

[9] Submarine Telecoms Forum, Submarine Telecoms Industry Report 2020/2021 Edition, Submar. Telecoms Forum. (2020). https://subtelforum.com/products/submarine-telecoms-industry-report/ (accessed January 19, 2022).

[10] L. Carter, D. Burnett, S. Drew, G. Marle, L. Hagadorn, D. Bartlett-McNeil, N. Irvine, Submarine Cables and the Oceans – Connecting the World, Cambridge, Lymington, 2009. https://www.iscpc.org/documents/?id=132.

[11] A. Mauldin, Cable Breakage: When and How Cables Go Down, TeleGeography Blog. (2017). https://blog.telegeography.com/what-happens-when-submarine-cables-break (accessed January 19, 2022).

[12] A. Xie, X. Wang, S. Lu, Risk Minimization Routing Against Geographically Correlated Failures, IEEE Access. 7 (2019) 62920–62929. https://doi.org/10.1109/ACCESS.2019.2916834.

[13] S. Chen, S. Sun, S. Kang, System integration of terrestrial mobile communication and satellite communication – The trends, challenges and key technologies in B5G and 6G, China Commun. 17 (2020) 156–171. https://doi.org/10.23919/JCC.2020.12.011.

[14] Economic and Social Commission for Asia and the Pacific (ESCAP), Broadband Connectivity in Pacific Island Countries, Bangkok, 2018. https://repository.unescap.org/bitstream/handle/20.500.12870/1315/ESCAP-2018-WP-Broadband-Connectivity-Pacific.pdf?sequence=1&isAllowed=y.

[15] E. Sutherland, Telecommunications in small island developing states, in: 37th Res. Conf. Commun. Inf. Internet Policy, Arlington, VA, 2009. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1999852.

[16] International Telecommunication Union, Small Island Developing States (SIDS) and ICTs, International Telecommunications Union, Geneva, 2019. https://doi.org/11.1002/pub/813cee7c-en.

[17] G. Aceto, A. Botta, P. Marchetta, V. Persico, A. Pescapé, A Comprehensive Survey on Internet Outages, J. Netw. Comput. Appl. 113 (2018) 36–63. https://doi.org/10.1016/j.jnca.2018.03.026.

[18] Y. Kitamura, Y. Lee, R. Sakiyama, K. Okamura, Experience with Restoration of Asia Pacific Network Failures from Taiwan Earthquake, IEICE Trans. Commun. E90-B (2007) 3095–3103. https://doi.org/10.1093/ietcom/e90-b.11.3095.

[19] C. Bueger, T. Liebetrau, Protecting hidden infrastructure: The security politics of the global submarine data cable network, Contemp. Secur. Policy. (2021) 1–23. https://doi.org/10.1080/13523260.2021.1907129.

[20] W. Chen, B. Wellman, The Global Digital Divide – Within and Between Countries, IT Soc. 1 (2004) 39–45. http://www.ifs.tuwien.ac.at/~dieter/teaching/GmA/Chen2004.pdf.

[21] J.A.G.M. van Dijk, Afterword: the state of digital divide theory, in: M. Ragnedda, G. Muschert (Eds.), Theor. Digit. Divid., Routledge, United Kingdom, 2018: pp. 199–206.

[22] TeleGeography, The State of the Network, Washington, D.C., 2021. https://www2.telegeography.com/hubfs/assets/Ebooks/state-of-the-network-2021.pdf.

[23] A. Feldmann, O. Gasser, F. Lichtblau, E. Pujol, I. Poese, C. Dietzel, D. Wagner, M. Wichtlhuber, J. Tapiador, N. Vallina-Rodriguez, O. Hohlfeld, G. Smaragdakis, The Lockdown Effect, in: Proc. ACM Internet Meas. Conf., ACM, New York, NY, USA, 2020: pp. 1–18. https://doi.org/10.1145/3419394.3423658.

[24] S. O'Malley, Assessing Threats to South Korea's Undersea Communications Cable Infrastructure, Korean J. Int. Stud. 17 (2019) 385–414. https://doi.org/10.14731/kjis.2019.12.17.3.385.

[25] M. Muneez, T. Vinesh, L. Nai-Shyan, Protection of submarine optical fibre cables on the coral reefs of the Maldives, Underw. Technol. 34 (2017) 149–156. https://doi.org/10.3723/ut.34.149.

[26] J. Cariolle, Telecommunication Submarine Cable Deployment and the Digital Divide in Sub-Saharan Africa (Revised Version), Clermont-Ferrand, 2019. https://doi.org/10.2139/ssrn.3202941.

[27] D. Thorat, Colonial Topographies of Internet Infrastructure: The Sedimented and Linked Networks of the Telegraph and Submarine Fiber Optic Internet, South Asian Rev. 40 (2019) 252–267. https://doi.org/10.1080/02759527.2019.1599563.

[28] C. Gerlach, R. Seitz, Economic Impact of Submarine Cable Disruptions, Singapore, 2013. http://publications.apec.org/-/media/APEC/Publications/2013/2/Economic-Impact-of-Submarine-Cable-Disruptions/2013_psu_-Submarine-Cables.pdf.

[29] A. Hummelholm, Undersea optical cable network and cyber threats, in: T. Cruz, P. Simoes (Eds.), Proc. 18th Eur. Conf. Cyber Warf. Secur. Proc. Eur. Conf. Inf. Warf. Secur., 2019.

[30] International Telecommunication Union, Maximising availability of international connectivity in the Pacific, Geneva, 2018. https://www.itu.int/pub/D-PREF-BB.GDI_AP-2018.

[31] M. Omer, R. Nilchiani, A. Mostashari, Measuring the Resilience of the Trans-Oceanic Telecommunication Cable System, IEEE Syst. J. 3 (2009) 295–303. https://doi.org/10.1109/JSYST.2009.2022570.

[32] A. Palmer-Felgate, P. Booi, How resilient is the global submarine cable network?, in: SubOptic, SubOptic, London, 2016: pp. 1–7.

[33] A. Palmer-Felgate, N. Irvine, S. Ratcliffe, S.S. Bah, Marine maintenance in the zones: A global comparison of repair commencement times, in: Suboptic Conf. From Ocean to Cloud, 2013: pp. 1–6. https://www.suboptic.org/wp-content/uploads/2014/10/MS02_Poster_78.pdf.

[34] L. Faramondi, G. Oliva, R. Setola, Multi-criteria node criticality assessment framework for critical infrastructure networks, Int. J. Crit. Infrastruct. Prot. 28 (2020) 100338. https://doi.org/https://doi.org/10.1016/j.ijcip.2020.100338.

[35] S. Oldham, B. Fulcher, L. Parkes, A. Arnatkevičiūtė, C. Suo, A. Fornito, Consistency and

differences between centrality measures across distinct classes of networks, PLoS One. 14 (2019) e0220061. https://doi.org/10.1371/journal.pone.0220061.

[36] G. Stergiopoulos, P. Kotzanikolaou, M. Theocharidou, D. Gritzalis, Risk mitigation strategies for critical infrastructures based on graph centrality analysis, Int. J. Crit. Infrastruct. Prot. 10 (2015) 34–44. https://doi.org/https://doi.org/10.1016/j.ijcip.2015.05.003.

[37] M. Oehlers, B. Fabian, Graph Metrics for Network Robustness – A Survey, Mathematics. 9 (2021) 895. https://doi.org/10.3390/math9080895.

[38] A. Barrat, M. Barthelemy, R. Pastor-Satorras, A. Vespignani, The architecture of complex weighted networks, Proc. Natl. Acad. Sci. 101 (2004) 3747–3752. https://doi.org/10.1073/pnas.0400087101.

[39] Y. Hao, L. Jia, Y. Wang, Z. He, Modelling cascading failures in networks with the harmonic closeness, PLoS One. 16 (2021) e0243801. https://doi.org/10.1371/journal.pone.0243801.

[40] Y. Hao, Y. Wang, L. Jia, Z. He, Cascading failures in networks with the harmonic closeness under edge attack strategies, Chaos, Solitons & Fractals. 135 (2020) 109772. https://doi.org/10.1016/j.chaos.2020.109772.

[41] Q. Nguyen, H.D. Pham, D. Cassi, M. Bellingeri, Conditional attack strategy for real-world complex networks, Phys. A Stat. Mech. Its Appl. 530 (2019) 121561. https://doi.org/10.1016/j.physa.2019.121561.

[42] V. Latora, M. Marchiori, Efficient behavior of small-world networks, Phys. Rev. Lett. 87 (2001) 198701. https://doi.org/10.17877/DE290R-11359.

[43] V. Latora, M. Marchiori, Economic small-world behavior in weighted networks, Eur. Phys. J. B - Condens. Matter Complex Syst. 32 (2003) 249–263. https://doi.org/10.1140/epjb/e2003-00095-5.

[44] A. Nagurney, Q. Qiang, A network efficiency measure with application to critical infrastructure networks, J. Glob. Optim. 40 (2008) 261–275. https://doi.org/10.1007/s10898-007-9198-1.

[45] C. Reuter, ed., Information Technology for Peace and Security, Springer Fachmedien Wiesbaden, Wiesbaden, 2019. https://doi.org/10.1007/978-3-658-25652-4.

[46] E. Calle, S.G. Cosgaya, D. Martínez, M. Pióro, Solving The Backup Controller Placement Problem In SDN Under Simultaneous Targeted Attacks, in: 2019 11th Int. Work. Resilient Networks Des. Model., 2019: pp. 1–7. https://doi.org/10.1109/RNDM48015.2019.8949096.

[47] D.F. Rueda, E. Calle, J.L. Marzo, Robustness comparison of 15 real telecommunication networks: Structural and centrality measurements, J. Netw. Syst. Manag. 25 (2017) 269–289.

[48] T. Freyburg, L. Garbe, Blocking the bottleneck: Internet shutdowns and ownership at election times in sub-Saharan Africa, Int. J. Commun. 12 (2018) 3896–3916.

[49] T. Reinhold, C. Reuter, Towards a Cyber Weapons Assessment Model -Assessment of the Technical Features of Malicious Software, IEEE Trans. Technol. Soc. (2021) 1–1. https://doi.org/10.1109/TTS.2021.3131817.

[50] Submarine Telecoms Forum, Submarine Cable Almanac, 34th, May 20 ed., Sterling, VA, 2020. https://subtelforum.com/products/submarine-cable-almanac/.

[51] TeleGeography, Submarine Cable Map, (2020). https://www.submarinecablemap.com/#/ (accessed January 19, 2022).

[52] Infrapedia, Infrastructure Map, (2020). https://www.infrapedia.com/app (accessed January 19, 2022).

[53] Network Startup Resource Center (NSRC), African Undersea and Terrestrial Fibre Optic Cables, (2020). https://afterfibre.nsrc.org/ (accessed January 19, 2022).

[54] G. Mahlknecht, Greg's Cable Map, (2016). https://cablemap.info/_default.aspx (accessed January 19, 2022).

[55] International Telecommunication Union, Interactive Transmission Map, (2020). https://www.itu.int/itu-d/tnd-map-public/ (accessed January 19, 2022).

[56] ITU Statistics, World Telecommunication/ICT Indicators Database online 23rd Ed., World Telecommun. Indic. Database Online. (2019). https://www.itu.int/pub/D-IND-WTID.OL-2019.

[57] R. Hadaway, E.R. Hartling, P. Mehta, M. Hubbard, D. Evans, L. Berg, M. Hinds, Submarine cable upgrades, in: Undersea Fiber Commun. Syst., Elsevier, 2016: pp. 577–603. https://doi.org/10.1016/B978-0-12-804269-4.00016-7.

[58] W. Qiu, Southern Cross NEXT Cable System Overview, Submar. Cable Networks. (2020). https://www.submarinenetworks.com/en/systems/trans-pacific/southern-cross-next/southern-cross-next-cable-system-overview (accessed January 19, 2022).

[59] A. South, rworldmap : a new R package for mapping global data, R J. 3 (2011) 35. https://doi.org/10.32614/RJ-2011-006.

[60] United Nations Statistics Division, Methodology: Standard country or area codes for statistical use (M49), (2018). https://unstats.un.org/unsd/methodology/m49/ (accessed January 19, 2022).

[61] I. McCulloh, A. Perrone, R Packages for Social Network Analysis, in: R. Alhajj, J. Rokne (Eds.), Encycl. Soc. Netw. Anal. Min., Springer New York, New York, NY, 2017: pp. 1–18. https://doi.org/10.1007/978-1-4614-7163-9_110209-1.

[62] C.T. Butts, sna: Tools for Social Network Analysis, (2019). https://cran.r-project.org/package=sna.

[63] G. Csardi, T. Nepusz, The igraph software package for complex network research, InterJournal. Complex Sy (2006) 1695. http://igraph.org.

[64] M.-J. Lee, igraphinshiny: Use "shiny" to Demo "igraph," (2016). https://cran.r-project.org/package=igraphinshiny.

[65] J.L. Marzo, E. Calle, S.G. Cosgaya, D. Rueda, A. Mañosa, On Selecting the Relevant Metrics of Network Robustness, in: 2018 10th Int. Work. Resilient Networks Des. Model., 2018: pp. 1–7.

https://doi.org/10.1109/RNDM.2018.8489809.

[66] H. Fouquet, China's 7,500-Mile Undersea Cable to Europe Fuels Internet Feud, Bloom. Businessweek. (2021). https://www.bloomberg.com/news/articles/2021-03-05/china-s-peace-cable-in-europe-raises-tensions-with-the-u-s (accessed January 19, 2022).

[67] Central Intelligence Agency, The World Factbook, CIA. (2021). https://www.cia.gov/the-world-factbook/ (accessed January 19, 2022).

[68] Union of Concerned Scientists, UCS Satellite Database, (2021). https://www.ucsusa.org/resources/satellite-database (accessed January 19, 2022).

[69] S. Liu, Z.S. Bischof, I. Madan, P.K. Chan, F.E. Bustamante, Out of Sight, Not Out of Mind: A User-View on the Criticality of the Submarine Cable Network, in: Proc. ACM Internet Meas. Conf., Association for Computing Machinery, New York, NY, USA, 2020: pp. 194–200. https://doi.org/10.1145/3419394.3423633.

[70] G. Stergiopoulos, P. Kotzanikolaou, M. Theocharidou, D. Gritzalis, Risk mitigation strategies for critical infrastructures based on graph centrality analysis, Int. J. Crit. Infrastruct. Prot. 10 (2015) 34–44. https://doi.org/10.1016/j.ijcip.2015.05.003.

[71] F. Kuntke, S. Linsner, E. Steinbrink, J. Franken, C. Reuter, Resilience in Agriculture: Communication and Energy Infrastructure Dependencies of German Farmers, Int. J. Disaster Risk Sci. (2022).

[72] J.R. Thompson, D. Frezza, B. Necioglu, M.L. Cohen, K. Hoffman, K. Rosfjord, Interdependent Critical Infrastructure Model (ICIM): An agent-based model of power and water infrastructure, Int. J. Crit. Infrastruct. Prot. 24 (2019) 144–165. https://doi.org/10.1016/j.ijcip.2018.12.002.

[73] P.F. Katina, C. Ariel Pinto, J.M. Bradley, P.T. Hester, Interdependency-induced risk with applications to healthcare, Int. J. Crit. Infrastruct. Prot. 7 (2014) 12–26. https://doi.org/10.1016/j.ijcip.2014.01.005.

[74] M. Van Eeten, A. Nieuwenhuijs, E. Luiijf, M. Klaver, E. Cruz, The State and the Threat of Cascading Failure across Critical Infrastructures: The Implications of Empirical Evidence from Media Incident Reports, Public Adm. 89 (2011) 381–400. https://doi.org/10.1111/j.1467-9299.2011.01926.x.

[75] L. Dickey, E. Downs, A. Taffer, H. Holz, D. Thompson, S.B. Hyder, R. Loomis, A. Miller, Mapping the Information Environment in the Pacific Island Countries: Disruptors, Deficits, and Decisions, Center for Naval Analysis, Arlington, VA, 2019. https://www.cna.org/CNA_files/centers/cna/cip/disinformation/IRM-2019-U-019755-Final.pdf.

[76] C. Duckett, Volcanic eruption takes out Tonga cables, ZDNet. (2022). https://www.zdnet.com/article/volcanic-eruption-takes-out-tonga-cables/ (accessed January 19, 2022).

[77] B. Doherty, T. McClure, Tonga could be cut off for weeks amid efforts to repair undersea communications cable, Guard. (2022).

https://www.theguardian.com/world/2022/jan/18/tonga-could-be-cut-off-for-weeks-amid-efforts-to-repair-undersea-communications-cable (accessed January 19, 2022).

[78] J. Brodkin, Broken cable reportedly disconnected US island territory from Internet, Ars Tech. (2015). https://arstechnica.com/information-technology/2015/07/broken-cable-reportedly-disconnected-us-island-territory-from-internet/ (accessed January 19, 2022).

Annex I: List of Territories

Territory	ISO 3 Code	Adjacent SCCs	Cross-border LCCs	Redundancy group
Albania	ALB	3	4	3
Algeria	DZA	7	8	3
Angola	AGO	7	0	3
Antigua and Barbuda	ATG	4	0	3
Argentina	ARG	5	19	3
Australia	AUS	16	0	3
Bahamas	BHS	4	0	3
Bahrain	BHR	6	0	3
Bangladesh	BGD	4	4	3
Barbados	BRB	5	0	3
Belgium	BEL	6	9	3
Belize	BLZ	2	2	2
Benin	BEN	4	8	3
Brazil	BRA	17	16	3
Brunei	BRN	6	0	3
Bulgaria	BGR	4	19	3
Cambodia	KHM	4	12	3
Cameroon	CMR	9	2	3
Canada	CAN	5	18	3

Cape Verde	CPV	4	0	3
Chile	CHL	4	11	3
China	CHN	22	28	3
Colombia	COL	15	3	3
Comoros	COM	2	0	2
Costa Rica	CRI	4	9	3
Croatia	HRV	1	6	3
Cuba	CUB	2	0	2
Cyprus	CYP	11	0	3
Dem. Rep. Of the Congo	COD	4	0	3
Denmark	DNK	8	5	3
Faroe Islands (DNK)	FAR	3	0	2
Greenland (DNK)	GLN	2	0	2
Djibouti	DJI	17	4	3
Dominica	DMA	4	0	3
Dominican Republic	DOM	7	3	3
Ecuador	ECU	5	5	3
Egypt	EGY	28	2	3
Equatorial Guinea	GNQ	3	0	2
Fiji	FJI	5	0	3
Finland	FIN	3	3	3
France	FRA	19	26	3
French Guiana (FRA)	GUF	3	2	2
French Polynesia (FRA)	PYF	2	0	2
Guadeloupe (FRA)	GLP	7	0	3
Martinique (FRA)	MTQ	7	0	3
Mayotte (FRA)	MYT	3	0	2
New Caledonia (FRA)	NCL	1	0	1
Reunion (FRA)	REU	4	0	3

Wallis and Futuna (FRA)	WLF	2	0	2
Gabon	GAB	4	0	3
Gambia	GMB	2	2	2
Georgia	GEO	2	6	3
Germany	DEU	7	19	3
Ghana	GHA	10	4	3
Greece	GRC	8	9	3
Grenada	GRD	4	0	3
Guatemala	GTM	6	7	3
Guinea	GIN	1	0	1
Guinea-Bissau	GNB	2	1	2
Guyana	GUY	2	1	2
Haiti	HTI	2	3	3
Honduras	HND	2	8	3
Hong Kong	HKG	25	3	3
Iceland	ISL	3	0	2
India	IND	29	13	3
Indonesia	IDN	20	0	3
Iran	IRN	4	9	3
Iraq	IRQ	4	1	3
Ireland	IRL	9	2	3
Israel	ISR	4	0	3
Italy	ITA	28	12	3
Ivory Coast	CIV	8	2	3
Jamaica	JAM	5	0	3
Japan	JPN	31	0	3
Jordan	JOR	2	4	3
Kenya	KEN	7	4	3
Kuwait	KWT	5	1	3

Latvia	LVA	1	6	3
Lebanon	LBN	3	0	2
Liberia	LBR	1	0	1
Libya	LBY	3	6	3
Lithuania	LTU	1	4	3
Madagascar	MDG	4	0	3
Malaysia	MYS	24	1	3
Maldives	MDV	3	0	2
Malta	MLT	3	0	3
Marshall Islands	MHL	1	0	1
Mauritania	MRT	4	1	3
Mauritius	MUS	3	0	3
Mexico	MEX	9	19	3
Pohnpei State (FSM)	FMP	1	0	1
Yap (FSM)	FMY	1	0	1
Monaco	MCO	2	4	3
Morocco	MAR	7	3	3
Mozambique	MOZ	4	5	3
Myanmar	MMR	6	6	3
Namibia	NAM	4	7	3
Netherlands	NLD	8	5	3
Dutch Caribbean (NLD)	DCB	14	0	3
New Zealand	NZL	5	0	3
Cook Islands (NZL)	COK	1	0	1
Niue (NZL)	NIU	1	0	1
Nicaragua	NIC	2	6	3
Nigeria	NGA	9	2	3
Norway	NOR	1	15	3
Oman	OMN	16	1	3

Pakistan	PAK	11	8	3
Palau	PAL	1	0	1
Panama	PAN	12	4	3
Papua New Guinea	PNG	4	0	3
Peru	PER	6	9	3
Philippines	PHL	17	0	3
Portugal	PRT	14	0	3
Azores (PRT)	AZO	2	0	2
Madeira (PRT)	MAD	4	0	3
Puerto Rico	PRI	15	0	3
Qatar	QAT	9	1	3
Republic of the Congo	COG	1	0	1
Romania	ROU	1	19	3
Russia	RUS	6	25	3
Saint Kitts and Nevis	KNA	4	0	3
Saint Lucia	LCA	6	0	3
Saint Vincent and the Grenadines	VCT	4	0	3
Samoa	WSM	2	0	2
Sao Tome and Principe	STP	1	0	1
Saudi Arabia	SAU	26	6	3
Senegal	SEN	10	6	3
Seychelles	SYC	1	0	1
Sierra Leone	SLE	1	0	1
Singapore	SGP	25	0	3
Solomon Islands	SLB	2	0	2
Somalia	SOM	4	2	3
South Africa	ZAF	6	11	3
South Korea	KOR	18	0	3

Spain	ESP	16	4	3
Canary Islands (ESP)	ICA	8	0	3
Sri Lanka	LKA	8	0	3
Sudan	SDN	4	4	3
Suriname	SUR	2	2	2
Sweden	SWE	6	17	3
Syria	SYR	3	4	3
Taiwan	TWN	18	0	3
Tanzania	TZA	5	6	3
Thailand	THA	13	9	3
Togo	TGO	2	8	3
Tonga	TON	1	0	1
Trinidad and Tobago	TTO	7	0	3
Tunisia	TUN	5	9	3
Turkey	TUR	7	12	3
Ukraine	UKR	2	15	3
United Arab Emirates	ARE	23	2	3
United Kingdom	GBR	33	2	3
Anguilla (GBR)	AIA	2	0	2
Bermuda (GBR)	BMU	4	0	3
British Virgin Islands (GBR)	VGB	5	0	3
Cayman Islands (GBR)	CYM	2	0	2
Gibraltar (GBR)	GIB	1	0	1
Montserrat (GBR)	MSR	2	0	2
Turks and Caicos Islands (GBR)	TCA	2	0	2
United States of America	USA	58	31	3
American Samoa (USA)	ASM	3	0	2
Guam (USA)	GUM	13	0	3

Northern Mariana Islands (USA)	MNP	2	0	2
United States Virgin Islands (USA)	VIR	10	0	3
Uruguay	URY	2	2	2
Vanuatu	VUT	2	0	2
Venezuela	VEN	11	3	3
Vietnam	VNM	12	16	3
Yemen	YEM	6	0	3

Declaration of interests

☒ The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

☐The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: