Hindawi
Complexity
Volume 2021, Article ID 6662232, 14 pages
https://doi.org/10.1155/2021/6662232

Research Article

Vulnerability of Submarine Cable Network of Mainland China: Comparison of Vulnerability between before and after Construction of Trans-Arctic Cable System

Yongshun Xie[1,2] **and Chengjin Wang**[1,2]

[1]*Institute of Geographic Sciences and Natural Resources Research, CAS, Beijing 100101, China*
[2]*College of Resources and Environment, University of the Chinese Academy of Sciences, Beijing 100049, China*

Correspondence should be addressed to Chengjin Wang; cjwang@igsnrr.ac.cn

Received 3 November 2020; Revised 2 December 2020; Accepted 7 January 2021; Published 18 January 2021

Academic Editor: Qiuye Sun

The submarine optical-fiber cable (submarine cable) is a large connectivity infrastructure, which plays an important role in international communication, cyber-physical systems, and even national security. Although submarine cable network interruption may cause serious consequences, researching its vulnerability has not attracted much attention. This paper proposes a quantitative method to measure the vulnerability of the submarine cable network and evaluates the influence of the upcoming trans-Arctic cable (TAC) system on the submarine cable network of mainland China. To address this issue, first, the submarine cable network of mainland China is constructed. Further, methodology based on complex network and geospatial perspective is proposed to simulate the changes of network eigenvalues under different attacks and to quantitatively analyze the variation degree of network vulnerability. With the proposed method, the vulnerability of the submarine cable network of mainland China before and after construction of the trans-Arctic cable system is compared. The results reveal the key node countries and sea channels of the submarine cable network of mainland China and show the significance of the TAC system.

1. Introduction

As an important carrier and channel for information transmission between different regions, the submarine optical cable networks comprise large-scale connectivity infrastructures. However, the vulnerability of the submarine cable network is often ignored. Although plenty of research studies have paid attention to the topology structure and optimal deployment of the submarine cable network, there are few researches on its vulnerability. To fill this gap, this paper draws on the complex network theory and method to analyze the vulnerability of the submarine cable network of mainland China and compares the vulnerability between before and after construction of the trans-Arctic cable system.

The global submarine cable network, consisting of approximately 450 submarine cable systems, covering 1.2 million kilometers in length [1], and handling 99 percent of international data traffic, is the backbone of the physical infrastructure of the global Internet, as well as the most important information transmission medium in the world, currently and for the foreseeable future [2]. The coming decades may see the large-scale deployment of networked cyber-physical systems (CPSs), which puts forward new requirements for the stability and invulnerability of the submarine cable network. For the submarine cable network, it is not only the underlying physical system of CPSs but also the information flow it brings constitutes the cyber system of CPSs. Therefore, the vulnerability of submarine cable network is very important for CPSs and even national development in the era of Industry 4.0.

Vulnerability is an important concept, referring to the extent to which a system is affected when a disaster occurs; it is widely used in the study of ecology [3–5], disaster management [6, 7], and urban economics [8, 9]. Watts and Strogatz [10] and Barabasi and Albert [11] found the small

world characteristics and scale-free characteristics of the real world and opened a new era of complex network system research. Subsequently, in the early 2000s, Albert et al. [12], Broder et al. [13], and Bollobás and Riordan [14] explored the vulnerability of complex networks with different characteristics; this work laid the foundation for later scholars to explore the vulnerability of complex networks and became important in recognizing the key nodes and edges in complex networks.

In fact, many telecommunication networks have been found to have the characteristics of complex networks. For example, Schintler et al. [15] examined and compared the North American physical fiber network and the pan-European fiber optic network; Gorman and Malecki [16] analyzed the complexities of ten backbone provider networks in the USA; Wheeler and O'Kelly [17] and Grubesic et al. [18] explored the network topology of the commercial Internet in the USA. Such studies address the position of nodes (e.g., cities and hubs) as well as the diffusion pattern of flows in the network, with due emphasis on route length, nodal clustering, and power-law and exponential connectivity distributions.

In large-scale communication networks, such as the Internet, scale-free characteristics evolve through self-organizing processes, in which new nodes tend to attach to other vertices that are already well connected [19–22]. As a result, the connections in the network are mainly routed by several high-level nodes, and the network diameter is small, while network efficiency is high: Albert et al. [12] indicated that scale-free networks, such as these, are very tolerant to random failures at nodes—providing a reliable system for information distribution. However, Grubesic et al. [18] and Schintler et al. [15] pointed out that scale-free network, when super connected nodes are removed, faces the risk of disconnection or significant interruption, either unintentionally or from a targeted attack or external force.

However, so far, the reliability, survivability, and resiliency of a communication network system, within the context of complex network theory, are still ignored to a great extent, meaning the related literature is relatively scant, especially concerning the survivability of a submarine cable network. In the literature, a few scholars have focused on the topological design of submarine cable networks [23–25]. A disaster in the network is often considered as a randomly placed disk of a particular radius (the closer the layout of submarine cables in the disaster area, the more the cables will be affected). Computational geometric techniques are used to compare and evaluate the network resiliency for various topologies, such as rectangular with rounded corner, rhombus, and elliptic topologies, and to find the vulnerable points within a network. Some studies even involve the constraints of the total cable cost [26]. The above research focuses on the vulnerability or survivability of a submarine cable network; however, the essence is to explore the optimization of spatial layouts of a submarine cable network in the context of communication engineering. All the above research studies are not based on complexity science and lack the dynamic evaluation of network complexity. The work of Albert et al. [12] and that of other scholars on the tolerance of the Internet to random failures or targeted attacks need to be further reflected in a submarine cable network using complex network theory.

The first international submarine cable system, invested by China, was completed and came into use in December 1993. In the subsequent 25 years, the number of submarine cable systems worldwide has increased, the capacity of submarine cable systems has improved, the number of connected countries and regions has increased, and undersea communication capacity has reached new heights [27]. Nevertheless, similar to the characteristics of shipping routes, a few sea lanes or landing countries have become the necessary places for network connectivity, greatly restricting the connectivity of China's submarine cable network. However, with global warming, the melting Arctic has provided an attractive route for submarine cables [28]. In March 2017, at the 4th International Arctic Forum held in Arkhangelsk, Russia, many parties, including the Ministry of Industry and Information Technology of China and China Telecom Group, discussed the planning and construction of a submarine cable across the Arctic circle along the Northeast channel. Such a project can shorten the submarine cable connection distance of Asia and Europe by about 40% and reduce the communication delay by half. Against this background, the submarine cable network of China will usher in a new round of changes. How network vulnerability will change requires a scientific answer from the perspective of academic.

Thus, this paper draws on the complex network theory and method to analyze the vulnerability of the submarine cable network of mainland China and compares the vulnerability between before and after construction of the trans-Arctic cable system. The main features and contributions of this paper can be summarized as follows.

(1) This paper is the first attempt to construct the submarine cable network of Mainland China. It paper presents its structural characteristics and makes up for the deficiency of existing research on this new large-scale connectivity infrastructure network.

(2) This paper proposes a quantitative method to measure the vulnerability of submarine cable network. This method fully combines the perspective of topological network and geographical space, which can not only simulate the change trend of network eigenvalues under different attack modes but also identify the important nodes and corridors in the global map.

(3) This paper proves the strategic significance of the trans-Arctic cable system to the submarine cable network of mainland China. It shows that the vulnerability of the submarine cable network of mainland China will be improved after construction of the trans-Arctic cable system, especially in the context of intentional attack.

The remainder of this paper is organized as follows. In Section 2, the data sources and study area are presented; the submarine cable network of mainland China is constructed. In

Section 3, the methodology is proposed, including assessment indicators, simulation strategy, and quantitative analysis. In Section 4, results about the vulnerability analysis of submarine cable network nodes and edges are separately provided. The conclusion and discussion are finally drawn in Section 5.

2. Data Sources and Network Construction

2.1. Data Sources and Study Area. The data for this study mainly come from TeleGeography (https://www.telegeography.com/), which is a telecommunications market research and consulting firm. TeleGeography collected the data for all existing submarine communications cables. For this study, we analyze the submarine cable network of mainland China, which comprises part of the global submarine cable network and consists of all the submarine cable systems arriving in mainland China. Fourteen submarine cable systems were selected as the research object (Table 1). Among them, 13 submarine cable systems have been built—3 have been abandoned, and ten are currently in use. The TAC system is expected to be completed and put into use in 2023. It should be noted that although the AAE-1 system landed first in Ngwe Saung, Myanmar, it directly connects with China through the China-Myanmar international fiber-optic cable system (CMI project), and the service object is still mainland China (Figure 1). This system is also the first overseas submarine cable built by China Unicom with its own landing station; therefore, the AAE-1 system belongs to the research consortium of the submarine cable network of mainland China.

Submarine cable network of Mainland China connects 44 countries and regions. Before completion of the TAC system (later called the T_1 era), the submarine cable network of mainland China was connected to the Asia-Pacific, South Asia, the Middle East, North Africa, and Europe by the west route of China and connected to the United States by the east route of China. After completion of the TAC system (later called the T_2 era), the new route along the Arctic Northeast channel connects Europe directly to mainland China, forming a closed-loop structure. The main routes, countries, and regions involved are shown in Figure 1.

2.2. Construction of the Submarine Cable Network. In order to facilitate theoretical analysis, the submarine cable network is abstracted as nodes, edges, and weights. The node set ($V = \{v_i: i = 1, 2, \ldots, n\}$) is defined as the landing countries or regions (v_i); the edge set ($E = \{e_i: i = 1, 2, \ldots, m\}$) comprises the node pairs with optical cable lines directly between nodes (e_i); the weight of each edge ($W = \{w_{ij}: i = 1, 2, \ldots, n\}$) is determined by the capacity (potential capacity, rather than lit capacity, is used here because redundancy is necessary to avoid meltdown [29]) of the submarine cable system. The matrix expression is as follows:

$$A = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1j} \\ a_{21} & a_{22} & \ldots & a_{2j} \\ \vdots & \vdots & \vdots & \vdots \\ a_{i1} & a_{i2} & \ldots & a_{ij} \end{bmatrix}. \quad (1)$$

According to equation (1), the submarine cable network of mainland China is constructed and visualized, as shown in Figure 2. The connection level of the submarine cable network of mainland China is characterized by clustering and distance attenuation. Countries or regions in East Asia have the highest connection level, and Southeast Asian groups the second-highest level. Europe, Africa, the Middle East, and South Asia have a low level of connection, while the United States has a medium level. After construction of the TAC system, Russia and northern Europe will also reach a medium level.

From preliminary observation, the network has complex connections and presents the characteristics of small world. The average shortest path and clustering coefficient of submarine cable of mainland China and same-size random network are calculated, respectively (Table 2). The results show that the clustering coefficient of submarine cable of mainland China is much larger than that of same-size random network, which indicates that submarine cable of mainland China has the characteristics of small world. In addition, the average shortest path of submarine cable of mainland China is slightly higher than that of same-size random network. Due to the limitation of marine geography, the submarine cable cannot be connected at will. On this basis, it is necessary to make a further analysis of its network vulnerability.

3. Methodology

3.1. Assessment Indicators. Network vulnerability refers to the extent to which network connectivity is affected when network structure is impacted. The vulnerability of a submarine cable network refers to the extent to which network connectivity is affected when several landing stations or submarine optical cable lines cannot operate normally due to random damage caused by natural factors, such as earthquake, tsunami, anchor damage, and shark bite or intentional destruction caused by unnatural factors, such as fishing vessel stealing, terrorism, and irregular war operations. Therefore, submarine cable network vulnerability can be analyzed using the changes in eigenvalues after the network is attacked.

To understand the impact of failures and attacks on network structure, we choose four mainstream indicators to measure network vulnerability when nodes are removed: the average degree of networks D, the clustering coefficient of the entire network C, the proportion of isolated nodes ΔN, and the global efficiency E.

3.1.1. Average Degree of Networks D. The average degree of networks D is the average value of all node degrees (the number of edges connected with nodes) in the network. When the network is attacked, with the corresponding decrease in network nodes and edges, the network average degree will inevitably change. The greater the change is, the more sensitive and vulnerable the network is, which can be expressed as follows:

Table 1: Major international submarine cable systems landing in Mainland China.

No.	System	Code	Bandwidth capacity	Length (km)	Completed time	Remarks
1	China-Japan fiber-optic submarine cable system	C-J	560 mbps	1252	Dec, 1993	Abandoned in 2006
2	China-Korea fiber-optic submarine cable system	C-K	1120 mbps	549	Feb, 1996	Abandoned in 2005
3	FLAG Europe Asia	FLAG	10 Gbps	27000	Sep, 1997	In service
4	South-East Asia-Middle East-West Europe 3	SMW3	960 Gbps	39000	1999	In service
5	China-US cable network	CUCN	80 Gbps	30800	Jan, 2000	Abandoned in 2016
6	Asia Pacific cable network 2	APCN2	2.56 Tbps	19000	Dec, 2000	In service
7	East Asia crossing	EAC	2.56 Tbps	19850	Jan, 2002	In service
8	City-to-City cable system	C2C	7.68 Tbps	17000	Aug, 2002	In service
9	Trans-Pacific Express	TPE	5.12 Tbps	17700	Sep, 2008	In service
10	South-East Asia Japan cable system	SJC	15 Tbps	10700	Feb, 2013	In service
11	Asia Pacific gateway	APG	54 Tbps	10400	2016	In service
12	Asia-Africa-Europe-1 cable system	AAE-1	40 Tbps	25000	2017	In service
13	New crossing-Pacific cable system	NCP	60 Tbps	13618	2018	In service
14	Trans-Arctic cable system	TAC	60 Tbps	12700	by 2023	Planned

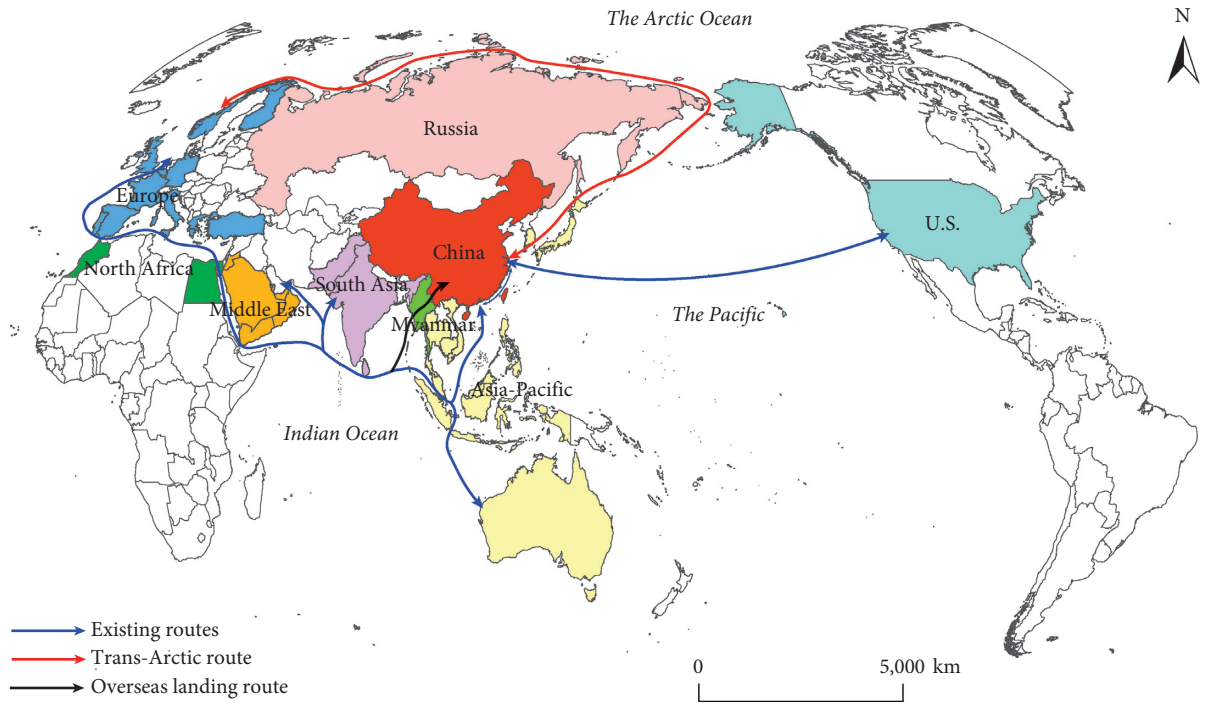

Figure 1: Main routes of the submarine cable network of mainland China.

$$D = \frac{1}{N}\sum_{i=1}^{N} D_i, \tag{2}$$

where N is the total number of nodes in the network, D_i is the degree value of node i, and D is the average degree of networks.

3.1.2. Clustering Coefficient of the Entire Network C. The clustering coefficient [30] reflects the connection between adjacent nodes in the network. The higher the clustering coefficient, the easier it is to form regional agglomeration between a point and its surrounding nodes; the lower the clustering coefficient, the more difficult it is to form regional agglomeration in the spatial distribution. In general, when the network is attacked, the clustering coefficient will decrease and network structure will become loose. This can be expressed as follows:

$$C_i = \frac{2M_i}{k_i(k_i - 1)}, i = 1, 2, 3, \ldots N, \tag{3}$$

where k_i is the number of nodes directly connected to node i, k_i $(k_i–1)/2$ is the maximum number of edges of node i connected pairwise, M_i is the number of edges between adjacent nodes of node i, and C_i represents the concentration level of the nodes.

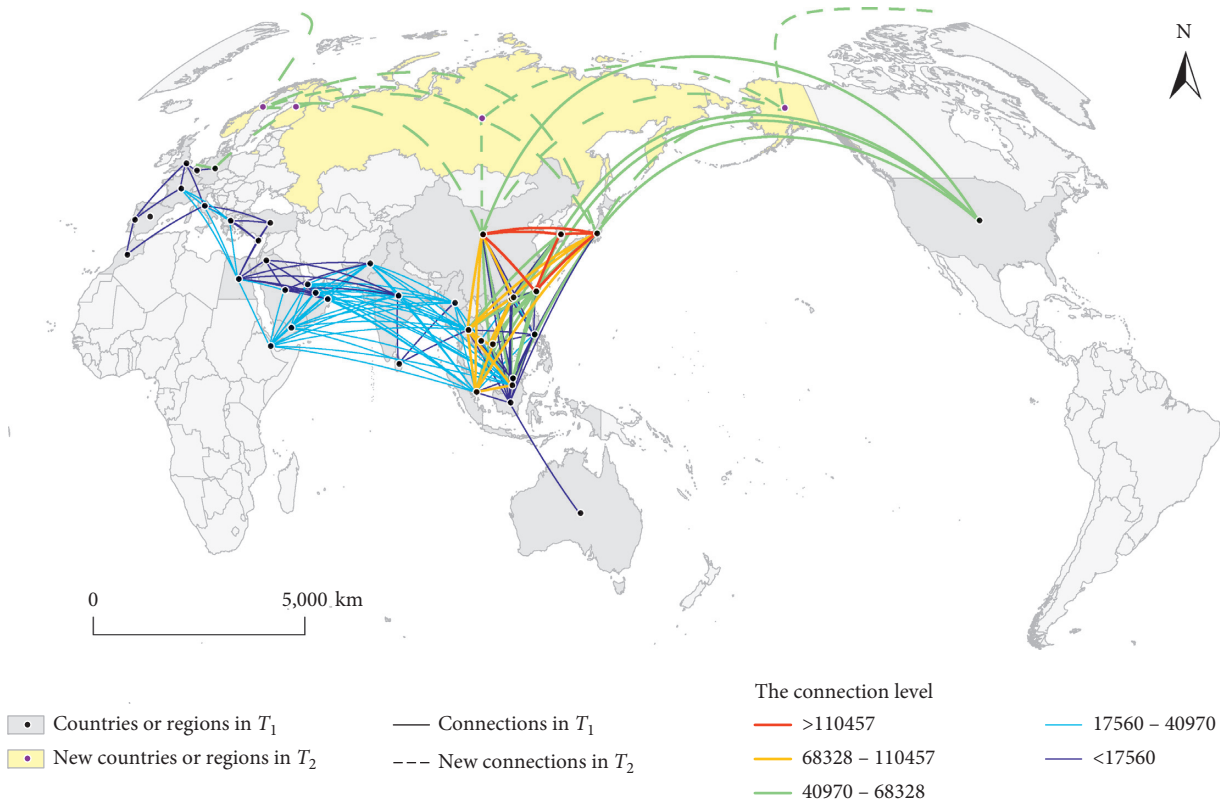

Figure 2: Connection of submarine cable network of mainland China.

Table 2: Comparison of submarine cable network of mainland China and same-size random network metrics.

	Number of nodes	Probability of linked edges	Average shortest path	Clustering coefficient
Submarine cable network of mainland China (T_1)	38	0.24	2.69	0.729
Random network (T_1)	38	0.24	1.844	0.237
Submarine cable network of mainland China (T_2)	42	0.21	2.649	0.727
Random network (T_2)	42	0.21	1.909	0.211

The clustering coefficient of the entire network C can then be obtained by calculating the average value of the clustering coefficient of each node:

$$C = \frac{1}{N}\sum_{i=1}^{N} C_i. \tag{4}$$

3.1.3. Proportion of Isolated Nodes ΔN. The proportion of isolated nodes in a network is the proportion of nodes without edges connected. When the network is attacked, the edges between some nodes become disconnected, creating some isolated nodes and affecting the scale and connectivity of the whole network. This can be expressed as follows:

$$\Delta N = \left(1 - \frac{N'}{N}\right) \times 100\%, \tag{5}$$

where N and N' represent the total number of nodes before and after attack, respectively, and ΔN represents the proportion of isolated nodes.

3.1.4. Global Efficiency E. The global efficiency E reflects the difficulty of information transmission between nodes in the network, defined by Latora and Marchiori [31]. The higher the network efficiency, the better the network connectivity. The efficiency between node i and node j in the network is the reciprocal of the shortest distance d_{ij} between the two nodes. When i and j are unconnected, $d_{ij} = +\infty$, so $1/d_{ij} = 0$. For the whole network, the mean value of efficiency between all nodes is the global efficiency, represented by E:

$$E = \frac{1}{N(N-1)}\sum_{i=1}^{N}\sum_{j=1}^{N}\frac{1}{d_{ij}}, \quad i \neq j. \tag{6}$$

3.2. Simulation Strategy

3.2.1. Node Attack. Our approach to analyze the network vulnerability involved conducting successive simulated attacks on the network to test its performance until it collapsed. The faults of submarine cable networks can be divided into an arc failure (the severing of an optical cable) and node failure (the failure of landing station equipment) [32]; the modes of failure can be divided into intentional attack and random attack.

Random attack: network nodes are attacked randomly with a certain probability; that is, the nodes in the network are randomly deleted according to the probability. Such a random selection is not related to the topological characteristics or any other attributes of a node. This attack method can simulate the impact of earthquake, tsunami, anchor damage, shark bite, and other random events, on the submarine cable network.

Intentional attack: network nodes with great influence sustain a targeted attack; that is, the nodes in the network are deleted according to node importance. This mode of attack can simulate the impact of intentional events, such as fishing vessel theft, terrorism, and military blockade, on the submarine cable network.

The routes in the submarine cable network of mainland China are concentrated in a minority of hub countries or regions. Due to differences in the capacity of optical fiber systems, the importance of network nodes with the same connection but different capacities is different; it is therefore necessary to weight the degree value of each node in the network, ranking the importance of nodes in the submarine cable network of mainland China. Among them, the top ten node countries or regions are shown in Table 3.

In order to reveal the vulnerability of the network more clearly, we gradually delete nodes to simulate random attack and intentional attack, respectively. We then evaluate the changes in the average degree of networks D, the clustering coefficient of the entire network C, the proportion of the isolated nodes ΔN, and the global efficiency E.

3.2.2. Edge Attack. Due to limitations in marine geography, the submarine cable lines must to be laid through channels or canals. Therefore, the security of these lanes has a direct impact on the vulnerability of the submarine cable network. The submarine cable of mainland China passes through eight main sea lanes (Figure 3; Table 4). As these sea lanes are accident-prone areas with a low security guarantee [32], they are important globally, strategically, and militarily. Therefore, it is important to analyze the impact of these sea lanes on the vulnerability of the submarine cable network.

The attack on each sea lane is simulated. When attacking, we break the edges and remove the isolated nodes, thus forming a new submarine cable network under attack. Based on this, each eigenvalue of the network is calculated and compared with the normal eigenvalue of the network so as to evaluate the vulnerability of the submarine cable network under edge attack.

3.3. Quantitative Analysis

3.3.1. Network Stress Testing. To quantitatively analyze the change degree of network vulnerability, the key is to determine the contribution degree of each network eigenvalue rate of change to network vulnerability—that is, the corresponding weight.

Therefore, we use the network stress test method, and the related concepts are as follows:

(i) *Network Half-Attenuation Degree G_s.* The network half-attenuation degree G_s represents the attack intensity when the rate of change in a given eigenvalue reaches 50% of its maximum value (that is, the network completely fails); s is the given eigenvalue. Generally, it is best to conduct stress testing at a ratio of 50%—that is, the median value of network integrity and complete failure. Therefore, we use the network half-attenuation degree G_s to determine the sensitivity coefficient.

(ii) *Sensitivity Coefficient O_s.* The sensitivity coefficient O_s is the ratio of the half-attenuation degree G_s of the network in T_2 to the half-attenuation degree G_s of the network in T_1, expressed as follows:

$$O_s = \frac{G_S(T_2)}{G_S(T_1)}, \quad s = 1, 2, \ldots. \tag{7}$$

(iii) *Weight of Impact Q_s.* The weight of impact Q_s refers to the contribution of a given eigenvalue to network vulnerability, expressed as follows:

$$Q_s = \frac{O_s}{\sum_s O_s}, \quad s = 1, 2, \ldots. \tag{8}$$

3.3.2. Variation Degree of Network Vulnerability. We define the variation degree of network vulnerability, which represents the value of change in network vulnerability before and after interconnection of the TAC system.

Let $U_{s,\ h}$ be the set of the rate of change in network eigenvalue s when the attack ratio is h. For example, $U_{1,\ 1\%}$ represents the rate of change in the network average degree when the attack ratio is 1%. Let $\overline{U_s}(T_t)$ be the average rate of change in a given eigenvalue s of the network under different attack ratios; then:

$$\overline{U_s}(T_t) = \frac{\sum_h U_{s,h}}{\mathrm{num}(h)}, \quad t = 1, 2; s = 1, 2, \ldots; h = 1\%, 2\%, \ldots. \tag{9}$$

Let $\Delta\overline{U_s}$ be the difference in the average rate of change in eigenvalues at T_1 and T_2; then:

$$\Delta\overline{U_s} = \overline{U_s}(T_2) - \overline{U_s}(T_1), \quad s = 1, 2, \ldots. \tag{10}$$

Let F be the variation degree of network vulnerability; then:

$$F = \sum_s [Q_s \times \Delta\overline{U_s}], \quad s = 1, 2, \ldots. \tag{11}$$

Table 3: Top ten countries or regions with the largest weighted degree.

Rank	T_1		T_2	
	Country or region	Weighted degree	Country or region	Weighted degree
1	Thailand	1060860	Mainland China	1080700
2	Singapore	970920	Japan	1069170
3	Malaysia	843860	Thailand	1060860
4	Mainland China	840700	Singapore	970920
5	Japan	829170	Malaysia	843860
6	Taiwan, China	729600	Taiwan, China	729600
7	Korea	727070	Korea	727070
8	Hong Kong, China	701830	Hong Kong, China	701830
9	Vietnam	557760	Vietnam	557760
10	Djibouti	485760	Djibouti	485760

Figure 3: Location of main sea lanes (see Table 4 for the meaning of the numbers in Figure 3).

Table 4: Main sea lanes.

No.	Sea lanes
1	Taiwan Strait
2	Strait of Malacca
3	Bab-el-Mandeb
4	The Suez Canal
5	Strait of Gibraltar
6	Strait of Hormuz
7	The Pacific
8	Bering Strait

4. Results

4.1. Vulnerability Analysis of Submarine Cable Network Nodes. In order to test the changes of each assessment indicator, a number of simulations under different attack scenarios have been performed through MATLAB 2019b, utilizing a personal computer with intel Core i7-8550U CPU @ 1.80 GHz and 8 GB of RAM. Different deletion strategies for network nodes are considered in Section 3.2.1. *Node attack*: to ensure the data stability in random attack mode, *numRandom* is set as 500. Considering the different network scale in different eras, the parameters of deleting nodes should be different, and thus *numdelete* is set as 38 and 42, respectively, in T_1 and T_2. Simulation results of changes in each network eigenvalues are shown in Figure 4.

4.1.1. Changes in the Eigenvalues. A comparison of the two different attack modes shows that under a random attack, D, C, and E decrease slowly with increasing attack proportion, while ΔN increases slowly. In the case of intentional attack, the above four eigenvalues change more significantly. When the attack ratio reaches a certain level, D, C, and E show a sharp decreasing trend, reaching 0, and ΔN increases sharply, reaching 1. These results show that the submarine cable network is relatively robust under a random attack but relatively vulnerable under an intentional attacked.

The same attack mode in different periods is then compared. In T_1 and T_2, the overall trends in network eigenvalue change are nearly the same in either attack mode. This indicates that construction of the TAC does not cause a dramatic change in the submarine cable networks of mainland China, but an additional supplement. Moreover, at the same proportion of attack nodes, there are slight or significant differences in the ranges of variation in network eigenvalues between the two periods. Although the ranges of variation in network eigenvalues in T_2 are slightly larger than that in T_1 for some intervals, the trend in variation of each eigenvalue of the submarine cable network in T_2 slightly lags behind that in T_1 (the specific analysis of each eigenvalue will be presented below). This indicates that the sensitivity of the submarine cable network to node attack is lower in T_2 than in T_1, which proves that construction of the TAC will reduce the vulnerability of the submarine cable network in mainland China.

In the following, we analyze the detailed characteristics of each eigenvalue change.

(i) D: the initial value of D in T_2 (8.32) is slightly smaller than that in T_1 (8.5), which is due to the addition of a few new nodes, such as Russia, Finland, and Norway. These new nodes are basically isolated from the other nodes in the original network, so D decreases slightly with increasing network scale. This is also the reason why the downward trend in D for intentional attack mode is not monotonous (the same principle applies to C). When the proportion of nodes deleted reaches about 80%, the D value for intentional attack being higher than that for random attack can also be explained by this. We compare the curves of the same attack mode for the two eras, and we find the following. (1) In random attack mode, 80% of the deleted nodes is a significant dividing line—before that, the trends of D in T_1 and T_2 are almost the same, but after that, D in T_1 drops sharply to 0. In T_2, when the proportion of deleted nodes reaches 84%, D drops abruptly, lagging 4% behind D in T_1. (2) In intentional attack mode, with increasing proportion of deleted nodes, the trend of D in T_1 and T_2 is uneven. When the proportion of deleted nodes is between 0–1% and 35–68%, D in T_2 is higher than D in T_1; when the proportion is between 1–35% and 68–82%, D in T_1 is higher than D in T_2. However, when D drops to 0, the proportion reaches 86% in T_2, lagging 4% behind T_1. The above shows that although the range of change in D in T_2 is larger in some intervals, the change trend of D in T_2 still lags behind that in T_1, whether random attack or intentional attack is considered.

(ii) C: firstly, it is clear that the descent speed of C under an intentional attack is significantly faster than that under a random attack, and the proportion of deleted nodes is 61% (T_1) and 67% (T_2), respectively, when C to drop to 0. However, in random attack mode, the proportion is 78% (T_1) and 82% (T_2), respectively. This proves that the submarine cable network in mainland China better resists random attack compared with intentional attack, under which it is relatively vulnerable. Moreover, under the same attack mode, the increase extent of the ratio of minimum deleted nodes with a C value of 0 for intentional attack (6%) is slightly higher than that for random attack (4%), which seems to indicate that the improvement in the response to intentional attack is more significant in T_2. From the details, in random attack mode, the change in C in T_2 is not always better than that in T_1. When the proportion of deleted nodes is less than 55%, the change in C in T_2 is similar to that in T_1, but when the proportion is between 55% and 78%, the decline speed of C in T_2 is faster. In intentional attack mode, the curves of T_1 and T_2 have similar peaks and troughs, but T_2 almost lags behind T_1.

(iii) ΔN: when the network is attacked, the number of isolated nodes will gradually increase, so ΔN shows an upward trend. However, the change in trend of ΔN under an intentional attack is obviously faster than that under a random attack. With regard to change characteristics, the rising trend in ΔN is basically the same for the two periods of random attack mode. In T_2, there is a slight lag phenomenon before 80% of the nodes are deleted. In intentional attack mode, the change in ΔN for T_1 and T_2 shows a characteristic of step-by-step increase. When the proportions of deleted nodes are 0–30% and 45–60%, ΔN in T_2 is lower than that in T_1; when the

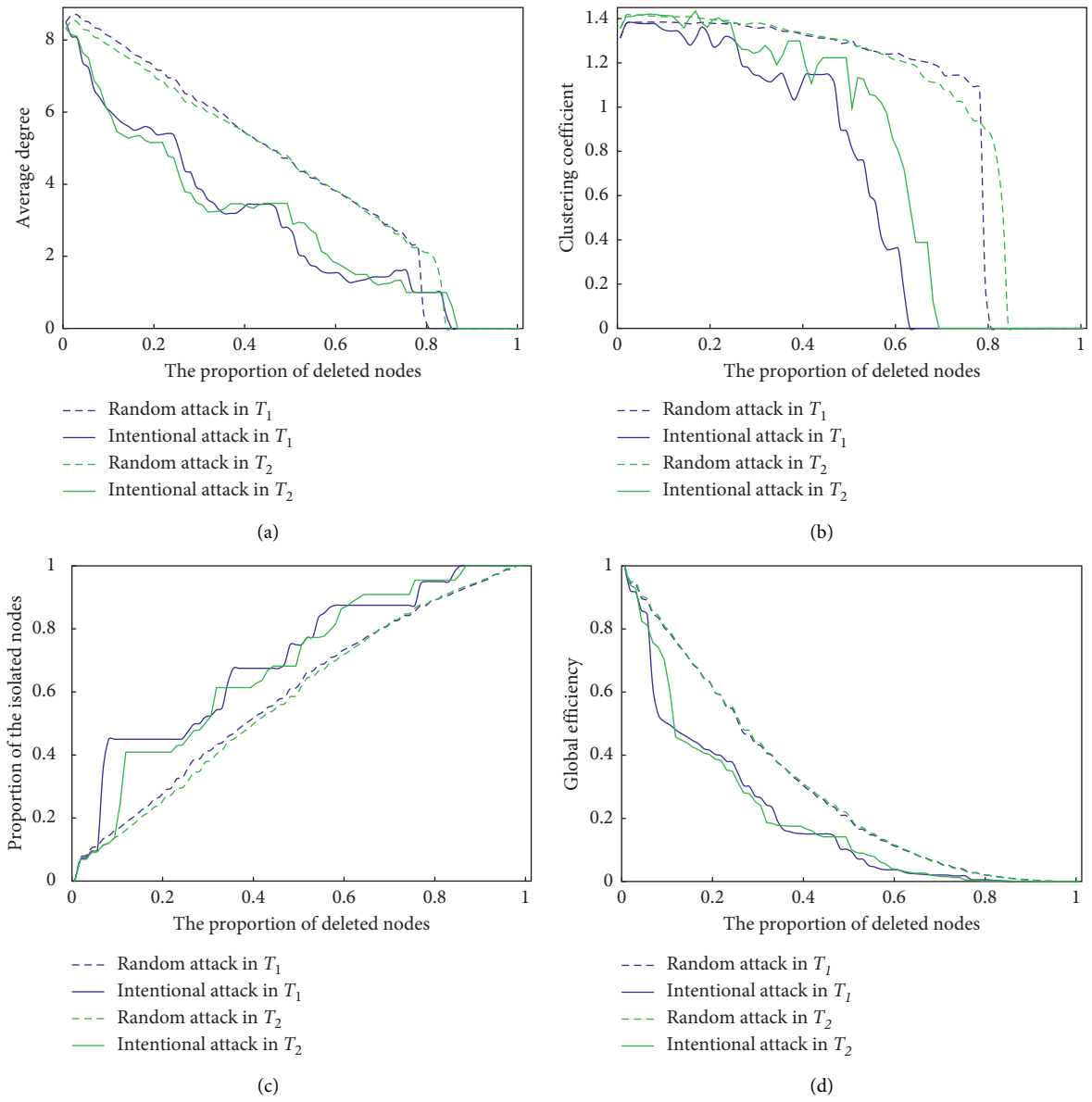

Figure 4: Changes in the network eigenvalues.

proportions are 30–45% and 60–82%, ΔN in T_1 is lower than that in T_2. In T_1, 82% of the nodes are deleted when ΔN decreases to 0; in T_2, the proportion of deleted nodes is 86%, which lags behind by 4%. This change is similar to that of D, which indicates that intentional attack has a greater impact on the submarine cable network in some intervals, but on the whole, the change in trend of ΔN in T_2 lags behind that in T_1.

(iv) E: in contrast with D and C, whether in random attack or intentional attack mode, the descending trend of E is at first fast and then slow. In random attack mode, the trend in E is basically the same for T_1 and T_2. When the proportion of deleted nodes reaches 95%, E tends to 0. In intentional attack mode, the curve of E for T_1 and T_2 traces a staggered downward trend. When the proportion of deleted nodes reaches about 85%, E drops to 0. When the proportion is within the range of 5–10%, E decreases fastest in T_1 and T_2, but the curve in T_2 obviously lags behind that in T_1. This proves that the construction of TAC can improve the ability of the submarine cable network of mainland China to deal with intentional attack under a certain proportion of deleted nodes.

Through the above analysis, a few hub landing stations in the submarine cable network of mainland China are of great importance; therefore, the network is relatively vulnerable under an intentional attack and relatively strong under a random attack. However, by comparing the changes in four eigenvalues in T_1 and T_2, we find that the influence of the submarine cable network of mainland China in T_2 lags

behind that in T_1, whether from the perspective of the critical point of network collapse or from the perspective of the change characteristics of each eigenvalue. This indicates that the construction of TAC reduces the vulnerability of the submarine cable network of mainland China to some extent, enhancing its ability to deal with attacks. Moreover, from the simulation results, the construction of TAC seems to have a different response effect on different attack modes—this is the goal of quantitative analysis in the following.

4.1.2. Quantitative Analysis. According to the analysis method in Section 3.3, we quantitatively analyze the vulnerability of the submarine cable network of mainland China under different attack modes. The calculation results are shown in Tables 5 and 6.

In random attack mode, $\Delta\overline{U_s}$ of D, C, ΔN, and E is −1.219%, 0.416%, −1.256%, and −0.406%, respectively. Among them, $\Delta\overline{U_s}$ of C is positive, indicating that this index is more vulnerable in T_2 than in T_1, while other network eigenvalues are negative, indicating that it is more vulnerable in T_1 than in T_2; Q_s of each eigenvalue is 0.248, 0.252, 0.252, and 0.248, respectively, and the difference is small. The contribution of each network characteristic to network vulnerability is −0.302%, 0.105%, −0.317%, and −0.101%, respectively. After the accumulation of all the contribution values, the variation degree of network vulnerability F is -0.615%. This value indicates that in random attack mode, the submarine cable network of mainland China in T_1 is more vulnerable than that in T_2, and the construction of TAC reduces network vulnerability.

In intentional attack mode, $\Delta\overline{U_s}$ of D, C, ΔN, and E is −0.983%, −7.538%, −2.236%, and −0.606%, respectively—all negative, which indicates that the submarine cable network of mainland China in T_1 is more vulnerable than that in T_2; Q_s of each eigenvalue is 0.213, 0.269, 0.252, and 0.266, respectively. The contribution of each network characteristic to network vulnerability is −0.209%, −2.025%, −0.564%, and −0.161%, respectively. After the accumulation of all the contribution values, the variation degree of network vulnerability F is −2.960%. This value indicates that in intentional attack mode, the submarine cable network of mainland China in T_1 is more vulnerable than that in T_2, and the construction of TAC reduces network vulnerability.

The results show that the submarine cable network of mainland China is more vulnerable now than after the construction of TAC, and the construction of TAC reduces network vulnerability to some extent. However, for different attack modes, the reduction of network vulnerability in intentional attack mode is more significant than that in random attack mode.

4.2. Vulnerability Analysis of Submarine Cable Network Edges. The curves of D, C, ΔN, and E are almost monotonous, directly reflecting the degree to which the network is affected by attack. Therefore, the above four network eigenvalues can be used to analyze the vulnerability changes in the network when the sea channels, that is, the edges in the network, are attacked.

4.2.1. Segmentation of Network by Edge Fracture. The submarine cable network of mainland China will be split in different ways due to the obstruction of different sea lanes. Table 7 lists the impacts of sea lane interruption on the submarine cable network of mainland China. The Taiwan Strait impacts the EAC and SMW3 systems, but it is not the sea lane through which the main cable passes, so the overall network structure is almost unchanged. The Strait of Malacca, Bab-el-Mandeb, the Suez Canal, and the Strait of Gibraltar are important sea lanes for mainland China to South Asia, the Middle East, Africa, and Europe. An attack on these sea lanes will break the network in T_1, meaning some areas become isolated subnetworks separated from mainland China. However, in T_2, an attack on these sea lanes will only cause some failures in the network, but the affected countries or regions still maintain contact with mainland China. The Strait of Hormuz is a branch lane, which only plays a key role in the branch route of the AAE-1 system—its breakage will affect the links between some Middle East countries and mainland China. The Pacific Ocean is an important sea lane of the submarine cable between China and the United States, and its obstruction will directly cause the United States to become an isolated subnet, no matter in T_1 or T_2. The Bering Strait becomes the only route which must be passed through in the TAC system in T_2—its breakage will cause Russia and other countries or regions to become separated from mainland China.

4.2.2. Importance Ranking of Sea Lanes. According to the simulation strategy in Section 3.2.2, this paper calculates the changes in network eigenvalues under the condition of each sea lane breaking so as to quantify and rank the importance of theses sea lanes (Table 8).

The results show that the Strait of Malacca is the most important sea lane in the submarine cable network of mainland China, both in T_1 and T_2. The average rate of change in network eigenvalues is highest when the Strait of Malacca is blocked. Bab-el-Mandeb and the Suez Canal rank second and third in importance in the network. The rankings for the Strait of Gibraltar, the Taiwan Strait, and the Pacific are relatively low, indicating a relatively low impact on the submarine cable network of mainland China. The Bering Strait becomes a new sea lane after completion of the TAC, with an average rate of change of 0.047, ranking fifth—its importance is less than that of the Strait of Hormuz.

However, from a comparison of the different periods, the average rate of change of the Malacca Strait, Bab-el-Mandeb, and the Suez Canal, ranked the top three in importance, decreases in T_2. Judging from the standard deviation of the changes in the eigenvalues, T_2 (0.083) is smaller than that of T_1 (0.124), which indicates that TAC construction reduces the importance of the Malacca Strait, Bab-el-Mandeb, and the Suez Canal in the submarine cable network of mainland China, and the difference of the importance of each sea lane in the whole network is reduced. From a geographical perspective, the Malacca Strait, Bab-el-Mandeb, and the Suez Canal are the only sea lanes connecting mainland China and the Middle East, and Africa and Europe, in T_1.

Table 5: Average rate of change in network eigenvalues.

Eigenvalues	Random attack			Intentional attack		
	$\overline{U_S}$ ($T1$)	$\overline{U_S}$ ($T2$)	$\Delta\ \overline{U_S}$	$\overline{U_S}$ ($T1$)	$\overline{U_S}$ ($T2$)	$\Delta\ \overline{U_S}$
D	50.185	48.966	−1.219	66.932	65.949	−0.983
C	23.360	23.776	0.416	50.140	42.602	−7.538
ΔN	60.380	59.123	−1.256	71.813	69.576	−2.236
E	71.565	71.159	−0.406	81.649	81.043	−0.606

Table 6: Analysis of variation degree of network vulnerability.

	Eigenvalues	Gs (T_1)	Gs (T_2)	Os	Qs	$\Delta\ \overline{U_S}$ (%)	F (%)
Random attack	D	53.731	55.309	1.029	0.248	−1.219	−0.302
	C	78.494	82.079	1.046	0.252	0.416	0.105
	ΔN	37.683	39.460	1.047	0.252	−1.256	−0.317
	E	25.363	26.093	1.029	0.248	−0.406	−0.101
	Total	—	—	5.144	1	—	**−0.615**
Intentional attack	D	27.860	25.258	0.907	0.213	−0.983	−0.209
	C	53.851	61.644	1.145	0.269	−7.538	−2.025
	ΔN	27.500	29.545	1.074	0.252	−2.236	−0.564
	E	9.666	10.970	1.135	0.266	−0.606	−0.161
	Total	—	—	4.261	1	—	**−2.960**

Table 7: Impact of sea lane interruption on the submarine cable network of mainland China.

No.	Sea lanes	Affected cable system	Impact on submarine cable network of mainland China	
			T_1	T_2
1	Taiwan Strait	EAC, SMW3	A few areas are affected, but the overall network structure is almost unchanged.	
2	Strait of Malacca	FLAG, SMW3, AAE-1	South Asia, the Middle East, Africa, and Europe become isolated subnetworks, separated from mainland China.	The network is partly broken, but the affected countries or regions can still maintain contact with mainland China.
3	Bab-el-Mandeb	FLAG, SMW3, AAE-1	Africa, Europe, and parts of the Middle East become isolated subnetworks, separated from mainland China.	
4	The Suez Canal	FLAG, SMW3, AAE-1	Africa and Europe become isolated subnetworks, separated from mainland China.	
5	Strait of Gibraltar	FLAG, SMW3	Parts of Europe become isolated subnetworks, separated from mainland China.	
6	Strait of Hormuz	AAE-1	Parts of the Middle East become isolated subnetworks, separated from mainland China.	
7	The Pacific	TPE, NCP,	The U.S. mainland becomes isolated subnetwork, separated from mainland China.	
8	Bering Strait	TAC	None.	Russia becomes separated from mainland China.

Table 8: Changes in the eigenvalues when sea lanes are interrupted.

Era	No.	Sea lanes	D		ΔN	C		E		Average rate of change	Rank
			Value	Rate	Rate	Value	Rate	Value	Rate		
T1	1	Taiwan Strait	8.895	0.006	0.000	0.730	−0.001	0.240	0.006	0.003	7
	2	Strait of Malacca	4.158	0.535	0.632	0.836	−0.147	0.112	0.535	0.389	1
	3	Bab-el-Mandeb	7.053	0.212	0.316	0.743	−0.019	0.191	0.212	0.180	2
	4	The Suez Canal	7.842	0.124	0.263	0.720	0.012	0.212	0.124	0.131	3
	5	Strait of Gibraltar	8.579	0.041	0.105	0.708	0.029	0.232	0.041	0.054	4
	6	Strait of Hormuz	8.421	0.059	0.026	0.697	0.044	0.228	0.059	0.047	5
	7	The Pacific	8.737	0.023	0.026	0.711	0.025	0.236	0.024	0.025	6
	—	Normal	8.947	—	—	0.729	—	0.242	—	—	—

Table 8: Continued.

Era	No.	Sea lanes	D		ΔN	C		E		Average rate of change	Rank
			Value	Rate	Rate	Value	Rate	Value	Rate		
	1	Taiwan Strait	8.381	0.038	0.048	0.694	0.045	0.204	0.038	0.034	6
	2	Strait of Malacca	4.333	0.503	0.500	0.768	−0.056	0.106	0.503	0.290	1
	3	Bab-el-Mandeb	6.952	0.202	0.286	0.795	−0.094	0.170	0.202	0.119	2
	4	The Suez Canal	7.667	0.120	0.214	0.773	−0.063	0.187	0.120	0.078	3
T2	5	Strait of Gibraltar	8.190	0.060	0.095	0.776	−0.067	0.200	0.060	0.030	7
	6	Strait of Hormuz	7.952	0.087	0.071	0.685	0.058	0.194	0.087	0.061	4
	7	The Pacific	8.524	0.022	0.024	0.689	0.052	0.208	0.022	0.024	8
	8	Bering Strait	8.095	0.071	0.095	0.729	−0.003	0.197	0.071	0.047	5
	—	Normal	8.714	—	—	0.727	—	0.213	—	—	—

However, after completion of the TAC system, the route through the Bering Strait becomes a new choice. This is conducive to a reduction in network vulnerability.

5. Conclusion and Discussion

This paper has taken a first step in analyzing the vulnerability of the submarine cable network of mainland China, comparing changes in vulnerability before and after construction of the TAC system, from both complex network and geographical perspectives. The results can be summarized as follows.

The submarine cable network of mainland China is more robust under a random attack but more vulnerable under an intentional one, just like any other transport network with complex characteristics [33]. This is because the connections in the network are mainly routed through high-level node countries (such as Thailand, Singapore, Japan) and significant sea lanes (such as the Strait of Malacca and the Suez Canal). Intentional attacks carried out on these nodes and edges will readily lead to a collapse of the submarine cable network of mainland China, especially with respect to the connection between China and European countries, which relies almost exclusively on a single route from east to west.

However, if the TAC is built, this problem will be alleviated. Whether under a random attack or an intentional attack, the change in trend of each network eigenvalue will lag behind the current change, and the comprehensive score of the vulnerability change will be reduced, proving that the TAC system can improve the robustness of the submarine cable network of mainland China. Notably, the variation in the degree of network vulnerability under an intentional attack decreases more significantly than under a random attack. This indicates that the TAC system helps to enhance the performance of the submarine cable network of mainland China, when under an intentional attack. In fact, the TAC system not only strengthens the existing network structure but also enriches it.

Although the Strait of Malacca and the Suez Canal always possess critical strategic significance, the TAC system will weaken their importance. Judging by the change in trend of F value, the downward trend is not significant; however, the TAC system will still become an important project to change the situation of China and even the world submarine cable network. From a geographical perspective, the TAC system provides a new connection path; from the perspective of topology, the TAC system changes the large-chain structure of the network into a large-ring structure.

Our results have important implications for network vulnerability, in intentional attack mode, which should be taken into account by managers who analyze and assess the communication network security. Historically, submarine cables usually have been vulnerable to damage from threats related to fisheries, anchors, earthquakes, and tsunamis, but the increasingly assertive foreign policies of some states mean that these cables are at risk of purposeful interference, as per the emerging "hybrid" security threat. For example, Russia cut the submarine cables between Crimea and Ukraine in 2013—a crucial step in controlling the Internet within the annexed territory [34]. Therefore, in the information age, it is necessary for managers to have a good knowledge of vulnerable nodes and lines of submarine cable networks. This paper makes up for the lack of research in this field, as well as proving the importance of TAC construction in the context of the submarine cable network of mainland China.

However, there are some limitations in this paper, which could be addressed in future work. Although we fully consider the scenario of submarine cable systems having multiple landing stations in different cities in the same country, we still regard the country rather than the city as the network node in the network attack simulation. This will not affect the result of network vulnerability, but it is necessary to study from the microperspective, which has been done in previous studies [26]. In this work, the submarine cable network of mainland China is regarded as an independent local-area network and is thus not affected by the global submarine cable network. However, the submarine cable network of mainland China is not an isolated system and has various relationships with other submarine cables and regions [35]. Therefore, details may be lost when building the network, and research on the global submarine cable network will be a goal for future work. Moreover, event detection, as the primary strategy to deal with submarine cable network attacks, should be the future direction of submarine cable network vulnerability research. Especially, the graph-theory-based network partitioning algorithm has been applied to power system [36], which has important enlightenment to submarine cable transmission system.

Data Availability

The data for this study mainly come from TeleGeography (https://www.telegeography.com/), which is a telecommunications market research and consulting firm.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This study was supported by the National Natural Science Foundation of China (no. 42071151) and the Strategic Priority Research Program of the Chinese Academy of Sciences (no. XDA20010101).

References

[1] V. Nagpal, *Convergence of Subsea Fiber, Terrestrial Fiber and Data Centers Leading to the Continental Edge and Subsea Colocation*, Offshore energy, Teesside, UK, 2019, https://suboptic2019.com/suboptic-2019-papers-archive/.

[2] H. Nakamoto, A. Sugiyama, and A. Utsumi, "Submarine optical communications system providing global communications network," *Fujitsu Scientific and Technical Journal*, vol. 45, pp. 386–391, 2009.

[3] D. A. Boughton and E. R. O. Smith, "Regional vulnerability: a conceptual framework," *Ecosystem Health*, no. 5, pp. 312–322, 1999.

[4] N. Adger and N. Kelly, "Social vulnerability to climate change and the architecture of entitlements," *Mitigation and Adaptation Strategies for Global Change*, no. 4, pp. 253–266, 1999.

[5] Y. Tian and H. Chang, "Bibliometric analysis of research progress on ecological vulnerability in China," *Acta Geographica Sinica*, vol. 67, no. 11, pp. 1515–1525, 2012.

[6] S. L. Cutter, B. J. Boruff, and W. L. Shirley, "Social vulnerability to environmental hazards ∗," *Social Science Quarterly*, vol. 84, no. 2, pp. 242–261, 2003.

[7] Yi Liu, J. Huang, and Li Ma, "The assessment of regional vulnerability to natural disasters in China based on DEA model," *Geographical Research*, vol. 29, no. 07, pp. 1153–1162, 2010.

[8] L. Adrianto and Y. Matsuda, "Developing economic vulnerability indices of environmental disasters in small island regions," *Environmental Impact Assessment Review*, vol. 22, no. 4, pp. 393–414, 2002.

[9] C. Fang, Y. Wang, and J. Fang, "A comprehensive assessment of urban vulnerability and its spatial differentiation in China," *Journal of Geographical Sciences*, vol. 26, no. 2, pp. 153–170, 2016.

[10] D. J. Watts and S. H. Strogatz, "Collective dynamics of "small-world" networks," *Nature*, vol. 393, no. 6684, pp. 440–442, 1998.

[11] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, no. 5439, pp. 509–512, 1999.

[12] R. Albert, H. Jeong, and A. L. Barabasi, "Attack and error tolerance in complex networks," *Nature*, vol. 406, no. 6794, pp. 387–482, 2000.

[13] A. Broder, R. Kumar, F. Maghoul et al., "Graph structure in the web," *Computer Networks*, vol. 33, no. 1-6, pp. 309–320, 2000.

[14] B. . Bollobás and O. Riordan, "Robustness and vulnerability of scale-free random graphs," *Internet Mathematics*, vol. 1, no. 1, pp. 1–35, 2003.

[15] L. A. Schintler, S. P. Gorman, A. Reggiani et al., "Complex network phenomena in telecommunication systems," *Networks and Spatial Economics*, vol. 5, no. 4, pp. 351–370, 2005.

[16] S. P. Gorman and E. J. Malecki, "The networks of the Internet: an analysis of provider networks in the USA," *Telecommunications Policy*, vol. 24, no. 2, pp. 113–134, 2000.

[17] D. C. Wheeler and M. E. O'Kelly, "Network topology and city accessibility of the commercial Internet," *The Professional Geographer*, vol. 51, no. 3, pp. 327–339, 1999.

[18] T. H. Grubesic, M. E. O'Kelly, and A. T. Murray, "A geographic perspective on commercial Internet survivability," *Telematics and Informatics*, vol. 20, no. 1, pp. 51–69, 2003.

[19] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelley, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *Control Systems Magazine*, vol. 21, no. 6, pp. 11–25, 2001.

[20] E. J. Malecki, "The economic geography of the internet's infrastructure," *Economic Geography*, vol. 78, no. 4, pp. 399–424, 2002.

[21] M. Barthélemy, "Crossover from scale-free to spatial networks," *Europhysics Letters (EPL)*, vol. 63, no. 6, pp. 915–921, 2003.

[22] S. P. Gorman and R. Kulkarni, "Spatial small worlds: new geographic patterns for an information economy," *Environment and Planning B: Planning and Design*, vol. 31, no. 2, pp. 273–296, 2004.

[23] P. K. Agarwal, A. Efrat, S. K. Ganjugunte et al., "Network Vulnerability to Single, Multiple, and Probabilistic Physical attacks," in *Proceedings of the MILICOM, Military Communication Conference*, San Jose, CA, USA, November 2010.

[24] S. Neumayer and E. Modiano, "Network reliability under random circular cuts," in *Proceedings of the IEEE GLOBECOM 2011*, pp. 1–6, Houston, Texas, USA, December 2011.

[25] L. M. Dawson, D. Ferhat, Z. Moshe et al., "Disaster-aware submarine fiber-optic cable deployment for mesh networks," *Journal Lightwave Technol*, vol. 34, pp. 4293–4303, 2016.

[26] C. Cao, M. Zukerman, W. Wu, J. H. Manton, and B. Moran, "Survivable topology design of submarine networks," *Journal of Lightwave Technology*, vol. 31, no. 5, pp. 715–730, 2013.

[27] Y. Ye, X. Jiang, G. Pan et al., *Submarine Optical Cable Engineering*, pp. 59–86, Academic Press, Cambridge, UK, 2018.

[28] J. Saunavaara and M. Salminen, "Geography of the global submarine fiber-optic cable network: the case for arctic ocean solutions," *Geographical Review*, 2020.

[29] J. Holt and P. Vonderau, "'Where the internet lives': data centers as cloud infrastructure," in *Signal Traffic: Critical Studies of Media Infrastructures*, L. Parks and N. Starosielski, Eds., pp. 71–93, University of Illinois Press, Champaign, IL, USA, 2015.

[30] O. Woolley-Meza, C. Thiemann, D. Grady et al., "Complexity in human transportation networks: a comparative analysis of worldwide air transportation and global cargo-ship movements," *The European Physical Journal B*, vol. 84, no. 4, pp. 589–600, 2011.

[31] V. Latora and M. Marchiori, "Efficient behavior of small-world networks," *Physical Review Letters*, vol. 87, no. 19, p. 198701, 2001.

[32] A. Lisser, R. Sarkissian, and J. P. Vial, *Survivability in Telecommunication Networks. Manuscript, HEC, Section of*

Management Studies, University of Geneva, Geneva, Switzerland, 1995.

[33] J. Lu and T. Gao, "Efficiency of safety control in key nodes of international sea lanes," *China Soft Scince*, no. 10, pp. 1–8, 2015.

[34] L. Robert and P. Stephen, *Little Green Men: A Primer on Modern Russian Unconventional Warfare*, Ukraine 2013-2014, Ukraine, European, 2019.

[35] Telegeography, "The submarine cable map," *Global Bandwidth Research Service*, Telegeography, Washington, DC, USA, 2016, http://www.submarinecablemap.com/.

[36] D. Ma, X. Hu, H. Zhang, Q. Sun, and X. Xie, "A hierarchical event detection method based on spectral theory of multidimensional matrix for power system," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 99, pp. 1–14, 2019.