Securing the Long-Chain of Cyber-Physical Global Communication Infrastructure

Nazli Choucri
Political Science Department
Massachusetts Institute of Technology
Cambridge, MA, United States of America
nchoucri@mit.edu

Gaurav Agarwal
Alumnus-SDM Researcher
Massachusetts Institute of Technology
Cambridge, MA, United States of America
gauravag@mit.edu

Abstract: **Executive Order, May 2019 states:**
"…foreign adversaries are increasingly creating and exploiting vulnerabilities in information and communications technology and services … in order to commit malicious cyber-enabled actions, including economic and industrial espionage against the United States and its people." **[1]**

This paper focuses on challenges of securing the long chain of global communication infrastructure, presents some illustrative data, and puts forth a multi-method research design for analysis of long-chain systems of information and or communications technology, infrastructure, services, ownership, providers, and networks -- within a state and outside its jurisdiction – all essential for unimpeded global operations. A proof of concept for data requirements to support end-to-end integrated research is provided, along with highlights of some initial empirical analysis, with China as a case in point.

Keywords— Long-chain communication infrastructure, undersea communication cables and landing points, Internet, autonomous system, networks and nodes.

I. INTRODUCTION

Recent work on "*Analytics for Cybersecurity of Cyber-Physical Systems*" [2] for the U.S. Department of Defense program on *Science of Security and Privacy Program* [3-4] – highlights several distinctive challenges to current investigations of "hard problems". This project focuses on cybersecurity for one distinct feature of critical infrastructure namely, smart grid for power systems. The fact is, however, all critical infrastructures constitute *system-of-systems*. Our research to date on cybersecurity for one ubiquitous cyber-physical system provides the overall motivation for:

1) Framining the global cyber-physical communication infrastructure as a long chain system-of-systems
2) Highlighting critical parameters, dependencies, and vulnerabilities, and
3) Providing an empirically-based proof-of-concept for data requirements to support integrated research on cybersecurity of the communication infrastructure worldwide.

If the global communication infrastructure system consists of a *long chain* of physical-cyber systems, then the "whole" is greater than the sum of its individual "parts". This is especially daunting for both research and policy when the "parts" harbor strategic value. The first of these two property-sets (cyber and physical) are well developed. The third (strategic) is framed by national goal-setting shaped by policy and priorities.

Our purpose here is to present a high-level view and a proof of concept for the importance of investigating the long chain. In terms of scale and scope, we focus on properties of (a) key global empirical parameters of "long chain" cyber-physical system-of-systems, (b) highlights of factors signaling potential vulnerabilities, (c) targeted analysis of specific countries, cable ownership, market power, and control mechanisms, and (d) relevance for national security.

II. GLOBAL COMMUNICATION INFRASTRUCTURE

A. Long Chain System of Systems

Our ability to communicate internationally and to transmit information for financial, strategic, economic or other transactions relies almost entirely on the global network of undersea telecommunication cables systems. By some counts, over 95% of today's Internet communication is transmitted via undersea cables [5].

We take the submerged networks for granted. But all submerged cable systems land in sovereign territory. For the most part, we tend to overlook the vulnerabilities and threats to cybersecurity, and we do not consider the connections to other segments of the global communication infrastructure. As a result, information and data are segmented and not readily usable for analytical and computational purposes. This is also true for the operational "tool-kits" of both theory and methods.

In short: *We ignore the fundamental functions of undersea communication cables as necessary enablers for all mobile and fixed cyber-physical systems in the long chain of global Internet communication infrastructure*.

Further, when parsed, each of the constituent terms in this "*long chain*" carries its own impediments to advances in science of security or to national security. More specifically:

First, the *long chain* infrastructure is generally seen in geo-spatial terms. This view obscures the diverse and dynamic properties and functionalities of essential cyber-physical systems – mobile and fixed – that depend on undersea communication cable systems.

Second, the term, *mobile* infrastructure, usually refers to user devices and/or to operating systems for mobile communication, focusing on end-use consumers, products and support systems.

978-1-7281-5092-5/19/$31.00 ©2019 IEEE

This view is limiting, perhaps dangerous. For example, mobile internet infrastructure connects to the fluidity enabled by autonomous systems and BGP Tables [6]. It is also relevant to cloud access and capabilities. Mobile infrastructure spans all segments of complex cyber-physical systems supporting transmission of data, as well as the configuration and reconfiguration of networks and pathways to final destinations.

Third, the overall global communication cyber-physical *infrastructure* consists of distinct systems, notably (a) telecommunication cable systems, their ownership, operations and destinations, (b) landing points (c) Internet exchanges (d) autonomous systems (e) BGP tables protocols (f) peering practices, (f) satellite Internet access – along with all supporting and enabling operations.

Fourth, individually or jointly, these three features can assume *strategic value* for national security. When this happens, the "facts" on the ground, undersea, and in space – mobile or fixed – can become highly contentious in potentially powerful ways.

B. Problem Statement

The problem is that the complex properties of this long chain global communication are generally examined as segmented (or siloed) systems despite mutual dependencies that often obscure system boundaries – all of which impede integrated analysis for science and policy.

Each individual system in the long chain is characterized by distinct cyber physical features, whose security is essential for the operation of the entire global communication infrastructure. Further, different systems – parts of a whole – are often situated in, or subject to, different legal regimes or regulatory mechanisms. This creates powerful barriers to effective cybersecurity practice. The point here is that we are dealing with the merging of computing and networking with physical systems, dynamic and mobile equipment, services and functionalities, that create new capabilities, produces, and processes – fixed and mobile. The complexities are compounded when we consider the "ecology" of undersea communication systems upon which the entire Internet depends.

In addition, it is difficult to ignore the basic reality that the long chain of global communication infrastructure – the parts and the whole – faces diverse threats on land, at sea, in space, and in cyberspace. To simplify, channels of threats include but are not limited to the following:

1) Publicly available network topology, including maritime "choke points'';

2) Strategic vulnerability of network end-points on land;

3) Shared and often insecure network management/control systems with backchannel remote access to malicious actors capable of inducing correlated failures; and

4) Advanced submarine capabilities and hybrid means of undersea reconnaissance with potentially disruptive properties

The result is that cybersecurity of this complex long chain global communication infrastructure is difficult to assess and analyze, let alone to protect. It may well be that prevailing risks and vulnerabilities far exceed any acceptable level.

C. Overall Objectives

Our purpose of this paper is to (a) present a high level a research design for an integrated end-to-end cybersecurity analysis of the long chain of global communication infrastructure (b) highlight different aspects of the strategic properties, and (c) present some initial results in support of the proof of concept. By definition, central to this undertaking is analysis of connections among specific segments of the long chain essential for the proper functioning of the communication cable system "ecology" that "feeds into" the Internet.

As an "entry point", we focus on undersea fiber optic cable systems and networks. These are large-scale, highly structured, and widely distributed built-systems. From there on we trace the various component systems of the global communication infrastructure. In this paper we focus on select "markers" of the long chain:

- Network of undersea telecommunication cables;
- Strategic and security-related properties of the landing points of undersea cables;
- Distribution and capability of physical as well as cyber reach of undersea cables to autonomous systems;
- Country specific network views.
- Country specific autonomous systems.

Not explicitly considered here are:

- Internet exchanges, locations, traffic, volume and type data exchanged;
- Cloud services; and specific fixed and mobile equipment; and
- Satellite Internet access.

D. Technical Barriers

We recognize that technical barriers are likely to create major challenges for our overall research initiative. We consider these barriers as *missing pieces* that impede advances in the science of security – over and above the siloed segmented research practices to date. Among the missing pieces are:

1) Analysis of reliability of core network functionalities (protocols, routing mechanisms);

2) Results of modeling analysis of capabilities, intents, and knowledge of key actors and entities;

3) Realistic synthesis of failure scenarios, operational security strategies, and estimates of risks; and

4) Net overarching assessment of the current status of cybersecurity for private or public entities

We appreciate the need for *silo-specific* research to build critical foundations or to address specific, well defined, problems. However, unless the "pieces" can be connected to a "whole", that practice in itself can impede progress in the science of security. As a result, despite notable exceptions [7-10], neither academic researchers, infrastructure security experts nor policy-makers pay needed attention to the status, vulnerabilities, and potential threats to undersea cable networks.

978-1-7281-5092-5/19/$31.00 ©2019 IEEE

III. Relevance to National Policy & Science of Security

A. Relevance to National Security – 2019 Executive Order

The Executive Order of May 15, 2019 for "Securing the Information and Communications Technology and Services Supply Chain" [1] explicitly prohibits:

> "… any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service (transaction) by any person, or with respect to any property, subject to the jurisdiction of the United States, where the transaction involves any property in which any foreign country or a national thereof has any interest (including through an interest in a contract for the provision of the technology or service)," [1]

Our problem statement and research design focus on elements of long chain global communication infrastructure – referred to as "transaction" in Executive Order [1] – that:

> "(A) poses an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of information and communications technology or services in the United States;
>
> (B) poses an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the digital economy of the United States; or
>
> (C) otherwise poses an unacceptable risk to the national security of the United States or the security and safety of United States persons." [1]

A related notification from the U.S. Department of Commerce adds the Chinese Huawei Technologies Company [11] to the Entity List that "…of names of certain foreign persons – including businesses, research institutions, government and private organizations, individuals, and other types of legal persons – that are subject to specific license requirements for the export, reexport and/or transfer (in-country) of specified items." [12] We return to this issue later on.

B. Relevance to National Security – NDAA 2019

Our problem-statement is directly relevant to Section 889 of 2019 NDAA [13] that puts "Prohibition on certain telecommunications and video surveillance services or equipment." With certain waivers, this section requires that the head of an executive agency may not—

> "(A) procure or obtain or extend or renew a contract to procure or obtain any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system; or
>
> (B) enter into a contract (or extend or renew a contract) with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system."

Note that the term ''covered telecommunications equipment or services'' applies to telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities) [13]. We revisit this issue later on.

C. Relevance to DoD Science of Security "Hard Problems"

This long chain problem-area is directly relevant to *Scalability and Composability* hard problem of the Department of Defense program on *Science of Security and Privacy*:

> "Develop methods to enable the construction of secure systems with known security properties from components with known security properties, without a requirement to fully re-analyze the constituent components." [4]

Further, it is bears on, or relates to, the hard problem of *Policy-Governed Secure Collaboration*, notably to:

> "Develop methods to express and enforce normative requirements and policies for handling data with differing usage needs and among users in different authority domains." [4]

System properties for such a problem-area are not readily discernable in situations where:

1) Issue-area or domain is understudied and fraught with uncertainty

2) Temporality is variable, not necessarily reflected in even intervals, and often defined by system function and process.

3) Data-creation is an essential, but not sufficient, condition for progress in science or policy;

4) System-boundary can be ambiguous, especially when dominated by overlapping system properties; and

5) Authority systems are diverse, with unequal in capabilities, and often harbor conflicting goals.

Conditions of this sort make it especially difficult to design a multi-dimensional, multi-method research approaches to identify, track, examine, and assess threats to, and propensity for, cybersecurity in the very diverse systems of the global communication infrastructure.

In sum, we expect that research on the long chain of global communication infrastructure system-of-systems will support, and potentially enhance, prevailing understandings of the *as-is state* of the nation's position in the global communication infrastructure, the position of its allies as well as of adversary states. Especially important will be sustained *assessments of contingencies*, that is, "What….If….?"

IV. Toward Global Empirical Analysis

Our purpose is to help articulate connectivities and linkages between, among, and across the "long chain" system-of-systems, rather than replicate the "siloed" research strategy. In addition, we anticipate the individual "parts" and the "whole" are subject to generic as well as specific vulnerabilities that can affect the entire global communication infrastructure. It goes

978-1-7281-5092-5/19/$31.00 ©2019 IEEE

without saying that, while addressing system-*threats*, we need also to take into account system-*supports.*

Earlier these background work has helped us consider: (i) challenges of mapping *ownership structures* and operational governance mechanisms; (ii) various analytical methods for *system representations* of physical infrastructure and information flow patterns, and identification of critical control points; and (iii) need for testing of *statistical significance* of structures and processes, and frames for threat identification and defense in competitive conditions. We have also put forth recommendations for terminology use when writing papers on cybersecurity and lay the ground work for interaction across disciplines and between technical and nontechnical stakeholders [14].

A. Complexity and Diversity

To simplify, the complexities at hand are due largely to (a) differences in the properties of the cyber, physical, and strategic systems, (b) diversity of decision-entities, (c) differences in objectives and capabilities, and (d) situated under diverse authority systems. Furthermore, Invariably, imperatives of national security dominate. Jointly they constitute facets of the long chain whose overarching properties defy simple description and whose system boundary is particularly thorny. However, ensuring its safety --vgiven security threats, periodic attacks, random faults, and natural events are also sources of major concern.

Formally, undersea communication cables are largely owned and installed by private parties. Cable owners are diverse and growing with new actors, public and private (note Google). Their security is typically in the realm of "low politics" domain for national governments. But when private parties are closely aligned to the state, they are essentially public actors (note China). In addition, governance of all undersea cable landing points are in sovereign territory. This simple fact can take on properties of "high politics" especially when co-located with Internet exchanges so critical to overall Internet infrastructure.

Diverse authority and jurisdictions are distributed throughout the "long chain." Although a wide range of legal regimes are in place – such as the United Nations Convention on the Law of the Sea (UNCLOS) [15] – security policy in this domain is diverse, diffused, fragmented, and piecemeal [7, 16-17]. Notably, UNCLOS [15] does not require states to monitor vulnerabilities of cable components or inspect suspicious actors. In short, international law is designed for the conventional role of cables in the last century, not for the salience of security threats in networked realities of the twenty-first century.

Prior incidents of damage – accidental as well as random faults – highlight the risk of localized cable outages for governments to communicate effectively, and these even cause significant economic losses. Threats of espionage or sabotage of undersea network infrastructure can be even more disruptive. Technological defense is always necessary, but it is not sufficient given the lack of private actors' incentives for security investment as well as the lack of monitoring and reporting/sharing of vulnerabilities. Thus, imperfect and asymmetric information negatively affect incentives for investments in security. Further, societal costs of correlated failure would far exceed the loss to individual entities who conduct network operations, and on whose actions the overall risk level depends.

B. Research Markers

Our approach is built around markers that serve as anchors for empirically-based scientific inquiry:

1) Parameters of cyber-physical systems;
2) Network structures and emergent patterns;
3) Actors and activities, reach, power and leverage;
4) Authority systems, strategic postures, and policy mechanisms; and
5) Cybersecurity for "parts" and "whole" of the long chain.

C. Propositions for Proof of Concept

It goes without saying that hypothesis testing as well as any applications of robust analytical tools can take place only to the extent that empirical data allows. For this reason, some empirically-centered proof of concept is generally necessary. For this reason, we now present and explore specific propositions (as questions). We frame each proposition below (1-5) in the form of an "if…then…:" statement.

1) If the empirical data enable mapping the global undersea cable system, then we can determine:

- Route
- Landing points

2) If the empirical data enable mapping the global system above, then we can identify state or state-related actors and determine:

- Ownership
- Route
- Landing points

3) If actors are identified, then we can track major state actors, affiliated entities, and/or private actors, with respect to:

- Current reach
- Future plans

4) If actor-traffic is identified, then we can we situate the networks connecting a state actor or entity to the global communication infrastructure with respect to:

- Autonomous systems
- Network structure
- Node centrality

5) If network systems are delineated, then we can situate actors, at specific nodes, with respect to:

- Salience
- Ownership
- Reach

Stated thus, these propositions are straightforward. They are contingent only on access to relevant data.

D. Anticipated Challenges

At this point, we anticipate many challenges. The first two, noted below, are of immediate importance. The third follows by necessity.

978-1-7281-5092-5/19/$31.00 ©2019 IEEE

The first pertains to *data collection*– drawing only on public access – and aligning such data with available metrics.

The second challenge is *standardization* of approach to control point identification across the long chain.

The third is about effective *calibration* of the system dynamics model, for example, by using part of the data collected above and then conducting verification validation using rest of the data.

V. RESULTS & RELEVANCE

Foundational work – supported by MIT Seed funds [18] – has helped us construct an empirical data base to examine each of the propositions presented earlier. We now turn to the results of propositions1-5.

1) Global undersea telecommunication networks

Insights into proposition 1 are shown in Figure 1. The figure displays existing and planned *global undersea network* and *landing Points (LPs)*, and it provides a quick sense of *what* and *where*. The figure displays existing and planned *global undersea network* and *landing Points (LPs)*, and it provides a quick sense of *what* and *where*. It shows the routes of data and information in the long chain global of communication infrastructure from undersea communication cables to land-based destinations worldwide. The figure also draws attention to points of constraints (or control) on capacity at specific (geographic) choke points and perhaps at a number of (strategic) chokepoints at the landing destination.

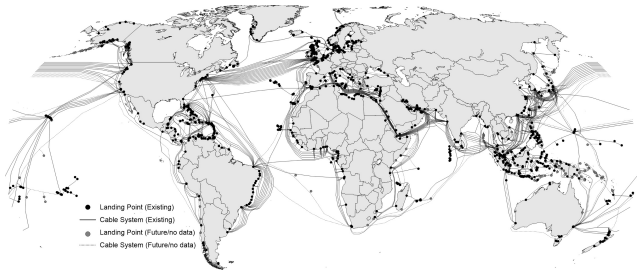

Fig. 1. Global network of undersea communication cables and landing points. *Source:* Constructed from data in Telegeography.com [19].

2) Ownership of undersea communication cables: China

Figure 2 demonstrates the worldwide reach of undersea telecommunication cables for one adversarial state, China. Especially notable in Figure 2 are three features of China's communication cable systems: first are the cables with partial Chinese ownership that do not land in China; second is the strong China focus on Africa and Indo-Pacific region; and third, are the notable absence of ownership in any of the trans-Atlantic cables connecting United States.

The figure identifies actual as well as planned undersea cable systems. The "partial" Chinese ownership in Figure 2 refers to China Mobile [20], China Telecom [21], China Unicom [22], CITIC Telecom International [23], HKBN Enterprise Solutions [24], Hyalroute [25], Pacific Light Data Communication Co. Ltd. [26], PCCW [27], Peace Cable Network Co. Ltd. [28].

Fig. 2. Global network of undersea communication cables with partial Chinese ownership. *Source*: Constructed from Telegeography.com [19].

3) Major state-affiliated actors: Huawei Marine, China

Earlier in this paper we took note of NDAA 2019 section 889 [13] that prohibits, subject to waivers, the use of communication systems being built by ZTE and Huawei for military applications. Current policy debates tend to focus on US use of next generation 5G mobile telecommunication technology.

Missing from prevailing debates, however, is attention to the reach of Huawei through its wholly owned subsidiaries, one of which is Huawei Marine. Figure 3 shows newly built and upgraded plans by China's Huawei Marine and the landing points. Huawei Marine is a wholly-owned subsidiary of Huawei.

Fig. 3. Global network of undersea communication cables built or upgraded by Huawei. *Source*: Constructed from data provided in HuaweiMarine.com [29].

4) Structure of Internet autonomous systems - China

Figure 4 presents a network mapping of autonomous systems for China's *inbound* and *outbound* data traffic. The locations of Internet Exchanges worldwide are shown elsewhere in [30]. Internet exchanges are heterogeneous in attributes, capabilities, legal context and local operational conditions. Figure 4 also shows autonomous systems (ASs) registered inside China, as well as those registered outside of China but are directly connected to Chinese ASs.

We recognize that such connections are dynamic, and that database are updated periodically in the BGP Tables. Nonetheless, this figure reveals some robust patterns that do not usually change radically on short order. In [31], we examine the strategic implications of the patterns in Figure 4, even as we recognize that these might change over time.

978-1-7281-5092-5/19/$31.00 ©2019 IEEE

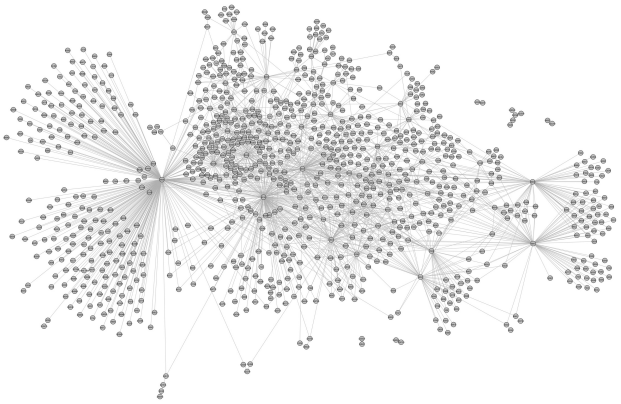

Fig. 4. Autonomous Systems (AS) nodes for Internet access in China. *Source*: Constructed from on data in RIPE [32-33] for a specific date in 2018.

5) Major Autonomous Systems - China

The most central autonomous systems carrying traffic to, and from, China are listed in Table I. All are registered in China. Some are state owned autonomous systems; others have a formal private sector status.

TABLE I. TOP-RANKING AUTONOMOUS SYSTEMS IN CHINA BASED ON THEIR EIGENVECTOR CENTRALITY SCORES.

AS Number	Name
4134	CHINANET-BACKBONE No.31
4837	CHINA169-BACKBONE CHINA UNICOM China169 Backbone
4809	CHINATELECOM-CORE-WAN-CN2 China Telecom Next Generation Carrier Network
45102	CNNIC-ALIBABA-CN-NET-AP Alibaba (China) Technology Co.
132203	TENCENT-NET-AP-CN Tencent Building
37963	CNNIC-ALIBABA-CN-NET-AP Hangzhou Alibaba Advertising Co.
7497	CSTNET-AS-AP Computer Network Information Center
9929	CUII CHINA UNICOM Industrial Internet Backbone
4538	ERX-CERNET-BKB China Education and Research Network Center
9808	Guangdong Mobile Communication Co.Ltd
45090	Shenzhen Tencent Computer Systems Company Limited

Source: Based on RIPE data [32-33]. Eigenvector scores for centrality are derived from analysis of the networks in Figure 4.

VI. ILLUSTRATING RELEVANCE FOR POLICY & SECURITY

The results shown above carry important implications for national security as well as science of security. They all require further and more detailed inquiry. Here we raise three issues and questions of interest:

1) China has made significant gains in activities, influence, and control beyond their established boundaries, whether for economic, political, military, scientific, religious, or other purposes. Does China's ownership of undersea cable systems reinforce its Belt and Road Initiative program [34] given that its overseas investments in Internet infrastructure developments (funded by the state and/or by private actors/organizations) focus on Africa, and Indo-Pacific region?

2) The United States through Executive Order [1] and NDAA 2019 section 889 [13] directly or indirectly prohibits the use of undersea cable systems that are either built or upgraded by non-allied states – in this case, by Huawei. Does that mean that the Unites States commands less control over secure infrastructure – both within United States and outside?

3) China and other states can influence inbound and outbound traffic to and from their jurisdiction throughout autonomous systems over which they have direct control. Does knowledge of network structure for a major state (in this case China) provide insights into its operational capabilities?

VII. END NOTE

This paper explores a set of "if…. then…" empirical propositions focusing on characteristic features of the long chain of global communication infrastructure. To date, the elements of the long chain have been examined on a "siloed" basis. Our overarching purpose is to establish the foundations for large scale empirical analysis of the entire long chain end-to-end, as a system-of–systems. We signal the relevance of the long chain to national security and to science of security and highlight our research approach. Then we show empirical evidence, and policy relevance with respect to one state, namely, China.

REFERENCES

[1] Exec. Order 13873. "*Securing the Information and Communications Technology and Services Supply Chain,"* 84 FR 22689. May 15, 2019. [Online]. Available: https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain

[2] K. Dey, "Analytics for Cyber-Physical System Cybersecurity." https://cps-vo.org. https://cps-vo.org/node/48269 (accessed May 16, 2019).

[3] K. Dey, "Science of Security and Privacy Research Initiative." https://cps-vo.org. https://cps-vo.org/node/5253 (accessed August 10, 2019).

[4] D. Nicol, B. Sanders, J. Katz, B. Scherlis, T. Dumitraş, L. Williams, and M. P. Singh, 2015. "Science of Security Lablets Progress on Hard Problems," 2018. [Online]. Available: https://cps-vo.org/node/21590 (accessed May 16, 2019).

[5] L. Carter, D. Burnett, S. Drew, G. Marle, L. Hagadorn, D. Bartlett-McNeil, and N. Irvine, "Submarine Cables and the Oceans – Connecting the World," UNEP-WCMC Biodiversity Series No. 31 ICPC/UNEP/UNEP-WCMC, 2009. Accessed: May 16, 2019. [Online] Available: https://www.unep-wcmc.org/resources-and-data/submarine-cables-and-the-oceans--connecting-the-world

[6] Y. Rekhter, T. Li, S. Hares, "A Border Gateway Protocol 4 (BGP-4), " *Request for Comments, no.* 427, 2006. Accessed: May 16, 2019. [Online] Avialable: https://tools.ietf.org/html/rfc4271

[7] M. Sechrist, C. Vaishanv, D. Goldsmith, and N. Choucri, "The Dynamics of Undersea Cables: Emerging Opportunities and Pitfalls," in *Proc. of the 30th Int. Conf. of the System Dynamics Society*, E. Husemann and D. Lane, Eds, St. Gallen, Switzerland, July 2012.

[8] P. K. Agarwal, A. Efrat, S. K. Ganjugunte, D. Hay, S. Sankararaman and G. Zussman, "The Resilience of WDM Networks to Probabilistic Geographical Failures," in *IEEE/ACM Transactions on Networking*, vol. 21, no. 5, pp. 1525-1538, Oct. 2013. doi: 10.1109/TNET.2012.2232111.

978-1-7281-5092-5/19/$31.00 ©2019 IEEE

[9] W. Wu, B. Moran, J. H. Manton and M. Zukerman, "Topology Design of Undersea Cables Considering Survivability Under Major Disasters," *2009 International Conference on Advanced Information Networking and Applications Workshops*, Bradford, 2009, pp. 1154-1159. doi: 10.1109/WAINA.2009.77.

[10] S. Neumayer, G. Zussman, R. Cohen and E. Modiano, "Assessing the Vulnerability of the Fiber Infrastructure to Disasters," in *IEEE/ACM Transactions on Networking*, vol. 19, no. 6, pp. 1610-1623, Dec. 2011. doi: 10.1109/TNET.2011.2128879.

[11] Bureau of Industry and Security, "Addition of Entities to the Entity List: A Rule by the Industry and Security Bureau on 05/21/2019*"* 84 FR 22961. May 16, 2019. [Online]. Available: https://www.federalregister.gov/d/2019-10616 (accessed August 10, 2019).

[12] Bureau of Industry and Security,. "FAQs - What is the Entity List?" [Online]. Available: https://www.bis.doc.gov/index.php/2011-09-12-20-18-59/export-and-reexport-faqs/faq/104-what-is-the-entity-list (accessed May 19, 2019).

[13] U.S. House. 115th Congress, (2018, August 13). *H. R.5515, John S. McCain National Defense Authorization Act for Fiscal Year 2019.* [Online]. Available: https://www.congress.gov/bill/115th-congress/house-bill/5515/text (accessed: May 16, 2019).

[14] R. Ramirez and N. Choucri, "Improving Interdisciplinary Communication With Standardized Cyber Security Terminology: A Literature Review," in *IEEE Access*, vol. 4, pp. 2216-2243, 2016. doi: 10.1109/ACCESS.2016.2544381.

[15] *Convention on the Law of the Sea*,. UNTS vol. 1833 (p.3), 1834 (p.3), 1835 (p.3), 1994. [Online]. Available: https://treaties.un.org/Pages/showDetails.aspx?objid=0800000280043ad5 (accessed: May 16, 2019).

[16] T. Davenport, "Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis". *Cath. U. Journal of Law & Technology*, vol. 1, issue 1, 2015. Available: http://scholarship.law.edu/jlt/vol24/iss1/4

[17] R. Sunak. *Undersea Cables: Indispensable, Insecure*. London: Policy Exchange, 2017.

[18] S. Amin, and N. Choucri, "Security of Global Undersea networks: Models, Defenses, and Policy Mechanisms." MIT Institute for Data, Systems, and Society Seed Fund Program, 2018.

[19] "How can I download the KML or a CSV of the dataset?" Telegeography/www.submarinecablemap.com https://github.com/telegeography/www.submarinecablemap.com (accessed April 16, 2019).

[20] China Mobile Limited. "About China Mobile: Overview." Chinamobileltd.com. https://www.chinamobileltd.com/en/about/overview.php (accessed May 16, 2019).

[21] China Telecom. "Overview." chinatelecom-h.com. https://www.chinatelecom-h.com/en/company/company_overview.php (accessed May 16, 2019).

[22] China Unicorn. "Company Profile." chinaunicom.com.hk. https://www.chinaunicom.com.hk/en/about/profile.php (accessed May 16, 2019).

[23] China Telecom International. "Major Shareholder." Citictel.com/en/. https://www.citictel.com/about-us/major-shareholder/ (accessed May 16, 2019).

[24] Hong Kong Broadband Network. "We are HKBN." hkbnes.net/en/. https://www.hkbn.net/new/en/about-us.shtml?utm_source=es_en&utm_medium=referral&utm_campaign=index_header (accessed May 16, 2019).

[25] HyalRoute. "Our Shared Communication Fiber Network Platform." Hyalroute.com. http://www.hyalroute.com/aboutus/company-profile/ (accessed May 16, 2019).

[26] Pacific Light Data Communication Co., Ltd. "About Us" pldcglobal.com. http://pldcglobal.com/#about (accessed May 16, 2019).

[27] PCCW Global. "Our History" pccwglobal.com. https://www.pccwglobal.com/en/about/our-history (accessed May 16, 2019).

[28] PEACE. http://www.peacecable.net. http://www.peacecable.net/#about (accessed May 16, 2019).

[29] Huawei Marine. "Experience." http://www.huaweimarine.com . http://www.huaweimarine.com/en/Experience (accessed April 1, 2019).

[30] N. Choucri and D.D. Clark, *International Relations in the Cyber Age: The Co-Evolution Dilemma*. Cambridge, MA, USA: MIT Press, 2019.

[31] N. Choucri and G. Agarwal, "Analysis of Autonomous Systems in China," unpublished.

[32] *Country ASNs: China*, RIPEstat Data API, December 15, 2018. [Online]. Available: https://stat.ripe.net/data/country-asns/data.json?resource=cn&lod=1&starttime=2018-12-15T12:00:00

[33] *ASN Neighbors for Autonomous System Numbers* (ASNs) identified in [32]. December 15, 2018. [Online]. Available: https://stat.ripe.net/data/asn-neighbours/data.json?resource=<resource>&starttime=<starttime>T12:00:00. Note: replace <resource> with ASN and <starttime> for ISO8601 or Unix timestamp. See https://stat.ripe.net/docs/data_api#asn-neighbours for details.

[34] World Bank. "Belt and Road Initiative". http://www.worldbank.org/. http://www.worldbank.org/en/topic/regional-integration/brief/belt-and-road-initiative (accessed May 16, 2019).

978-1-7281-5092-5/19/$31.00 ©2019 IEEE