Informaatioteknologian tiedekunnan julkaisuja
No. 78/2019

Martti Lehto, Aarne Hummelholm, Katsuyoshi Iida, Tadas Jakstas,
Martti J. Kari, Hiroyuki Minami, Fujio Ohnishi ja Juha Saunavaara

Arctic Connect Project and cyber security control, ARCY

JYVÄSKYLÄN YLIOPISTO

Informaatioteknologian tiedekunnan julkaisuja
No. 78/2019

Editor: Pekka Neittaanmäki
Covers: Petri Vähäkainu ja Matti Savonen

ISBN 978-951-39-7721-4 (verkkoj.)
ISSN 2323-5004
Jyväskylä 2019

Arctic Connect Project and Cyber Security Control, ARCY

Martti Lehto
Aarne Hummelholm
Katsuyoshi Iida
Tadas Jakštas
Martti J. Kari
Hiroyuki Minami
Fujio Ohnishi
Juha Saunavaara

UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION TECHNOLOGY
2019

EXECUTIVE SUMMARY

The submarine communication cables form a vast network on the seabed and transmit massive amounts of data across oceans. They provide over 95% of international telecommunications—not via satellites as is commonly assumed. The global submarine network is the "backbone" of the Internet, and enables the ubiquitous use of email, social media, phone and banking services.

To these days no any other technology than submarine cables systems has not been such a strategic impact to our society without being known it as such by the people. This also means that it is at the same time a very interesting destination for hackers, cyber attackers, terrorist and state actors. They seek to gain access to information that goes through the networks of these continents that are connected to each other with sea cables.

The main conclusion

Tapping fiber optic cables to eavesdrop the information is a conscious threat. Tapping into the cables requires sophisticated techniques to access the delicate fibers inside the cable without exposing them to seawater. In practice, the super powers have this capability

Sabotage would be simpler to perform, but difficult to scale up for meaningful effect. This is because networks are designed with a high degree of redundancy as cables are routinely damaged by falling anchors, sharks, fishing lines, earthquakes, human mischief makers and so forth. Cable breaks average fifty per year in the Atlantic alone. If a few of the cables go down, data requests are simply shunted to other cables while a fleet of specially appointed, repair boats cruise over and repair the breakages.

The submarine communication cables have extensive redundancies. It would therefore take a coordinated, massed attack to truly cripple the cables is logistically impractical. Even in that event, satellite communications could be used for vital tasks.

A massive physical cable attack is probably overestimated for the redundancy. Nonetheless, the extensive military activity around the submarine cables surely reveals that they are perceived as a valuable avenue for asymmetric attack and intelligence gathering, and a capacity to launch a more targeted attack against selected cables could cause significant disruptions.

The focus of the study

In this study, geopolitical analyses concentrate to China and Russia. China as the end-user of the planned Arctic cable, has a growing dependence on international bandwidth, it needs to improve his communication connections for example with Europe. The other area of interest of this analysis, Russia is the owner of the seabed for the Arctic cable and it has his own needs to improve communication connections in the Russian Arctic.

Strategic situation in Artic

Because of fast economic growth, China needs more and more reliable communica-tion infrastructure and is more depending on international bandwidth. One of the main counter partners of China is Europa. China is connected with Europe through two communication routes, land connection trough Kazakhstan and Russia and sea cables in the south, through Red sea and Suez channel. Both routes can be considered in some cases not reliable enough and that can cause a need for China to have more reliable route, or at least alternative to Europe. The trade war between China and the USA may turn China more towards to Europe. All this might support the idea about Arctic cable connecting between China (and Japan) and Europe.

Russia has plans to develop his Arctic areas. These plans are related mainly to exploitation of natural resources and to development of the Arctic passage as a sea route for trade. To protect this, Russia has increased military activity and for example border guarding in Arctic areas. All this requires, as is said in Russian Arctic Policy and Strate-gy, modern information and telecommunication technologies, including by laying submarine fiber-optic communication lines along the Northern Sea Route and integrating with other networks. Russia has a need for the fiber-optic communication line connecting Arctic areas, but Russia has not own technology to fulfill these needs.

Strategic intelligence

Strategic intelligence means collection, processing, analysis, and dissemination of strategic level intelligence that is required for forming policy and military plans at the national and international level. This intelligence can include both threats and possibilities, depending on situation. Strategic intelligence´s sources have traditionally been Human Intelligence (HUMINT) and Signal Intelligence (SIGINT). During last ten years, Cyberspace has become an important source for strategic intelligence and today computer networks are one of the main environments for collection intelligence, including strategic intelligence.

Most important tasks for strategic intelligence are early warning about strategic level threats and threat actors and possibilities and achieve time for decision makers.

Threats against submarine cable systems

Because submarine cable systems have been so big a strategic impact to our society, that also means that it is at the same time a very interesting destination for hackers, cyber attackers, terrorist and state actors. We need to look at potential adverse threats as the undersea optical cable routes are long and going under the water. And there are in many countries who have the ability to join (tapping) fiber optic cables to eavesdrop the information what is being transmitted there or hacking or sniffing a fiber optic cable by tapping cable under the water or at a landing station. All the states through area, which the cable is running, have interest, motivation and technical ca-pabilities to collect intelligence information from these cables at least in the points, where the cable is on the land. **Point-to-point encryption is one way to fight against the intelligence collection from undersea communication cables.**

In addition to the technical design criteria, we also need to take account of different type of threats like natural threats, accidental threats and malicious threats. These threats can contribute to prolonging cable routes or partial routes or even altering the original planned routes.

The system to be built is technically very complicated and there will be many new technical solutions to meet the required transmission rates and meet the usability and quality requirements they require. This places considerable demands on the management and control of the system as well as on the organization of its maintenance. We should be also seen about the long-life cycle of undersea optical cable, about 25 years, to be taken it into account in design.

Legal aspects of the protection of the submarine cables

Between 1884 and 1982, international community adopted four international instruments which set out substantive provisions on the rights and obligations of States related to submarine cables. These are:

1. The 1884 Convention for the Protection of Submarine Telegraph Cables;
2. The 1958 Geneva Convention on the High Seas;
3. The 1958 Convention on the Continental Shelf; and
4. The 1982 United Nations Convention on the Law of the Sea (UNCLOS).

Apart from these four main international documents, there are also other international conventions and treaties that may apply to submarine cables, such the 1972 Convention on the International Regulations for Preventing Collision at Sea, the 1972 Convention on the Prevention of Marine Pollution by Dumping from Wastes and Other Matter, the 1997 International Convention for the Suppression of Terrorist Bombings, the 2001 Convention on Cybercrime, the 1992 Constitution of the International Telecommunication Union.

The law of armed conflict including Geneva Conventions of 1949 and Additional Protocols I, II to the Geneva Conventions of 1977, Hague Convention XIII applies to submarine cables during both international and non-international armed conflicts.
The UN Chapter applies to submarine cables in the case of the use of force and the right of self-defence, regardless of the weapons employed.

The international maritime law does not give an opportunity to enact laws and regulations for the protection of submarine cables outside territorial sea, including using new technologies, as well as against new threats with using cyber, unmanned and autonomous weapon systems. The international maritime law only establishes a crime for damage to a submarine cable. Although, it is possible to conduct operational actions within the framework of a criminal investigation or the prevention of a crime. Taking in an account the specifics of maritime zone which are located outside of state sover-eignty this is not enough to ensure and build an effective system for the protection of submarine cables outside the territorial waters of the state against all types of threats, including cyberattacks, unmanned and autonomous weapon systems.

International law will be applying the right to self-defence or authorize by the Security Council collective security operations in the case of cyberattacks, includes the necessary requirements for its implementation, and establishes the necessary standards of evidence to justify the use of force. The speed and anonymity of cyberattacks makes proving State responsibility and distinguishing among the actions of terrorists, crimi-nals and nation states difficult. However, international law does not have the tools to carry out the identification of the attacker, especially in the case of cyberattacks, be-cause it is not a purpose for the international law. This is the competence of technical experts, methodologies and special programs. It is worth noting that for effective iden-tification and attribution, there must be a relationship between the international legal instrument to protection submarine cables in the case of cyberattacks and technical means of protection in cyberspace.

Future work

Because arctic fiber optic cable is a critical system and it will be used by a number of countries, organizations and people for their own purposes, it is essential to study key issues affecting the functioning of the system.

- In relation to cyber security, the reliability of the scrambling mechanisms to protect the telecommunications used in those new nodes should be investigated.

- The Undersea optical cables systems different protection mechanisms must be study.

- Artificial intelligence (AI) use needs to be investigate and clarified it`s possibilities to protect undersea fiber optic cable systems in order to better protect it malware and cyber-attacks against.

- The use of Coherent Optical Time Domain Reflectometry (COTDR) should be investigated as it is used for searching for faults and can also be used to detect tapping via cable connections.

- Different type of protections mechanisms to power supply systems must be study.

FIGURES

FIG 1. THE STRUCTURE OF THE RESEARCH PROJECT 2
FIG 2. MAP OF THE WORLDWIDE UNDERSEA SUBMARINE CABLE NETWORK 49
FIG 3. ARTIC CONNECT CABLE SYSTEM 49
FIG 4. COMMUNICATIONS NETWORKS IN THE FUTURE BETWEEN DIFFERENT SMART CITIES 50
FIG 5. OVERVIEW OF ARTIC CONNECT CABLE SYSTEM 51
FIG 6. EVOLUTION OF HIGH-CAPACITY OPTICAL TRANSPORT NETWORK..... 52
FIG 7. HIGH-CAPACITY OPTICAL TRANSPORT NETWORK OPTICAL BANDS 53
FIG 8. SUBSEA CABLE SYSTEM ARCHITECTURE WITH CABLE LANDING STATION AND DATA CENTER..... 54
FIG 9. OPTICAL UNDERSEA FIBRE OPTIC CABLES DEPENDING ON THE DEPTH OF THE OCEAN..... 61
FIG 10. FIGURE OF OPTICAL UNDERSEA FIBRE OPTIC SYSTEM FROM ITU-T RECOMMENDATION 62
FIG 11. OTN OPTICAL TRANSPORT NETWORK (G.709) 64
FIG 12. OTN OPTICAL TRANSPORT NETWORK (G.709) 65
FIG 13. EXAMPLE OF FAULT LOCATION USING COTDR FOR OF A WITH OUTPUT-TO-OUTPUT LOOPBACK COUPLING. 66
FIG 14. EXAMPLE OF FAULT LOCATION IN THE FIRST FIBRE USING COTDR FOR OF A SYSTEMS USING OUTPUT-TO-INPUT COUPLER. 66
FIG 15. EXAMPLE OF FAULT LOCATION IN THE SECOND FIBRE USING COTDR FOR OF A SYSTEMS USING OUTPUT-TO-INPUT COUPLER 67
FIG 16. RUSSIAN OPTICAL TRANS-ARCTIC SUBMARINE CABLE SYSTEM 72

TABLES

TABLE 1. COMPARISON OF SUBMARINE CABLES BETWEEN CHINA AND MAJOR COUNTRIES IN THE WORLD 9
TABLE 2. AN EXAMPLE OF A POSSIBLE POWER BUDGET TEMPLATE 58
TABLE 3 UPPER LEVEL CONCEPTUAL SUBMARINE CABLE SEGMENT THREAT MATRIX BASED ON THREATS TO UNDERSEA CABLE COMMUNICATIONS 60

CONTENT

1 INTRODUCTION 1
1.1 The Research objective 1
1.2 The Research organization 3
2 FINLAND SECURITY AND COMMUNICATIONS 4
2.1 Global security environment, and security in Finland 4
2.2 Finland is dependent of the secure global networks 5
2.3 Governmental intelligence affects national security solutions 5
3 GEOPOLITICAL ANALYSIS AND STRATEGIC CYBER INTELLIGENCE 6
3.1 Geopolitical Analysis 6
3.1.1 Importance and role of Arctic cable 6
3.1.2 China as the end user of possible Arctic Cable 7
3.1.3 Role of Russia in the project of Arctic cable 9
3.1.4 Conclusion 12
3.2 Strategic Cyber Intelligence 13
3.2.1 Strategic intelligence 13
3.2.2 Cyberspace and Cyberspace Operations cables system 14
3.2.3 Strategic cyber intelligence 15
3.2.4 Intelligence Collection from Submarine Communication Cables 17
3.2.5 Conclusion 22
References 23
4 THE INTERNATIONAL LEGAL REGIME GOVERNING SUBMARINE CABLES 26
4.1 The main international legal regimes governing submarine cables 26
4.1.1 International peacetime legal regime 27
4.1.2 International legal regime during armed conflicts 33
4.1.3 International legal regime in the case of use of force 35
4.2 Challenges and legal gaps in international law with respect to submarine cable protection 36
4.2.1 Challenges and legal gaps in international law during peacetime legal regime 36
4.2.2 Challenges and legal gaps in international law during armed conflicts 39
4.3 Recommendations for strengthen submarine cable protection 42
4.3.1 The international agreement between states concerning to the protection of submarine cables outside of the territorial sea 42
4.3.2 Development of national legislation regarding protection of submarine cables 42

4.3.3 Adoption of a Global Convention on the Protection of Submarine Critical Information Infrastructure 43
4.3.4 Right of visit according to Article X of the 1884 Cable Convention 43
4.3.5 The right of self-defence according Article 51 of UN Charter in the case of Armed Attack against submarine cables 44
4.3.6 Considering submarine cables as civil objects (non-lawful targets) during armed conflicts 44
4.3.7 National Crisis Response Exercise Capability 44
References 46
5 CYBER SECURITY THREATS AND PROTECTION IN SUBMARINE CABLE SYSTEMS 48
5.1 Introduction 48
5.2 Undersea submarine cable network 49
5.3 Technology evolution 51
5.4 Long distance optical undersea systems 53
5.5 Installation main principles 54
5.6 Designing undersea optical cable systems 55
5.7 Factors affecting the fiber quality 55
5.7.1 Attenuation 55
5.7.2 Dispersions 56
5.8 Impact of non-linearity 56
5.9 Long distance cable systems attenuation calculations 57
5.10 Threats to taking care 59
5.11 Long distance cable systems, examples 61
5.12 Long distance optical cable systems, management and control 63
5.13 Fault location, ITU-T recommendation, G.977/2015 65
5.14 Cyber security 67
5.15 Conclusion 68
5.16 Future work 69
References 70
Annex 1 ROTAKS 71

1 INTRODUCTION

1.1 The Research objective

The international community's ever-increasing reliance on the Internet and web-based information and communications technologies (ICT) has meant that cybersecurity is becoming one of the most pressing concerns in the 21st century. It's been 160 years since the world's first submarine cable linked a remote corner of Trinity Bay, Newfoundland, with Valentia Island on the west coast of Ireland in 1858. Between 2013 and 2017, the submarine cable industry has added an average of 32 percent of capacity annually on major submarine cable routes. Now ninety-nine per-cent of international data is transmitted by wires at the bottom of the ocean in sub-marine communications cables. In total, they are hundreds of thousands of miles long.

Cinia Ltd has set out to implement the Arctic Connect project at the initiative of the Finnish Ministry of Transport and Communications. The project explores the possibilities to construct a digital bridge between Europe and Asia via the Northeast Passage. This research project's prediction model includes key features and ad-hoc information about the capabilities for responding to issues in arctic connect.

With support, decision makers can make informed decisions. As an overall result, the project will contribute in geopolitical and other security sciences, information systems sciences, and produce the prototype in collaboration with commendable researchers from different branches of science and representatives of many significant security authorities in the country. The consortium parties the University of Jyväskylä, Hokkaido University and NATO Energy Security Centre of Excellence represent highest levels of knowledge on their respective fields and allow best possible analysis of threats.

The main research questions are:

What is the geopolitical situation in arctic?
What is strategic intelligence from Undersea Submarine Cable Network perspective?
How the international legal regime governing submarine cables?
What are the cyber security threats of the Undersea Submarine Cable Network?

The project consists of different subprojects (also described in Figure 1):

- Geopolitical analysis and strategic cyber intelligence (SP1),
- The International Legal Regime Governing Submarine Cables (SP2),
- Cyber security threats and protection in submarine cable systems (SP3)

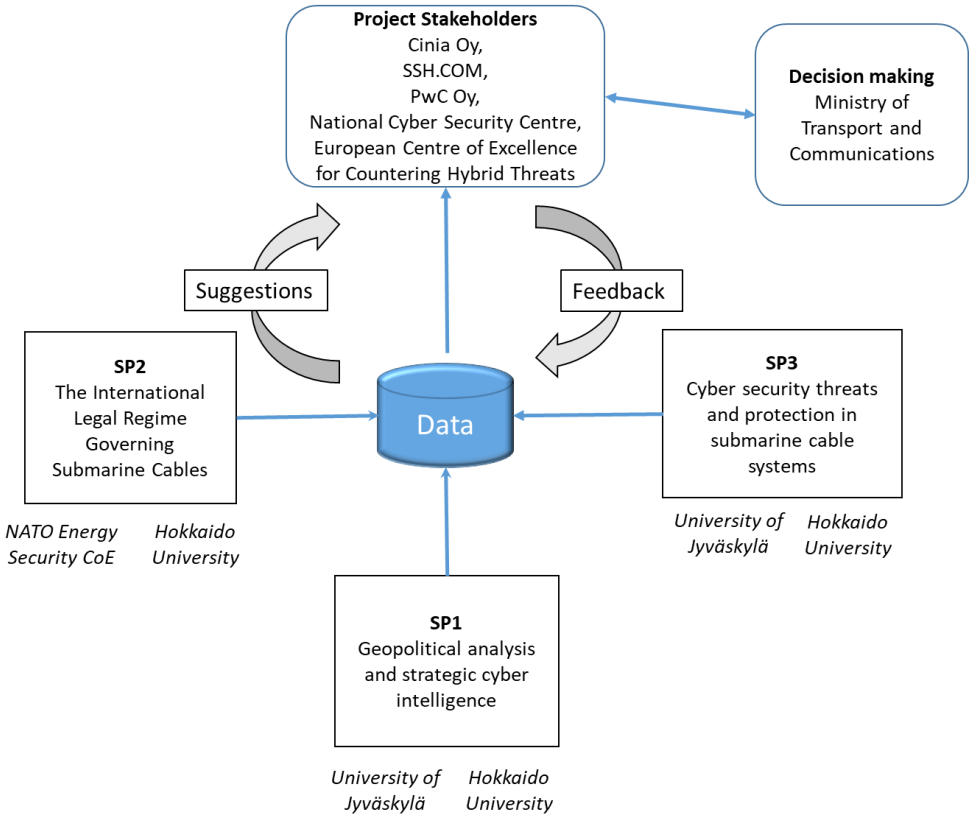


Fig 1. The structure of the research project

1.2 The Research organization

Principal Investigator: Martti Lehto, Professor, University of Jyväskylä, Jyväskylä, Finland

Subproject 1:
Leader: Martti J. Kari, University teacher and researcher, University of Jyväskylä, Jyväskylä, Finland
Contributors: Associate Professor Fujio Ohnishi, Hokkaido University, Sapporo, Japan, Assistant Professor Juha Saunavaara, Hokkaido University, Sapporo, Japan

Subproject 2:
Leader: Dr. Tadas Jakštas, NATO Energy Security CoE, Vilnius, Lithuania
Contributors: Associate Professor Fujio Ohnishi, Hokkaido University, Sapporo, Japan, Assistant Professor Juha Saunavaara, Hokkaido University, Sapporo, Japan

Subproject 3:
Leader: Aarne Hummelholm, Researcher, University of Jyväskylä, Jyväskylä, Finland
Contributors: Prof. Hiroyuki Minami, Hokkaido University, Sapporo, Japan
Associate Professor Katsuyoshi Iida, Hokkaido University, Sapporo, Japan

2 FINLAND SECURITY AND COMMUNICATIONS

2.1 Global security environment, and security in Finland

The submarine communication cables form a vast network on the seabed and transmit massive amounts of data across oceans. They provide over 95% of international telecommunications—not via satellites as is commonly assumed. The global submarine network is the "backbone" of the Internet, and enables the ubiquitous use of email, social media, phone and banking services.

The Arctic Connect project at the initiative of the Finnish Ministry of Transport and Communications. The project explores the possibilities to construct a digital bridge between Europe and Asia via the Northeast Passage.

The Arctic Connect project is part of the efforts to improve the connectivity in Arctic areas, in line with the objectives of the Arctic Council. The scale of the Arctic Connect project is extremely large. When completed, Arctic Connect would bring together three continents, which influence approximately 85 % of the world's population. In terms of technical capacity, the outset of the current plan is a total of six fiber pairs, a capacity of 60 Tbit/s and an overall length of approximately 18 000 km.

Arctic areas can be a game changer for global connectivity and therefore infrastructure investments and growth plans should be planned and developed with both private and public interests. There are 900 planned projects in the region requiring 1 trillion USD investments; need the infrastructure in the area is eminent. Building data centers in areas with renewable energy also provides growth and development. Data centers and cloud providers are an important part of the ecosystem together with operators.

The transition in the global operating environment and the establishment of a new order are estimated to take a long time. It is possible that the technological and financial transition will continue to be rapid for a long time, making it difficult to achieve a new and permanent balance. The control of global co-operation commons, such as space, the atmosphere, oceans and cyberspace, and the streams of interaction passing through them are becoming more important. With the recent developments in Russia, the threat of conflict between great powers has, in part, returned to the global security environment and may have impacts also to Finland's neighborhood. The return of geopolitics and the link between the complexity of internal and external security factors make the prediction more challenging. A possibility of hybrid warfare in our neighborhood underlines the need for

understanding the threat environment. The project “Arctic Connect Project and Cyber Security Control” seeks the solutions for these comprehensive challenges.

2.2 Finland is dependent of the secure global networks

The long-term adequate comprehensive situational awareness is the bedrock to anticipate and to manage the preventive actions taken by the different authorities. Due to Finland´s high dependence on global networks, an activity designed to ensure continuity in the operations of organizations and networks that provide critical infrastructure and services are priorities. Our economy increasingly depends on the functioning of international networks and logistics systems. The worst-case threat scenario is a situation where critical imported accessories or services, which are critical to avoid the predicted threats, are temporarily unavailable. It is necessary to assess and develop security more comprehensively than in the past and from the international perspective, taking into account all actors influencing the security.

2.3 Governmental intelligence affects national security solutions

Citizen’s overall sense of security is based on one of the nation’s vital functions, the psychological resilience to cope with crisis. The comprehensive understanding of the possible developments in our security environment will enable proactive and timely government communication offering correct situation-specific content. The project connects the information network, governmental intelligence and strategic preparedness to a comprehensive form.

Important principles in governmental communications are prediction of future events, transparency, reliability and speed, as well as equality and inter-activeness. When studying the citizens´ overall sense of security, (EcoHuCy-project concentrating on human security aspect) the cyber environment is a novel domain parallel with our physical environment. Individuals, public and private organizations alike depend on the cyber world. From the citizens using social media, to governmental vital actions, every sector of the society increasingly depends on technology and networked systems. This digital information technology society contains inherent vulnerabilities which may generate security risks to citizens, or the vital functions of the society. Without adequate awareness of the risks in cyber world, however, behavioral decisions and unseen threats can negatively impact the security of the critical infrastructure and can cause physical damage in the real world.

3 GEOPOLITICAL ANALYSIS AND STRATEGIC CYBER INTELLIGENCE

3.1 Geopolitical Analysis

3.1.1 Importance and role of Arctic cable

Geopolitics is the study of the effects of geography on politics and international relations. According to Foreign Affairs Magazine, the year 2014 was the year of the return of geopolitics. Russian forces seized Crimea, China made aggressive claims in its coastal waters, Japan responded with an increasingly assertive strategy, Iran tried to use its alliances with Syria and Hezbollah to dominate the Middle East, and old-fashioned power plays came back in international relations.[1]

At the level of international relations, geopolitics is a method of studying foreign policy to understand, explain and predict international political behavior through geographical variables. These include area studies, climate, topography, demography and natural resources. Oil and international competition over oil and gas resources has been one of the main areas of the geopolitics from 1950´s. According some statements, the world's most valuable resource is no longer oil, but data.[2]

Therefore, data and infrastructure to save, process and transfer the data will probably be main topics of geopolitics discuss. Important part of this infrastructure are telecommunication lines, especially undersea cables. Undersea cables have irreplaceable role for world´s economy and communication because 99 percent of all transoceanic data traffic goes through undersea cables, which is also faster than satellite transmissions, by up to eight-fold. The importance of undersea cables is increasing because of the need of the reliable and fast international communication channels. A large study on reliability of global undersea cable communications infrastructure, the Rogucci report[3] stated already almost decade ago, that

"There appears to be a gap between the growing dependence on international bandwidth and the reliability of its underpinning infrastructure at a global level. This is not so much that the reliability of the systems is any less, but that the dependence has grown so great. ... There is no sufficient alternative back up in the case of

---

[1] Mead, W. R., The Return of Geopolitics - The Revenge of the Revisionist Powers. Foreign Affairs, 2014

[2] Parkins, D., The world's most valuable resource is no longer oil, but data. The Economist, 2017.

[3] Rauscher, K. F., The ROGUCCI Study and Global Summit Report: Reliability of global undersea cable communications infrastructure, 2010.

catastrophic loss of regional or global connectivity. Satellites cannot handle the volume of traffic – the available capacity is not even close."

In this study, geopolitical analyses concentrate to China and Russia. China as the end-user of the planned Arctic cable, has a growing dependence on international bandwidth, it needs to improve his communication connections for example with Europe. The other area of interest of this analysis, Russia is the owner of the seabed for the Arctic cable and it has his own needs to improve communication connections in the Russian Arctic. While Japan is obviously another important end-user of the planned cable, it has not been analyzed as a part of this study. Japan's Arctic strategy does not specifically mention the Arctic submarine fiber-optic cable projects and the government's possibilities to influence the decisions of private companies interested in the Arctic are very limited. Furthermore, in the Japanese context, the planning and implementation of international submarine communication cable projects belong to the realm of private enterprises.

3.1.2 China as the end user of possible Arctic Cable

Possible Artic cable, connecting Europa with the East Asia and the North, is extremely important for both Europa and China. China's fast economic growth, active diplomacy and new international role are facts that should be understood as some of the instrumental factors affecting economic and other types of planning in Finland. Because of the increasing economic activities and entanglements – that owe a lot to the Chinese investors' interest in European technology and knowhow (including ICTs, data centers etc.).[4]

China also needs more reliable and faster communication connections with its cooperating partners. According to a recently published Chinese assessment, North America is the most important connection direction for China´s Internet services. However, Europe is another important destination for China's international communications services and the growth rate of data transfer between Asia and Europe is expected to be very high.[5]

Currently, there are terrestrial optical cable channels connecting China-Russia-Europe, China-Kazakhstan/Mongolia-Russia-Europe, and submarine cable channels (such as SWM3 and AAE-1) connecting China with Europe through Singapore, Red sea

---

[4] European Think-tank Network on China (ETNC), Chinese Investment in Europe. A Country-Level Approach, 2017.

[5] CAICT, China Academy of Information and Communications Technology. White Paper on China International Optical Cable Interconnection, 2018.

and Suez channel. It is expected that, at least in the medium and long term, there is a need for more connections between China and Europe6. Simultaneously, the ongoing trade disputes/trade war between China and the United States may also have effects on Europe and, potentially, initiate new demand for China-Europe connections.

China's white paper on Arctic policy, published in January 2018, demonstrates its interest in the region. Through this document China acknowledges that its Arctic interests are not only limited to scientific research but extend to a variety of commercial activities. While stressing the Arctic states sovereign rights and China's commitment to maintain the existing institutional and legal framework for Arctic governance, the white paper cites China's right to participate in Arctic affairs under the international law. The Arctic aspirations have also been bound to the Belt and Road Initiative, China's grand geopolitical strategy, through the introduction of the concept "Polar Silk Road", which is to facilitate connectivity and sustainable economic and social development of the Arctic.7 At the same time, it is worth noticing that the Belt and road Initiative is not only about the construction of physical infrastructure, but has included, among others, cooperation between Chinese and European companies in order to launch a global connection management platform aiming to accelerate the deployment of IoT solutions and services.[8]

The Arctic white paper makes also direct references to submarine cables. According to the document, China enjoys the freedom or rights of scientific research, navigation, overflight, fishing, laying of submarine cables and pipelines, and resource exploration and exploitation in the high seas, the Area and other relevant sea areas, and certain special areas in the Arctic Ocean, as stipulated in treaties such as the UNCLOS and the Spitsbergen Treaty, and general international law. 9 (The State Council, 2018)."

As shown by the table 1, China is behind for example the USA and Japan in number of submarine cables and international bandwidth and it sees that decreasing of this gap is important for maintain the economic growth.

---

[6] Ibid.

[7] The State C European Parliamentary Research Service (EPRS), Briefing: China's Arctic policy. How China aligns rights and interests. Council, The People's Republic of China (2018). Full text: China's Arctic Policy, 2018.

[8] Ericsson, China Telecom and Ericsson launch open IoT platform, July 5, 2017

[9] The State C European Parliamentary Research Service (EPRS), Briefing: China's Arctic policy. How China aligns rights and interests. Council, The People's Republic of China, 2018. Full text: China's Arctic Policy

Table 1. Comparison of submarine cables between China and major countries in the world[10]

	China	US	Japan	UK	Singapore
Number of submarine cables	10	80	23	53	24
Total international bandwidth in 2017 (Gbps)	43 445	201 527	38 799	151 066	46 544
Per capita international band width (Mbps)	0.031	0.618	0.306	2.289	8.297

3.1.3 Role of Russia in the project of Arctic cable

The law on the strategic planning of the Russian Federation (FZ-172 2014) defines the hierarchy of Russian official documents of strategic planning. The main documents of Russian strategic planning related with Arctic are Russian Arctic Policy (2008), Russian Arctic Strategy (2103) and Russian Arctic Plan 2016.[11]

President Medvedev signed in 2008 a document called *Fundamentals of the state policy of the Russian Federation in the Arctic for the period up to 2020 and beyond*, hereinafter Russian Arctic Policy 2008.[12] Russian Arctic Policy determines the main goals, main objectives, strategic priorities and mechanisms for implementing the state policy of the Russian Federation (RF) in the Arctic, as well as a system of measures for the strategic planning of the socio-economic development of the Arctic zone of the RF and ensuring Russia's national security.

Based on the Russian Arctic Policy was drafted a document called t*he development strategy of the Arctic zone of the Russian Federation and national security for the period up to 2020*, hereinafter Russian Arctic Strategy 2013[13]. The President Vladimir Putin approved this strategy in February 2013.

---

[10] TeleGeography and MIIT

[11] FZ-172, Strategic planning Act of Russian Federation. Федеральный закон от 28 июня 2014 г. N 172-ФЗ "О стратегическом планировании в Российской Федерации" (с изменениями и дополнениями).

[12] PP-1969, Основы государственной политики Российской Федерации в Арктике на период до 2020 года и дальнейшую перспективу. Fundamentals of the state policy of the Russian Federation in the Arctic for the period up to 2020 and beyond, 2008.

[13] PP-2013, Стратегия развития Арктической зоны Российской Федерации и обеспечения национальной безопасности на период до 2020 года. Strategy for the development of the Arctic zone of the Russian Federation and ensuring national security for the period up to 2020, 2013.

The Russian Arctic Strategy 2013 identifies the main mechanisms, methods and means of achieving the strategic goals and priorities for the sustainable development of the Arctic zone of the Russian Federation and ensuring national security. The strategy is aimed at the realization of the sovereignty and national interests of the Russian Federation in the Arctic and contributes to the solution of the main tasks of the state policy of the Russian Federation in the Arctic, defined in Russian Arctic Policy 2008.

In 2016, Prime Minister Medvedev signed *the implementation plan for the Strategy for the development of the Arctic zone of Russia and ensuring national security*, hereinafter Russian Arctic Plan 2016.[14] This implementation plan includes 80 events in six directions. One of the directions is development of information and telecommunication infrastructure.

In Russian Arctic Policy 2008, the Arctic zone of the RF is understood as a part of the Arctic, which includes all or part of the territory of the Sakha Republic (Yakutia), Murmansk and Arkhangelsk Regions, Krasnoyarsk Territory, Nenets, Yamalo-Nenets and Chukotka Autonomous Districts. The Arctic zone of the RF includes also the internal waters adjacent to these territories, lands and islands, the territorial sea, the exclusive economic zone and the continental shelf of the Russian Federation, within which Russia has sovereign rights and jurisdiction in accordance with international right.[15]

The main national interest of the RF in Arctic is to use of the Arctic zone of the RF as a strategic resource base, ensuring the solution of the tasks of the socio-economic development of the country. Russia's socio-economic interests in the Arctic are based on two things - natural resources and maritime transport.[16]

Arctic is important of Russian natural resources. More than 90% of Russian nickel and cobalt, 60% of copper, 96% platinum group metals and about 80% of gas and 60% of oil are extracted in Russian Arctic. Poor condition of infrastructure in the Arctic hinders exploitation of natural resources, reducing the attractiveness of the region's

---

[14] PP-2016, План мероприятий по реализации Стратегии развития Арктической зоны Российской Федерации и обеспечения национальной безопасности на период до 2020 года. Plan of measures to implement the Strategy for the development of the Arctic zone of the Russian Federation and ensure national security for the period up to 2020, 2016.

[15] PP-1969, 2008

[16] Ibid.

resources for development. The infrastructure is worse in the eastern part of Russia, which also contains more resources.[17]

The Northern Sea Route, in use for centuries and officially defined by Russian legislation, is an Arctic shipping route from the Barents Sea to the Bering Strait through Arctic waters. Travel along Northern Sea Route takes only one-third the distance needed to go through the Suez Canal. The route is currently open for up to eight weeks a year, and studies are predicting that climate change will lead to further reduction in Arctic ice, which can lead to greater use of the route. To secure the goals of Russian Arctic policy Russia maintain and increase military presence in the region as well as strengthen the border guard presence there.

The priority areas of development of the Arctic zone include: integrated socio-economic development of the region, the development of science and technology, the creation of modern information and telecommunications infrastructure, environmental security, international cooperation in the Arctic, military security, protection and protection of the state border of the Russian Federation in the Arctic.

Two possible arctic cable related objectives of the state policy of the RF in the Arctic is formation of a single information space of the RF in its Arctic zone, taking into account natural features and introduction of modern information and telecommunication technologies and means (including mobile) communications, broadcasting, management the movement of ships and flights of aviation. [18]

According to **Russian Arctic Strategy 2013,** the lack of a modern information and telecommunication infrastructure hinder Russia to provide telecommunications services to the population and business entities in Arctic zone of the RF. Lack of modern information and telecommunication infrastructure in the Russian Arctic has negative influence also to Russian defense capabilities in Arctic. There is a shortage of technical facilities and technological capabilities for the research, development and use of the Arctic spaces and resources, insufficient readiness for the transition to the innovative path of development of the Arctic zone.[19]

---

[17] SF-2016, Развитие российского законодательства об Арктической зоне и деятельность Совета Федерации. The development of Russian legislation on the Arctic zone and the activities of the Federation Council, 2016

[18] PP-1969, 2008

[19] PP, 2013

Comprehensive development of the Russian Arctic includes improving the quality of life of the population and the social conditions of economic by using advanced technologies, modernization and development of the infrastructure of the Arctic transport the system, modern information and telecommunications infrastructure and fisheries complex. The aim is to provide access of the population throughout the Russian Arctic zone to modern information and telecommunication services.[20]
In order to develop information technologies and communications and form a single information space in the Russian Arctic zone of the Russian Federation, the following measures are planned[21]:

- Introduction of modern information and telecommunication technologies and systems (including mobile) communications, broadcasting, traffic control of aircraft and flights of aviation
- Creation of a reliable system for the provision of communication services, navigation, hydro meteorological and information services
- Creation of a modern information and telecommunication infrastructure that allows the provision of telecommunications services to the population and business entities throughout the Russian Arctic zone, including by laying submarine fiber-optic communication lines along the Northern Sea Route and integrating with other networks

In the Russian Arctic Plan 2016 there is no clearly mentioned project for laying submarine fiber-optic communication lines along the Northern Sea Route. The measure 62 is establishing modern information telecommunication infrastructure allowing provide services communication to the public and business entities on throughout the Arctic zones of the Russian Federation. Responsible authorities for establishing this information telecommunication infrastructure are Ministry of Communications, Ministry of Defense and Roskosmos[22].

3.1.4 Conclusion

Because of fast economic growth, China needs more and more reliable communication infrastructure and is more depending on international bandwidth. One of the main counter partners of China is Europa. China is connected with Europe through two communication routes, land connection trough Kazakhstan and Russia and sea cables in the south, through Red sea and Suez channel. Both routes can be considered in some cases not reliable enough and that can cause a need for China to have more reliable route, or at least alternative to Europe. The trade war between

[20] Ibid.
[21] Ibid.
[22] Roscosmos (State Corporation for Space Activities) (Russian: Роскосмос), is a state corporation responsible for the space flight and cosmonautics program for the Russian Federation.

China and the USA may turn China more towards to Europe. All this might support the idea about Arctic cable connecting between China (and Japan) and Europe.

Russia has plans to develop his Arctic areas. These plans are related mainly to exploitation of natural resources and to development of the Arctic passage as a sea route for trade. To protect this, Russia has increased military activity and for example border guarding in Arctic areas. All this requires, as is said in Russian Arctic Policy and Strategy, modern information and telecommunication technologies, including by laying submarine fiber-optic communication lines along the Northern Sea Route and integrating with other networks. Russia has a need for the fiber-optic communication line connecting Arctic areas, but Russia has not own technology to fulfill these needs.

3.2 Strategic Cyber Intelligence

3.2.1 Strategic intelligence

Strategic intelligence means collection, processing, analysis, and dissemination of strategic level intelligence that is required for forming policy and military plans at the national and international level. This intelligence can include both threats and possibilities, depending on situation. Strategic intelligence´s sources have traditionally been Human Intelligence (HUMINT) and Signal Intelligence (SIGINT). During last ten years, Cyberspace has become an important source for strategic intelligence and today computer networks are one of the main environments for collection intelligence, including strategic intelligence. Strategic intelligence includes the following system of abilities:[23]

- Foresight, the ability to understand trends that present threats or opportunities for an organization;
- Visioning, the ability to conceptualize an ideal future state based on foresight and create a process to engage others to implement it
- System thinking, the ability to perceive, synthesize, and integrate elements that function as a whole to achieve a common purpose.
- Motivating, the ability to motivate different people to work together to implement a vision. Understanding what motivates people is based upon another ability, personality intelligence
- Collaborating, the ability to develop strategic alliances with individuals, groups and organizations. This quality also depends on personality intelligence

[23] Maccoby, Michael, Successful Leaders Employ Strategic Intelligence, Research Technology Management, Volume 44. No. 3. May-June 2001. pp. 58-60

Most important tasks for strategic intelligence are early warning about strategic level threats and threat actors and possibilities and achieve time for decision makers.

3.2.2 Cyberspace and Cyberspace Operations cables system

Cyberspace is interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[24]

Cyberspace has become geopolitical entity and part of geopolitical analysis because of digitalization, geographic attributes of cyberspace architecture and role and power of sovereign states in the cyberspace. Cyberspace has become an environment of geopolitical competition. Digitalization and increasing importance of cyberspace to strategic and state level communications has become a national security concern for governments. This has also made Strategic Cyber Intelligence (SCI) and capabilities to counter SCI vital for state in global relations.

In recent years, the cyber space has turn into the fifth domain of warfare. NATO Warsaw summit in June 2016, declared cyberspace as a warfare domain in which NATO must defend itself. In addition, according to Russian authorities, the formation of cyber space as a warfare domain poses a threat to Russia's national interests. Both offensive and defensive cyber space operations have become a part of the operative practices in many countries. Some offensive cyber space operations are implemented and are under implementation already in the peacetime. For example, cyberspace exploitation, i.e. cyber intelligence or cyber espionage is a part of intelligence gathering processes. The importance of cyber space exploitation as a way of intelligence collection has been increased because communication is transferred more and more in cyber environment.

Geopolitical thinking has influence on cyber security discourse and policy and power struggle and geopolitical competition, and militarization have started already in cyberspace, especially between the USA and Russia and China. China and Russia have highlighted that, states have the same right to cyberspace sovereignty, or to digital sovereignty, as they have had in traditional way. This has caused partial overlapping

---

[24] NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, 2018.

of man-made cyberspace boundaries and geopolitical boundaries and geopoliticized cyberspace.[25]

An information system (IS) is a combination of hardware, software, infrastructure and trained personnel organized to facilitate planning, operative activity, control and decision-making in an organization by collection, organization, storage and communication of information. Information system can also be described as a combination of hardware, software, data, business process and functions, which can be used to increase efficiency and management of an organization.
Cyber threats to strategic communications have not only tactical but also strategic level geographical impact for state security or organization´s activities. Cyberspace is asymmetric environment and its use for crime, espionage and other cyber activities has been increased. Difficulties in attribution, the low cost of entry, the legal ambiguity has made cyberspace an attractive domain for nation-states as well as non-state actors in cyber conflict.

3.2.3 Strategic cyber intelligence

Cyberspace operations (CO) are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. CO comprise the military, national intelligence, and ordinary business operations in and through cyberspace. Cyberspace operations are divided in JP 3-12.[26]

- Offensive Cyberspace Operations (OCO)
- Defensive Cyberspace Operations (DCO)
- DODIN

Offensive cyberspace operations (OCO) are CO missions intended to project power in and through foreign cyberspace through actions taken in support national objectives. OCO consist of cyberspace attacks and cyberspace exploitation. Cyberspace attack creates noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial effects in the physical domains. Unlike cyberspace exploitation actions, which are often intended to remain clandestine to be effective, cyberspace attack actions will be apparent to system operators or users, either immediately or eventually, since they remove some user functionality.[27]

---

[25] Cai, Cuihong, Geopolitics in the cyberspace: a new perspective on U.S.-China relations, 2018.
[26] JP 3-12, Joint Publication 3-12 Cyberspace Operations, 2018.
[27] Ibid.

Cyberspace exploitation includes intelligence activities, maneuver and information collection. Cyberspace exploitation includes all actions in neutral or target cyberspace that do not create cyberspace attack effects. Cyberspace exploitation includes activities to gain intelligence through actions such as gaining and maintaining access to networks, systems, and nodes of military value; maneuvering to positions of advantage; and positioning cyberspace capabilities to facilitate follow-on actions.[28] Cyberspace exploitation can be called also as cyber espionage or cyber intelligence.

Defensive Cyberspace operations (DCO) are executed to defend own networks, or another cyberspace. They are intended to preserve the ability to utilize own cyberspace capabilities and protect data, networks, cyberspace-enabled devices, and other designated systems by defeating on-going or imminent malicious cyberspace activity. DCO missions are conducted in response to specific threats of attack, exploitation, or other effects of malicious cyberspace activity and leverage information from maneuver, intelligence collection, counterintelligence (CI), law enforcement (LE), and other sources as required. [29]

The US adds a Department of Defense Information Network (DoDIN) Operations mission category to OCO and DCO. US cyber forces use cyberspace security actions, that are network focused and threat agnostic to accomplish the DoDIN Operations mission. The DODIN operations mission includes operational actions taken to secure, configure, operate, extend, maintain, and sustain DOD cyberspace and to create and preserve the confidentiality, availability, and integrity of the DODIN. [30] Each armed force implements threat agnostic cyber security and resilience.

Digitalization and increasing importance of cyberspace to strategic and state level communications has become a national security concern for governments. This has also made Strategic Cyber Intelligence (SCI) and capabilities to counter SCI vital for state in global relations. Cyber threats to strategic communications have not only tactical but also strategic level geographical impact for state security or organization´s activities. Cyberspace is asymmetric environment and its use for crime, espionage and other cyber activities has been increased. Difficulties in attribution, the low cost of entry, the legal ambiguity has made cyberspace an attractive domain for nation-states as well as non-state actors in cyber conflict.

Strategic cyber intelligence is strategic level cyberspace exploitation, which includes collection, analysis and dissemination of information, which is not available in other

---

[28] Ibid.
[29] Ibid.
[30] Ibid.

means, in and from information systems. Information can help governmental and business organizations understand the type, methods and means, targets and subjects of threats or possibilities in the strategic level. This intelligence enables organizations to plan and implement their activities. The main aim is to gain reliable information and time for strategic decision making of these organizations. Strategic cyber intelligence can be defensive or offensive.

Strategic defensive cyber intelligence provides a big picture at how threat and attacks are changing over time. It may be able to identify historical trends, motivations, or attributions as to who is behind a cyber-attack or an operation. Accurate defensive strategic intelligence is a starting point for deciding which defensive measures will be most effective. Strategic defensive cyber intelligence can include information on the following topic areas:

- Political, technical and juridical attribution for intrusions and data breaches
- Attack and attacker group descriptions and trends
- Attack vector and targeting trends of attacks for industry sectors and geographies
- Mapping cyber-attacks and cyber espionage to geopolitical conflicts and events as for example Russia- USA, South China Sea, Arab Spring, Russia-Ukraine
- Global statistics and analysis on breaches, malware and information theft
- Major attacker Tactics, Techniques, and Procedures (TTP) changes over time

Strategic offensive cyber intelligence collects strategic level information in and through the cyberspace.

3.2.4 Intelligence Collection from Submarine Communication Cables

Submarine communication cables have been important for strategic communication since the mid-19th century, and fiber optics in the 1990s made modern sea cabling even more critical. Nowadays sea cables transfer nearly all our global telecommunications data. Questions concerning national security and cybersecurity have always been relevant from the perspective of the development of submarine communications networks. Security concerns have not only affected decisions concerning the route and landings, but also used as arguments when, in different parts of the history, the role of cable networks and wireless solutions have been debated. Furthermore, security concerns have hindered, for example, plans aiming at the utilization of submarine fiber-optic infrastructure for scientific purposes[31].

[31] Starosielski N., The undersea network. Duke University Press, Durham and London, 2015.

During the early days of the history of submarine cables, the terrestrial links and coastal segments were considered as the weakest and most vulnerable parts vis-à-vis the external security threats. However, the underwater cables, which cannot be kept under constant surveillance, have been targeted by intelligence services since the beginning of the 20th century. As a part of operations, military has cut the cables of the other sides to redirect the information, flow into cables that were being monitored their own intelligence service.

Collecting intelligence from the undersea communication cables and from equipment and facilities related with the cables can be done by cable collection, i.e. by tapping or by hacking, i.e. by infiltrating by malware to the system. Cable collection**,** i.e. tapping is routine activity of intelligence and security services of super powers. They have intention and need, technical equipment and skills and practice to collect intelligence from cables.

United Kingdom managed to cut German cables in the beginning of First World War and redirect the traffic between Germany and America through the cables, which were in UK. UK Intelligence managed to intercept from the cable and to decrypt so-called Zimmermann telegram in January 1917, which was send from German Foreign Ministry to German Ambassador in Mexico. In telegram, Germany proposed a military alliance between Germany and Mexico in the event, that the US entered World War I against Germany Mexico would recover Texas, Arizona and New Mexico.

During the Cold War, the US Navy and NSA successfully placed wiretaps, i.e. intelligence collection devices on Soviet underwater communication lines in Sea of Okhotsk during Operation Ivy Bells in 1970s. Modified submarine USS Halibut delivered divers close to the cable. The divers were able to locate the cable in the depth of 120 meters. The divers installed a six-meter long intelligence collection device around the cable without causing any damage to the cable. Divers retrieved once in a month collected recordings and installed a new set of tapes. The recordings were delivered to the NSA for processing. The tapes recorded revealed that the Soviets were so sure of the cable's security that the majority of the conversations made over it were unencrypted. After a defector had revealed operation Ivy Bells in the beginning 1980s, Soviet Navy removed the intelligence collection device from the cable.

Both the USA and Russia have intention and need, technical equipment and skills and practice to collect intelligence from undersea cables also in the demanding environment, including the Arctic. Cable collection is technically possible in the bottom of the sea and in the points, where the cable is not in the bottom of sea, i.e.

on the ground, in practice in the points where the traffic is amplified or where there is another physical access to the cable (for example in tele operator facilities). The USA and Russia has equipment to deliver intelligence collection devices to the undersea cable.

According to open source reports, the modified Seawolf-class submarine USS Jimmy Carter is almost certainly able to tap the undersea communication cables. In USS Jimmy Carter is constructed multimission platform, which enables the use of Remotely Operated Underwater Vehicle (ROV). ROV can be used for installing tapping devices to undersea communications cables. Even this is technically possible; some experts consider this kind of intelligence collection too risky and expensive.[32]

The Russia´s Defense Ministry Main Directorate of Deep-Sea Research (Russian abbreviation GUGI), Military Unit 40056 is responsible for Russian 'underwater engineering'. The task of this unit is to bug communications cables, install movement sensors, and collect the wreckage of ships, aircraft, and satellites from the seabed. These divers work at depths of 3000-6000 meters in miniature submarines. One of the ships of GUGI is special purpose intelligence collection ship Yantar. To the equipment of belongs Yantar devices that are designed for deep-sea tracking, as well as equipment for connecting to top-secret communication cables.[33]

The home port of Yantar is Severomorsk in Kola Peninsula. Yantar can act as a mothership to Rus- (AS-37) and Konsul- (AS-39) class deep diving submersibles, which can operate at depth up to 6000 meters. (Peter, 2018). Yantar can also be used as a mothership for ARS-600 deep diving manned submersible, which can operate at 600 meters.[34]

Hacking is the other way to collect intelligence from the undersea cables. All the main intelligence services have access to undersea cable system by hacking remote controlled network manage systems. Equipment like Reconfigurable Optical Add/Drop Multiplexers (ROADM) in control facilities of submarine cable systems can be remotely manipulated for either intelligence collection or malicious activity (malware etc.) as cutting the connection in the cable. In addition, some non-state actors might have capabilities to intrude to submarine communication cable at least in the landing stations.

---

[32] Axe, D., The Navy's underwater eavesdropper, 2013.
[33] Parlamentskaja Gazeta, Корабль спецназначения «Янтарь» вошёл в Среди-земное море, 2016
[34] Sutton, H., Russian ship loitering near undersea cables, 2017.

Intelligence collection from Arctic Connection (AC) subsystems can be done by tapping, exploiting optical overflow or hacking control systems of AC. Tapping means connecting/installing tapping device(s) i.e. intelligence collection device to the cable or to the fiber pair either on the ground, in a landing point, in points where the traffic is amplified or in the sea bed. Exploiting of optical overflow can be done either in the cross-connection's points of fiber pairs/cable or from one fiber pair to another. Intelligence operator can also intrude to the control systems of AC by malware.

If for example Russian Intelligence is tapping the AC 3Continentals Subsystem, the best geographical area to install tapping device to the cable in the West is in the Russian territorial waters but before the first connection of Russian Subsystem (Teriberka) to the cable, or after the first repeater/amplifier. The connection before the Russian subsystem enable the intelligence collection from fiber pairs 1-4 of the 3Continents Subsystem without interference of the traffic of Russian subsystem traffic.
In the East, the same kind of exclusion is possible by collecting the traffic of the 3Continents Subsystem after Vladivostok, when in the cable there is no (Russian) traffic between Murmansk - Vladivostok. Another option is to install tapping device after repeater/amplifier or amplifiers. This is plausible, if subsystems share amplifiers and possible, if they use their own amplifiers. The geographical area of installation of tapping device depends on the depth of the sea and the distance of the installation place from the mainland. Deep sea complicates the installation of tapping device. The distance from the tapping device to the mainland, where the remote-control unit and the selectors are, should be as short as possible for practical reasons.

The third option to collect intelligence from the 3Continents Subsystem of the AC is to hack, i.e. to intrude to the control systems of the 3Continents Subsystem or to the control systems of Russian Subsystem of the AC depending on the attacker.

In some cases, the undersea cables can also be used to collect intelligence and other information. For example, the so-called "dual-purpose" undersea cables refer to the identified possibilities to utilize submarine fiber-optic cables for scientific purposes, without disturbing their primary functions. The dual-purpose cables could be constructed by putting sensors on the repeaters of new transoceanic cables as they are laid. The sensors could collect a range of data about, for example, the movement of ocean currents; levels of oxygen and greenhouse gases; seismic movements; temperature; geophysical, biological and chemical data; and even underwater video.

The proponents of the dual-purpose cable have argued that, with only a slight modification of the existing system, the companies could build a network that would monitor for tsunamis and rises in sea level. Concerns over the reliability and unresolved questions concerning funding have been the major obstacles preventing the implementation of various plans, the idea of transferring commercial transoceanic cables into remote sensing technologies have raised security concerns as well. These cables could also be used for military surveillance.[35]

Meanwhile, researchers have recently introduced a new way, how the existing submarine telecommunications network could be used in order to create a global, real-time seismic network if the fiber itself is used as the sensing element. The basic idea is that the submarine cables could be used to detect, for example, earthquakes even without adding sensors in the submarine part of the cable (e.g. repeaters). The optical fibers can detect seismic events using Distributed Acoustic Sensing techniques (DAS). DAS systems use backscatter of the injected optical signal to extract information about local perturbations along the fiber. Traditional DAS has severe limitations concerning its useable range, but researchers seem to have found ways to extend it. In addition to this, it has been shown that, one can exploit the sensitivity to environmentally induced perturbations to detect seismic waves, vibration, and any other source of other acoustic noise.

The experiment that was introduced in Science in 2018 used light from an Ultra-Low Expansion (ULE) cavity stabilized laser, which was injected at one end of a submarine optical link that consisted of a fiber pair, one fiber used for each direction of propagation. Two fibers were connected at the far end of the optical link to form a loop such that the light returned to the transmitter after a round trip. The injected and returned optical signals were combined on a photodetector and their phase difference was measured. The seismically induced phase changes of the returned optical signal detected local and remote earthquakes. In their conclusions, researchers propose that the submarine fiber networks could also be used for applications beyond seismic monitoring, from marine mammal migration tracking to sea noise pollution monitoring.[36]

The new technological solution proposed seems to offer some solutions for the earlier problems concerning the dual-purpose approach. It would include all existing cables, not only systems to be build, it would be cheaper method and it would not

---

[35] Starosielski N., The undersea network. Duke University Press, Durham and London, 2015.

[36] Marra, G; Clivati, C; Luckett, R; Tampellini, A; Kronjäger, J; Wright, L; Mura, A; Levi, F; Robinson, S; Xuereb, A; Baptie, B; Calonico, D., Ultrastable laser interferometry for earthquake detection with terrestrial and submarine cables. Science 14 Jun 2018.

compromise the reliability of the repeaters. However, the potential security concerns are yet to be debated.

3.2.5 Conclusion

Collection of intelligence from undersea communication cables, i.e. hacking or sniffing a fiber optic cable by tapping cable under the water or at a landing station had to be taken in to the consideration. All the states through area, which the cable is running, have interest, motivation and technical capabilities to collect intelligence information from these cables at least in the points, where the cable is on the land. Point-to-point encryption is one way to fight against the intelligence collection from undersea communication cables.

REFERENCES

1. Axe, D., The Navy's underwater eavesdropper. 2013. http://blogs.reuters.com/great-debate/2013/07/18/the-navys-underwater-eavesdropper/
2. CAICT, China Academy of Information and Communications Technology. White Paper on China International Optical Cable Interconnection, 2018. http://www.caict.ac.cn/english/yjcg/bps/201808/P020180829385778461678.pdf
3. Cai, C., Geopolitics in the cyberspace: a new perspective on U.S.-China relations, 2018. http://jtp.cnki.net/bilingual/detail/html/GJZY201801001#341
4. Ericsson, China Telecom and Ericsson launch open IoT platform, July 5, 2017. https://www.ericsson.com/en/press-releases/2017/7/china-telecom-and-ericsson-launch-open-iot-platform
5. European Parliamentary Research Service (EPRS), Briefing: China's Arctic policy. How China aligns rights and interests, 2018.
6. http://www.europarl.europa.eu/RegData/etudes/BRIE/2018/620231/EPRS_BRI(2018)620231_EN.pdf
7. European Think-tank Network on China (ETNC), Chinese Investment in Europe. A Country-Level Approach, 2017. https://www.ifri.org/sites/default/files/atoms/files/etnc_reports_2017_final_20dec2017.pdf
8. FZ-172, Strategic planning Act of Russian Federation. Федеральный закон от 28 июня 2014 г. N 172-ФЗ "О стратегическом планировании в Российской Федерации" (с изменениями и дополнениями). http://base.garant.ru/70684666/
9. Ivanov, M., Россия построит собственную трансарктическую кабельную систему, 2011. http://archive.li/1gEdM
10. JP 3-12, Joint Publication 3-12 Cyberspace Operations, 2018. https://fas.org/irp/doddir/dod/jp3_12.pdf
11. Maccoby, M., Successful Leaders Employ Strategic Intelligence, Research Technology Management, Volume 44. No. 3. May-June 2001. pp. 58-60.
12. Marra, G., Clivati, C., Luckett, R., Tampellini, A., Kronjäger, J., Wright, L., Mura, A., Levi, F., Robinson, S., Xuereb, A., Baptie, B., Calonico, D., Ultrastable laser interferometry for earthquake detection with terrestrial and submarine cables. Science 14 Jun 2018. http://science.sciencemag.org/content/early/2018/06/13/science.aat4458.full
13. Mead, W. R., The Return of Geopolitics - The Revenge of the Revisionist Powers. Foreign Affairs, 2014. https://www.foreignaffairs.com/articles/china/2014-04-17/return-geopolitics
14. Navy Recognition, Russian Navy to lay fiber optic cables to connect Arctic and Far East. Navy Recognition, April 25, 2018. http://www.navyrecognition.com/index.php/news/defen ce-

news/2018/april-2018-navy-naval-defense-news/6161-russian-navy-to-lay-fiber-optic-cables-to-connect-arctic-and-far-east.html

15. Nilsen, T., Russia plans to lay trans-Arctic fiber cable linking military installations. The Independent Barents Observer, April 24, 2018. https://thebarentsobserver.com/en/security/2018/04/russia-slated-lay-military-trans-arctic-fibre-cable
16. NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, 2018. https://csrc.nist.gov/publications/detail/sp/800-39/final
17. Parkins D., The world's most valuable resource is no longer oil, but data. The Economist, 2017. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data
18. Parlamentskaja Gazeta, Корабль спецназначения «Янтарь» вошёл в Средиземное море, 2016. https://www.pnp.ru/politics/korabl-specnaznacheniya-yantar-voshyol-v-sredizemnoe-more.html
19. PP-1969, Основы государственной политики Российской Федерации в Арктике на период до 2020 года и дальнейшую перспективу. Fundamentals of the state policy of the Russian Federation in the Arctic for the period up to 2020 and beyond, 2008. https://rg.ru/2009/03/30/arktika-osnovy-dok.html
20. PP-2013, Стратегия развития Арктической зоны Российской Федерации и обеспечения национальной безопасности на период до 2020 года. Strategy for the development of the Arctic zone of the Russian Federation and ensuring national security for the period up to 2020, 2013. http://legalacts.ru/doc/strategija-razvitija-arkticheskoi-zony-rossiiskoi-federatsii-i/
21. PP-2016, План мероприятий по реализации Стратегии развития Арктической зоны Российской Федерации и обеспечения национальной безопасности на период до 2020 года. Plan of measures to implement the Strategy for the development of the Arctic zone of the Russian Federation and ensure national security for the period up to 2020, 2016. http://static.government.ru/media/files/ObB3ODIP9rOAwfYbgWrOzHIxaHTla8s1.pdf
22. Rauscher, K. F., The ROGUCCI Study and Global Summit Report: Reliability of global undersea cable communications infrastructure, 2010. http://www.ieee-rogucci.org/files/The%20ROGUCCI%20Report.pdf
23. SF-2016, Развитие российского законодательства об Арктической зоне и деятельность Совета Федерации. The development of Russian legislation on the Arctic zone and the activities of the Federation Council, 2016. http://council.gov.ru/media/files/41d58bd72efd2e881a12.pdf
24. Sib.FM-2011, Высокоскоростной интернет появится на севере Сибири к 2014 году, 2011. http://sib.fm/news/2012/04/02/vysokoskorostnoj-internet-na-severe-sibiri-k-2014-godu
25. Starosielski N., The undersea network. Duke University Press, Durham and London, 2015.

26. Sutton, H., 2017, Russian ship loitering near undersea cables, 2017. http://www.hisutton.com/Yantar.html

4 THE INTERNATIONAL LEGAL REGIME GOVERNING SUBMARINE CABLES

4.1 The main international legal regimes governing submarine cables

Three international legal regimes regulate the governance of submarine cables during peacetime, conduct of hostilities, and during the use of force.

Between 1884 and 1982, international community adopted four international instruments which set out substantive provisions on the rights and obligations of States related to submarine cables. These are:[37]

1. The 1884 Convention for the Protection of Submarine Telegraph Cables;
2. The 1958 Geneva Convention on the High Seas;
3. The 1958 Convention on the Continental Shelf; and
4. The 1982 United Nations Convention on the Law of the Sea (UNCLOS).

Apart from these four main international documents, there are also other international conventions and treaties that may apply to submarine cables, such the 1972 Convention on the International Regulations for Preventing Collision at Sea[38], the 1972 Convention on the Prevention of Marine Pollution by Dumping from Wastes and Other Matter[39], the 1997 International Convention for the Suppression of Terrorist Bombings[40], the 2001 Convention on Cybercrime[41], the 1992 Constitution of the International Telecommunication Union[42].

---

[37] Davenport, Tara, Beckman, Robert C., Burnett, Douglas R., "Submarine Cables: The Handbook of Law and Policy", (Leiden, Boston: Martinus Nijhoff Publishers, 2014), pp 64.

[38] The 1972 Convention on the International Regulations for Preventing Collision at Sea, https://treaties.un.org/doc/Publication/UNTS/Volume%201050/volume-1050-I-15824-English.pdf

[39] The 1972 Convention on the Prevention of Marine Pollution by Dumping from Wastes and Other Matter, https://treaties.un.org/doc/publication/unts/volume%201046/volume-1046-i-15749-english.pdf

[40] The 1997 International Convention for the Suppression of Terrorist Bombings, https://treaties.un.org/doc/Treaties/1997/12/19971215%2007-07%20AM/ch_XVIII_9p.pdf

[41] The 2001 Convention on Cybercrime, https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

[42] The 1992 Constitution of the International Telecommunication Union, https://www.itu.int/council/pd/constitution.html

The law of armed conflict including Geneva Conventions of 1949 and Additional Protocols I, II to the Geneva Conventions of 1977, Hague Convention XIII[43] applies to submarine cables during both international and non-international armed conflicts. The UN Chapter applies to submarine cables in the case of the use of force and the right of self-defence, regardless of the weapons employed.[44]

4.1.1 International peacetime legal regime

4.1.1.1 The 1884 Convention for the Protection of Submarine Telegraph Cables

The 1884 Cable Convention with 40 State Parties was the first international treaty governing submarine telegraph cables.[45] The Cable Convention applies outside territorial waters to all submarine cables landed on the territories, colonies or possessions of one or more of the High Contracting parties.[46] The Convention applies to all submarine cables beyond national jurisdiction.[47] Article XV of the Cable Convention indicated that the stipulations of the present Convention do not in any way restrict the freedom of action of belligerents.[48] The convention's primary goal was to require State adoption of legislation that protected cables laying outside of territorial waters.[49]

The 1884 Cable Convention contains three provisions relating to breakage or injury of cables.[50] First, Article II provides that it is a punishable offence to break or injure a cable, wilfully or by culpable negligence, in such a manner as might interrupt or obstruct telegraphic communications, either wholly or partially, such punishment being without prejudice to any civil action for damages. This provision does not apply

---

[43] Treaties, States Parties and Commentaries, International Committee of the Red Cross, https://ihl-databases.icrc.org/ihl

[44] United Nations Charter, 26 June 1945, http://www.un.org/en/sections/un-charter/chapter-vii/index.html; Nuclear Weapons advisory opinion: Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 ICJ 226 (8 July), para. 39, http://www.icj-cij.org/files/case-related/95/095-19960708-ADV-01-00-EN.pdf

[45] Davenport, Tara, Beckman, Robert C., Burnett, Douglas R., "*Submarine Cables: The Handbook of Law and Policy*", (Leiden, Boston: Martinus Nijhoff Publishers, 2014), 65.

[46] The 1884 Convention for the Protection of Submarine Telegraph Cables, Art. 1, https://cil.nus.edu.sg/wp-content/uploads/formidable/18/1884-Convention-for-the-Protection-of-Submarine-Telegraph-Cables.pdf r

[47] Stuart Kaye, International Measures to Protect Oil Platforms, Pipelines, and Submarine Cables from Attack, 31 Tul. Mar. L.J. 377 (2007), 396.

[48] Ibid, Art. 15

[49] Davenport Tara, Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis, 24 Cath. U. J. L. & Tech 57 (2015), 67.

[50] Davenport, Tara, Beckman, Robert C., Burnett, Douglas R., "*Submarine Cables: The Handbook of Law and Policy*", (Leiden, Boston: Martinus Nijhoff Publishers, 2014), 67.

to cases where those who break or injure a cable do so with the lawful object of saving their lives or their ship, after they have taken every necessary precaution to avoid so breaking or injuring the cable.[51]

Prosecution of these offences rested with the flag state of the offending vessel.[52] The tribunals competent to take cognizance of infractions of the Cable Convention are those of the country to which the vessel on board of which the offence was committed belong or so far as the subjects and citizens of those States respectively are concerned, with the general rules of criminal jurisdiction prescribed by the laws of that particular State, or by international treaties.[53]

Offences against the present Convention may be verified of proof allowed by the legislation of the country of the court. Article X further anticipates that a warship could conduct a right of visit against a vessel when there was reasonable suspicion of a cable violation.[54] When the officers commanding the ships of war, or ships specially commissioned for the purpose by one of the High Contracting Parties, have reason to believe that an infraction of the measures provided for in the present Convention has been committed by a vessel other than a vessel of war, they may demand from the captain or master the production of the official documents proving the nationality of the said vessel.[55] It may be verified through investigation with the flag State and witness statements.[56]

The second provision dealing with breakage or injury to cables is Article IV which addresses damage to cables in the situation of cable crossings.[57] The owner of a cable who, on laying or repairing his own cable, breaks or injures another cable, must bear

---

[51] The 1884 Convention for the Protection of Submarine Telegraph Cables, Art. 2, https://cil.nus.edu.sg/wp-content/uploads/formidable/18/1884-Convention-for-the-Protection-of-Submarine-Telegraph-Cables.pdf r

[52] Klein N., "*Maritime Security and the Law of the Sea*", UK: Oxford University Press, 2011), 101.

[53] The 1884 Convention for the Protection of Submarine Telegraph Cables, Art. 7, https://cil.nus.edu.sg/wp-content/uploads/formidable/18/1884-Convention-for-the-Protection-of-Submarine-Telegraph-Cables.pdf r

[54] Klein, N. "*Maritime Security and the Law of the Sea*", UK: Oxford University Press, 2011), 101.

[55] Ibid, Art. 10

[56] Schmitt Michael N., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (UK: Cambridge University Press, 2017), 257. "In 1959, the United States invoked Article 10 to board and investigate the Soviet trawler Novorossiisk for damaging five transatlantic cables. With the master's consent, a US warship inspected the vessel, and determined that there was a 'strong presumption' that the Novorossiisk violated the proscription in Article 2 of the Convention against intentional, wilful, or culpably negligent breaking or injuring a submarine cable", Ibid p. 257

[57] Davenport, Tara, Beckman, Robert C., Burnett, Douglas R., "*Submarine Cables: The Handbook of Law and Policy*", (Leiden, Boston: Martinus Nijhoff Publishers, 2014), 67.

the cost of repairing the breakage or injury.[58] The third provision on breaking or injury to cables is Article VII.[59] Owners of ships or vessels who can prove that they have sacrificed an anchor, a net or other fishing gear in order to avoid injuring a submarine cable, shall receive compensation from the owner of the cable.[60]

The Cable Convention also has provisions on the protection of cable ships engaged in laying and repairing operations. Article V of the Convention requires that vessels maintain a distance of one nautical mile from a cable ship laying cable. Article VI requires vessels to maintain a safety distance of one-quarter nm from a cable repair buoy.[61]

4.1.1.2 The 1958 Geneva Convention on the High Seas and the 1958 Convention on the Continental Shelf

The 1958 Geneva Conventions on the High Seas and the Continental Shelf, that are ratified by 63 and 58 State Parties respectively, are broad, comprehensive treaties that address various aspects of the law of the sea.[62]

The 1958 Convention on the Continental Shelf and the 1958 Convention on the High Seas contain provisions on the protection of submarine cables and the freedom to lay cables. The three provisions from the 1884 Cable Convention on the protection of cables (articles II, IV and VII) were adopted in the High Seas Convention in Articles 27, 28, 29.[63] Article 27 of the 1958 High Seas Convention then extended this protection to telephonic cables, high-voltage power cables, and submarine pipelines.[64]

Regarding the freedom to lay cables, both the High Seas Convention and Continental Shelf Convention recognized the freedom to lay cables in high seas, a right to take

---

[58] The 1884 Convention for the Protection of Submarine Telegraph Cables, Art. 4, https://cil.nus.edu.sg/wp-content/uploads/formidable/18/1884-Convention-for-the-Protection-of-Submarine-Telegraph-Cables.pdf r

[59] Davenport, Tara, Beckman, Robert C., Burnett, Douglas R., "*Submarine Cables: The Handbook of Law and Policy*", (Leiden, Boston: Martinus Nijhoff Publishers, 2014), 68.

[60] The 1884 Convention for the Protection of Submarine Telegraph Cables, Art. 7, https://cil.nus.edu.sg/wp-content/uploads/formidable/18/1884-Convention-for-the-Protection-of-Submarine-Telegraph-Cables.pdf r

[61] Davenport, Tara, Beckman, Robert C., Burnett, Douglas R., "*Submarine Cables: The Handbook of Law and Policy*", (Leiden, Boston: Martinus Nijhoff Publishers, 2014), 69.

[62] Davenport, Tara, Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis, 24 Cath. U. J. L. & Tech 57 (2015), 67.

[63] Davenport, Tara, Beckman, Robert C., Burnett, Douglas R., "*Submarine Cables: The Handbook of Law and Policy*", (Leiden, Boston: Martinus Nijhoff Publishers, 2014), 72.

[64] Klein, N. "*Maritime Security and the Law of the Sea*", UK: Oxford University Press, 2011), 101.

reasonable measures for the exploration of the continental shelf and the exploitation of its natural resources, the coastal State may not impede the laying or maintenance of such cables.[65]

However, it should be noted that compared with provisions of the 1884 Cable Convention, neither Convention on the High Seas nor the Convention on the Continental Shelf provide the right of visit against a vessel of another flag in outside of territorial sea when there was reasonable suspicion of a cable violation.[66]

4.1.1.3 The 1982 United Nations Convention on the Law of the Sea (UNCLOS)

UNCLOS adopted in 1982 reflected demarcating zones of juridical competence: the territorial sea, the contiguous zone, archipelagic waters, continental shelf, Exclusive Economic Zone (EEZ) and high seas where different rights and obligations were extended to coastal States and other users of the sea.[67]

UNCLOS has provisions related to cable operations (cable route surveys, laying, repair, and maintenance) and the protection of submarine cables.

Territorial sea and Archipelagic Waters (areas under territorial sovereignty). Coastal States and archipelagic States clearly have extensive authority to regulate ships engaged in cable operations i.e. the surveying of cable routes and the laying, repair and maintenance of cables, pursuant to their sovereignty over their territorial seas and archipelagic waters.[68] According to Schmitt "In this sense, they are generally treated in the same fashion as cyber infrastructure located on land territory".[69] Both coastal States and archipelagic States are allowed to adopt regulations on innocent passage in relation to cable operations and the protection of submarine cables.[70] Coastal States will usually require the whole gamut of permits, licenses, and

---

[65] Davenport, Tara, Beckman, Robert C., Burnett, Douglas R., "*Submarine Cables: The Handbook of Law and Policy*", (Leiden, Boston: Martinus Nijhoff Publishers, 2014), 73.

[66] The 1958 Geneva Convention on the High Seas, Art. 22, https://treaties.un.org/doc/Treaties/1964/06/19640610%2002-10%20AM/Ch_XXI_01_2_3_4_5p.pdf

[67] Davenport, Tara, Beckman, Robert C., Burnett, Douglas R., "*Submarine Cables: The Handbook of Law and Policy*", (Leiden, Boston: Martinus Nijhoff Publishers, 2014), 74.

[68] Ibid, p. 76-77, See also The 1982 United Nations Convention on the Law of the Sea, Art. 2, 3, 17, 19, 21, 49, http://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

[69] Schmitt Michael N., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (UK: Cambridge University Press, 2017), 253.

[70] The 1982 United Nations Convention on the Law of the Sea, Art. 21, 52, http://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

environmental conditions to be met before permission is given to deploy a submarine cable in these maritime zones.[71]

However, under UNCLOS there is no obligation on coastal States to adopt laws and regulations to protect submarine cables within territorial waters.[72]

The Exclusive Economic Zone and Continental Shelf (areas outside sovereignty but within national jurisdiction). In EEZ and Continental Shelf, all States, whether coastal or land-locked, enjoy the freedoms referred to in article 87 laying of submarine cables and other internationally lawful uses of the sea related to these freedoms, such as those associated with the operation of submarine cables. The maintenance and repair of cables by cable ships is considered to fall under "other internationally lawful uses of the sea related to these freedoms.[73] EEZ and Continental Shelf are areas in which the coastal State did not have sovereignty but instead had sovereign rights to resources that could affect the freedom to lay cables and vice versa.[74]

In exercising their rights and performing their duties under this Convention in the EEZ and Continental Shelf, States shall have due regard to the rights and duties of the coastal State and shall comply with the laws and regulations adopted by the coastal State in accordance with the provisions of UNCLOS.[75] In turn, the coastal State shall have due regard to the rights and duties of other States.[76] The principle of due regard means that all countries shall respect the rights and duties of other countries. In this regard, a state should take into account of all circumstances of the case in light of necessity. The state acts in accordance with the principle of due regard if it has taken all necessary actions to avoid violation of the rights of other states. When laying submarine cables, States shall have due regard to cables in position. In particular, possibilities of repairing existing cables or pipelines shall not be prejudiced.[77] The

---

[71] Davenport Tara, Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis, 24 Cath. U. J. L. & Tech 57 (2015), 76.

[72] Davenport, Tara, Beckman, Robert C., Burnett, Douglas R., "*Submarine Cables: The Handbook of Law and Policy*", (Leiden, Boston: Martinus Nijhoff Publishers, 2014), 84;

[73] Ibid 84; See also The 1982 United Nations Convention on the Law of the Sea, Art. 56, 58, 79, 87, http://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

[74] Davenport Tara, Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis, 24 Cath. U. J. L. & Tech 57 (2015), 71.

[75] The 1982 United Nations Convention on the Law of the Sea Art. 58, http://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

[76] Ibid, Art. 56

[77] Ibid, Art. 79

delineation of the course for submarine cables is not subject to the consent of the coastal State.[78]

Landlocked States are entitled to lay submarine communication cables, in particular with a view to connecting their territories to the global cyber infrastructure. Transit of cables over the territory of neighbouring coastal States is subject to agreement between the landlocked State and the neighbouring States.[79]

Articles 113 to 115 of UNCLOS, based on the 1884 Cable Convention provisions of articles II, IV and VII, address the protection of submarine cables on the high seas, EEZ and on the continental shelf.[80] Article 113 essentially extends a State's criminal jurisdiction (usually limited to territory) over acts of breaking or injury to submarine cables done "wilfully or through culpable negligence" only to ships flying its flag on the high seas or EEZ or to their nationals who commit such acts, consistent with general principles of international law on the prescription of extra-territorial jurisdiction.[81]

The High Seas and Deep Seabed (areas beyond national jurisdiction). The high seas and deep seabed are areas beyond the national jurisdiction of any State.[82] All States are entitled to lay submarine cables on the bed of the high seas beyond the continental shelf. However, there are obligations on States which lay submarine cables on the seabed/high seas. First, Article 112(2) requires States to have due regard to cables already in position and not to prejudice the possibility of repairing existing cables. Second, Article 87(2) requires that the freedom to lay submarine cables be exercised with due regard for the interests of other States in their exercise of high seas freedoms.[83] The high seas shall be reserved for peaceful purposes.[84]

4.1.1.4 Other International conventions and treaties

The 1972 Convention on the International regulations for preventing Collisions at Sea provides that a vessel engaged in laying, servicing or picking up a submarine cable ("a

---

[78] Ibid, Art. 79

[79] Schmitt, Michael N. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (UK: Cambridge University Press, 2017), 255.

[80] Davenport, Tara, Beckman, Robert C., Burnett, Douglas R., "*Submarine Cables: The Handbook of Law and Policy*", (Leiden, Boston: Martinus Nijhoff Publishers, 2014), 85.

[81] Ibid, p. 85

[82] Ibid, 83.

[83] Ibid, p. 84

[84] The 1982 United Nations Convention on the Law of the Sea Art. 58, http://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

cable ship") is considered a "vessel restricted in their ability to manoeuvre".[85] Similarly, the 1972 Convention on the prevention of marine pollution by Dumping from of wastes and other matter and its 1996 protocol may also be relevant to the abandonment of cables on the seabed when they have reached the end of their operating life.[86]

The International Convention for the Suppression of Terrorist Bombings adopted in 1997 provides that it is an offense to unlawfully and intentionally use an explosive or lethal device against an infrastructure facility with the intent to cause extensive destruction of such facility or where such destruction results in or likely to result in major economic loss. An "infrastructure facility" is defined as "any publicly or privately owned facility providing or distributing services for the benefit of the public such as water, sewage, energy, fuel or communications.[87] The 2001 Convention on Cybercrime provides that each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction cybercrimes established in accordance with Articles 2, when the offence is committed: on board a ship flying the flag of that Party.[88] The 1992 Constitution of the International Telecommunication Union sets forth three distinct obligations for States: to ensure the establishment of infrastructure that facilitates rapid and uninterrupted international telecommunications; to safeguard that infrastructure; and to maintain it.[89]

4.1.2 International legal regime during armed conflicts

To date, there are no generally accepted definitions of international and non-international armed conflicts. However, international treaties signed by most of the countries must be applicable during wartime.

International armed conflict is in all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them. Geneva Convention (1) of 1949

---

[85] Davenport, Tara, Beckman, Robert C., Burnett, Douglas R., "*Submarine Cables: The Handbook of Law and Policy*", (Leiden, Boston: Martinus Nijhoff Publishers, 2014), 89.

[86] Ibid, p. 89

[87] Davenport, Tara, Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis, 24 Cath. U. J. L. & Tech 57 (2015), 89.

[88] The 2001 Convention on Cybercrime, Art. 13, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

[89] The 1992 Constitution of the International Telecommunication Union, Art. 38, http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/5.12.61.en.100.pdf

shall also apply to all cases of partial or total occupation of the territory of a High Contracting Party, even if the said occupation meets with no armed resistance.[90] Non-international armed conflict is in all armed conflicts which take place in the territory of a High Contracting Party between its armed forces and dissident armed forces or other organized armed groups which, under responsible command, exercise such control over a part of its territory as to enable them to carry out sustained and concerted military operations.[91]

Thus, it should be noted that international legal regime during armed conflicts related to protection submarine cables should be covered by Geneva Conventions of 1949, Hague Convention (XIII) concerning the Rights and Duties of Neutral Powers in Naval War and Additional Protocols I, II to the Geneva Conventions of 1977. The 1884 Convention for the Protection of Submarine Telegraph Cables, the 1958 Geneva Convention on the High Seas, the 1958 Convention on the Continental Shelf and UNCLOS are not applicable during armed conflicts.

However, the 1884 Cable Convention makes clear in Article XV that its provisions concern to protection submarine cables do not apply in wartime, rejecting the approach of an earlier 1864 treaty between France, Brazil, Haiti, Italy, and Portugal that decreed these parties would not cut or destroy cables in time of war.[92] Even more, some authors and researchers[93] support positions that State practice is consistent with the principle that international cables are legitimate wartime targets.[94]

---

[90] Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Geneva, 12 August 1949, Art.2, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?action=openDocument&documentId=4825657B0C7E6BF0C12563CD002D6B0B, Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Art. 1, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?documentId=D9E6B6264D7723C3C12563CD002D6CE4&action=openDocument

[91] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977, Art. 1, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument&documentId=93F022B3010AA404C12563CD0051E738

[92] Davenport, Tara, Beckman, Robert C., Burnett, Douglas R., "*Submarine Cables: The Handbook of Law and Policy*", (Leiden, Boston: Martinus Nijhoff Publishers, 2014), 66.

[93] Davenport, Tara, Beckman, Robert C., Burnett, Douglas R and others

[94] Ibid, p. 66

This approach is in controversy with current principles of the law of armed conflicts, such as distinction, proportionality, and precaution in attack.[95]

4.1.3 International legal regime in the case of use of force

Article 2 (4) of UN Charter provides that all Members of UN shall refrain in their international relations from the threat or use of force against another country.[96] For peaceful uses of the seas, States Parties shall refrain from any threat or use of force against the territorial integrity or political independence of any State at the sea.[97] However, there are two recognized exceptions to the international law prohibition of the use of force: the exercise of the right of self-defence and actions implementing a United Nations Security Council resolution under Chapter VII of the United Nations Charter.[98]

According to Article 51 of the United Nations Charter, "nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations (…)".[99]

Thus, Member States of UN have the right of individual or collective self-defence in the event of an "Armed Attack" against submarine cables. This requirement applies not only to a defensive reaction with traditional weapons, but also to one with cyber means to the extent that it amounts to a use of force under Article 2(4) of UN Charter[100].
Necessity refers to the existence of an armed attack or the imminent threat of attack. It also refers to the absence of feasible alternatives. Proportionality means the action must be directed to end an attack and to prevent further attacks in the near future. Immediacy could apply if it is reasonable to conclude that further cyber operations are likely to follow. In the case of cyberattacks, compliance with immediacy criteria

---

[95] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Art. 52, 54, 57, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?documentId=D9E6B6264D7723C3C12563CD002D6CE4&action=openDocument

[96] United Nations Charter, 26 June 1945, Art. 2, http://www.un.org/en/sections/un-charter/chapter-i/index.html

[97] The 1982 United Nations Convention on the Law of the Sea, Art. 301, http://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

[98] Chapter United Nations Charter VII, 26 June 1945, Article 51, http://www.un.org/en/sections/un-charter/chapter-vii/index.html

[99] Ibid, Art. 51

[100] Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, North Atlantic Council, para 72, 5 September 2014, https://www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=en

is very important, because the identification process and attribution of the attacker can take quite a long time.

4.2 Challenges and legal gaps in international law with respect to submarine cable protection

During the formation of the fundamental international legal documents that related to the governance and protection of submarine cables, there was no understanding of the importance and criticality the cables. This is especially valid in the context of emerging type of threats, such as cyber security issues.

4.2.1 Challenges and legal gaps in international law during peacetime legal regime

Territorial sea and Archipelagic Waters (areas under territorial sovereignty).
According to Article 21 of UNCLOS, the coastal State may adopt laws and regulations, in conformity with the provisions of this Convention and other rules of international law, relating the protection of submarine cables within their territorial sea and archipelagic waters.[101] However, there is no obligation for them to do so under UNCLOS or otherwise.[102]

Very few States have adopted provisions criminalizing damage to submarine cables in their territorial waters[103], although in some cases offences against submarine cables in the territorial sea will be covered by general legislation criminalizing damage to installations used for telecommunications.[104] In the absence of national regulations related to the protection submarine cables within their territorial sea, countries do not have a possibility to provide effective means of prevention and investigation attacks against submarine cables in this maritime zone.

---

[101] The 1982 United Nations Convention on the Law of the Sea Art. 21, http://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

[102] Davenport, Tara, Beckman, Robert C., Burnett, Douglas R., "*Submarine Cables: The Handbook of Law and Policy*", (Leiden, Boston: Martinus Nijhoff Publishers, 2014), 287.

[103] "For example, in the review of the national legislation of Southeast Asian States, none of the States had an express provision criminalizing intentional or willful damage to submarine fiber optic cables", Ibid 287

[104] "See, for example, Section 21 of Brunei's Telecommunications order 2001, Section 41 of Singapore's Telecommunications Act, Sections 44, 72 and 73 of Thailand's Telecommunications business Act (2001)", Ibid p. 287

In Areas Outside of Territorial Sovereignty. The most challenges in international law during peacetime legal regime relates to the protection of submarine cables outside of territorial sea. Article 113 of UNCLOS which provides prescriptive jurisdiction acts of breaking or injury to submarine cables done "wilfully or through culpable negligence is inadequate for several reasons. First, most States have not adopted laws or regulations incorporating this provision into their national laws. More importantly, Article 113 is inadequate because it does not apply to foreign nationals who intentionally break or damage cables, it only applies to nationals of that State or ships flying its flag. Third, Article 113 only addresses prescriptive jurisdiction and not enforcement jurisdiction over perpetrators who intentionally damage submarine cables.[105] It means that countries have no possibility to use the right to board and arrest vessels in the EEZ and High Seas in the case of damage to submarine cables.

The right of visit within EEZ and the high seas regarding a foreign ship has not the provision related to circumstance when the submarine cable is damaged compare with Article X of the 1884 Cable Convention[106]. The same situation is in the 1958 Geneva Convention on the High Seas and the 1958 Convention on the Continental Shelf. In fact, Article X is only binding on States Parties (which to date, numbers at 40; UNCLOS includes 167) and States Parties have not often exercised their rights under this provision[107].

In turn, it is unsettled whether coastal States are entitled to establish cable protection zones within EEZ, the continental shelf and the high seas that restrict certain activities, such as anchoring, bottom trawling, and sand mining that pose threats to the integrity of submarine communication cables. Australia and New Zealand were among the first States to create cable corridors/protection zones that, within the territorial sea and EEZ, shield cables one mile on each side from vessel traffic and from other hazardous activities[108]. While international law provides a sufficient basis

---

[105] Ibid, p. 288

[106] The 1884 Convention for the Protection of Submarine Telegraph Cables, Art. X, "Article X of the 1884 Cable Convention, allows warships to require the master of a vessel suspected of having broken a cable to provide documentation to show the ship's nationality and thereafter to make a report to the flag State.", The 1884 Convention for the Protection of Submarine Telegraph Cables, Art. 4, https://cil.nus.edu.sg/wp-content/uploads/formidable/18/1884-Convention-for-the-Protection-of-Submarine-Telegraph-Cables.pdf r

[107] "There is only one reported case of a State Party relying on Article X of the 1884 Convention and this was the boarding and inspection of log books of the Soviet Trawler Novorossik by officers of the US naval vessel Roy O Hale in 1959", Davenport, Tara, Beckman, Robert C., Burnett, Douglas R., "*Submarine Cables: The Handbook of Law and Policy*", (Leiden, Boston: Martinus Nijhoff Publishers, 2014), 289.

[108] "Cited from: Telecommunications and Other Legislation Amendment (Protection of Submarine Cables and Other Measures) Act (2005), No. 104, 2005 (Austl.); Submarine Cables and Pipeline

for cable protection zones within the territorial sea, there is no equivalent clear provisions with respect to either the EEZ or the continental shelf, and certainly not for the high seas.[109]

As we mentioned before that in exercising rights and performing duties under UNCLOS in the EEZ and Continental Shelf, States shall have due regard to the rights and duties of the coastal State including the right to lay submarine cables. In turn, the coastal State shall have due regard to the rights and duties of other States. For instance, there could be a case when one state lays a submarine cable in EEZ, and another conducts military exercises. Therefore, there is no clear understanding of how to find the balance between the rights and duties of Coastal State and other States.

Moreover, there is a serious international challenge regarding protection rights and obligations of States to respect submarine cables by using international judicial procedures. Article 309 of UNCLOS does not preclude a State, when signing, ratifying or acceding to this Convention, from making declarations or statements.[110] For example, Russia Federation declared that, in accordance with article 298 of the United Nations Convention on the Law of the Sea, it does not accept the procedures, provided for in section 2 of Part XV of the Convention, entailing disputes concerning military activities, including military activities by government vessels and aircraft, and disputes concerning law-enforcement activities in regard to the exercise of sovereign rights or jurisdiction[111]. These opting-outs could be used against critical infrastructure in maritime domain, including submarine cables.

Cyberattacks against submarine cables and using unmanned weapons. The international maritime law does not give an opportunity to enact laws and regulations for the protection of submarine cables outside territorial sea, including using new technologies, as well as against new threats with using cyber, unmanned and autonomous weapon systems. The international maritime law only establishes a crime for damage to a submarine cable. Although, it is possible to conduct operational actions within the framework of a criminal investigation or the prevention of a crime. Taking in an account the specifics of maritime zone which are

---

Protection Act (1996), Public Act No. 22, 16 May 1996 (NZ)", Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (UK: Cambridge University Press, 2017), 256.

[109] Ibid, p. 256.

[110] The 1982 United Nations Convention on the Law of the Sea Art. 310, http://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

[111] United Nations, Treaty Collection, United Nations Convention on the Law of the Sea, Declaration of Russia Federation, https://treaties.un.org/Pages/ViewDetailsIII.aspx?src=TREATY&mtdsg_no=XXI-6&chapter=21&Temp=mtdsg3&clang=_en

located outside of state sovereignty this is not enough to ensure and build an effective system for the protection of submarine cables outside the territorial waters of the state against all types of threats, including cyberattacks, unmanned and autonomous weapon systems.

These legal gaps in the international maritime law justify lack of understanding importance of creating protection submarine cable systems from intentional damage during negotiations procedure between states regarding concluding the Convention for the Protection of Submarine Telegraph Cables in 1884.

International law will be applying the right to self-defence or authorize by the Security Council collective security operations in the case of cyberattacks, includes the necessary requirements for its implementation, and establishes the necessary standards of evidence to justify the use of force. The speed and anonymity of cyberattacks makes proving State responsibility and distinguishing among the actions of terrorists, criminals and nation states difficult.[112] However, international law does not have the tools to carry out the identification of the attacker, especially in the case of cyberattacks, because it is not a purpose for the international law. This is the competence of technical experts, methodologies and special programs. It is worth noting that for effective identification and attribution, there must be a relationship between the international legal instrument to protection submarine cables in the case of cyberattacks and technical means of protection in cyberspace.

4.2.2 Challenges and legal gaps in international law during armed conflicts

The 1884 Convention for the Protection of Submarine Telegraph Cables, the 1958 Geneva Convention on the High Seas, the 1958 Convention on the Continental Shelf and the 1982 United Nations Convention on the Law of the Sea (UNCLOS) do not prohibits states from treating undersea cables as legitimate military targets during wartime[113]. Indeed, the 1884 Convention explicitly states that its stipulations do not "in any way restrict the freedom of action of belligerents"[114]. Wartime regulation will be applicable to another international legal regime and other international treaties.[115]

---

[112] "Cited from: Shackelford & Andres, supra note 211, at 974 (quoting David Held, Models of Democracy 293-97 (2006)", Tara Davenport, Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis, 24 Cath. U. J. L. & Tech 57 (2015), 87

[113] Sunak, R., "Undersea cables: indispensable, insecure", (UK: Policy Exchange, 2017), 17

[114] Ibid, p. 17.

[115] Geneva Conventions of 1949, Hague Convention (XIII) concerning the Rights and Duties of Neutral Powers in Naval War and Additional Protocols I, II to the Geneva Conventions of 1977

However, in light Article XV of the 1884 Cable Convention which indicated that the stipulations of the present Convention do not in any way restrict the freedom of action of belligerents. Most authors[116] recognise that during wartime belligerents could consider submarine cables as lawful targets without principle distinction. Moreover, on signing of the Cable Convention, Britain made the following declaration: "Her Majesty's Government takes article XV to mean that in time of war, a belligerent, who is signatory to the Convention, will be free to act, with respect to submarine cables, as if the Convention did not exist."[117] In World War I, both Britain and Germany undertook offensive action against the submarine cables of the other.[118]

Davenport pointed out that submarine cables today are still legitimate targets during wartime. Although, submarine cables between neutral countries, even during wartime, are inviolable and cannot be seized or destroyed except in the case of absolute necessity.[119]

However, it should be noted that Article 48 of Additional Protocol I codifies the customary international law principle: 'in order to ensure respect for and protection civilian objects, the Parties to the conflict shall at all times distinguish between civilian objects and military objectives and accordingly shall direct their operations only

---

[116] Davenport, Tara, Beckman, Robert C., Burnett, Douglas R: "State practice since the 1884 Cable Convention is consistent with the principle that international cables are legitimate wartime targets"; "Right to Cut Cables in war; Admiral Dewey Created a new precedent under the law of nations in manila bay" The New York Times, 23 may 1898; Stuart Kaye: "Thus, breaking a belligerent State's cable during wartime would not be restricted by the Convention"; Laurence Reza Wrathall: "The Cable Convention does not restrict breaking a belligerent state's cable during wartime"

[117] "Cited from John MacDonnell, Recent Changes in the Rights and Duties of Belligerents & Neutrals According to International Law, 17 J. ROYAL UNITED SERV. INST., July-Dec. 1898", Tara Davenport, Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis, 24 Cath. U. J. L. & Tech 57 (2015), 80.

[118] Stuart Kaye, International Measures to Protect Oil Platforms, Pipelines, and Submarine Cables from Attack, 31 Tul. Mar. L.J. 377 (2007), 397; See Tara Davenport, Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis, 24 Cath. U. J. L. & Tech 57 (2015), 80, "Indeed, the first act of the British in World War I was to cut Germany's undersea telegraph cable that left Germany with just one cable, which was in any event under British control.193 Germany retaliated by attempting to destroy Allied telegraph cables in the Pacific and Indian Oceans and attacking telegraph stations and cables at Fanning Island and the Cocos Island in 1914, starting the notorious cables wars".

[119] "Cited from: Convention (IV) Respecting the Laws and Customs of War on Land, art. 54, Oct. 18, 1907, 36 Stat. 2277, 2308, T.S. No. 539", Tara Davenport, Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis, 24 Cath. U. J. L. & Tech 57 (2015), 80

against military objectives.[120] The principle applies in both international and non-international armed conflict.[121]

Civilian objects are all objects that are not military objectives. Military objectives are those objects which by their nature, location, purpose, or use, make an effective contribution to military action and whose total or partial destruction, capture or neutralisation, in the circumstances ruling at the time, offers a definite military advantage.[122] When a civilian object or facility is used for military ends, it becomes a military objective through the 'use' criterion.[123] The Article 52(3) of Additional Protocol I provides: 'in case of doubt whether an object which is normally dedicated to civilian purposes . . . is being used to make an effective contribution to military action, it shall be presumed not be so used'.[124] In other words, doubt is legally resolved in favour of civilian status.[125]

Thus, submarine cables should be considered as civil objectives unless cables used by military forces or for military purposes. In order to ensure respect for and the protection of submarine cables as civilian objects, the Parties to the conflict shall not direct their operations against them except when such objects are used for military purpose. Hence, to consider such targets as legitimate contradicts the existing principles and norms of the law of armed conflicts.

---

[120] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Art. 48, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?documentId=D9E6B6264D7723C3C12563CD002D6CE4&action=openDocument

[121] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (UK: Cambridge University Press, 2017), 421.

[122] Ibid p. 435; Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Art. 52, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?documentId=D9E6B6264D7723C3C12563CD002D6CE4&action=openDocument

[123]"Cited from: Hague Regulations, Art. 27 (noting that civilian objects enjoy protected status unless 'used at the time for military purposes'). See also ICRC Additional Protocols 1987 Commentary, para. 2022", Ibid 438

[124] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Art. 52, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?documentId=D9E6B6264D7723C3C12563CD002D6CE4&action=openDocument

[125] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (UK: Cambridge University Press, 2017), 448.

4.3 Recommendations for strengthen submarine cable protection

4.3.1 The international agreement between states concerning to the protection of submarine cables outside of the territorial sea

There are currently no international treaties or any legal provisions which directly regulate the protection of submarine cables outside of the territorial sea. Currently existing international instruments that set out substantive provisions on the rights and obligations of States concerning submarine cables establishes only a crime for damage to a submarine cable. In addition, Article 110 of UNCLOS gives the possibility to states provide a universal jurisdiction by a separate treaty.

Recommendation (s): International agreement between states concerning the protection of submarine cables outside of the territorial should:

- Address the protection of submarine cables against all types of threats, including cyberattacks,
- Provide assistance from other states in case of attack against submarine cables;
- Create protective zones in which certain shipping activities such as such as anchoring, bottom trawling, and sand mining, that pose threats to the integrity of submarine communication cables would be prohibited,
- Provide the right to visit the ship's board under a flag or foreign nationalities in case of suspicion of a crime by establishing universal jurisdiction

This agreement could be recommended between to all parties involved Artic Connect Project. Nevertheless, the countries involved in the project should all agree on the exact details of such an agreement.

4.3.2 Development of national legislation regarding protection of submarine cables

Very few States have expressed provisions criminalizing damage to submarine cables in their territorial waters and outside of territorial sea. In the case of absence of national regulations related protection submarine cables within their territorial sea or outside of territorial waters, states lose possibility to provide effective means of prevention and investigation attacks against submarine cables in these maritime zones.

Recommendation (s): States should adopt national legislation regarding protection submarine cables within territorial waters and outside of territorial sea (EEZ and high seas) through implementation Article 21 (c) and Article 113 of UNCLOS. Apart from that, states should conclude National Contingency Plans in place to ensure the security and recovery of the submarine cables. National Contingency Plans should include provisions related to exchange information and full cooperate in the event of attacks. Provisions should also include cooperation between Government of States and cable industry in order to enable them to act quickly.

4.3.3 Adoption of a Global Convention on the Protection of Submarine Critical Information Infrastructure

The absence of a modern international convention for the protection of a critical information infrastructure in maritime domain raises serious problems in the implementation of such protection under international law.

Recommendation (s): States should aim to adopt a Global Convention on the Protection of Submarine Critical Information Infrastructure which would replace the Convention for the Protection of Submarine Telegraph Cables in 1884. This Convention should thoroughly address rights and obligations of states regarding protection submarine cables, including from intentional damages in light of kinetic/non-kinetic threats within territorial sea and outside of territorial waters. The adoption of a Global Convention could be especially challenging endeavour, especially taking into account current geopolitical and security situation and the existence of different interests.

4.3.4 Right of visit according to Article X of the 1884 Cable Convention

On the contrary from Article X of the 1884 Cable Convention, UNCLOS does not provide right to visit when submarine cable is damaged in Article 110. There is only one reported case of a State Party relying on Article X of the 1884 Convention.

Recommendation (s): States should apply and use Article X of the 1884 Cable Convention which provides that a warship could conduct a right to visit against a vessel of another flag when there is reasonable suspicion of a cable violation. In order to apply such provisions, states should be participants of the 1884 Cable Convention, because these legal provisions may not reflect the customary international law in its entirety.

4.3.5 The right of self-defence according Article 51 of UN Charter in the case of Armed Attack against submarine cables

Member States of UN have the right of individual or collective self-defence in the event of an "Armed Attack" against submarine cables. This requirement applies not only to a defensive reaction with traditional weapons but also to one with cyber means to the extent that it amounts to a use of force under Article 2(4) of UN Charter. According to UNCLOS, warships on the high seas or EEZ have complete immunity from the jurisdiction of any State other than the flag State. This legal provision does not give an opportunity for states to ensure effective protection of submarine cables in the case of damage by warship other than the flag State.

Recommendation (s): States should apply and use right of self-defence according to Article 51 of UN Charter in the case of Armed Attack including cyberattack against submarine cables. This rule would apply in the case cause of damage to submarine cables by warship despite on immunity from the jurisdiction of any State.

4.3.6 Considering submarine cables as civil objects (non-lawful targets) during armed conflicts

The 1884 Cable Convention makes clear in Article XV that its provisions concerning the protection of submarine cables do not apply in wartime. In addition, some authors and researchers claim that State practice since the 1884 Cable Convention is consistent with the principle that international cables are legitimate wartime targets. However, this approach goes against current principles of the law of armed conflicts such as the distinction, proportionality, and precautions in attack.

Recommendation (s): The Parties to the conflict should consider submarine cables as civil objects unless cables are used by military forces or for military purposes. Parties to the conflict shall not direct their operations against submarine cables unless if/when such objects become military.

4.3.7 National Crisis Response Exercise Capability

The ability to exercise real-world national crisis scenarios in case of damages to submarine cables should be an integral part of established national crisis response plans. For example, crisis management exercises (TTXs, Wargames) allow the government to assess gaps in plans, organizational structures, management processes, crisis protocol, and resource capacity. Without the capacity to exercise, states do not have the ability to explore various threat scenarios, determine if

allocated resources can properly handle predicted crises, and train its forces in crisis response.

Recommendation (s): Develop annual national and regional level crisis management exercises (TTX, Wargames, and so on) that include interfacing with international agency representatives in order to assess, refine, and/or establish National Contingency Plans in the case kinetic and non-kinetic attacks on submarine cables and another kind of damages.

REFERENCES

1. Advisory Opinion, 1996 ICJ 226 (8 July), para. 39. http://www.icj-cij.org/files/case-related/95/095-19960708-ADV-01-00-EN.pdf
2. Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Geneva, 12 August 1949, Art.2. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?action=openDocument&documentId=4825657B0C7E6BF0C12563CD002D6B0B
3. Davenport T., Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis, 24 Cath. U. J. L. & Tech 57, 2015.
4. Davenport T., Beckman R. C., Burnett D. R., "*Submarine Cables: The Handbook of Law and Policy*", (Leiden, Boston: Martinus Nijhoff Publishers, 2014)
5. Hague Convention (XIII) concerning the Rights and Duties of Neutral Powers in Naval War and Additional Protocols I, II to the Geneva Conventions of 1977
6. Klein, N., Maritime Security and the Law of the Sea, UK: Oxford University Press, 2011.
7. Nuclear Weapons advisory opinion: Legality of the Threat or Use of Nuclear Weapons.
8. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?documentId=D9E6B6264D7723C3C12563CD002D6CE4&action=openDocument
9. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977, Art. 1. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument&documentId=93F022B3010AA404C12563CD0051E738
10. Schmitt M. N., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, UK: Cambridge University Press, 2017.
11. Stuart K., International Measures to Protect Oil Platforms, Pipelines, and Submarine Cables from Attack, 31 Tul. Mar. L.J. 377, 2007.
12. The 1884 Convention for the Protection of Submarine Telegraph Cables, Art. 1. https://cil.nus.edu.sg/wp-content/uploads/formidable/18/1884-Convention-for-the-Protection-of-Submarine-Telegraph-Cables.pdf r
13. The 1972 Convention on the International Regulations for Preventing Collision at Sea. https://treaties.un.org/doc/Publication/UNTS/Volume%201050/volume-1050-I-15824-English.pdf
14. The 1972 Convention on the Prevention of Marine Pollution by Dumping from Wastes and Other Matter.

https://treaties.un.org/doc/publication/unts/volume%201046/volume-1046-i-15749-english.pdf

15. The 1982 United Nations Convention on the Law of the Sea. http://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf
16. The 1992 Constitution of the International Telecommunication Union. https://www.itu.int/council/pd/constitution.html
17. The 1997 International Convention for the Suppression of Terrorist Bombings. https://treaties.un.org/doc/Treaties/1997/12/19971215%2007-07%20AM/ch_XVIII_9p.pdf
18. The 2001 Convention on Cybercrime. https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561
19. Treaties, States Parties and Commentaries, International Committee of the Red Cross. https://ihl-databases.icrc.org/ihl
20. United Nations Charter, 26 June 1945. http://www.un.org/en/sections/un-charter/chapter-vii/index.html
21. United Nations, Treaty Collection, United Nations Convention on the Law of the Sea, Declaration of Russia Federation. https://treaties.un.org/Pages/ViewDetailsIII.aspx?src=TREATY&mtdsg_no=XXI-6&chapter=21&Temp=mtdsg3&clang=_en
22. Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, North Atlantic Council, para 72, 5 September 2014. https://www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=en

5 CYBER SECURITY THREATS AND PROTECTION IN SUBMARINE CABLE SYSTEMS

5.1 Introduction

Almost all services and most of the traditional services are totally dependent on the digital environment. Few users are aware of the revolutionary nature of modern technology. We use day-to-day real-time access to any existing digital service in our home country or we use social media (SoMe) to communicate with friends in Finland or elsewhere in the world. We can communicate with them in real time with text messages or even real-time videos. People can watch millions of movies anytime and anywhere at an appropriate time. Modern communications connect data centers and data networks of different continent together, enabling this real-time communication throughout the world. We can order different goods from all over the world, pay invoices electronically and get the goods home. Companies use the same channels of communication for daily communications, trading, sending invitations to tender and transferring money through banks in real time.

As a result of the development described above, people and systems produce huge amounts of data that need to be processed and stored. However, technical solutions for all new service environments are not yet in line with international standards and their connections to telecommunications and service networks are very different depending on the situation. At the same time, technically outdated solutions and new technologies are used. Future information and communication systems need to be designed and adapted to work in this challenging business environment where security threats and cybercrime occur everywhere.

Each function has its own service and communication needs depending on the user group. Such groups include design and maintenance staff, financial management staff, telecom operators, service provider staff, virtual service providers and operators, administrative agents, citizens, manufacturers, banks, etc. To these days no any other technology than submarine cable systems has not been such a strategic impact to our society without being known it as such by the people. This also means that it is at the same time a very interesting destination for hackers, cyber attackers, terrorist and state actors. They seek to gain access to information that goes through the networks of these continents that are connected to each other with sea cables.

5.2 Undersea submarine cable network

Figure 2 shows how different parts of the World today are connected to each other by optical submarine cables.

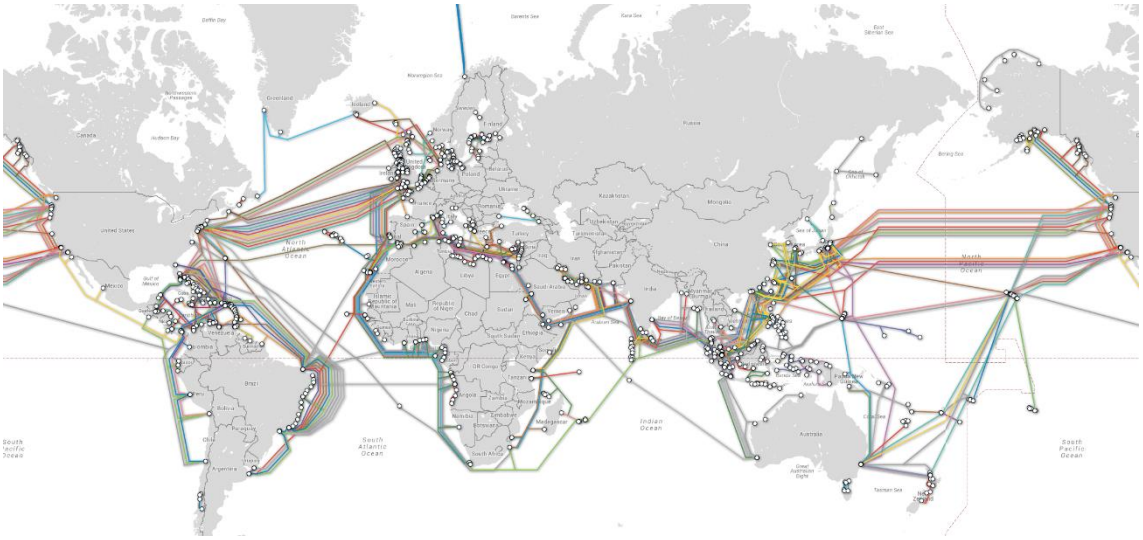


Fig 2. Map of the Worldwide Undersea Submarine Cable Network[126]

Current optical submarine cables are focused on the southernmost seas of the globe, and the terminals of optical submarine cables are located in areas where it is relatively easy to build cable endpoints, including cable telecommunication and energy systems. At present, the world has no optical submarine cables connection between Europe, Russia's northern regions, Japan and China.

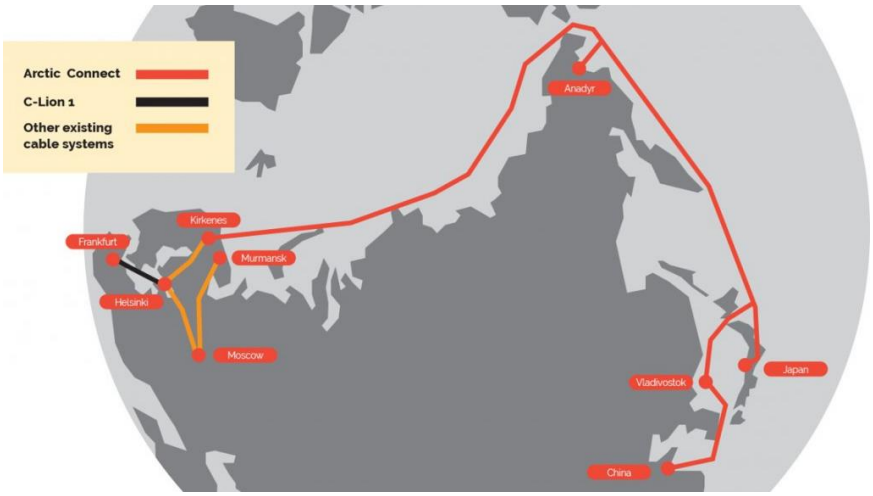


Fig 3. Artic connect cable system[127]

126 www.reddit.com/r/MapPorn/comments/73ekox/map_of_underwater_cables_that_supply_the_worlds/

127 http://asia.blog.terrapinn.com/submarine-networks/2018/02/13/navigating-the-arctic/

In this study we are discussed for technical solutions and cyber threats (see Figure 3) related to the construction of an optical undersea cable. An optical undersea cable will be built on the arctic ocean area and it starts in northern Finland and runs along the Russian coast to Japan and China. The undersea cable system is about 18,000 km long. But we must remember that the capacity of optical cables is limited by the signal-to-noise ratio, including amplifier noise, fiber dispersions, and the phenomena caused by fiber nonlinearities. Those limits must be taking care design this kind of systems. Despite these factors which are limiting the functionalities of fiber optic cables almost every day are reported in the news how the submarine optical cable systems reach several terabits per second (Tbits) capacities.[128] [129] [130]

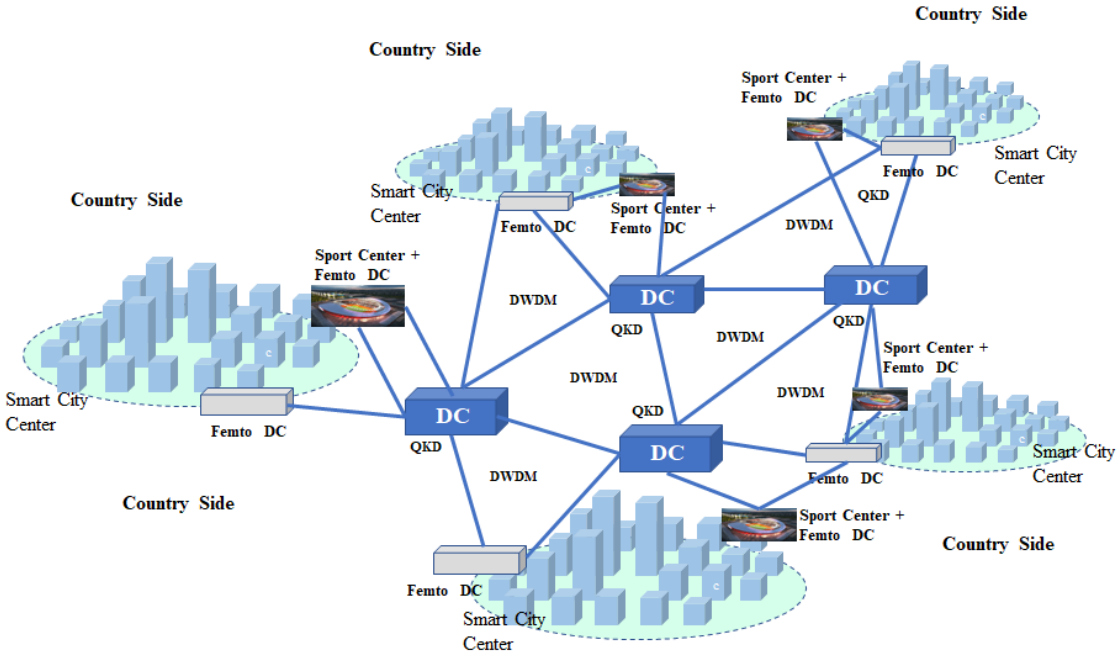


Fig 4. Communications Networks in The Future between different Smart Cities

---

[128] Terabytes are currently the largest transmission rates available for submarine optical cables. March 30, 2016 Alcatel-Lucent announced that Alcatel-Lucent Submarine Networks and Cinia have achieved 144 Tbits transmission capacity in the C-Lion1 submarine cable system. TE SubCom Sets Record for Transmission capacity C + L technology has reached a speed of 70.4 Tbits over 7,600 km, sets the industry standard and opens unprecedented trails for capacity lifting in marine cables.
When a new undersea communications cable becomes operational late this year, it will break the record for a key metric: data rate times distance. In a single second, its six fiber-optic pairs, stretching roughly 13,000 kilometers (8,000 miles) between Hong Kong and Los Angeles, will be able to send some 144 terabits in both directions. Now the latest news is telling that some test group have achieved even if 144 Tbits transmission capacity.

[129] Miyamoto Yutaka and Kawamura Ryutaro, NTT Technical Review, Feature Articles: State-of-the-art Space Division Multiplexing Technologies for Future High-capacity Optical Transport Networks, Space Division Multiplexing Optical Transmission Technology to Support the Evolution of High-capacity Optical Transport Networks, Vol. 15 No. 6, June 2017

[130] NEC has demonstrated speeds of 50.9 Tbps across subsea cables of up to 11,000km on a single optical fiber through the use of C+L-band erbium-doped optical fiber amplifiers (EDFA), amounting to speeds of 570 petabits per second-kilometer, by Corinne Reichert, May 15, 2017.

We can look at submarine optical cable networks a bit more. Each country has its own fiber network that connects cities and countryside to each other. In addition, these fiber-optic networks are connected to fiber-optic networks in the other countries. Today, these submarine optical cable networks connect these networks on different continents with each other through a large capacity underwater optical cable system, Figure 4 and 5. The structure of a submarine optical cable communication system is basically the same as that of terrestrial optical cable system.

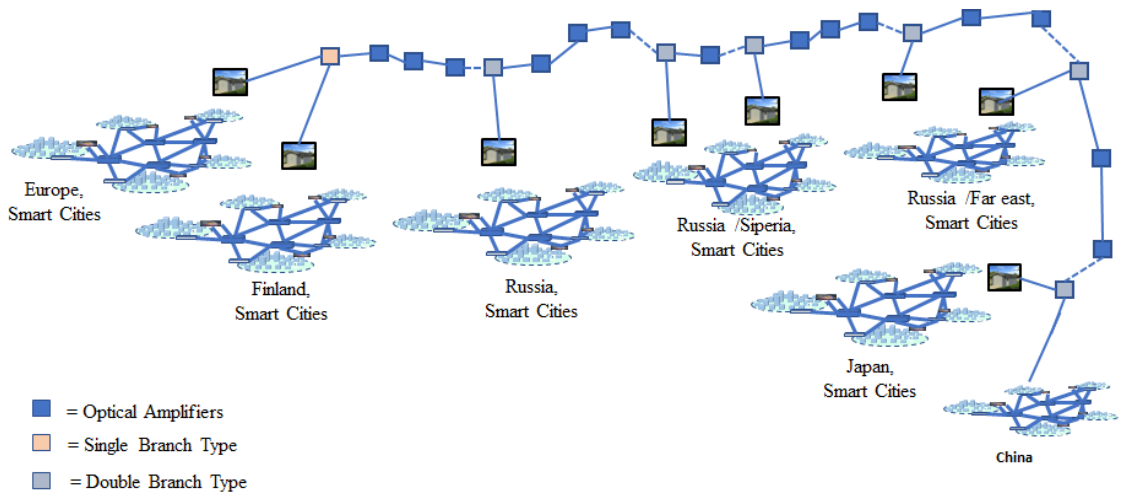


Fig 5. Overview of Artic connect cable system

Figure 5 is a general overview of Artic Optical Cable Systems, which combines different regions of Europe, the western parts of Russia, the Siberian Russian regions, the Russian far east areas, the smart cities in Japan and from here to China. Between these areas, a lot of communication capacities and new contact points will be needed in the future in order to satisfy the data transfer needs of users, businesses and governments.

5.3 Technology evolution

Since the life cycle of a fibre optic cable to be built is long, up to 25 years, maybe more, we must know at least in part of technical evolution, what occurs in optical telecommunication technology and what we which way must taking care those things concerning in these long connections. In Figure 6 we can see which directions the evolution˘ But the optical channel capacity cannot be increased indefinitely, despite the wide optical bandwidth available in the optical range. We can calculate optical channel capacity which is possible to get.[131]

[131] Miyamoto Yutaka and Kawamura Ryutaro, NTT Technical Review, Feature Articles: State-of-the-art Space Division Multiplexing Technologies for Future High-capacity Optical Transport Networks, Space

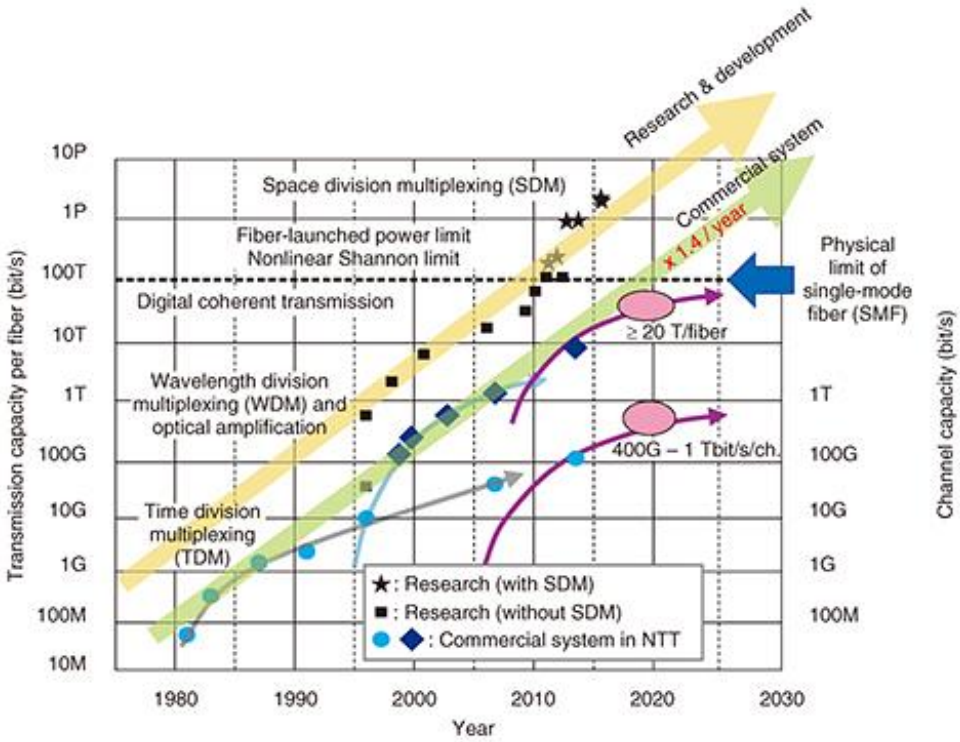


Fig 6. Evolution of high-capacity optical transport network

We see also from Figure 6 the physical limits of single-mode fiber (SMF). There are also two other limits for optical communications - Fiber-launched power limit and Non-linear Shannon limit. When designing a telecommunications system based on long-distance optical undersea cables, we must take very strictly into account to those limiting factors relating to optical fibers.

At the same time, we must take into account the features and operational models of these optical undersea cable systems parameters in practical networks to provide more accurate information about the functions of the existing system so that we can detect possible intrusion attempts.

Since more capacity is needed per fiber pair, new optical signal band, L-band has to be introduced. The C and L bands form the basic band of future long-distance optical networks that come together to use, and the optical amplifiers, for example, are planned to start from this point of view (see Figure 7).

Division Multiplexing Optical Transmission Technology to Support the Evolution of High-capacity Optical Transport Networks, Vol. 15 No. 6 June 2017

Since fiber band attenuation also in L-band is reasonable, it is quite useful to use for high-capacity optical transport network. From that is coming one challenge to network designers to find optical amplifier in which is enough capacity working with C-band and L-band same time as one amplifier.

Figure 7 we can see that there are in C-band 80 optical channel and also in L-band 80 optical channel. If we transmit 100 Gbit/s through one optical channel, this means that we have 80 X 100 Gbit/s capacity in our use in this kind of network. We can see later on, is there possible solutions or not later in that presentation.

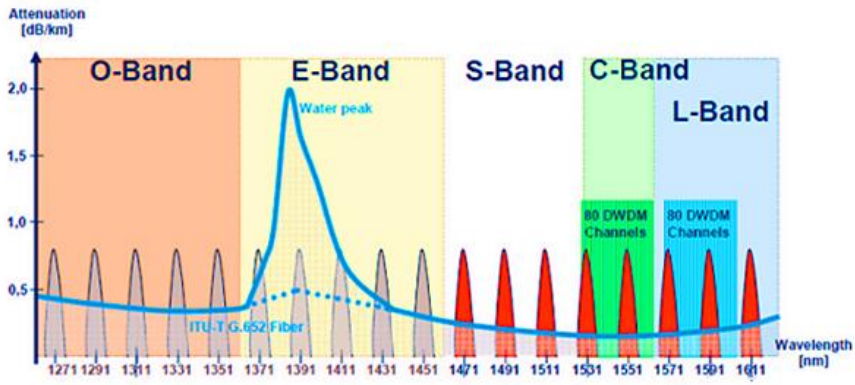


Fig 7. High-capacity optical transport network Optical Bands[132]

5.4 Long distance optical undersea systems

About 10 years ago second generation 10 Gbit/s capacity was quite normal in undersea optical cable systems in one wavelength capacity and same time there was 40 Gbit/s systems ready to come market.

By 2015 there was competition between telco operators and other service providers to offer new services in submarine optical cables, resulting in a mature product of 100 Gbit/s of capacity per optical wavelength. Since then development work has continued to find new solutions aimed at increasing wavelength capacity so that more information can be transferred in submarine optical cable systems from one continent to another. As a result of development, the following capacities is 200 Mbit/s and 400 Mbit/s.

---

[132] Chen Cheer, Fiber Optic Cabling Solutions, October 13, 2015. http://www.cables-solutions.com/tag/edfa

Today, 600 to 10,000 km long links use coherent modulation techniques, such as QPSK / 8QAM, to allow for data transfer at 100 Gbit / s and 200 Gbit / s at these connections.

For such transmission rates to be obtained with a longer fibre optic link such as 100 Mbit/s or more, optical amplifiers are required, which are about 50 km intervals. This division provides enough quality of service across continents.

5.5 Installation main principles

In this project we install 18,000 km long undersea optical cable system (Figure 4). There are six branching points, from which are connection to the continent. Between continent cable station points, those branching points and other end of undersea cable systems, there are many optical amplifiers every 50 km.[133] In some parts of cable systems, there are also equalizers (passive or active) (see Figure 8).

The main reason why the distance between optical amplifiers is only 50 km is due to the dispersions and non-linear properties of optical cables, the characteristics of the optical amplifiers, and the characteristics of the fibres. As the modulation techniques of optical data transfer become more complex, the above described features of fibres and optical amplifiers are emphasized, and the design of connections is more accurate. The distance between the amplifiers is optimized based on the usability and quality of the services, the performance and the cost optimization for cost-effectiveness of € / bit / Hz.
This whole system also needs electrical energy. Energy input to the system can be made from one or more earth points, taking into account the energy supply protection if there is damage in cable systems.

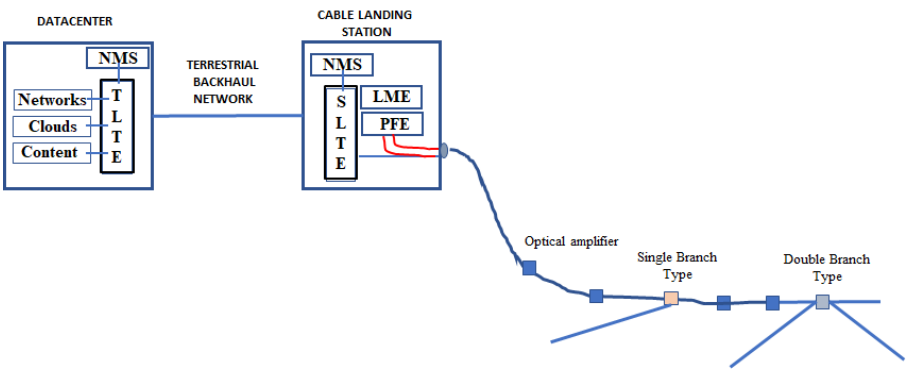


Fig 8. Subsea Cable System Architecture with Cable landing Station and Data Center

[133] Chesnoy Jose, Undersea Fiber Communication Systems, Elsevier ltd, 2016, pages 119 -160, 165-233

Abbreviations:

NMS = Network Management System	NMS = Network Management System	PFE = Power Feed Equipment
TLTE = Terrestrial Line terminal Equipment	LME = Line Monitoring Equipment	SLTE = Submarine Line terminal Equipment.

Like in Figure 8 every cable landing station have been built at all cable landing station sites in the same way, depending on the beach area, of course, how undersea optical cables can be brought there.

5.6 Designing undersea optical cable systems

We need to take into account the following factors (chapters 5.7-5.9) in order to achieve the required usability and quality requirements for very long optical undersea cable connections. Apart from that, we also need to understand the parameters and impairments of optical submarine cables so that we can find out if there are any faults in the cable connection and links or whether hackers or cyber attackers are is connected to the cable in one way or another in order to gather information there for their purposes or even to spy.

5.7 Factors affecting the fiber quality

5.7.1 Attenuation

Attenuation values varies between different wavelength bands 800, 1300nm and 1550nm and is smallest in 1550 nm band, where is it about 0.2 db/km or smaller.

Several factors can cause attenuation, but it is generally categorized as either intrinsic or extrinsic. Intrinsic attenuation is caused by substances inherently present in the fiber, whereas extrinsic attenuation is caused by external forces such as bending. Extrinsic attenuation maybe reason from macro bending or micro bending and both rises fiber attenuation values higher. This mechanism gives possibilities to use it also in cyber-attacks to get information from optical cables without anybody can see it what has happened.

5.7.2 Dispersions

Rayleigh Scattering

- As light travels in the core, it interacts with the silica molecules in the core. Rayleigh scattering is the result of these elastic collisions between the light wave and the silica molecules in the fiber. Rayleigh scattering accounts for about 96 percent of attenuation in optical fiber.

Chromatic dispersion

- Chromatic dispersion is the spreading of a light pulse as it travels down a fiber. Light has a dual nature and can be considered from an electromagnetic wave as well as quantum perspective. This enables us to quantify it as waves as well as quantum particles.

Polarization Mode Dispersion (PMD)

- Polarization mode dispersion (PMD) is caused by asymmetric distortions to the fiber from a perfect cylindrical geometry. The fiber is not truly a cylindrical waveguide, but it can be best described as an imperfect cylinder with physical dimensions that are not perfectly constant. The mechanical stress exerted upon the fiber due to extrinsically induced bends and stresses caused during cabling, deployment, and splicing as well as the imperfections resulting from the manufacturing process are the reasons for the variations in the cylindrical geometry.

Optical Signal-to-Noise Ratio

- The optical signal-to-noise ratio (OSNR) specifies the ratio of the net signal power to the net noise power and thus identifies the quality of the signal. Attenuation can be compensated for by amplifying the optical signal. However, optical amplifiers amplify the signal as well as the noise. Over time and distance, the receivers cannot distinguish the signal from the noise, and the signal is completely lost.

5.8 Impact of non-linearity

Non-linearity, Nonlinear Characteristics. Nonlinear characteristics include Self-Phase Modulation (SPM), Cross-Phase Modulation (XPM), Four-Wave Mixing (FWM), Stimulated Raman Scattering (SRS), and Stimulated Brillouin Scattering (SBS).

Four-Wave Mixing (FWM)

- Four-Wave Mixing can be compared to the intermodulation distortion in standard electrical systems. When three wavelengths ($\lambda 1$, λ 2, and λ 3) interact in a nonlinear medium, they give rise to a fourth wavelength (λ 4), which is formed by the scattering of the three incident photons, producing the fourth photon. This effect is known as four-wave mixing (FWM) and is a fiber-optic characteristic that affects WDM systems.

Self-phase Modulation (SPM)

- Self-phase Modulation of an optical signal by itself is known as self-phase modulation. SPM is primarily due to the self-modulation of the pulses. Generally, SPM occurs in single-wavelength systems. At high bit rates, however, SPM tends to cancel dispersion. SPM increases with high signal power levels.

Cross-phase modulation (XPM)

- Cross-phase Modulation is a nonlinear effect that limits system performance in Wavelength-Division Multiplexed (WDM) systems. XPM is the phase modulation of a signal caused by an adjacent signal within the same fiber. XPM is related to the combination (dispersion/effective area). XPM results from the different carrier frequencies of independent channels, including the associated phase shifts on one another.

Stimulated Brillouin Scattering (SBS)

- Stimulated Brillouin scattering is due to the acoustic properties of photon interaction with the medium. When light propagates through a medium, the photons interact with silica molecules during propagation.

Stimulated Raman Scattering (SRS)

- When light propagates through a medium, the photons interact with silica molecules during propagation. The photons also interact with themselves and cause scattering effects, such as Stimulated Raman Scattering (SRS), in the forward and reverse directions of propagation along the fiber. This results in a sporadic distribution of energy in a random direction

5.9 Long distance cable systems attenuation calculations

The power budget tables should compute margins that should be considered as a minimum requirement for the system at BOL. These margins should be expressed in terms of a Q factor value. The contractors should provide, as a minimum, the values

of the parameters used to compute the power budget and specify all necessary complementary relevant information, for instance, the use of any optical polarization scrambling or phase modulation to minimize the polarization effects or nonlinear effects. An example of a possible power budget template is shown in Table 2.[134]

Table 2. An example of a possible power budget template

	Parameter		BOL Q in dB	EOL Q in dB
1	Mean Q value (from a simple SNR calculation)			
1.1	Propagation impairments due to combined effects of chromatic dispersion, non-linear effects, FWM effects, stimulated Raman scattering effects, etc.			
1.2	Gain flatness impairments			
1.3	Non-optimal optical pre-emphasis impairment			
1.4	Wavelength tolerance impairment			
1.5	Mean PDL penalty			
1.6	Mean PDG penalty			
1.7	Mean PMD penalty			
1.8	Supervisory impairment			
1.9	Manufacturing and environmental impairment			
2	Time-varying system penalty (5 sigma rule)			
3	Line Q value (1-1.1 to 1.9-2)			
4	Specified TTE Q value (back-to-back)			
5	Segment Q value (computed from 3 and 4)			
5.1	BER corresponding to segment Q without FEC			
5.2	BER corresponding to segment Q with FEC			
5.3	Effective segment Q value with FEC			
6	Q limit compliance with [ITU-T G.826] or [ITU-T G.8201] after FEC			
7	Repair margin, component- and fiber-ageing penalty, pump(s) failure penalty, non-optimal decision threshold			
8	Segment margins			
9	Unallocated supplier margin			
10	Commissioning limits			

[134] Recommendation ITU-T G.977 (01/2015)

Abbreviations:

BER = Bit Error Ratio	PDG = Polarization-Dependent Gain	Q = Quality factor
BOL = Beginning of Life	PDL = Polarization-Dependent Loss	TTE = Terminal Transmission Equipment
EOL = End of Life	PMD = Polarization Mode Dispersion	

5.10 Threats to taking care

In addition to the technical design criteria, we also need to take account of different type of threats like natural threats, accidental threats and malicious threats. These threats can contribute to prolonging cable routes or partial routes or even altering the original planned routes.

Natural threats we can divide next way like sharks, earthquake, landslide, volcano, tsunami, iceberg, sea currents, storm winds and so on.

Accidental threats in everyday work at sea, such as fishing, dragging the anchor, dredging can damage undersea optical cables, and these jobs are a threat to the performance of marine light cables.

We also need to look at potential adverse threats as the undersea optical cable routes are long and going under the water. And there are in many countries who have the ability to join (tapping) fiber optic cables to eavesdrop the information what is being transmitted there. Every situation we must look for possibilities which way they are trying to do cyber-attacks to undersea optical fibers - tapping possibilities or other methods like side channel attacks, side channel eavesdropping. Also, we must look for encryption systems for layers 1, 2 and 3 so that we can protect our communications systems against cyber-attacks. The table 3 is done regarding phenomena in nature, offshore works and cyber threats impact levels.

From table 3 we can see upper level conceptual submarine cable segments` threat matrix. We need to take account when we are designing and developing undersea optical cable systems those threats which we are seeing in table. [135] [136]

Table 3 Upper level conceptual submarine cable segment threat matrix based on Threats to Undersea Cable Communications

Submarine Cable Segment Threat	Land and Beach Area	Near Shore Area ~50 m	Off Shore Area ~ 50 – 100 m	Continental Shelf ~ 100 – 200 m	Deep Sea ~200 m +
Natural Threats					
Sharks					
Earthquake					
Landslide					
Volcano					
Tsunami					
Iceberg					
Ocean currents					
Accidental Threats					
Fishing					
Anchor dragging					
Dredging					
Malicious and undersea warfare					
Cyber Attacks					
Vandalism					
Activists					
Theft					
Terrorist					
State-actors					
Undersea warfare					

Threat impact level in colors: Green = Low; Yellow = Medium; Red = High

[135] Threats to Undersea Cable Communications, September 28, 2017, Public-Private Analytic Exchange Program
Ye Yincan, Jiang Xinmin, Pan Guofu, Jiang Wei, Submarine Optical Cable Engineering, Elsevier Inc. 2018
The World's Major Earthquake Zones, https://www.thoughtco.com/seismic-hazard-maps-of-the-world-1441205
[136] Axe, David (2013) The Navy's underwater eavesdropper.
Parlamentskaja Gazeta. (2016). Корабль спецназначения «Янтарь» вошёл в Среди-земное море
Sutton, H. (2017) Russian ship loitering near undersea cables.

When looking at the threats to different segments, account must be taken of the areas in which the sea cable has been lowered, as well as the possibilities for different organisations and state operators to operate under sea level. The Arctic sea area is cold, and some of the sea area is also frozen. Only states or organisations with appropriate equipment for deep undersea activities that can only be found in large countries, such as China, Russia and the United States, can penetrate underwater optical cable systems. There are submarines in these countries, which include small submarines, which also allow underwater activities in a deeper sea area

5.11 Long distance cable systems, examples

As can be seen from Figure 9, the undersea cables types is depend on the depth of the sea and the vicinity of the coast in the areas where the above-mentioned threats exist and the threats are realized.

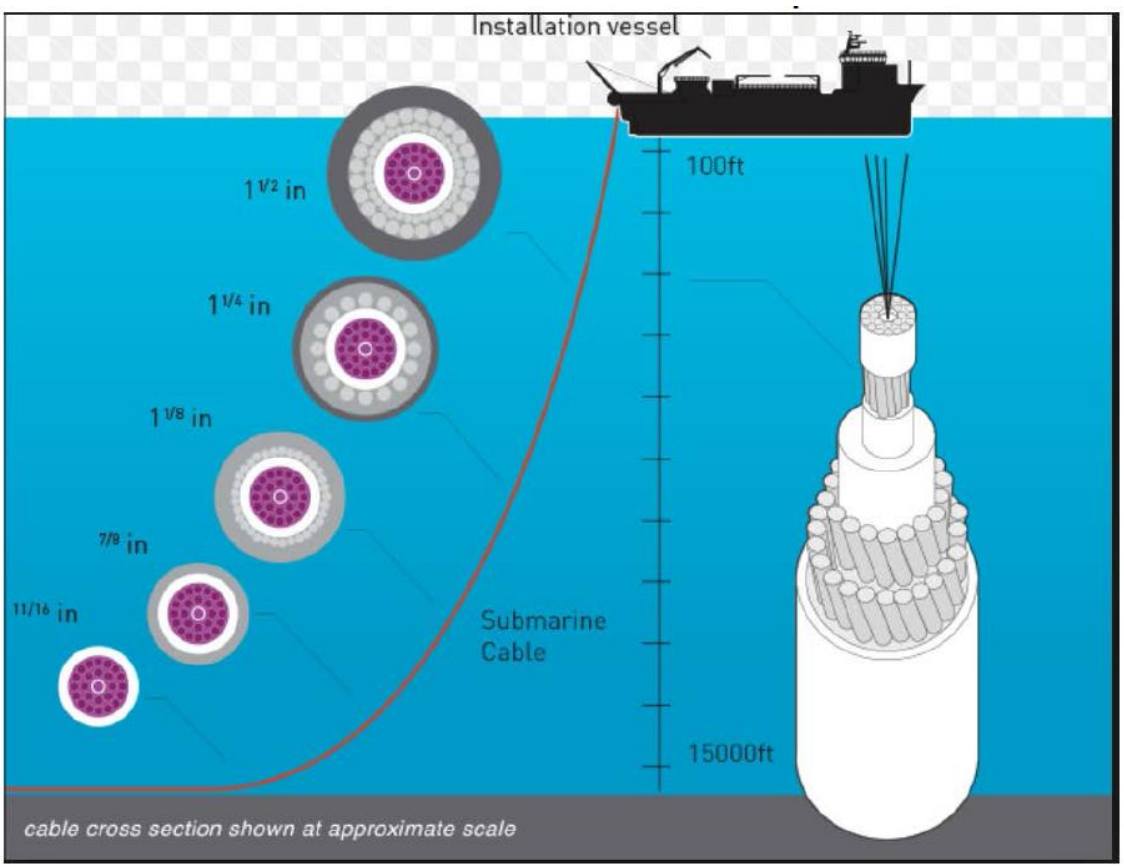


Fig 9. Optical undersea fibre optic cables depending on the depth of the ocean[137]

[137] Chesnoy Jose, Undersea Fiber Communication Systems, Elsevier ltd, 2016, pages 403-419

If we look at the cyber attackers' possibility to joining the optical cable, it would be easiest to penetrate the cable exactly where the cable armoring layers are smaller. This also means that the attacker must be able to operate deeply below the sea level. In practice, this ability is only a few large states.

If we look at this planned undersea optical cable system of 18,000 km, where the distances between the optical amplifier will be around 50 km. It also means that it allows cyber criminals to connect to underwater optical cables after each optical amplifier.

Next, we can look at the underwater optical system, based on ITU-T Recommendation G.709 (see Figure 10). It is divided into a land section, an underwater section, and a second part of a land section. In the section under water section there are the necessary branching equipment. In the figure 8, the land area is divided into a part of the Data Center and a part of the Cable Landing Station.

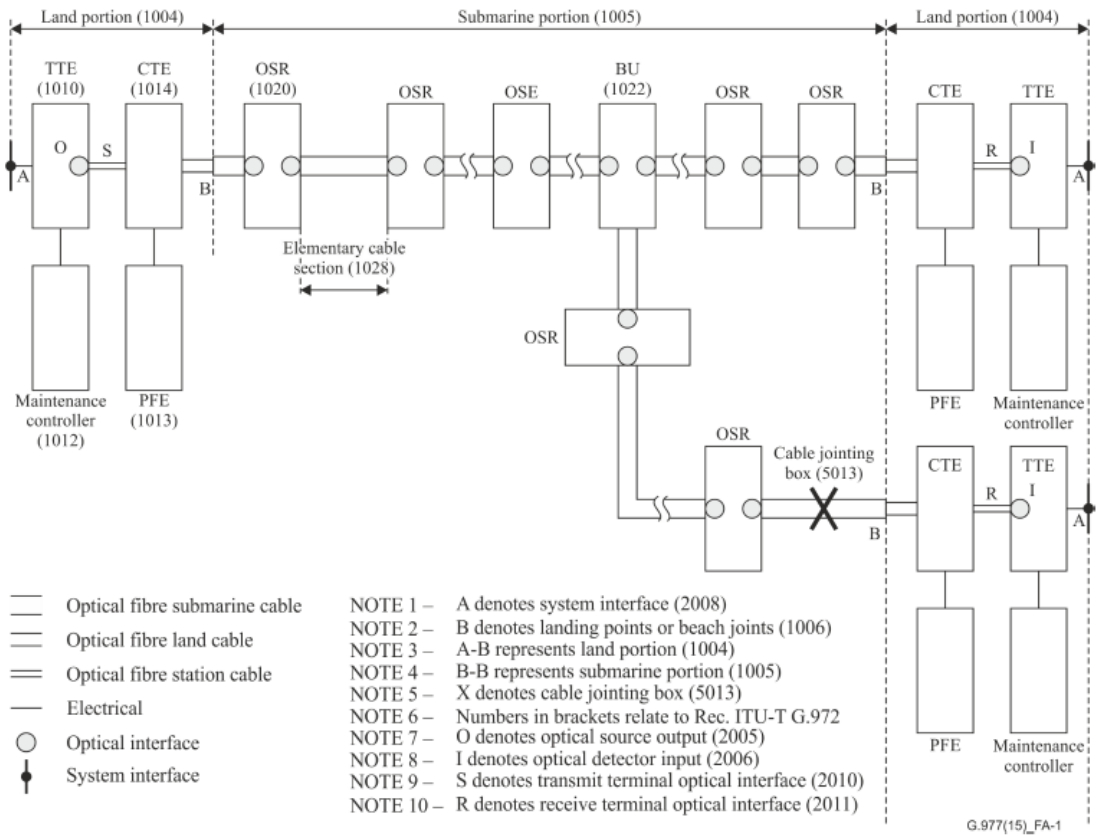


Fig 10. Figure of Optical undersea fibre optic system from ITU-T recommendation[138]

[138] Recommendation ITU-T G.977 (01/2015)

Abbreviations:

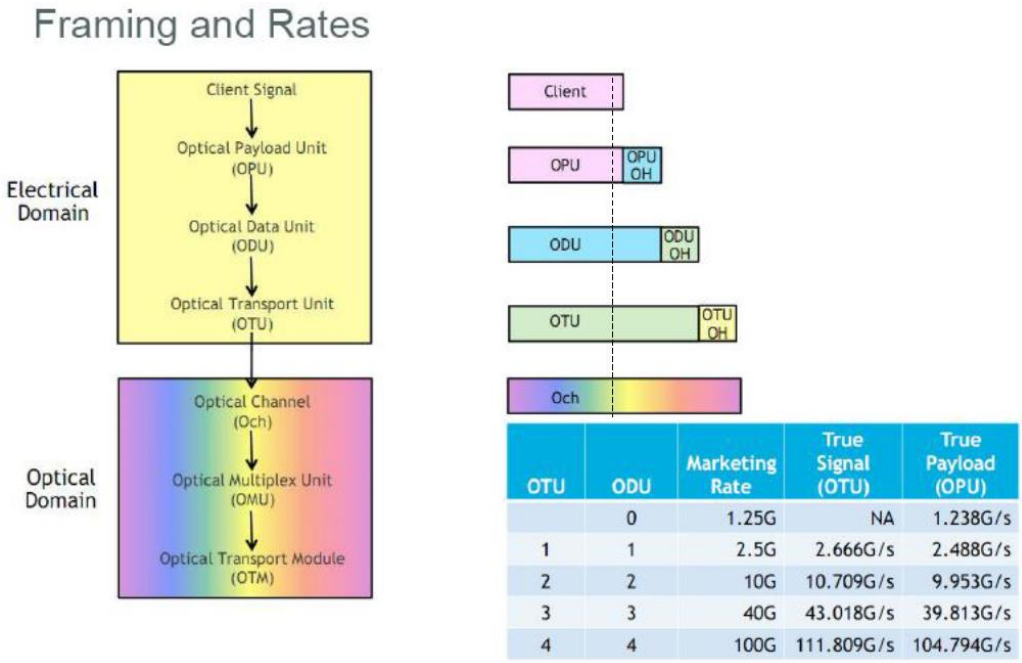
BU = Branching Unit	OSR = Optical Submarine Repeater	TTE = Terminal Transmission Equipment
CTE = Cable Terminating Equipment	PFE = Power Feeding Equipment	

When we have a 18,000 km long underwater fibre optic cable system in the use, we will need it also for management and control equipment and the necessary analytical equipment. In Figure 8 we can see Network Management System for both Data Center`s and Cable Landing Station`s. We need also Power Feed Equipment to our undersea systems, figure 8. We need also different types Optical Time Domain Reflectometers (OTDR) to certify the performance of fiber optics links and detect problems with existing fiber links. High capacity systems nowadays are possible to use measurement system like Coherent Optical Time Domain Reflectometry (COTDR). It is very important to use Coherent Optical Time Domain Reflectometry because 18,000 km optical systems we use different types of fiber cables compensating dispersion phenomena. This means also, that there are quite many branching points and cables extension points.

5.12 Long distance optical cable systems, management and control

Management and control systems are most critical In undersea optical cable systems. They must be protected in security against different type of attacks and they must be also protected for different types of faults. Architecture and management of submarine networks. [139] Today, optical signals have been used in scrambling technology. But is this scrambling technology good enough to protect management and control systems against cyber attackers, we can see.

[139] Chesnoy Jose, Undersea Fiber Communication Systems, Elsevier ltd, 2016, pages 341-379



OTU	ODU	Marketing Rate	True Signal (OTU)	True Payload (OPU)
	0	1.25G	NA	1.238G/s
1	1	2.5G	2.666G/s	2.488G/s
2	2	10G	10.709G/s	9.953G/s
3	3	40G	43.018G/s	39.813G/s
4	4	100G	111.809G/s	104.794G/s

Fig 11. OTN Optical Transport Network (G.709)

Figure 11 shows the Optical Transport Network (OTN, G.709), where the client signal is seen and how the header areas of the different layers are placed in relation to the client signal up to the transmission rate of up to 100 Gbit/s.

Figure 12 can be seen at a more precise level that what information by a cyber attacker can find out and use them which way they want if we do not encrypt the signals. For example, they can change the ROADM, Reconfigurable Optical Add-Drop Multiplexer, routing in whatever way they want and disrupt traffic or drive traffic to the desired connection point, for example, for analysis.

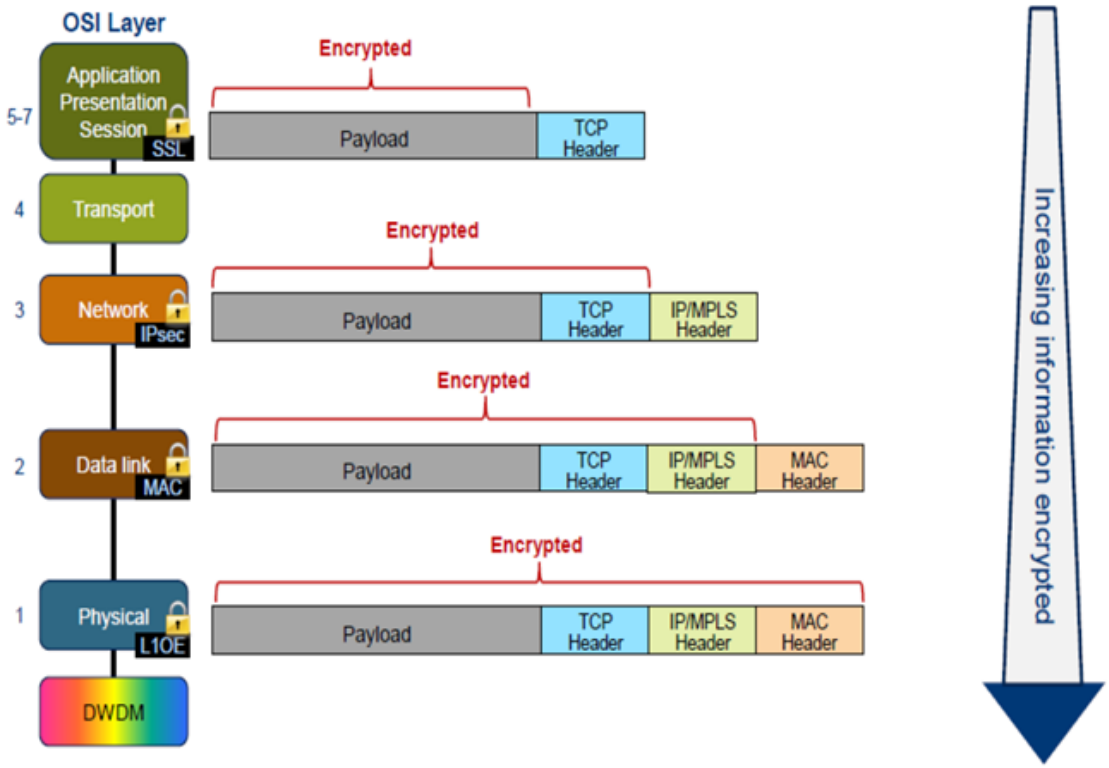


Fig 12. OTN Optical Transport Network (G.709)

5.13 Fault location, ITU-T recommendation, G.977/2015

A cable-break point is usually located in an out-of-service condition. Generally, an optical time domain reflectometry (OTDR) is employed for this purpose, a coherent optical time domain reflectometry (COTDR) is used especially in a long distance OFA system fault location because of its higher sensitivity and higher frequency selectivity. If optical isolators are used within each OFA, the back-scattered optical pulse, which is indispensable for OTDR measurement, is blocked. One solution for solving this problem is the use of a return path (COTDR path) that should not disturb the in-service traffic as shown in Figures. The transmission penalty induced by the COTDR path should be taken into account in the power budget. By using such a solution, COTDR facilities may be implemented in OFA systems to monitor the fiber span status. Moreover, if COTDR is employed in an in-service condition in the OFA systems via a return path, this method will have the potential to monitor the gain status of each OFA.

Two different ways may be chosen to implement a COTDR path inside a repeater:

- The first consists of connecting both outputs of one amplifier pair through optical couplers (refer to Figure 13).
- The second consists of connecting the output of one optical amplifier (OA) to the input of the OA located in the reverse direction (refer to Figures 14 and 15).
- Both solutions allow a bidirectional monitoring.

The definitions and parameters for OTDR and COTDR and related test methods are described in ITU-T G.976.

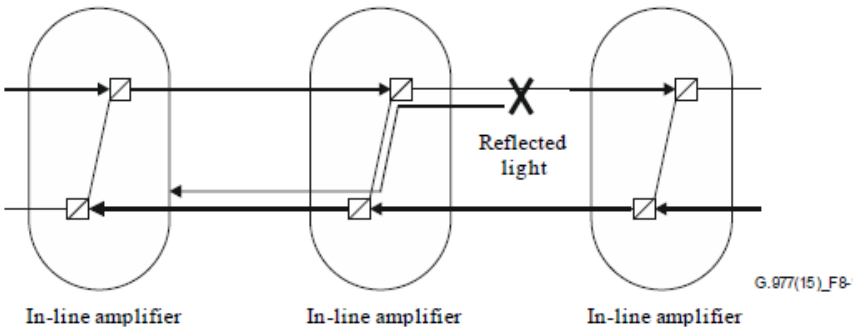


Fig 13. Example of fault location using COTDR for OF A with output-to-output loopback coupling.[140]

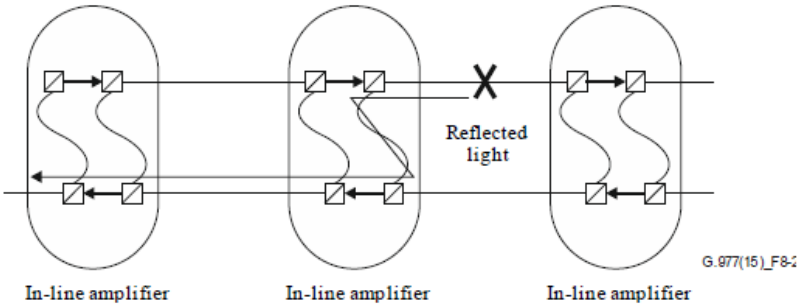


Fig 14. Example of fault location in the first fibre using COTDR for OF A systems using output-to-input coupler.[141]

[140] Recommendation ITU-T G.977 (01/2015)

[141] Ibid.

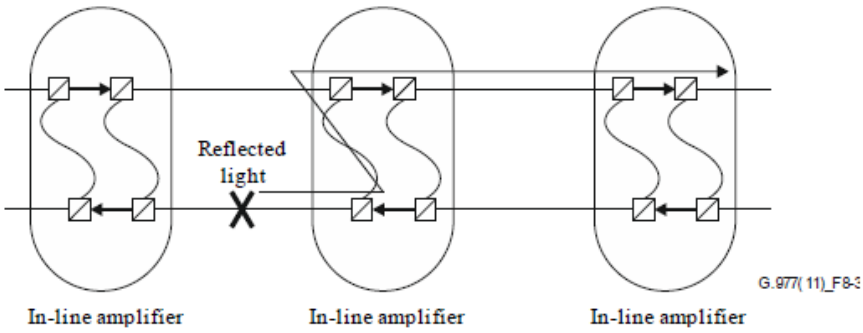


Fig 15. Example of fault location in the second fibre using COTDR for OF A systems using output-to-input coupler[142]

And we can find more from reference Technologies for the mitigation of transmission impairments in ultra-long band submarine networks. [143]

5.14 Cyber security

There are many possibilities from which cyber attackers should be possibilities to get inside the undersea optical cable systems and to its managements and control systems. From table 3 we can see upper level conceptual submarine cable segment threat matrix based on threats to Undersea Cable Communications. We also have a good note that cyber attackers, hackers and terrorists can use artificial intelligence to enable them to search from vulnerabilities in undersea optical cable systems through which they can penetrate systems and its services. After that they have possibilities to attack also to the Data Centers, which are different continents.[144] Undersea optical cable systems land and beach areas are easiest area to attackers to penetrate in to systems.

When using large capacity systems and new types of modulation technology in systems, undersea area the best possible cable tapping points for cyber attackers are after every optical amplifier. After that they have possibilities to get lot of information from different companies, organizations and governments.[145] [146]

---

[142] Ibid.

[143] Chesnoy Jose, Undersea Fiber Communication Systems, Elsevier ltd, 2016, pages 237-325

[144] Wargo Robert & Davenport Tara, Protecting Submarine Cables from Competing Uses, in Submarine Cables: The Handbook of Law and Policy, (in Douglas R. Burnett et al. eds., 2014)

[145] Threats to Undersea Cable Communications, September 28, 2017, Public-Private Analytic Exchange Program
Ye Yincan, Jiang Xinmin, Pan Guofu, Jiang Wei, Submarine Optical Cable Engineering, Elsevier Inc. 2018
The World's Major Earthquake Zones, https://www.thoughtco.com/seismic-hazard-maps-of-the-world-1441205

[146] Axe, David (2013) The Navy's underwater eavesdropper.
Parlamentskaja Gazeta. (2016). Корабль спецназначения «Янтарь» вошёл в Среди-земное море
Sutton, H. (2017) Russian ship loitering near undersea cables.

From figures 10, 11 and 12, we can see that if attackers get to join the optical marine cable system, they will also have access to the undersea optical cable systems, management system, and after that they have possibilities to do what they want and what suits their purposes. We also need to take care of power supply system's so that we can be certain that they do not have any vulnerabilities that an attacker can take advantage of and attack this way to our systems.

When we look for figure 4, Communications Networks in The Future, between different smart cities, and, we must look communications inside the cities, there are lot of challenges, which are coming from the operating environment and from heterogeneous telecommunication networks. There new devices and systems are seamlessly interconnected. These include the IoT (Internet of Things), D2D (Device-to-Device), M2M (Machine-to-Machine) or V2X (Vehicle to Everything) systems and lot of people`s smart devices. These systems have expanded into homes, building automation systems, cars and various control and energy systems and people are using their smart devices everywhere. These smart city systems also need applications and they are stored in the Data Center, shown in Figure 4 and 5. This also means that hackers, terrorists and Cyber attackers have a lot of possibilities to find vulnerabilities in this environment and attack those Smart city`s applications and services against. This allows also hackers and Cyber attackers to attack to services and service systems, which are on the other continents because the Data Center are interconnected.

5.15 Conclusion

The system to be built is technically very complicated and there will be many new technical solutions to meet the required transmission rates and meet the usability and quality requirements they require. This places considerable demands on the management and control of the system as well as on the organization of its maintenance. We should be also seen about the long-life cycle of undersea optical cable, about 25 years, to be taken it into account in design.
We must also look changes in social structures, that take place very quickly and they also affect the implementations and operating models, structures and people 's everyday lives and working environments. The current powerful digitalization trend increases the range of services offered and facilitates their easier use. These developments have also a strong impact on the service chains of the provided services, including subcontractors with subcontracting chains, hardware solutions, service providers and operating models to every part of the service chain in every continent.

Today and in the future modern communications connect data centers and data networks of different continents together, enabling real-time communication throughout the world. This type communications is possible through undersea optical cable systems, which we use for daily communications. Because submarine cables systems have been such a big strategic impact to our society, they are also a very interesting target for hackers, cyber attackers, terrorist and state actors. They seek to gain access to the information that goes through the networks of these continents which are connected to each other with sea cables.

For example, we need to be aware of the possibility of cyber attackers being able to connect to optical fibers, they have the option to change the ROADM routes, which can lead to the communication or disruption of traffic between the entire continents.

When considering the cyber security in systems design, we must take into account the upcoming technologies, which means there are more challenges ahead of us. In addition, changes in the cable technology due to dispersion phenomena make their own challenges in detecting intrusion into the cable. We have to be really careful about the design.

5.16 Future work

Because it is a critical system and it will be used by a number of countries, organizations and people for their own purposes, it is essential to study key issues affecting the functioning of the system.

- In relation to cyber security, the reliability of the scrambling mechanisms to protect the telecommunications used in those new nodes should be investigated.
- Artificial intelligence (AI) use needs to be investigate and clarified it`s possibilities to protect undersea fiber optic cable systems in order to better protect it malware and cyber-attacks against.
- The use of COTDR should be investigated as it is used for searching for faults and can also be used to detect tapping via cable connections.
- We must study undersea optical cable systems different protection mechanisms because of the it is extremely central fiber optic connection between different continents.
- We must study different type of protections mechanisms to power supply systems because they are most critical part of that systems.
- One study area would be different encryption systems, such as quantum encryption and or Layer 1 - 2 encryption systems.

REFERENCES

1. Carter Lionel et al., Submarine Cables and the Oceans: Connecting the World, 2009, http://www.iscpc.org/publications/ICPC-UNEP_Report.pdf
2. Chang Frank, Datacenter Connectivity Technologies: Principles and Practice, River Publisher, 2018
3. Chen Cheer, Fiber Optic Cabling Solutions, October 13, 2015. http://www.cables-solutions.com/tag/edfa
4. Chesnoy Jose, Undersea Fiber Communication Systems, Elsevier ltd, 2016
5. Davenport Tara, Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis, 24Cath. U. J. L. & Tech (2015). Available at: http://scholarship.law.edu/jlt/vol24/iss1/4
6. Miyamoto Yutaka and Kawamura Ryutaro, NTT Technical Review, Feature Articles: State-of-the-art Space Division Multiplexing Technologies for Future High-capacity Optical Transport Networks, Space Division Multiplexing Optical Transmission Technology to Support the Evolution of High-capacity Optical Transport Networks, Vol. 15 No. 6, June 2017
7. NTT, Technical Review, Space Division Multiplexing Optical Transmission Technology to Support the Evolution of High-capacity Optical Transport Networks, 2018. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201706fa1.html
8. Parlamentskaja Gazeta. (2016). Корабль спецназначения «Янтарь» вошёл в Среди-земное море
9. Sutton, H. (2017) Russian ship loitering near undersea cables.
10. Recommendation ITU-T G.977 (01/2015), file:///C:/Users/Martti/Downloads/T-REC-G.977-201501-I!!PDF-E.pdf
11. Sechrist Michael, New Threats, Old Technology: Vulnerabilities in Undersea Communications Cable Network Management Systems, Harvard Kennedy School, Belfer Center, Discussion Paper No. 2012-03, 2012, https://citizenlab.ca/cybernorms2012/sechrist.pdf
12. The World's Major Earthquake Zones, https://www.thoughtco.com/seismic-hazard-maps-of-the-world-1441205.
13. Threats to Undersea Cable Communications, September 28, 2017, Public-Private Analytic Exchange Program
14. Wargo Robert & Davenport Tara, Protecting Submarine Cables from Competing Uses, in Submarine Cables: The Handbook of Law and Policy, (in Douglas R. Burnett et al. eds., 2014).
15. Ye Yincan, Jiang Xinmin, Pan Guofu, Jiang Wei, Submarine Optical Cable Engineering, Elsevier Inc. 2018

ANNEX 1 ROTAKS

As a part of implementation of Russian Arctic Policy, the Ministry of Communications of the Russian Federation decided to build a submarine communication cable in Arctic areas in October 2011. The state-owned project's name is Rotacs (Russian Optical Trans-Arctic Submarine Cable System), or in Russian, ROTAKS (Российской оптической трансарктической кабельной системы). While commenting plans to build ROTAKS Minister of Communications and Mass Media of the Russian Federation Igor Shchegolev highlighted in 2011 that *"Strengthening Russia's northern borders is a strategically important topic. For this, according to the decision of the Security Council of the Russian Federation, it is necessary to develop the information and communication environment in the Arctic."*

ROTAX is a project of a transcontinental telecommunications route, which is to sail along the bottom of the Arctic Ocean along the London-Tokyo route. The total length of the communication line is 16,373 km. The capacity of the line is 60 Tbit/s; the guaranteed lifetime of the system is 25 years. The submarine optical cable, with a capacity of six pairs of optical fibers, provides a separate subsystem for servicing Russia's national interests in the Arctic region. This subsystem can serve as a basic physical platform for the Unified Protected Information and Transport System of the Transport Complex of the Arctic Zone of the Russian Federation (EKIS TKA).[147]

According to Russian sources the first phase of the construction of a system equipped with six pairs of fibers, along the route Bude (Great Britain) - Murmansk - Anadyr - Vladivostok - Tokyo is expected to be divided into three segments, which are Western, Arctic and Eastern segments. Western segment is from UK to Teriberka, Arctic from Teriberka to Anadyr and Eastern segment from Anadyr to Japan. At the second stage, it is planned to build cable outlets on the coast of the Russian Arctic in the adjacent northern territories (Arkhangelsk-Norilsk-Khatanga). The third stage is the passage of the main road through the southern and central regions (Samara-Omsk-Taishet).[148] (Sib.FM, 2011). Expenses for the first stage are estimated at $ 860 million. The second and third stages - the construction of outlets on the coast of the Russian Arctic and the Far East and the construction of a land route in partnership with the company Transneft are estimated at $ 500 million each.[149]

The figure 16 illustrates the Russian Optical Trans-Arctic Submarine Cable System.

---

[147] Ivanov, M., Россия построит собственную трансарктическую кабельную систему, 2011

[148] Sib.FM, Высокоскоростной интернет появится на севере Сибири к 2014 году, 2011. http://sib.fm/news/2012/04/02/vysokoskorostnoj-internet-na-severe-sibiri-k-2014-godu

[149] Ivanov, M., Россия построит собственную трансарктическую кабельную систему, 2011

Fig 16. Russian Optical Trans-Arctic Submarine Cable System

In April 2012, the Polarnet Project Company signed an agreement with the US-based Tyco Electronic Subcom (TES) for the construction of a ROTAKS submarine cable system based on the "turnkey" principle. The work did not start when Russia took over in February 2014 Crimean and Ukrainian war started in the same spring. Relations between the West and Russia have cooled down and the Western countries imposed severe sanctions, especially on high technology exports to Russia. Marine cables, especially those in extreme conditions such as the Arctic region, which are used for a minimum of 25 years, are high technology products. Russia does not produce these high-performance and sufficiently reliable optical sea cables. The ROTAKS system, which would also transfer Western information, should meet Western standards. This means that the cables should in practice be manufactured in the West. Russia cannot build the ROTAKS system without the participation of westerners in the project. The sanctions prevent the sale and installation of a sea cable to Russians. While new information concerning the ROTAKS has not been heard recently, another Russian-based initiative emerged in April 2018 when the Russian Ministry of Defense announced its plan to install a fiber-optic cable between Severomorsk and Vladivostok. This new connection was to serve the Navy and coastal troops (Nilsen 2018; Navy Recognition 2018). However, hardly anything has been heard from this project since its inauguration.[150]

---

[150] Navy Recognition, Russian Navy to lay fiber optic cables to connect Arctic and Far East. Navy Recognition, April 25, 2018
Nilsen, T., Russia plans to lay trans-Arctic fiber cable linking military installations. The Independent Barents Observer, April 24, 2018

Informaatioteknologian tiedekunnan julkaisuja
No. 78/2019

ISBN 978-951-39-7721-4 (verkkoj.)
ISSN 2323-5004

JYVÄSKYLÄN YLIOPISTO