INTERNATIONAL SUBMARINE COMMUNICATION CABLES AND CYBER SECURITY THREATS

INTRODUCTION

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 it 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. In present day, no technology other than submarine cable systems, have not had such a strategic impact on our society without being known as such by the people. This also means that it is at the same time a very interesting target for hackers, cyber attackers, terrorist and state actors. They seek to gain access to information that travels through the networks of the continents that are connected to each other with sea cables.

Submarine Communication Cables

Submarine communication cables have been important for strategic communication since the mid-19th century, and fibre optics in the 1990s made modern sea cabling even more critical. Nowadays sea cables transfer nearly all our global telecommuni cations data. Questions concerning national security and cyber security have always been relevant from the perspective of the development of submarine communication networks. Security concerns have not only affected decisions concerning the route and landings, but also used as arguments when, in different stages of history, the role of cable networks and wireless solutions have been debated. Furthermore, security concerns have hindered, for example, plans aiming at the utilisation of submarine fibre-optic infrastructure for scientific purposes. Every cable landing station has been built in the same way, depending on the beach area, of course, which is the delivery site for the submarine optical cables. When using large capacity systems and new types of modulation technology in submarine cable systems, the best possible cable tapping points for cyber attackers are after every optical repeaters or amplifiers. Between continent cable station sites, the branching points and other submarine cable system ends, there are many optical

amplifiers every 50 km. In some parts of cable systems, there are also equalisers (passive or active).

Dense Wavelength Division Multiplexing (DWDM) is an optical multiplexing technology used to increase bandwidth over existing fibre networks. DWDM works by combining and transmitting multiple signals simultaneously at different wavelengths on the same fibre. The device and components used in DWDM technology cause some form of crosstalk in one form or another. Devices used in DWDM technology include filters, wavelength multiplexers and demultiplexers, switches, and optical amplifiers. Crosstalk is also caused by the fibre itself due to its non-linearity. Therefore, eavesdropping over the cable cannot be prevented.

This whole system also needs electrical energy. Energy input to the system can be made from one or more earth points. We also need to take care of power supply systems, so that we can be certain that they do not have any vulnerabilities that an attacker can take advantage of, and in this way gain access to our systems.

Cyber Threats Against Submarine Communication Cables

There are many possibilities from which cyber attackers could get access into the submarine optical cable systems and to its management and control systems. We also have a good indication that cyber attackers, hackers and terrorists can use artificial intelligence to enable them to use vulnerabilities in submarine optical cable systems, in order to penetrate systems and its services. After that, they also have the possibility to attack the data centres, which are located in different parts of the world. Submarine optical cable systems on land and beach areas, are the easiest areas for attackers to penetrate systems.

Cyber intelligence against submarine communication cables

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 opposing side to redirect the information flow into cables that were being monitored by their own intelligence service.

Intelligence collection from submarine cables can be done by eavesdropping (tapping) or side channel eavesdrop ping exploiting optical overflow or hacking control systems of cables. The

geographical location of the installation of a tapping device depends on the depth of the sea and the distance of the installation place from the mainland.

Eavesdropping of the cables

Tapping means connecting/installing intelligence collection device(s) to the cable or to the fibre pair either on the ground, at a landing point, in points where the traffic is amplified or in the seabed. The exploitation of optical overflow can be done either in the cross-connection points of the fibre pairs/cable or from one fibre pair to another. The geographical location of the installation of a 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 devices. 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 superpowers have the intention and need, technical equipment, skills, and practice to collect intelligence from submarine cables also in the demanding environment. Cable collection is technically possible in the bottom of the sea and in the points, where the cable is not in the sea, i.e. on the ground. In practice, it is also possible at points where the traffic is amplified or where there is another physical access to the cable (for example in teleoperator facilities).

According to open-source reports, the modified Seawolf class submarine USS Jimmy Carter is almost certainly able to tap the submarine communication cables. In the USS Jimmy Carter, there is a constructed multi-mission platform, which enables the use of a Remotely Operated Underwater Vehicle (ROV). ROV can be used for installing tapping devices to submarine communication cables. Even if this is technically possible; some experts consider this kind of intelligence collection too risky and expensive. Russia's Defense Ministry Main Directorate of Deep-Sea (GUGI) Military Unit 40056 is responsible for Russian 'underwater engineering'. The task of this unit is to eavesdrop communications cables, install movement sensors, and collect the wreckage of ships, aircraft, and satellites from the seabed. The divers work at depths of 3000-6000 meters in miniature submarines. One of the ships of GUGI is a special purpose intelligence collection ship Yantar. Yantar's equipment and devices are designed for deep-sea tracking, as well as for connecting to top-secret communication cables. The home port of Yantar is Severomorsk in Kola Peninsula. Yantar can act as a mothership to Rus (AS-37) and Consul (AS-39) class deep-sea vehicles. The task of this unit is to eavesdrop communications cables, which can operate at depth up to 6000 meters. Yantar can also be used as a mothership for ARS-600 deep diving manned submer sible, which can operate at depth of 600 meters.

Hacking of the Cables

Hacking is the other way to collect intelligence from the submarine cables. All the main intelligence services have possibility to access to submarine 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.) such as cutting the connection in the cable. In addition, some non-state actors might have the capability to intrude the submarine communication cable at least in the landing stations.

If attackers hack the submarine optical cable systems, they will also have access to the submarine optical cable management system, and after that they have the opportunity to do what they want and what suits their purpose.

High Seas

Customary international law has always recognized military activities including intelligence gathering has a lawful use of the high seas associated with the operation of warships exercising the freedom of navigation.360 The list of high seas freedoms set forth in Article 87 of UNCLOS was not intended to be an exhaustive list,361 and although not explicitly mentioned in Article 87 of UNCLOS, it is generally agreed that intelligence gathering is a high seas freedom.362 As mentioned above, the laying of cables is also a high seas freedom,363 and thus, prima facie, a country's military forces would be free to lay cables with underwater listening stations used specifically for military purposes pursuant to this right.

The International Maritime Law Does Not Protect Against Cyber Attacks

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 unmanned and autonomous weapon systems. The international maritime law only consider damage to submarine cable as a crime. Although, it is possible outside territorial sea to conduct operational action within the framework of a criminal investigation or the prevention of a crime. Taking in an account the specifics of maritime zones which are located outside of state sovereignty, it is not possible 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 cyber- attacks, using unmanned and

autonomous weapon systems. There is a need for more comprehensive threat intelligence and protection.

The international maritime law only consider damage to submarine cable as a crime

International law will be applying the right to self-defence or collective security operations authorised by the Security Council in the case of cyberattacks, including the necessary requirements for its implementation, and establishes the necessary standards of evidence to justify the use of force. The momentum and attribution of cyberattacks makes distinguishing between the actions of terrorists, criminals and nation-state sponsored attackers difficult. 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.

Conclusion

Because submarine cable systems have such a considerable strategic impact on our society, that also means that it is a very interesting target for hackers, cyber attackers, terrorist and state actors. We need to look at potential adverse threats as the submarine optical cable routes are extensive and run under water. In addition, there are many countries who have the ability to join (tapping) fibre optic cables under the water or at a landing station to eavesdrop information or hacking or sniffing the cables. All the states that are in the area, which the cable is running through, have interest, motivation, and technical capabilities to collect intelligence information from these cables at least in the points, where the cable is on land. Real point-to-point encryption is the only way to fight against the cyber intelligence in submarine communication cables. Technology may help in cyber security. High-capacity systems, nowadays, have the capability to use a measurement system like Coherent Optical Time Domain Reflectometry (COTDR). The use of COTDR should be investigated more carefully as it is used for searching for faults and may also be used to detect tapping via cable connections.

Furthermore, Artificial intelligence (AI) tools and methods will be solutions to protect submarine fibre-optic cable systems. AI based systems using Neural Networks and Deep Learning are, even today, capable of detecting and preventing different cyber-attacks. The submarine cable system is technically very complex, and in the future, there will be many new technical solutions, transmission speeds will increase, and usability and quality requirements will also increase. This places significant demands on the management and control of the system as well as its cyber security. We should also take into consideration the long-life cycle of submarine optical cables, which is about 25 years, in security design.