CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Strategic importance of, and dependence on, undersea cables

November 2019

About this paper

This paper is a collaborative view of the NATO CCDCOE Strategy and Law Branch researchers highlighting the strategic importance of undersea cables in cyber security and the dependence of states on their functioning. This is not a complete catalogue of states' dependence on undersea cables for cyber security, neither are the issues presented in any particular order. While the authors have made an effort to describe the dependence on undersea cables from a global perspective, it is acknowledged that there may be national and regional differences.

The authors of this paper are independent researchers at the NATO CCDCOE; they do not represent NATO, nor does this paper reflect NATO's position. The aim of the paper is solely to make member states and partnering countries reflect on the transmission of data via undersea cables and where necessary, strengthen their security efforts in this area.

1. What are undersea cables and why do we depend on them?

a. More than 97% of all internet traffic is transmitted via undersea cables.[1] Today, practically everyone is reliant on the internet on a daily basis. We are connected via the internet, both personally and as part of society. Modern societies put more and more emphasis on cloud computing – the practice of using a network of remote servers hosted on the internet to store, manage and process data, rather than a local server or a personal computer. The "cloud" is therefore in reality nothing but servers, which may be on another continent but linked to you via cables.

b. Even if drastically improved, transmitting data via satellite would only be able to cope with a fraction of our requirements. Transmission of data via cables is both cheaper and many times faster than via satellite and the technological possibilities therefore dictate the use of cables for internet connectivity. On land, this poses relatively few complications as the cables are protected by their owners and national jurisdiction. Protection at sea, however, both physical and legal, is more difficult.

c. When connecting continents or land divided by sea, undersea or *submarine* cables are installed on the ocean floor. Without the functioning of these cables, connectivity would be lost between nations or territories divided by sea.

Just as we are reliant on the electrical power grid for the functioning of modern society, we have become reliant on internet connectivity. The cables providing this connectivity are therefore part of our critical infrastructure, and must be protected as such to safeguard the sovereignty of the data needed for a modern society to function.

d. Modern undersea cables use fibre-optic technology to pass data literally at the speed of light. Even though the cables may be strengthened near the shore, the average diameter of a fibre-optic cable is not much greater than that of a garden hose.

The diagram below (**Fig.1**) illustrates the cable composition.

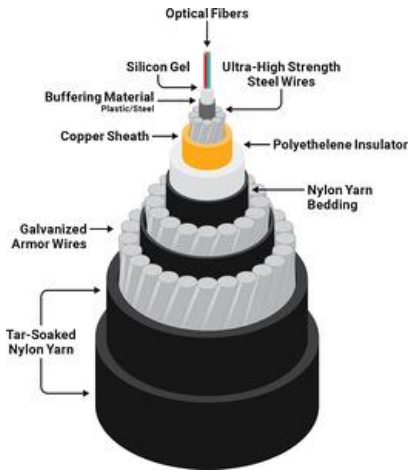

Fig. 1. Diagram of an undersea cable (www.telegeography.com).

e. As the central nervous system of the global internet, undersea cables are strategically important and as such are part of the critical infrastructure of societies. Most countries have identified their critical infrastructure and made plans for its protection. However, as undersea cables joining countries and continents must pass through international waters, they cannot solely be protected by national legislation,

national law enforcement or the military.

With the roll-out of 5G, the internet will become much faster and will enable an even higher amount of data to be sent and received. As a result, more devices may be connected to the internet, and as the amount of data grows, so will our reliance on undersea or submarine cables.

f. As of 2019, it is estimated that there are globally more than 378 undersea cables in service totalling more than 1.2 million kilometres – and the number is growing. There are on average more than 100 undersea cable breaks each year, most of which are caused by human activity such as anchoring or fishing. [2] Naturally, protecting cables becomes even more important where resilience and redundancy are low and countries or islands are only connected through one or two cables.

The map below (**Fig. 2**) gives an impression of how the world is connected by undersea cables.

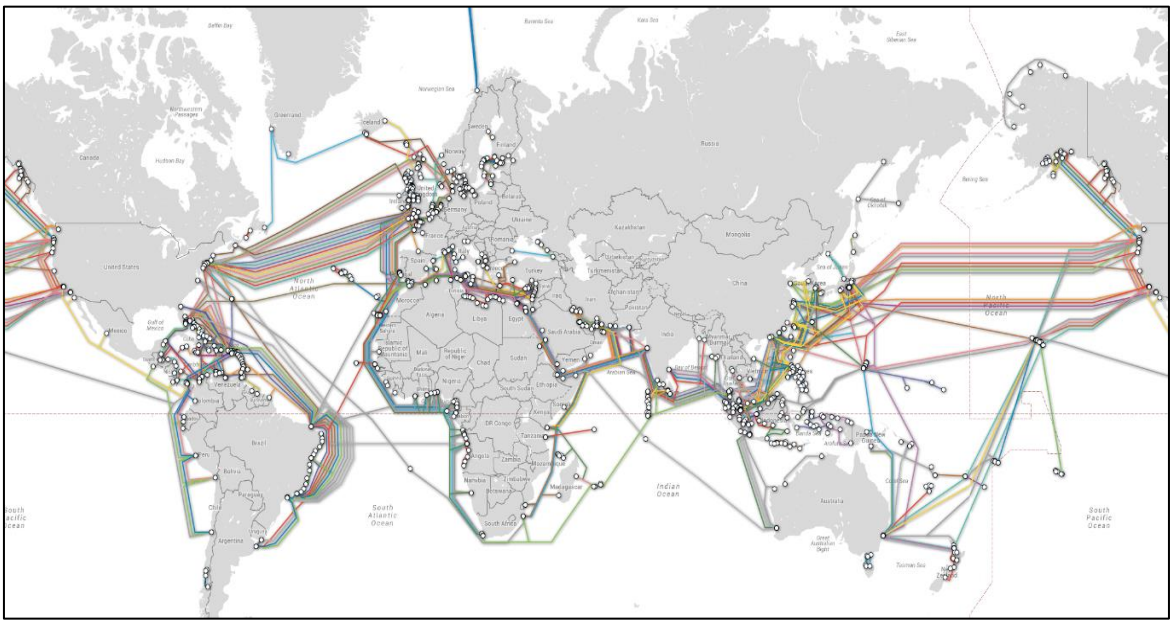

Fig. 2. Map showing undersea cables worldwide (www.telegeography.com). The cable routes are stylised and do not reflect the actual paths taken by the various systems.

2. What are the threats to undersea cables?

a. Interruption of services may happen to all cables but the consequences of a severed undersea cable, in particular, may be more profound and costly to repair. According to telecommunications market research and consulting firm *TeleGeography*, accidents caused by fishing vessels and ships dragging anchors account for about two-thirds of all faults to undersea cables, but environmental factors such as earthquakes may of course also contribute to cable damage. Furthermore, underwater components may fail of their own accord – but that is less common.[3]

b. Threats to undersea cables may be categorised as either ***natural threats*** or ***threats caused by human activity***. The latter may be divided into ***intentional*** or ***unintentional*** human activity. Threats arising from unintentional activity such as fishing, dredging or anchoring and natural threats such as those resulting from, for instance, an earthquake or landslide, are not the focus of this paper. Rather this paper is focused instead on threats arising from *intentional human activity*.

c. Broadly speaking, threats posed by intentional human activity may be sub-categorised into either sabotage or espionage. The effect of sabotaging an undersea cable is obvious, as it would stop users sending and receiving data through it and, depending on the resilience, possibly cut off an area from use of the internet. In most cases, however, data may be rerouted through other cables or even via satellite. In operational terms, this may be compared to destroying a road or rail bridge, thereby denying passage or channelling traffic through a certain area. The other threat, espionage, requires special equipment only available to a few states. Specially equipped submarines, or submersibles operating from ships such as

the Russian *Yantar,* are able to access the data in fibre-optic cables without damaging them, and can thereby listen in to, jam, and possibly also alter data passed through cables.

The most vulnerable point of undersea cables is, however, where they reach land at cable landing stations (CLS). Here they are more accessible without specialised equipment, and may be targeted by terrorists or other criminal organisations.

d. **Maintaining cyber security is not only about protecting the data – the binary "zeros and ones" – but also the means by which this data is transmitted.** As the "cloud" is in reality nothing more than cables used as a "freeway" for data on which we are increasingly dependent, we, as societies, must make a greater effort to protect this means of transportation.

   Legislation and general awareness of the importance of and dependence on undersea cables is generally lacking and, perhaps, considered less important than maintaining cyber security through algorithms. Also lacking is a general understanding of the inherent vulnerabilities of these cables and, consequently, the mechanisms, including legislation, required to protect them.

e. **When an undersea cable is severed or damaged, it is both costly and time-consuming to repair.** Depending on the location of the incident, the availability of a cable repair ship and the weather, it may take several weeks and cost in excess of one million USD for a repair to be completed.

f. **As critical infrastructure, undersea cables should be protected to the best of our ability.** Needless to say, the consequences of losing the ability to send and receive sovereign data via an undersea cable may be grave for individuals as well as companies and nations. Most often, data may be rerouted via other cables; but in cases where redundancy is low or non-existent, with only one or a few cables available, resilience will be low and vulnerability consequently great.

3. Strengthening physical security

a. **Undersea cables are normally physically better protected in areas where there is a greater risk of damage.** Near the shore, for instance in shallow waters where ships may anchor, cables will be strengthened by thicker armour and often also protected by surrounding piping and dug into the seabed and/or shore.

b. **Some governments may in addition have imposed cable protection zones and penalties for damage.** Such procedures are, however, not generally implemented, but they could reduce *unintended* cable damage.

c. **To reduce the threat from *intentional* cable damage, more could be done to protect cable landing stations (CLS).** Often the infrastructure surrounding the CLS is not sufficiently protected to prevent damage from either natural or human activity. Placing CLS where they are not likely to be affected by flooding, tsunamis or other weather extremes should be done automatically, but often that is not the case.

d. **With changing security threats, there should be more emphasis on securing CLS from *intentional human activity*.** Restricting unwanted access by setting up perimeter fences, video surveillance cameras and movement sensors, together with a physical access control or guard, would strengthen security. Undersea cables support billions of dollars' worth of trade and yet many CLS are less protected than the average bank.

e. **In order to ensure connectivity, it is also important to think about protecting Submarine Line Terminating Equipment (SLTE) and other associated infrastructure.** All the systems needed for the functioning of cables – such as electrical power, heating, ventilation, air-conditioning, emergency generators, line monitoring equipment etc. – are also vulnerable and must be protected from both physical interference, cyber-attack and electro-magnetic pulse (EMP). The latter may be done through the installation of a Faraday cage around installations to block electro-magnetic fields.

f. **Undersea cables have traditionally been owned by a consortium of telecom carriers.** Later, entrepreneurial companies selling off internet capacity to users laid many cables. Even though both of these models still exist, recently content providers such as Google, Facebook, Microsoft, and Amazon have entered the market as major investors in new cables, and the amount of capacity deployed by these content providers has now overtaken that provided by internet operators as they are getting ready for 5G Internet.

g. **If the service provider cannot guarantee continual integrity, those buying the service may find another provider.** Ultimately, governments rely on the uninterrupted functioning of the internet to provide many services of society. Therefore, pending national legislation, some governments and service providers may wish to form Public Private Partnerships (PPP) to take a more proactive role in guaranteeing the provision of services.

4. Protection of Submarine Cables – a Legal Perspective

Recognising undersea cables as part of the critical infrastructure for both individual nations and the Alliance, and strengthening the physical security surrounding them, is important. However, understanding the legal framework governing undersea cables is also essential to protecting them. It is not within the scope of this paper to give an in-depth analysis of the legal framework relevant to the protection of undersea cables. The physical layer of cyberspace, including undersea cables, within a state's territorial sea is quite evidently subject to that state's sovereignty.[4] Still, there are three international conventions that may be relevant as a legal basis for protection in the High Sea: *The Convention for the Protection of Submarine Telegraph Cables; The Geneva Convention on the High Seas;* and *The United Nations Convention on the Law of the Sea (UNCLOS)*.

a. **The Convention for the Protection of Submarine Telegraph Cables[5] (1884)** is the first convention to regulate the protection of undersea cables. The convention only focuses on undersea cables located in the high seas. Article 2 makes it a punishable crime to *"break or injure a submarine cable, wilfully or by culpable negligence, in such manner as might interrupt or obstruct telegraphic communication."* However, according to Article 15, *"It is understood that the stipulations of this Convention shall in no wise affect the liberty of action of belligerents."* This convention is therefore not applicable to situations of armed conflict.

b. **The Geneva Convention on the High Seas (1958)[6]** in its Article 27 reiterates the 1884 Convention by stating that states party shall "*take necessary legislative measures*" to make breaking of cables a "*punishable offense*." However, the High Seas Convention fails to address cases of intentional damage.

c. **The United Nations Convention on the Law of the Sea (UNCLOS)[7]** was adopted and signed in 1982 and came into effect in 1994. It supersedes the Geneva Convention on the High Seas, and defines the rights and responsibilities of nations regarding their use of the world's oceans and establishes guidelines for businesses, the environment, and the management of marine natural resources.

   There are currently 162 states party to UNCLOS, and although Turkey and the US are not parties, many (but not all) of the rules therein may be regarded as an expression of customary law.

Articles 113-115 of UNCLOS repeat the demand from the High Seas Convention that states party to the convention must adopt domestic legislation penalising damage to cables by ships or persons belonging to their jurisdictions. UNCLOS supersedes part of the Submarine Cable Convention, in particular with regard to the right of visit on the High Seas. Therefore, the provision found in the Submarine Cables Convention is no longer legally applicable among states party to UNCLOS. States not party to UNCLOS could, however, continue to invoke the Submarine Cable Convention (among NATO member states only the US might qualify in this regard).

UNCLOS further permits states the sovereignty to, among other things, lay cables in their Exclusive Economic Zone (EEZ), extending up to 200 nautical miles from their territorial waters. The freedom for signatory states to lay cables on the continental shelf follows from UNCLOS, Article 79.

Article 113 of UNCLOS implies that the breaking or injury of a cable need only be punished under domestic law if it is *"liable to interrupt or obstruct […] communications".*[8] On the other hand, Article 113 also expands its scope of *"a punishable offence"* to include *"conduct calculated or likely to result in such breaking or injury"* (of a submarine cable). Under UNCLOS, a state "would, for the first time, be able to act to *prevent* cable breaks from occurring".[9] Leaving aside the issue of whether attempted damage is to be included in its scope, at least the prohibition on the infliction of damage to cables is, according to the *Tallinn Manual 2.0*, a matter of customary international law.[10] Hence, it is binding on states that are not party to UNCLOS such as Turkey and the US.

An intelligence operation against an undersea cable may not be punished unless it meets the requirements set forth in Article 113, such as both physical effect (damage) to the cable and the disruption of communication. This is unlikely to be the case, as tapping or tampering with undersea cables could be done without any tangible impact.

UNCLOS provides that a coastal state has jurisdiction with regard to Marine Scientific Research (MSR) in the EEZ. UNCLOS does not, however, define MSR. A certain number of coastal states, such as China, insist that a coastal state jurisdiction based on the sovereign right covers not only MSR but also any other military exercises and surveys,[11] and non-coastal states must obtain consent from a coastal state when they conduct both MSR and any military activities. However, such views are the minority.[12] Belgium, Germany, Italy, the Netherlands and Sweden clearly indicate the opposite position in their declarations to UNCLOS.

d. **The *Tallinn Manual 2.0* on the International Law Applicable to Cyber Operations** has been developed by the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE) in order to map international law applicable to cyber operations. The manual, which has formulated 154 rules, is a product of the findings of an independent group of legal experts and covers operations in both armed conflict and peacetime.

   Rule 32 of the *Tallinn Manual 2.0* states that "[a]lthough peacetime cyber espionage by States does not *per se* violate international law, the method by which it is carried out might do so."[13] It is therefore relevant to look at whether cyber espionage such as submarine intelligence operations against undersea cables would be prohibited or restricted by the United Nations Convention on the Law of the Sea (UNCLOS)[14] and other conventions on the Law of the Sea.

   Unlike warships and submarines,[15] cables used for military purposes do not explicitly enjoy sovereign immunity. The relevant provisions in UNCLOS and other international conventions concerning the protection of undersea cables are, however, equally applied.[16] In this regard, the *Tallinn Manual 2.0* in Rule 54 states that "[t]he rules and principles of international law applicable to submarine cables apply to submarine communication cables".[17]

   For the purposes of this Rule, "submarine communication cable" refers to any cable owned, operated or laid by a state, as well as privately owned cables, authorised by that state for telecommunications and data traffic.[18]

e. **States may "adopt laws and regulations" in their territorial sea for the protection of their undersea cables**, as long as these do not impose restrictions impeding innocent passage (Rule 48).[19] In the same vein, states "may also regulate activities involving [undersea cables] in international straits, unless the regulations impede or hamper transit passage through them" (Rule 52).[20]

   Legally, it is disputed whether a state has the right to establish cable protection zones restricting certain activities, such as anchoring or fishing, that pose a threat to cable integrity. Australia and New Zealand were among the first to create cable corridors/protection zones within their territorial sea and EEZ.[21]

f. **Without prejudice to the rules applicable during armed conflict,** the group of legal experts behind the *Tallinn Manual 2.0* found that infliction of damage to undersea cables by a state would be prohibited as a matter of customary international law.[22] Within a hybrid warfare scenario, actions taken which may be attributed to a state would therefore fall under this rule. However, the rule implicitly implies that undersea cables may be targeted in an armed conflict (as long as the rules therein are followed).

g. **Physically tapping an undersea cable in order to collect data transmitted through it** would, according to Rule 4,[23] constitute a violation of a state's sovereignty if the tapping were done in that state's territorial or archipelagic waters. It would, however, not be a violation of the sovereignty of other states such as those that laid or operated the cable. The use of a submarine or unmanned underwater vehicle would be inconsistent with the right of innocent passage (described in Rule 48),[24] requiring submarines to travel on the surface.

h. **As concluding remarks, this paper has stated that undersea cables are to be regarded as critical infrastructure** for both nations and the Alliance and should be protected as such.

   It is impossible to guarantee the constant integrity and functioning of undersea cables, but there are ways to protect not only the cables themselves but also the CLS and SLTE.

   Better protection may be achieved if there is collaboration between the cable's owners and the state in which it is laid. Public Private Partnerships (PPP) could, where national legislation permits, help close any gaps in the physical protection within the jurisdiction of a state.

   On the High Seas, the legal regime found in The Convention for the Protection of Submarine Telegraph Cables, The Geneva Convention on the High Seas and The United Nations Convention on the Law of the Sea (UNCLOS) plays an important role in defining which actions may and may not be permissible.

   The *Tallinn Manual 2.0,* although intended for lawyers, may also help non-lawyer decision-makers in understanding the legal framework under which undersea cable protection must be strengthened.

[1] In 2016, the World Economic Forum estimated that 99% of all internet traffic goes through undersea cables

https://www.weforum.org/agenda/2016/11/this-map-shows-how-undersea-cables-move-internet-traffic-around-the-world/

[2] TeleGeography - Submarine Cable Frequently Asked Questions
https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions

[3] Ibid.

[4] Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017), p. 14.

[5] Signed on 14th March 1884, came into effect on 1st May 1888. The original text of the Convention can be accessed at the International Cable Protection Committee website, https://www.iscpc.org/information/government-and-law/

[6] Signed on 29th April 1958, came into effect on 30th September 1962. *The United Nations Treaty Series*, Vol. 450, p. 11

https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XXI-2&chapter=21

[7] Signed on 10th December 1982, came into effect on 16th November 1994, *The United Nations Treaty Series*, Vol. 1833, p. 3, https://treaties.un.org/pages/ViewDetailsIII.aspx?src=TREATY&mtdsg_no=XXI-6&chapter=21&Temp=mtdsg3&clang=_en

[8] Ibid. p. 308.

[9] Eric Wagner, "Submarine Cables and Protections Provided by the Law of the Sea," *Marine Policy*, Vol. 19, No. 2 (1995), p. 136.

[10] Schmitt, *Tallinn Manual 2.0*, p. 256, para. 15.

[11] The number of nations that restrict military activities in the EEZ is known to be 29.

(1) Nations that restrict military activities in the EEZ: 19-
Bangladesh, Brazil, Burman, Cape Verde, China, Ecuador, India, Indonesia, Iran, Kenya, Malaysia, Maldives, Mauritius, North Korea, Pakistan, the Philippines, Portugal, Thailand, Uruguay.

(2) Nations that claim territorial waters in excess of 12-nm: 7-
Benin, Congo, Ecuador, Liberia, Peru, Somalia, Togo.

(3) Nations that claim security jurisdiction in their 24-nm contiguous zone: 5-
Cambodia, China, Sudan, Syria, Vietnam.

Raul (Pete) Pedrozo, "Preserving Navigational Rights and Freedoms: The Right to Conduct Military Activities in China's Exclusive Economic Zone," *Chinese Journal of International Law*, Vol. 9 (2010), p. 27; idem., "Military Activities in the Exclusive Economic Zone: East Asia Focus," *The U.S. Naval War College International Law Studies*, Vol. 90 (2014), pp. 521-522.

[12] Pedrozo, "Preserving Navigational Rights and Freedoms," p. 27.

[13] Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017), Rule 32, p. 168.

[14] Signed on 10th December 1982, came into effect on 16th November 1994, *The United Nations Treaty Series*, Vol. 1833, p. 3, https://treaties.un.org/pages/ViewDetailsIII.aspx?src=TREATY&mtdsg_no=XXI-6&chapter=21&Temp=mtdsg3&clang=_en

[15] As stated in Rule 5 of *the Tallinn Manual*, warships and ships owned or operated by a state and used only for government non-commercial service, state aircraft, and persons or objects on such vessels or aircraft enjoy sovereign immunity. Schmitt, *Tallinn Manual 2.0*, pp. 27-28, commentary para. 1.

[16] J. Ashley Roach, "Military Cables," in Douglas R. Burnett, Robert C. Beckman, and Tara M. Davenport, eds., *Submarine Cables : The Handbook of Law and Policy* (Martinus Nijhoff Publishers, 2014), p. 343.

[17] Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017), Rule 54, p. 252.

[18] Ibid. p. 253.

[19] Ibid. p. 241.

[20] Ibid. p. 249.

[21] Ibid. p. 256.

[22] Ibid.

[23] Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017), Rule 4, p. 17.

[24] Ibid. p. 241.