Padjadjaran Journal of International Law
International Law Department Universitas Padjadjaran
ISSN: 2549-2152, EISSN: 2549-1296
Volume 6, Number 1, January 2022
DOI: 10.23920/pjil.v6i1.772

Wiretapping On Submarine Communications Cable: Questioning Its Legality Amidst Long Standing Practice

Hafidz L. Botua[1]
Chloryne Trie Isana Dewi[2]
R. Achmad Gusman Catur Siswandi[3]

ABSTRACT
Up to 95% of the communication infrastructures are currently served by the submarine communications cable networks, which in their utilisation connect a wide variety of communications data. The increasingly advanced infrastructure is in fact unable to go hand in hand with legal transformation. At the present time, international law provides only partial protection in form of prevention against damage to the cable networks. Consequently, in the event that data transmissions across the cable networks are illegally exploited by foreign parties through "wiretapping" without inflicting any damage, as long as it is committed in the body of waters outside the state's sovereignty, the international law is unable to explicitly address this situation. The wiretapping has occurred in a couple of instances, however, the proper preventive measures are still in question. Fortunately, the most recent practice of international law in the field of human rights has provided some clarities through case law. Despite the fact that it has only been applied regionally, this endeavour is at the very least capable of supporting future proposed legal reforms. This article will further elaborate on the legality of wiretapping on submarine communications cable networks based on the relevant field of international law, which eventually revealed that such conduct is contrary to cyber law, international law of the sea and human rights law.

Keywords: Cyber Law, Human Rights Law, International Law of The Sea, Submarine Communications Cable, Wiretapping.

A. INTRODUCTION

The submarine communications cable (hereinafter "**SCC**") networks are the backbone of modern telecommunication capability, where its illegal access would undermine the state security and basic rights of the citizens. Despite the imminent threat, the legality of wiretapping into it remains unclear to a certain extent. The utilization of SCC networks serve a high transmission speed and has contributed up to 95% to the

[1] Associate at Solon Law, Rozel Les Varioufs St Martin GUERNSEY GY4 6TE, Guernsey, hlbotua@hotmail.com.
[2] Lecturer of the Faculty of Law Universitas Padjadjaran, Secretary of Indonesian Center for International Law of the Sea, Jl. Imam Bonjol No. 21 Bandung 40132 Indonesia, e-mail: chloryne.dewi@unpad.ac.id.
[3] Lecturer of the Faculty of Law Universitas Padjadjaran, Director of Indonesian Center for International Law of the Sea, Jl. Imam Bonjol No. 21 Bandung 40132 Indonesia, e-mail: ahmad.gusman@unpad.ac.id.

ease of communications.[4] The United Nations (hereinafter "**UN**") later designated the networks as "*vitally important to the global economy and the national security of all States*".[5] With more than 470 networks globally, SCC networks cored with *optical fiber* have surpassed satellite communication capacity and become the primary international telecommunication medium.[6] Their locations span across a variety of maritime zones, stretching from the land-based cable landing points to the territorial sea, continental shelf, surface of the deep seabed, and continuing to another cable landing points.

The SCC networks connect a variety of data sources and place a significant reliance on communication infrastructures. The SCC networks, for example, support and facilitate from all types of electronic social media as well as enterprises operating in the global economy via the Internet, such as shipping companies, airlines, and banks.[7] Under the international law, all states entitled the right to lay SCC outside their sovereign territory, where its protection guaranteed under several international legal instruments that are classified into several scopes in relation to the SCC networks.

From the scope of international law of the sea, its protection has been established through treaty-based regulations which later transformed into customary international law. It was first pioneered in 1884 through the Convention for the Protection of Submarine Telegraph Cables (hereinafter "**Cable Convention"**). The provisions of Cable Convention have significantly affected the rights and obligations of the State in regulating the utilization of Telegraph SCC which were later supplemented by two of the four 1958 Geneva Conventions on the Law of the Sea, *inter alia*, through the High Seas Convention and the Continental Shelf Convention. In subsequent developments, the provisions of the Geneva Conventions were repealed through the 1982 United Nations Convention on the Law of the Sea (hereinafter "**UNCLOS"**) which simultaneously expanded the scope of protection under various maritime zones and for various types of cables.

In addition to arrangements from the scope of international law of the sea, there are also regulations before the cyberspace, through the 2001 Budapest Convention on Cybercrime (hereinafter "**Cybercrime Convention"**) and the Constitution and Convention of the International Telecommunication Union adopted by the 2018 Plenipotentiary Conference (hereinafter "**ITU Convention"**) which mandates the member states to safeguard the channels and installations of international telecommunication circuits within their jurisdiction.[8]

Despite the existence of the above instruments, the history of utilizing SCC networks has shown a considerable record of experiencing physical attacks that lead to communication breakdowns. In such case, international law has provided a protection through the Cable Convention under Articles II, IV and VII; and through UNCLOS under Articles 113, 114 and 115. Such a protection is significant considering the losses of cable breaks can reduce the communication capabilities of some countries for several weeks.[9]

Eventually, the utilization of SCC networks threatened with the data interference that passes through it due to

---

4 Carter, Lionel, Submarine Cables and the Oceans: Connecting the World-Issue 31 of UNEP-WCMC biodiversity series, *UNEP/Earthprint*, 2010, at 8.

5 General Assembly Resolution 65/37, Oceans and the law of the sea, A/RES/65/37 ¶121 (7 December 2010), at 3.

6 TeleGeography, "Submarine Cable Map", https://www.submarinecablemap.com/#/, accessed on May 20, 2021.

7 Stewart Ash, *The Development of Submarine Cables* in Burnett, Douglas R. et.al, *Submarine Cables: The Handbook of Law and Policy*, Martinus Nijhoff Publishers, 2013, at 5.

8 The Provisions relating to the protection of telecommunication channels provided by Article 38 of the ITU Convention. However, it does not specifically address the protection of SCC networks.

9 Sechrist, Michael, *Cyberspace in Deep Water: Protecting Undersea Communication Cables by Creating an International Public-Private Partnership*, Harvard Kennedy School of Government Policy Analysis Exercise, 2010, at 19-20.

espionage. For the present discussion, we will refer espionage which carried out by wiretapping, thus able to collect a large amount of data by non-consensual interference (bulk interception). The focus of wiretapping in the present discussion is not the same as directly intervening the communication networks in cyberspace, instead, through physical activity, by attaching devices on the cable that do not cause any physical harm, so that these actions will directly intersect with the scope of international law of the sea. Yet, the approach through cyber law is still relevant due to the intersectoral interference in such activity.

The wiretapping on the SCC network was first identified by the US intelligence activity amidst the Cold War through Operation Ivy Bells in the 1970s.[10] Following its years of operation with full secrecy, it later leaked to the Soviet by a former National Security Agency (NSA) officer in 1980. In the post-cold war era, such activity was widely known during the Global Surveillance Disclosures in 2013. Wiretapping occurred in **Southern Cross Cable**, which was carried out to obtain a domestic bulk data collection by New Zealand Government Communications Security Bureau (GCSB).[11] Moreover, it happened to the transatlantic SCC network **TAT-14** and **Atlantic Crossing 1**, as well as South-East Asia-Middle East-Western Europe on the **SEA-ME-WE3** network by the United Kingdom Government Communications Headquarters (GCHQ) known as its codename TEMPORA.[12] The GCHQ activity further relates to the wiretapping on the **SEA-ME-WE4** network carried out alongside the Australian Signals Directorate, United States, and Singapore.[13] Once again, despite the high-level secrecy, it was exposed to the public by former NSA officer, Edward Snowden in 2013.

Following to the Snowden disclosure, the governance of human rights law on the activity related to wiretapping on SCC networks established. Another landmark case is now known as Big Brother Watch v. United Kingdom (hereinafter "**BBW v. UK**") which was rendered by European Court of Human Rights (hereinafter "**the Court**") in May 2021.[14]

The SCC network is a vital infrastructure that requires a complete protection, including not only physical security but also the integrity and confidentiality of data passing through it. Despite the fact that the aforementioned cases' targets were reached via the cable points in territorial sea, it is important to note that the majority of SCC locations are outside of state sovereignty (consisting of the continental shelf and the surface of the deep seabed) with a length of about 314,350 kilometres.[15] The utilization of SCC networks in the territorial sea is protected by both national and international law, where it stated that any interference is a violation thus a passage is not innocent.[16] Beyond the territorial sea, international law only explicitly provides the guarantee of protection towards the physical damage.

Based on the descriptions above, it could be found that the law of the sea remains unclear in the situation where the wiretapping occurred outside the body of waters outside states sovereignty (covering continental shelf and surface of deep seabed), necessitating the urgency for the protection of the data integrity passing through the SCC networks. To find out the legality of such conduct, we will first address

---

10 Sontag, Sherry (et. al.), *Blind Man's Bluff: The Untold Story of American Submarine Espionage*, Public Affairs, 1998, §8.

11 Greenwald, Glenn, and Ryan Gallagher. "New Zealand launched mass surveillance project while publicly denying it." *The Intercept* 15 (2014).

12 Goetz, John, Hans Leyendecker, and Frederik Obermaier. "Britischer Geheimdienst zapft Daten aus Deutschland ab." *British secret service taps data from Germany]. Süddeutsche Zeitung. Retrieved* 3 (2020).

13 Dorling, Philip. "Australian spies in global deal to tap undersea cable." *Sydney Morning Herald* 29 (2013).

14 ECHR, Big Brother Watch and Others v. the United Kingdom [GC], no. 58170/13, 25 May 2021.

15 Burnett, Douglas R. & Carter, Lionel, *International Submarine Cables and Biodiversity of Areas beyond National Jurisdiction: The Cloud beneath the Sea*, Brill, 2017, at 52.

16 Article 19.2 of UNCLOS.

the technical and legal aspects of the wiretapping itself (**B**). Following the provided approach, it will be continued with the discussion of wiretapping in cyberspace (**C**) then the approach from the law of the sea considering its nature and close relation with the utilization of SCC networks (**D**). Lastly, this article will provide the recent standpoint of human rights law where the wiretapping is contrary to the rights of privacy and freedom of expression (**E**).

B. WIRETAPPING ON SCC NETWORKS

According to its historical conduct, wiretapping on SCC networks could be classified as a clandestine activity, an espionage, thus undermine state's interest to keep its secrecy. Yet, the international law does not provide an explicit approach on the conduct of espionage. However, in the present discussion, such clarity aimed to be found, at least by a layered interpretation. This section will provide the technical matters necessary to be known on the conduct of wiretapping (**1**) and the cases occurred (**2**). Based on those two understanding, it will be continued to discuss the relevant concept of espionage to the conduct of wiretapping (**3**).

1. The Technical Features of Wiretapping

Wiretapping is carried out by attaching a special device capable of collecting data on the cable. It could be placed on the cable wherever possible.[17] However, the cable layers must be examined during the installation; in theory, tapping can be done on the cable with the thinnest coating. Wiretapping requires the use of sophisticated techniques to access the cable without exposing it to seawater. Alternatively, the wiretapping device could be attached on the cable amplifier.[18]

A more concrete illustration can be seen in the implementation of Operation Ivy Bells.[19] Accordingly, the wiretapping was carried out by the USS Halibut which dived to the seabed before releasing the divers.[20] At the seabed, the Divers used pneumatic airguns to clear sand and debris off around the cable. Once that was done, the divers installed a one-meter-long device that had a recorder powered by a lithium battery. A connecting device was wrapped around the cable and will absorb any data that passes through it, where it worked through induction.[21] This first recording captured the conversations that took place over several days on some of the dozens of channels available through the cable, which later decoded by NSA. To obtain the footage for several months, the Central Intelligence Agency (CIA) made a larger recording device. It was almost two meters long and more than one meter wide. This device recorded data for months on a 7 centimetres tape that went along the wheel with a diameter of almost 1 meter.[22]

In the present day, the disclosure provided by Snowden (which later contested into BBW v. UK) mentioned that GCHQ was handling 600 million "telephone events" everyday, had tapped more than 200 cables and was able to process data from at least 46 of them at a time. In regards of the intercepted materials, the wiretapping had the ability to tap into and store massive amounts of data gathered. It could not only view the data live but also store it for up to 30 days before sifting and analysing it for months. This includes call recordings, email

---

17 Lehto, Martti, et al. "Arctic Connect Project and cyber security control, ARCY." *Informaatioteknologian tiedekunnan julkaisuja*, *Jyväskylän yliopisto*, 2019, at 20.

18 *Ibid*.

19 Sontag, Sherry, *supra* note 7.

20 To deploy the divers, USS halibut is mounted with a DSRV (Deep-submergence rescue vehicle), in Sontag, Sherry, *supra* note 7.

21 Induction is a physical phenomenon where when an object that was previously neutral or not electrically charged becomes electrically charged due to the influence of an electric force or from another charged object that is brought close to it, in Ponto, Hantje, *Dasar Teknik Listrik*, Deepublish, 2018, at 36.

22 Sontag, Sherry, *supra* note 7.

content, and the history of any internet user's access to websites, including both content data and metadata.[23]

2. The Cases of Wiretapping

There are at least two primary cases of wiretapping on SCC networks classified in two distinctive periods. The first known cases occurred during the Cold War under the supervision of US Navy, CIA and NSA through Operation Ivy Bells (**a**) and other cases grouped under the Global Surveillance Disclosures in 2013 (**b**).

a. Operation Ivy Bells

This operation aimed to acquire more information on Soviet submarine and missile technologies, additionally, the Intercontinental ballistic missile (ICBM) test and nuclear first-strike capability.[24] The US government was aware of the Soviet cable in the Sea of Okhotsk, which connected the Soviet Pacific Fleet's main naval base at Petropavlovsk, Kamchatka Peninsula, to the mainland headquarters of the Soviet Pacific Fleet in Vladivostok. Later, the wiretapping carried out by sending submarines and dive crews to attach the tapping device on the cable.

This operation become a landmark case in the cable wiretapping activity, where it is important to highlight that the operation could only successfully conducted due to the development of submarine technology and modern military capability, thus it could be left unnoticeable in the long term. The operation ran smoothly for around ten years, and the operation's objectives were accomplished. Despite its secrecy, this operation could be revealed after an officer from the National Security Agency (NSA) leaked the operation to the Soviet embassy in 1980.

Although Soviet aware of the violation in its territorial water, there was no diplomatic or legal settlement known regarding this issue. Later, Ronald William Pelton who leaked the information to the Soviet, was later tried and convicted of espionage in 1986, sentenced to three concurrent life sentence and fined $100, which then released on November 24, 2015.[25] On the other hand, Soviet discovered the wiretapping device and keep it in the Museum of the Great Patriotic War in Moscow.[26]

b. Wiretapping Operations Revealed on Global Surveillance Disclosures 2013

In post-cold war era, wiretapping on SCC networks became widely known after Edward Snowden exposed NSA classified documents related to global surveillance in 2013. The following are some of the SCC networks that were secretly taped:

i. **Southern Cross Cable**, conducted by Government Communications Security Bureau (GCSB) of New Zealand for a domestic data collection.[27] The program known as *X Keyscore*, in which GCSB collected the data and then shared it with NSA. The program was implemented in several stages, starting with the *Speargun* program in 2012-2013 which entailed attaching a wiretapping device to the SCC network. Proceed in stage two to insert "metadata probes" in the network. The operation took advantage of the enormous flow of information in real time from SCC network, which makes it possible to extract the date, time, sender, and

[23] MacAskill, Ewen, et al. "GCHQ taps fibre-optic cables for secret access to world's communications." *The Guardian* 21 (2013).

[24] Sontag, Sherry, *supra* note 7.

[25] Aftergood, Steven. "Soviet Spy Ronald W. Pelton to be Released from Prison." *Online News. Federation of American Scientists* 23 (2015).

[26] Sontag, Sherry, *supra* note 7.

[27] Greenwald, Glenn, and Ryan Gallagher, *supra* note 8.

recipient of emails, phone conversations, and another associated data.

ii. **TAT-14**, **Atlantic Crossing 1**, and South-East Asia-Middle East-Western Europe on the **SEA-ME-WE3** network, was conducted by Government Communications Headquarters (GCHQ) known as *TEMPORA*.[28] On August 28, 2013, it was discovered that GCHQ had gained access to some SCC networks. *TEMPORA* technically observed on 13 SCC networks, including those connecting Europe to Africa and Asia, as well as intra-European networks.

iii. **SEA-ME-WE4,** was conducted by GCHQ where it was also related to the operation above.[29] The wiretapping was in cooperation with the Australian Signals Directorate, the United States, and Singapore. This network utilizes SCC networks that connect Asia, the Middle East, and Europe covering several countries such as Japan, via Singapore, Djibouti, Suez and the Strait of Gibraltar to Germany. Singapore intelligence was also working with Australia to access and share communications carried by the SEA-ME-WE-3 and SEA-ME-WE-4 networks that landed on the western edge of Singapore, according to an Australian intelligence source. The operation also shared the information to the 5 eyes intelligence alliance which includes retrieval of all data, sent and received emails, instant messaging, calls, passwords and much more, in and out of the UK via SCC networks.

3. Espionage and the Conduct of Wiretapping

There is no legal instrument under international law that regulates the definition of wiretapping. So as to provide a reference, "wiretapping" according to *Black's Law Dictionary* is referred to by several terms, including:[30]

i. **Bugging**, a form of electronic surveillance by which conversations may be electronically intercepted, overheard, or recorded covertly, eavesdropping by electronic means;

ii. **Eavesdropping**, the act of secretly listening to the private conversation of others without their consent;

iii. **Intercept**, to covertly receive or listen to a communication; and

iv. **Wiretapping**, electronic or mechanical eavesdropping, done by law-enforcement officers under court order, to listen to private conversations.

Additionally, according to the *Merriam-Webster Legal Dictionary*, the term "wiretapping" is defined as:[31]

> *"Interception of the contents of communication through a secret connection to the telephone line of one whose conversations are to be monitored usually for purposes of criminal investigation by law enforcement officers."*

From the several provided definitions, there are important elements that can be obtained which consist of:

i. to listen/to receive;

---

[28] Goetz, John, Hans Leyendecker, and Frederik ObermaierSueddeutsche, *supra* note 9.

[29] Dorling, Philip, *supra* note 10.

[30] Garner, Bryan A., & Henry Campbell Black, *Black's Law Dictionary*, 9th ed, St. Paul, MN: West, 2009.

[31] *Merriam-Webster.com Legal Dictionary*, s.v. "wiretapping,"accessed December 20, 2021, https://www.merriam-webster.com/legal/wiretapping.

ii. Private information; and
iii. Conducted secretly.

It is important to note that the present discussion regarding the concept of wiretapping is not carried out within the scope of law enforcement (criminal procedural law) but will be linked to the concept of espionage in cyberspace (cyber espionage).

To provide a specific illustration on cyber espionage, we will refer its rationale according to the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operation (hereinafter "**Tallinn Manual 2.0**") where it defined as:[32]

> *"…to any act undertaken clandestinely or under false pretensions that uses cyber capabilities to gather, or attempt to gather, information. Cyber espionage involves, but is not limited to, the use of cyber capabilities to surveillance, monitor, capture, or exfiltrate electronically transmitted or stored communications, data, or other information…"*

Based on the description of the various terms above, wiretapping can be categorized as an act of espionage in cyberspace, where practically referred as Signals intelligence (SIGINT). Regarding its legality, referring to Tallinn Manual 2.0, it is stated that **espionage is not necessarily unlawful**, however, **it can be unlawful if the methods employed are unlawful**.[33] The provision further states that its legality depends on its implementation as long as it does not conflict with several international legal principles related to sovereignty (Rule 4) and non-intervention (Rule 66) which refers to Articles 2.1 and 2.4 of the United Nations Charter. In practice and academic discussions in the scope of international law, wiretapping as an act of espionage is widely discussed in the specific scope of diplomatic and consular law.

Wiretapping is prohibited in connection with the obligations of diplomatic and consular staff to the receiving country. Under The Vienna Convention on Diplomatic Relations of 1961 (hereinafter "**VCDR**"), it requires the diplomatic and consular staff **to legally obtain all information** from the receiving state which conveyed to the sending state.[34] The case for this violation was found in 2013 where the diplomatic representative of the United States wiretapped the authorities of the German government.[35]

Furthermore, wiretapping is also prohibited in regards to the obligation of the receiving state to guarantee freedom of communication for diplomatic and consular staff in its country.[36] Wiretapping cases that violate these provisions were recorded in 1973, where France found 42 secret microphone networks at its diplomatic building in Warsaw, Poland.[37] In 1985, the half-finished US embassy in the Soviet Union was found equipped with hearing aids allegedly installed by Soviet

---

[32] Rule 32.2 of Tallinn Manual 2.0; Regardless of its potential to become a source of international law, considering the purpose of its formulation and the opinions of the experts mentioned in the document, Tallinn Manual 2.0 will only be referred to as a scholarly document without any legal significance.

[33] Rule 32.6 of Tallinn Manual 2.0.

[34] Article 3.1(d) of VCDR.

[35] Peters, Anne. "There is no explicit rule that prohibits espionage. But that doesn't mean it's allowed." *Verfassungsblog: On Matters Constitutional* (2013).

[36] Article 27.1 of VCDR.

[37] Satow, Ernest, *Satow's Guide to Diplomatic Practice*, 5th ed, Lord Gore-Booth ed., London & New York: Longman, 1979, at 116.

authorities.[38] During the Cold War there were many cases where hearing aids were found in diplomatic and consular missions.[39] Although there is no specific reference to legal recourse in dealing with such acts, in the context of the conduct of diplomatic and consular missions engaging in espionage, expulsion of accused diplomats has been considered as a normal practice.[40]

The use of wireless communication device is allowed as stated in Article 27.1 of VCDR, however it can only be used if it is approved by the receiving state. In practice, a more secure communication method is then equipped with an encryption system for data that is streamed through a wireless network to avoid eavesdropping.[41] However, the problem is that only countries that have well-developed technology are able to use it, and in some cases, it is installed without the permission of the receiving state.[42]

C. WIRETAPPING AND CYBERSPACE

The law applied on cyberspace might not be the most relevant reference in the conduct of wiretapping on SCC networks. However, it could be useful to provide a little clarity on its legal status. The threat comes from the sea, attached to the communications backbone, which later could access the cloud of cyberspace, thus quite important to be addressed. This section will first elaborate the concept of state sovereignty in the cyberspace (**1**), followed by the approach of the relevant instrument (**2**).

1. Sovereignty in the Cyberspace

State sovereignty includes applying the law within its jurisdiction. Within the framework of law enforcement or certain intelligence activities, wiretapping is allowed. However, wiretapping cannot necessarily be carried out transnationally (across the internet domains of other countries), due to the limited jurisdiction and the obligation to respect the sovereignty of other countries.

By sovereignty, a state is obliged to protect its citizens from all forms of foreign intrusion, including wiretapping in the communication networks. This protection, in a broader sense, also includes cyberspace which in further discussion will be referred as "cyber sovereignty".

Yet, cyber sovereignty does not have an explicit reference in international law, however, the term is closely related to the territorial sovereignty. Sovereignty is linguistically derived from the *superanus* which derived from the adagium *sui juris, esse suae potestatis, superanus or summa potestas* which means that sovereignty refers to the highest authority, which in the concept of international law is applied to the authority of the state towards its entire territory.[43] In some cases, sovereignty is expressed as:[44]

> *"Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein,*

[38] Moutzouris, Maria. "Sending and receiving: Immunity sought by diplomats committing criminal offences.", PhD dissertation, *Rhodes University*, 2008, at 80.

[39] *Ibid*.

[40] Edmondson, L. S. "Espionage in Transnational Law", *Vanderbilt Journal of Transnational Law*, 1971-1972, at 445; Grzybowski. "The Regime of Diplomacy and the Tehran Hostages", *International & Comparative Law Quarterly*, 1981, at 42.

[41] Satow, Ernest, supra note 33.

[42] Kerley, Ernest L. "Some Aspects of the Vienna Conference on Diplomatic Intercourse and Immunities", *American Journal of International Law*, Vol. 1, 1962, at 112.

[43] Oppenheim, Lassa, *Oppenheim's International Law*, 9th edn, Robert Jennings & Arthur Watts eds., 1992, at 564.

[44] Island of Palmas (or Miangas) (The Netherlands / The United States of America) ICJ 1928.

> *to the exclusion of any other State, the functions of a State."*

Later on, it is stated as:[45]

> *"By sovereignty, we understand the whole body of rights and attributes which a State possesses in its territory, to the exclusion of all other States, and also in its relations with other States".*

When applied to cyberspace, international law has formed a special concept that was formed through the Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG) consisting of several members of the United Nations to discuss the development of cyberspace towards international security. Subsequently, it is implemented by formulating the governance through at least twenty-eight meetings.[46]

From the latest meeting, through Resolution A/76/135, the UN General Assembly stated that countries need to carry out their activities in cyberspace with reference to the Reports of the GGE in 2010, 2013 and 2015. This is due to the fact that cyberspace needs to be viewed as a man-made environment that requires physical architecture including cable networks, microwave relay towers, satellite transponders, Internet routers, etc. so that it does not stand alone from the physical world but is rooted within. The concept of the application of sovereignty over cyberspace, from the GGE Reports in 2013 and 2015 stated that:[47]

> *"State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory."*

In the development of the practice, most countries have paid attention to the importance of cyber infrastructure in their respective jurisdictions. As of 2018, it is known that documents regarding cybersecurity and cyberdefense strategies from 93 countries discuss "sovereignty" and "cyber sovereignty".[48] The understanding that attacks on cyberspace are a threat to state sovereignty was adopted by NATO as an example, at the 2016 meeting it was stated that:[49]

> *"70. Cyber-attacks present a clear challenge to the security of the Alliance and could be as harmful to modern societies as a conventional attack. We agreed in Wales that cyber defense is part of NATO's core task of collective defence. Now, in Warsaw, we reaffirm NATO's defensive mandate, and recognize cyberspace as a domain of operations in which*

---

[45] Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania) Judge Alvarez separate opinion §V.

[46] United Nations, "Developments in the field of information and telecommunications in the context of international security", https://www.un.org/disarmament/ict-security/, accessed January 20, 2022.

[47] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc A/68/98, 24 June 2013, ¶20; Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc A/70/174, 22 July 2015, ¶27.

[48] Baezner, M., and P. Robin. "Trend Analysis: Cyber Sovereignty and Data Sovereignty." *Centre for Security Studies, Zurich*, 2018, at 16.

[49] NATO, Warsaw Summit Communiqué, July 9, 2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm. Accessed December 20, 2021.

> *NATO must defend itself as effectively as it does in the air, on land, and at sea. . ."*

Apart from the use of the term "cyber-attacks" which is academically distinguished from "cyber-espionage",[50] by analogizing its impact as a similar threat to a country's cyber sovereignty, NATO's understanding is likely to include on the espionage in cyberspace. This is proven, that in the same document, the results of the meeting stated:[51]

> *"Each Ally will honour its responsibility to improve its resilience and ability to respond quickly and effectively to cyber-attacks, including in hybrid contexts."*

Based on the aforementioned elaboration, the jurisdiction of the state to employ the wiretapping is limited to the cyber sovereignty of another state which covers all state activities in cyberspace and against all cyber infrastructure within its territory, anything beyond that would be illegal under international law.

2. The Approach of Cybercrime Convention

In cyber law, wiretapping has been regulated in the Budapest Convention on Cybercrime 2001, which currently has 65 participating countries.[52] This instrument was formed to protect against cybercrimes, in the case of wiretapping, these actions can take the form of illegal access (Article 2) and illegal wiretapping (Article 3), the provisions for illegal access are described as follows:

> *"Article 2 – Illegal access*
>
> *Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offenses under its domestic law, when committed intentionally,* ***the access to the whole or any part of a computer system without right****. A Party may require that the offense be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system."*

Based on the explanatory document from the Cybercrime Convention, the elements of illegal access include all forms of criminalization of data security (confidentiality, integrity and existence). The terms are known in practice as "hacking", "cracking" or "computer trespassing". The purpose of criminalization is to protect data owners, both individuals and corporations, from tampering with confidential data (passwords or other information about the target sought by the perpetrator), including the use of a system without mandatory payments and to prevent further forms of cybercrime from occurring that could allow illegal interception and other crimes regulated in this convention.[53] Furthermore, the provisions for illegal wiretapping are as follows:

> *"Article 3 – Illegal interception*

---

50 According Talinn Manual 2.0, those terms distinguished under Rule 32 and Rule 92.

51 NATO, *supra* note 44.

52 Convention on Cybercrime Budapest, 23.XI.2001 - European Treaty Series - No. 185, effective July 1, 2004.

53 Explanatory Report to the Convention on Cybercrime Budapest, 23.XI.2001, at 44.

> *Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offenses under its domestic law, when committed intentionally,* ***the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data****. A Party may require that the offense be committed with dishonest intent, or in relation to a computer system that is connected to another computer system."*

Provisions regarding illegal interception are aimed at protecting the right to privacy. Criminalization includes invasion of privacy by means of interception and recording of conversations in various forms of electronic data transfer, including telephone, fax, e-mail or manual file transfer.[54]

Although quite comprehensive, the provisions of the Cybercrime Convention in fact are unapplicable in this situation. Referring to the preamble of the convention, the convention was formed with consideration of the need for unification of criminal policies to protect against cybercrimes and the need for cooperation in handling them. The concept is further supported by the history of the formulation of the convention showing that the focus of the instrument is on joint law enforcement capability.[55]

The Convention may be applicable in the case of wiretapping carried out by non-state actors who are not affiliated with state activities on espionage. However, law enforcement cooperation may be hampered by considering that the convention has not been universally accepted when considering the number of member countries. Referring to our analysis on the sovereignty in cyberspace above as well as the law of the sea and human rights law below, we would argue that to settle the wiretapping conducted by states is unpractical and quite sceptical to resort the framework of Cybercrime Convention.

D. WIRETAPPING TOWARDS THE LAW OF THE SEA

Apart from the development of the practice of protecting SCC networks (other than damage) especially outside the body of waters outside states sovereignty has not been much discussed,[56] the ocean is not an area without a law (*vacuum juris*).[57] Despite the fact that all of these laws already made, albeit in a less explicit form, efforts to preserve the law can be implemented through layered interpretation.

---

[54] Explanatory Report to the Convention on Cybercrime Budapest, 23.XI.2001, at 51.

[55] Decision CDPC/103/211196, the European Committee on Crime Problems (CDPC) decided in November 1996.

[56] Guilfoyle, *Article 89* in Nordquist, Myron, ed. *United Nations Convention on the law of the sea 1982, Volume VII: A Commentary*, Brill, 2011.

[57] Daniel P. O'Connell, The International Law of the Sea, vol. II (1984), at 792, 796; *cf*. Gilbert Gidel, Le droit international public de la mer: le temps de paix, vol. I (1932), at 225.

Referring to UNCLOS as the constitution in regulating the rights and duties of states in the maritime environment, it states that the principle of peaceful uses of the seas as its main embodiment.[58] Subsequently, this principle is transformed into several *peaceful use clauses*, some of which are relevant in the discussion of SCC networks including Article 88 and Article 301 of UNCLOS which limits the state's interests in various maritime zones.

The delimitation of maritime zones outside the state's sovereign territory consists of the EEZ, the Continental Shelf and the High Seas. Under international law, the state possesses limited jurisdiction over the EEZ and the Continental Shelf, known as "sovereign rights".[59] This authority has the following scope:

i. The authority to implement national law within the framework of international law;[60]
ii. The implementation of the law applies to anyone and ships with any flag as long as they are in the EEZ and the Continental Shelf so that they do not have limits on *ratione personae*.[61]
iii. Sovereign rights are exclusive to the coastal state and may not be employed by other parties without prior authorisation (in the context of the use of natural resources).[62]

According to Article 56 of UNCLOS, the coastal state has several rights in the EEZ, including the authority to exercise jurisdiction over natural resources, the establishment and use of artificial islands, installations and buildings, marine scientific research, and environmental protection and preservation of the sea. Furthermore, other States have the following rights:[63]

> *". . . the freedoms referred to in article 87 Navigation and overflight and of the laying of submarine cables and pipelines, and other internationally lawful uses of the sea related to these freedoms, such as those associated with the operation of ships, aircraft and submarine cables and pipelines, and compatible with the other provisions of this Convention."*

Considering the Articles 56 and 58 of UNCLOS, it is necessary to have a *sui generis* alignment that is important to fulfil in the enjoyment of rights between Coastal States and other Countries in activities in the EEZ.[64] This alignment shall be maintained by the principle of "due regard" which requires the state not to take actions that are not in accordance with UNCLOS and may result in "abuse of rights" in the enjoyment of their rights.[65] Due Regard shall be maintained by the Coastal State to exercise its rights in accordance with UNCLOS,[66] at the same time, other States need to exercise their rights in accordance with the laws of the Coastal State and other international law provisions.[67] In particular, with regard to the SCC networks, the coastal state has exclusive jurisdiction to establish "cable protection zones" in the EEZ and the Continental Shelf to provide protection for the SCC networks.[68]

On the high seas and its seabed, all states have the freedom stated in Article 87 of UNCLOS as follows:

i. freedom of navigation;
ii. freedom of overflight;

---

58 Preamble of UNCLOS.
59 Case Concerning Continental Shelf (Libya v. Malta), ICJ 1985, ¶33.
60 EEZ under Article 73 of UNCLOS and the continental shelf under Article 77 of UNCLOS.
61 Article 73 of UNCLOS.
62 Article 77.2 of UNCLOS, read together with Articles 62.2, 69 and 70 of UNCLOS; South China Sea Arbitration (Philippines v. China), Award of 12 July 2016, ¶243.
63 Article 58.1 of UNCLOS.
64 Myron H. Nordquist/Satya N. Nandan/Shabtai Rosenne (eds.), *United Nations Convention on the Law of the Sea 1982: A Commentary*, vol. II (1993), at 526.
65 Churchill, Robin Rolf, & Alan Vaughan Lowe, *The Law of The Sea*, Manchester University Press, 1999, at 170.
66 Article 56.2 of UNCLOS.
67 Article 58.3 of UNCLOS; ITLOS, The M/V 'Saiga' (St. Vincent and the Grenadines v. Guinea), Merits, Judgment of 1 July 1999, ¶121.
68 EEZ under Article 60 of UNCLOS and the continental shelf under Article 80 of UNCLOS.

iii. freedom to lay submarine cables and pipelines, subject to Part VI;
iv. freedom to construct artificial islands and other installations permitted under international law, subject to Part VI;
v. freedom of fishing, subject to the conditions laid down in section 2;
vi. freedom of scientific research, subject to Parts VI and XIII.

The duty of due regard for state activities also applies including the high seas. Conducting wiretapping will violate the principle of peaceful uses which is then regulated in Articles 88 and 301 of UNCLOS, respectively, as follows. Article 88 states:

"*Article 88-Reservation of the high seas for peaceful purposes*

The high seas shall be reserved for peaceful purposes."

Further, Article 301 states:

> *"Article 301-Peaceful uses of the seas*
>
> *In exercising their rights and performing their duties under this Convention, States Parties shall refrain from any threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the principles of international law embodied in the Charter of the United Nations"*

Referring to several other international legal documents in particular, in the Antarctic Treaty and the Outer Space Treaty, the meaning of "peaceful purposes" is followed by a special prohibition on carrying out military manoeuvres and weapons testing.[69] Furthermore, in the General Assembly's 1970 Declaration of Principles Governing the Sea-Bed and the Ocean Floor, and the Subsoil Thereof, Beyond the Limits of National Jurisdiction, the phrase has the meaning of specifically prohibiting the placement of nuclear weapons on the seabed outside national jurisdiction.[70]

Article 301 of UNCLOS reflects Article 2.4 of the United Nations Charter which prohibits the use of force against the territorial sovereignty of states.[71] Wiretapping on SCC networks can violate the principle of peaceful uses of the seas from the two articles due to abuse of freedom by carrying out military activities.

International law, especially in the maritime sphere, does not prohibit the use of force,[72] the general provisions in the use of armed force refer to the United Nations Charter, that in Article 51 of the United Nations Charter states that the use of armed force is justified as a form of self-defense in the event of violations of the use of armed force by other countries. Furthermore, the development of international humanitarian law supports this notion which regulates its proportional conduct.

However, the use of force has certain limitations. The use of force at sea, other than in the context of nuclear armament, is related to the activities of warships in utilizing the freedom of navigation.[73] In principle, warships enjoy the freedom to carry out their military activities in the context of the freedom of the high seas subject to three basic obligations:[74]

i. the obligation to refrain from the threat or unlawful use of force;
ii. obligations due regard to the rights of other countries to use the sea; and

---

69 Oxman, Bernard H. "The regime of warships under the United Nations Convention on the Law of the Sea." *Va. J. Int'l L.*, 1983, at 830.

70 Treaty on the Prohibition of the Emplacement of nuclear weapons and other Weapons of Mass Destruction on the Seabed and the Ocean Floor and in the Subsoil Thereof 1971.

71 O'Brien, *Article 301* in Nordquist, Myron, ed., *United Nations Convention on the law of the sea 1982, Volume VII: A Commentary*, Brill, 2011, at 1945.

72 Oxman, Bernard H, *supra* note 63 at 831; Wolfrum, Rudiger, "Restricting the Use of the Sea to Peaceful Purposes: Demilitarization in Being." *German YB Int'l L.*, 1981, at 213.

73 Nordquist, Myron/Nandan, Satya N./Rosenne, Shabtai (eds.), *United Nations Convention on the Law of the Sea 1982: A Commentary*, Vol. VI, 2002, at 81; Article 17–20 of UNCLOS; Article 38–45 of UNLCOS; Article 52–53 of UNCLOS; PCA, Arctic Sunrise Arbitration (Netherlands v. Russia), Merits, Award of 14 August 2015, ¶227.

74 Oxman, Bernard H, *supra* note 63 at 837.

iii. obligations to comply with applicable obligations under treaties or other rules of international law.

Various balancing efforts have been arranged by UNCLOS that every freedom is accompanied by various obligations. Although these forms of freedom are not stated in a specific form, they are limited by the freedoms of other countries.

The Academic discussion shows that the state interests in exercising freedom on the high seas are classified in two forms. **First**, related to inclusive interests, these interests include freedom for their own interests such as freedom of navigation and rights of fishing.[75] **Second**, exclusive interests, including security interests, conducting naval warfare and interests to intervene in the voyage of a ship which is entirely carried out by warships.[76] From the implementation of these two interests, the provisions of Article 87.2 of UNCLOS state that states may not pursue their interests in any form without due regard to the interests of other countries.

As a development of "reasonable regard" from the High Seas Convention, the application of due regard in practice does not have any explicit obligations or specific standards, however, the ILC states that it is a Customary of International Law which means:[77]

> *"States are bound to refrain from acts which might adversely affect the use of the high seas by nationals of other States."*

The installation of wiretapping devices can be classified as a form of interference with SCC networks, which has an impact on non-consensual data exploitation which is detrimental to parties who should have exclusive benefits from the cable that is able to intervene in the interests of the State. This is because the government has the right to develop its domestic and foreign policies without being monitored by foreign powers, the wiretapping interfered a sovereign decision on whom it wants to share these secret government deliberations with.[78] This action further led to an intervention against the state sovereignty in cyberspace.

Whereas as described in previous section, the position regarding state sovereignty in cyberspace refers to the GGE Reports in 2013 and 2015 which stated that international law in the concept of territorial sovereignty also applies to state activities in cyberspace and to jurisdiction over cyber infrastructure that exists in their territory.

States exercise territorial sovereignty over computer networks and systems through cyber infrastructure that is physically located within their territory. Sovereignty is broad in nature, including computer networks and systems operated by state organs or private parties, including types of personal and political information. When a state engages in cyber activities that penetrate the networks and computer systems of other countries without permission to obtain information that cannot be accessed openly, this action causes an intervention in the state sovereignty.[79]

Subsequently, further issue occurs on the law enforcement mechanism to safeguard the cables against wiretapping. Within the scope of the EEZ and Continental Shelf, referring to Article 73 of UNCLOS, the Coastal State has the authority to take actions such as "boarding, inspection, arrest and judicial proceedings, as may be necessary to ensure compliance with the laws and regulations". Meanwhile, within

---

[75] M. McDougal & W. Burke, *The Public Order of the Oceans: A Contemporary International Law of the Sea*, Yale University Press, 1962, at 37.

[76] *Ibid.*

[77] ILC, Report of the International Law Commission: Commentaries to the Articles Concerning the Law of the Sea, UN Doc. A/3159 (1956), GAOR 11th Sess. Suppl. 9, 12, 24 (Art. 27).

[78] Terry, Patrick, ""Absolute Friends": United States Espionage against Germany and Public International Law." *Revue québécoise de droit international/Quebec Journal of International Law/Revista quebequense de derecho internacional*, Vol. 28, No. 2, 2015, at 173.

[79] Russell Buchan, *Cyber Espionage and International Law*, Hart Publishing, 2019, §8.

the scope of the violation occurring on the high seas, the provisions of the Right of Visit (Article 110 UNCLOS) and Right of Hot Pursuit (Article 111 UNCLOS) apply in certain actions.

However, the two provisions in fact cannot be easily invoked, this is taking into account the wiretapping activity in the history of its implementation carried out by ships affiliated with the government (Navy Ships/War Ships). Law enforcement efforts will be difficult to carry out considering that warships have their own immunity guaranteed by under international law.[80]

Efforts to exercise law enforcement jurisdiction over foreign warships on the high seas are actually a form of threat or use of force against the sovereignty of a country.[81] Furthermore, such circumstances will be prolonged into the situation of use of force and self defense within Article 2 and Article 51 of the UN Charter which will later be able to deal with armed conflicts at sea.

Referring to the development of known wiretapping practices, particularly in Operation Ivy Bells, the development of the use of the Unmanned Underwater Vehicle (UUV),[82] and considering the implementation capacity and technology used, wiretapping activities towards SCC networks are military activities that trigger violations of the peaceful uses of the sea.

E. WIRETAPPING AND ENJOYMENT OF HUMAN RIGHTS

Wiretapping is highly related to human rights. The main principles of human rights that are vulnerable to wiretapping activity includes the right to privacy and freedom of expression which can be found in the Universal Declaration of Human Rights (UDHR). The provision regarding the Right to Privacy states:

> *"Article 12. No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."*

Furthermore, the right to freedom of expression states:

> *"Article 19. Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."*

The UDHR provisions were subsequently developed into various binding instruments,[83] including the European Convention on Human Rights (hereinafter "**ECHR**"), in particular Article 8 (Right to Privacy) and Article 10 (Right to Freedom of Expression) which have been applied in BBW v. UK.

The case and governance of human rights law towards the wiretapping on SCC networks provided by the framework of European Union (EU), to serve more comprehensive discussion, this section will first address the EU approach on wiretapping (**1**) then goes on to the ruling of BBW v. UK (**2**).

---

[80] The immunity of warships firstly regulated in International Convention for the Unification of Certain Rules relating to the Immunity of State-owned Vessels, signed at Brussels, April 10th, 1926, and Additional Protocol, signed at Brussels, May 24, 1934, Resolution of Stockholm on the regime of maritime vessels and their crews in foreign ports in time of peace 1928, later under Convention on the High Seas 1958, and at the present time at Article 95 of UNCLOS.

[81] Delupis, Ingrid. "Foreign warships and immunity for espionage." *American Journal of International Law,* 1984, at 55.

[82] Парламентская газета, *Корабль спецназначения «Янтарь» вошёл в Средиземное море*, https://www.pnp.ru/politics/korabl-specnaznacheniya-yantar-voshyol-v-sredizemnoe-more.html, accessed December 20, 2021.

[83] International Covenant on Civil and Political Rights, Privacy Rights on Article 17 and Freedom of Expression on Article 19; American Convention on Human Rights, Privacy Rights on Article 11 and Freedom of Expression on Article 13.

1. The EU Approach on Wiretapping

EU referred wiretapping as an "interception", the Court rules that it is not necessarily illegal, thus it may be conducted with certain limitations. The conduct itself separated into two distinct categories, so called, **targeted interception** which means surveillance of telecommunications in a criminal context,[84] and later is **bulk interception** or "signals intelligence".[85]

Another reference provided by 2015 Venice Commission Report and the development of the case decided by the Court,[86] shows the necessity to conduct the wiretapping in strict manner. The development of the practice emphasizes "three data protection tests" which, based on Article 8.2 of the ECHR, to intervene in privacy rights (e.g., wiretapping) is necessary to fulfil three basic principles, including:[87]

i. "in accordance with the law", meaning as stated in Article 5 of Convention 108,[88] that personal data that is processed automatically must be obtained and processed fairly and legally. That the phrase complies with the law requires wiretapping has some basis in domestic law. Domestic laws must be in line with conventions and include the principle of "accessibility" which means that the law must be accessible to the public and "foreseeability" which means that the public knows the impact of wiretapping;[89]
ii. must pursue a "legitimate aim", meaning as stated in Article 5 of Convention 108, that personal data that undergoes automatic processing must be collected for clear, specific and legitimate purposes; as well as
iii. must be "necessary in a democratic society", meaning that in order to be necessary in a democratic society, any action that interferes with the protection of personal data must meet urgent and necessary social needs in proportion to the legitimate objectives to be achieved. This principle also requires to provide adequate and effective protection and guarantees against misuse.[90]

Furthermore, the practice in the European Union establishes "six minimum safeguards" in conducting wiretapping, this formula is formed to avoid the implementation of "abuse of power". The six principles of protection include:

i. the nature of offenses which may give rise to an interception order;
ii. a definition of the categories of people liable to have their communications intercepted;
iii. a limit on the duration of interception;
iv. the procedure to be followed for examining, using and storing the data obtained;

---

84 Guide on Article 8 of the European Convention on Human Rights - Right to respect for private and family life, home and correspondence, at 131.

85 Guide on Article 8…, *supra* note 78, at 134.

86 The 2015 Report of the European Commission for Democracy through Law ("the Venice Commission") on the Democratic Oversight of Signals Intelligence Agencies.

87 Guide to the Case-Law of the of the European Court of Human Rights - Data protection, at 23-29.

88 The European Union's regulation of personal data has a *lex specialis* through *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* (*Convention 108)* on Article 5.

89 Roman Zakharov v. Russia [GC], no. 47143/06, ECHR 2015, § 228; Rotaru v. Romania [GC], no. 28341/95, ECHR 2000-V, § 52; S. and Marper v. the United Kingdom [GC], nos. 30562/04 and 30566/04, ECHR 2008, § 95; Kennedy v. the United Kingdom, no. 26839/05, 18 May 2010, § 151.

90 Roman Zakharov v. Russia [GC], no. 47143/06, ECHR 2015, § 236; Kennedy v. the United Kingdom, no. 26839/05, 18 May 2010, § 155)

v. the precautions to be taken when communicating the data to other parties; and
vi. the circumstances in which intercepted data may or must be erased or destroyed.

Aforementioned safeguards have been consistently held by the court, developed and applied by the case law to safeguard the private life of the citizen.[91] However, the six minimum safeguards are not sufficient to accommodate the Bulk Interception. The court later consider the urgency to develop and adapt these requirements to the specificities of bulk interception and, finally, outlines a list of eight criteria which the domestic legal framework must clearly define for their conduct. The new criteria are formed as follows:[92]

i. the grounds on which bulk interception might be authorised;
ii. the circumstances in which an individual's communications might be intercepted;
iii. the procedure to be followed for granting authorisation;
iv. the procedures to be followed for selecting, examining and using intercept material;
v. the precautions to be taken when communicating the material to other parties;
vi. the limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed;
vii. the procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address noncompliance; dan
viii. the procedures for independent ex post facto review of such compliance and the powers vested in the competent body in addressing instances of non-compliance.

2. The Standard of Legality Derived from BBW v. UK

The governance of human rights law on the activity related to wiretapping on SCC networks established through BBW v. UK where the case first referred to the Court in 2015 due to violation in Article 8 (Right to Privacy) and Article 10 (Right to Freedom of Expression) of ECHR.[93] In this case, the Applicants stated that if their electronic communications had been illegally accessed in three of methods, *inter alia*, their electronic communications were likely to have either been intercepted by the United Kingdom intelligence services (hereinafter "**Bulk Interception Regime**"), obtained by the United Kingdom intelligence services after

[91] Referring to ECHR cases, *inter alia*, ECHR, Huvig v. France, 24 April 1990, Series A no. 176 B; ECHR, Kennedy v. the United Kingdom, no. 26839/05, 18 May 2010; ECHR, Klass and Others v. Germany, 6 September 1978, Series A no. 28; ECHR, Kruslin v. France, 24 April 1990, Series A no.176-A; ECHR, Liberty and Others v. the United Kingdom, no. 58243/00, 1 July 2008; ECHR, Roemen and Schmit v. Luxembourg, no. 26419/10, ECHR 2003-IV; ECHR, Roman Zakharov v. Russia [GC], no. 47143/06, ECHR 2015; ECHR, Rotaru v. Romania [GC], no. 28341/95, ECHR 2000-V; ECHR, S. and Marper v. the United Kingdom [GC], nos. 30562/04 and 30566/04, ECHR 2008; ECHR, Weber and Saravia v. Germany no. 54934/00, ECHR 2006-XI.

[92] It was first applied to Huvig v. France, April 24, 1990, 34, Series A no. 176 B and Kruslin v. France, 24 April 1990, 35, Series A no.176-A, and has been consistently applied by the Court in cases concerning interception of communications and in two special cases concerning interception of bulk interception such as Weber and Saravia v. Germany no. 54934/00, ECHR 2006 XI and Liberty and Others v. the United Kingdom, no. 58243/00, 1 July 2008.

[93] The applications were lodged with the European Court of Human Rights on 4 September 2013, 11 September 2014 and 20 May 2015, the first section judgment rendered on September 13, 2018. On 12 December 2018 the applicants requested that the case be referred to the Grand Chamber and the judgment rendered on May 25, 2021.

being intercepted by foreign governments (hereinafter "**Surveillance and Intelligence Sharing Regime**"); and/or obtained by the United Kingdom authorities from communications service providers (hereinafter "**CSP Data Acquisition Regime**").

Of those three methods, the Court is of the opinion that the second method is proven to be conducted lawfully. The consideration is based on the application of domestic law, showing a fairly clear procedure for requesting the intercepted materials from foreign intelligence agencies.[94] These circumstances include adequate legal safeguards for the examination, use, storage, transmission of data, and destruction of the intercepted material, and are subject to independent supervision.[95] Thus, the second method will not be described further. By the first and third methods, the Court ruled unanimously that such conducts violated Articles 8 and 10 of the ECHR. However, to provide a specific elaboration in line of the scope of this research, further discussion will only focus on the Bulk Interception Regime.

The interception mainly conducted by GCHQ which authorized through the Regulation of Investigatory Powers Act 2000 (RIPA) and the Interception of Communications Code of Practice (IC Code). That under those provisions, bulk interception warrants may be issued, if necessary, in accordance with national interest, security, for the purpose of preventing or detecting serious crimes, or for the purpose of safeguarding the economic well-being of UK to the extent that such interests are also relevant to national security interests.

The Court established a limitation on Bulk Interception regime, which includes several elements:[96]

a. Wiretapping is directed at international communications (that is, communications that are physically transnational in nature), so as to monitor communications outside the territorial jurisdiction of the State;
b. Conducted for the purpose of investigating certain crimes, including for the purpose of gathering foreign intelligence data, early detection and investigation of cyber attacks, counter-espionage and counter-terrorism; as well as
c. In obtaining individual data, a selector system is formed.

With regard to ECHR, bulk interception is illegal since it violates the elements of "no interference by public authority" stated in Article 8 and 10 of ECHR so that it interferes with the fulfilment of rights. Towards Article 8 of ECHR, tested by the eight criteria made by the court, bulk interception regime found unable to fulfil the requirement number 3 regarding "the procedure to be followed for granting authorization".[97] In this case, the absence of supervision over the category of selectors at the authorization stage was a lack of compliance with the law, violating the due process of bulk interception. With these shortcomings, bulk interception is not in accordance with the law due to a considerable potential for its implementation to be misused in a

[94] Grand Chamber Case of Big Brother Watch and Others V. The United Kingdom 2021, ¶ 516.
[95] Grand Chamber Case of Big Brother Watch and Others V. The United Kingdom 2021, ¶ 513.
[96] Grand Chamber Case of Big Brother Watch and Others V. The United Kingdom 2021, ¶ 344.
[97] Grand Chamber Case of Big Brother Watch and Others V. The United Kingdom 2021, ¶383.

way that harms the right of individuals to respect the right to privacy.

When viewed as a whole, the provisions of RIPA, apart from the protections available, do not in fact contain "end-to-end safeguards" to provide adequate and effective guarantees against arbitrariness and the risk of abuse. These problems include:

a. the absence of independent authorisation;[98]
b. the failure to identify the categories of selectors in the application for a warrant and the failure to subject those selectors linked to identifiable individuals to prior internal authorisation;[99] and
c. the lack of foreseeability of the circumstances in which communications could be examined.[100]

Additionally, based on the legal considerations above, judging from the three data protection tests, the bulk interception did not fulfil the element of "necessary in a democratic society".

Towards Article 10 of ECHR, the purpose of obtaining confidential journalistic data is an issue before the law. RIPA has the capacity to access confidential journalistic material in three ways:[101]

a. intentionally;
b. through the deliberate use of selectors or search terms connected to a journalist or news organisation; or
c. unintentionally, as a "bycatch" of the bulk interception operation.

That of the three methods above, bulk interception is illegal with the analogy that such acts are tantamount to disturbances caused by raids at journalists' homes or workplaces. Regardless of whether the intelligence service's intention is to identify the source or not, the use of selectors or search terms related to journalists is likely to result in the acquisition of large amounts of classified journalistic material.[102]

This situation shows that the third criterion of the eight criteria established by the Court (the procedure to be followed for granting authorisation) is not met, that in such circumstances it is necessary to obtain authorization from the competent authority (the Court or an independent body that is authorized). Additionally, to examine the conduct against Article 10, the Court itself considered the subjective element of the Applicant. This is due to the fact that the court consistently maintains the standpoint that the guarantee for the fulfilment of Article 10 of the ECHR always intersects with Article 8 in the context of to obtain journalistic data which is related to the privacy of journalists themselves.[103] Taking into account the status of the Applicant as a journalist, therefore a violation of Article 8 will automatically constitute a violation of Article 10.

To conduct a lawful interception itself can actually refer to several considerations of other wiretapping cases (not related to SCC networks) which were also formed by the court with the following considerations. Whereas in the context of establishing regulations regarding wiretapping, which

---

98 Grand Chamber Case of Big Brother Watch and Others V. The United Kingdom 2021, ¶ 377.

99 Grand Chamber Case of Big Brother Watch and Others V. The United Kingdom 2021, ¶381, 382.

100 Grand Chamber Case of Big Brother Watch and Others V. The United Kingdom 2021, ¶391.

101 Grand Chamber Case of Big Brother Watch and Others V. The United Kingdom 2021, ¶449.

102 Roemen and Schmit v. Luxembourg, no. 26419/10, ECHR 2003-IV, ¶57.

103 Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands, no. 39315/06, 22 November 2012, ¶97, 102; Saint-Paul Luxembourg S.A. v. Luxembourg, no. 26419/10, 18 April 2013, ¶44; Ernst and Others v. Belgium, no. 33400/96, 15 July 2003, ¶116; Nagla v. Latvia, no. 73469/10, 16 July 2013, ¶101.

authorizes state officials to intercept telephone communications without public notification, it is legal. This is with consideration of the need for state intervention in the interests of national security and for crime prevention. That the threats to forms of espionage and terrorism are so sophisticated that the State must be able, to counter these threats effectively, to carry out covert surveillance of elements operating within the jurisdiction of the State. The establishment of legislation in the interest of national security and/or for crime prevention so as not to violate Article 8.[104] Furthermore, wiretapping of state officials against a person is legal as long as it fulfils the procedures for authorizing and processing wiretapping warrants as well as processing, communicating, and destroying the collected data.[105]

It should be noted again that in BBW v. UK, the case is cross-border and not a case of internal wiretapping in domestic context. This case demonstrates the absent of proportionality in wiretapping, which refers to a failure to comply upon the ruleset of criteria established by the court. Since those conditions are not met, so that the freedom of privacy and freedom of expression is violated.

F. CONCLUSION

That wiretapping on SCC networks is a violation of international law. Under Rule 32.6 of Tallinn Manual 2.0, although cyber espionage does not in itself violate international law, the methods employed may violate international law due to the methods employed are unlawful. The installation of wiretapping devices on the SCC networks would violate international law mainly from three approaches.

Under international law applicable on cyberspace, the wiretapping violates the states sovereignty due to illegal access and data exploitation on the cyberspace which rooted from the installations established in state's territory. Under international law of the sea, it would violate the principle of peaceful uses of the seas as further embodied in Article 88 and 301 of UNCLOS. This is due to the fact that installation of wiretapping device employed by use of force which later breaches the cable owner's exclusive control over all information that flows. Lastly, under international human rights law, it violates the fundamental rights of the citizens under the principles of the right to privacy and the right to freedom of expression which have been promoted by UDHR and have been concretized through various international agreements.

States need to restrain their interests in illegally exploiting data through wiretapping on SCC networks. Such action is a violation of international law applicable on cyberspace, peaceful uses on the seas environment and human rights. To safeguard the public's interest in the need and dependence on communication networks, it is necessary to develop regulations to protect SCC networks that are outside the territory of state sovereignty from wiretapping. The formation of this new instrument is expected to be able to codify a new law either in form of legal principles or binding legal norms to protect SCC networks.

REFERENCE

Books

Burnett, Douglas R. & Carter, Lionel, *International Submarine Cables and Biodiversity of Areas beyond National Jurisdiction: The Cloud beneath the Sea*, Brill, 2017.

Carter, Lionel, Submarine Cables and the Oceans: Connecting the World-Issue 31 of UNEP-WCMC

[104] Klass and Others v. Germany, 6 September 1978, Series A no. 28.

[105] Kennedy v. the United Kingdom, no. 26839/05, 18 May 2010.

biodiversity series, *UNEP/Earthprint*, 2010.

Churchill, Robin Rolf, & Alan Vaughan Lowe, *The Law of The Sea*, Manchester University Press, 1999.

Daniel P. O'Connell, The International Law of the Sea, vol. II (1984).

Garner, Bryan A., & Henry Campbell Black, *Black's Law Dictionary*, 9th ed, St. Paul, MN: West, 2009.

Gilbert Gidel, Le droit international public de la mer: le temps de paix, vol. I (1932).

Guilfoyle, *Article 89* in Nordquist, Myron, ed. *United Nations Convention on the law of the sea 1982, Volume VII: A Commentary*, Brill, 2011.

M. McDougal & W. Burke, *The Public Order of the Oceans: A Contemporary International Law of the Sea*, Yale University Press, 1962.

Myron H. Nordquist/Satya N. Nandan/Shabtai Rosenne (eds.), *United Nations Convention on the Law of the Sea 1982: A Commentary*, vol. II (1993).

Nordquist, Myron/Nandan, Satya N./Rosenne, Shabtai (eds.), *United Nations Convention on the Law of the Sea 1982: A Commentary*, Vol. VI, 2002.

O'Brien, *Article 301* in Nordquist, Myron, ed., *United Nations Convention on the law of the sea 1982, Volume VII: A Commentary*, Brill, 2011.

Oppenheim, Lassa, *Oppenheim's International Law*, 9th edn, Robert Jennings & Arthur Watts eds., 1992.

Ponto, Hantje, *Dasar Teknik Listrik*, Deepublish, 2018.

Russell Buchan, *Cyber Espionage and International Law*, Hart Publishing, 2019.

Satow, Ernest, *Satow's Guide to Diplomatic Practice*, 5th ed, Lord Gore-Booth ed., London & New York: Longman, 1979.

Sechrist, Michael, *Cyberspace in Deep Water: Protecting Undersea Communication Cables by Creating an International Public-Private Partnership*, Harvard Kennedy School of Government Policy Analysis Exercise, 2010.

Sontag, Sherry (et. al.), *Blind Man's Bluff: The Untold Story of American Submarine Espionage*, Public Affairs, 1998.

Stewart Ash, *The Development of Submarine Cables* in Burnett, Douglas R. et.al, *Submarine Cables: The Handbook of Law and Policy*, Martinus Nijhoff Publishers, 2013.

Journals

Baezner, M., and P. Robin. "Trend Analysis: Cyber Sovereignty and Data Sovereignty." *Centre for Security Studies, Zurich*, 2018.

Delupis, Ingrid. "Foreign warships and immunity for espionage." *American Journal of International Law,* 1984.

Edmondson, L. S. "Espionage in Transnational Law", *Vanderbilt Journal of Transnational Law*, 1971-1972.

Grzybowski. "The Regime of Diplomacy and the Tehran Hostages", *International & Comparative Law Quarterly*, 1981.

Kerley, Ernest L. "Some Aspects of the Vienna Conference on Diplomatic Intercourse and Immunities", *American Journal of International Law*, Vol. 1, 1962.

Lehto, Martti, et al. "Arctic Connect Project and cyber security control, ARCY." *Informaatioteknologian tiedekunnan julkaisuja*, *Jyväskylän yliopisto*, 2019.

Moutzouris, Maria. "Sending and receiving: Immunity sought by diplomats committing criminal offences.", PhD dissertation, *Rhodes University*, 2008.

Oxman, Bernard H. "The regime of warships under the United Nations Convention on the Law of the Sea." *Va. J. Int'l L.*, 1983.

Terry, Patrick, ""Absolute Friends": United States Espionage against Germany and Public International Law." *Revue québécoise de droit international/Quebec Journal of International Law/Revista quebequense de derecho internacional*, Vol. 28, No. 2, 2015.

Wolfrum, Rudiger, "Restricting the Use of the Sea to Peaceful Purposes: Demilitarization in Being." *German YB Int'l L.,* 1981.

Legal Documents

1982 United Nations Convention on the Law of the Sea.

American Convention on Human Rights.

Case Concerning Continental Shelf (Libya v. Malta), ICJ 1985.

Constitution and Convention of the International Telecommunication Union adopted by the 2018 Plenipotentiary Conference.

Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108).

Convention on Cybercrime Budapest, 23.XI.2001 - European Treaty Series - No. 185, effective July 1, 2004.

Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania) Judge Alvarez separate opinion.

Decision CDPC/103/211196, the European Committee on Crime Problems (CDPC).

ECHR, Big Brother Watch and Others v. the United Kingdom [GC], no. 58170/13, 25 May 2021.

Explanatory Report to the Convention on Cybercrime Budapest, 23.XI.2001.

General Assembly Resolution 65/37, Oceans and the law of the sea, A/RES/65/37 (7 December 2010).

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc A/68/98, 24 June 2013.

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc A/70/174, 22 July 2015.

Guide on Article 8 of the European Convention on Human Rights - Right to respect for private and family life, home and correspondence.

Guide to the Case-Law of the of the European Court of Human Rights - Data protection.

Huvig v. France, 24 April 1990, Series A no. 176 B.

ILC, Report of the International Law Commission: Commentaries to the Articles Concerning the Law of the Sea, UN Doc. A/3159 (1956), GAOR 11th Sess. Suppl. 9, 12, 24 (Art. 27).

International Covenant on Civil and Political Rights.

International Convention for the Unification of Certain Rules relating to the Immunity of State-owned Vessels, signed at Brussels, April 10th, 1926, and Additional Protocol, signed at Brussels, May 24, 1934.

Island of Palmas (or Miangas) (The Netherlands / The United States of America) ICJ 1928.

ITLOS, The M/V 'Saiga' (St. Vincent and the Grenadines v. Guinea), Merits, Judgment of 1 July 1999.

Kennedy v. the United Kingdom, no. 26839/05, 18 May 2010.

Klass and Others v. Germany, 6 September 1978, Series A no. 28.

Kruslin v. France, 24 April 1990, 35, Series A no.176-A.

Liberty and Others v. the United Kingdom, no. 58243/00, 1 July 2008.

PCA, Arctic Sunrise Arbitration (Netherlands v. Russia), Merits, Award of 14 August 2015.

Resolution of Stockholm on the regime of maritime vessels and their crews in foreign ports in time of peace 1928.

Roemen and Schmit v. Luxembourg, no. 26419/10, ECHR 2003-IV.

Roman Zakharov v. Russia [GC], no. 47143/06, ECHR 2015.

Rotaru v. Romania [GC], no. 28341/95, ECHR 2000-V.

S. and Marper v. the United Kingdom [GC], nos. 30562/04 and 30566/04, ECHR 2008.

South China Sea Arbitration (Philippines v. China), Award of 12 July 2016.

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operation.

The 2015 Report of the European Commission for Democracy through Law ("the Venice Commission") on the Democratic Oversight of Signals Intelligence Agencies.

Treaty on the Prohibition of the Emplacement of nuclear weapons and other Weapons of Mass Destruction on the Seabed and the Ocean Floor and in the Subsoil Thereof 1971.

Weber and Saravia v. Germany no. 54934/00, ECHR 2006 XI.

Other Documents

Aftergood, Steven. "Soviet Spy Ronald W. Pelton to be Released from Prison." *Online News. Federation of American Scientists* 23 (2015).

Dorling, Philip. "Australian spies in global deal to tap undersea cable." *Sydney Morning Herald* 29 (2013).

Goetz, John, Hans Leyendecker, and Frederik Obermaier. "Britischer Geheimdienst zapft Daten aus Deutschland ab." *British secret service taps data from Germany]. Süddeutsche Zeitung. Retrieved* 3 (2020).

Greenwald, Glenn, and Ryan Gallagher. "New Zealand launched mass surveillance project while publicly denying it." *The Intercept* 15 (2014).

MacAskill, Ewen, et al. "GCHQ taps fibre-optic cables for secret access to world's communications." *The Guardian* 21 (2013).

Merriam-Webster.com Legal Dictionary, s.v. "wiretapping," accessed December 20, 2021, https://www.merriam-webster.com/legal/wiretapping.

NATO, Warsaw Summit Communiqué, July 9, 2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm. Accessed December 20, 2021.

Парламентская газета, *Корабль спецназначения «Янтарь» вошёл в Средиземное море*, https://www.pnp.ru/politics/korabl-specnaznacheniya-yantar-voshyol-v-sredizemnoe-more.html, accessed December 20, 2021.

Peters, Anne. "There is no explicit rule that prohibits espionage. But that doesn't mean it's allowed." *Verfassungsblog: On Matters Constitutional* (2013).

TeleGeography, "Submarine Cable Map", https://www.submarinecablemap.com/#/, accessed on May 20, 2021.