E-ISSN 2579-9487
P-ISSN 0215-899X
Kertha Patrika
Vol. 44, No. 2, Agustus 2022
https://ojs.unud.ac.id/index.php/kerthapatrika

The Impact of Cyber Warfare on Indonesian Cellular Frequency Operators Based on the International Information Technology Law

Ria Wierma Putri[1], Rudi Natamiharja[2], Orima Melati Davey[3], Febryani Sabatira[4], Yunita Maya Putri[5]

[1] Faculty of Law, Universitas Lampung, email: ria.wierma@fh.unila.ac.id
[2] Faculty of Law, Universitas Lampung, email: rudi.natamiharja@fh.unila.ac.id
[3] Faculty of Law, Universitas Lampung, email: orima.davey23@gmail.com
[4] Faculty of Law, Universitas Lampung, email: febryani.sabatira@gmail.com
[5] Faculty of Law, Universitas Lampung, email: yunita.maya@fh.unila.ac.id

Article's Info

Received: 23rd November 2021
Accepted: 8th April 2022
Published : 30th August 2022

Keywords :
Frequence, Cyber Warfare, International Law

Kata kunci:
Frekuensi, Cyberwarfare, Hukum Internasional

Corresponding Author:
Febryani Sabatira, E-mail: febryanisabatira@gmail.com

DOI :
10.24843/KP.2022.v44.i02.p.02

Abstract

The Radio Frequency Spectrum is a limited Natural Resource, which in terms of its management has a strategic and economic impact on the community. These limitations require the government to make quite strict regulations in the utilization of these resources. Indonesia is one of the countries that uses frequency as the consumption of daily life. This is illustrated using communication tools for the telephone network. To avoid using license frequencies, Indonesia must adjust without national and international frequency rules, considering that Indonesia is already a member of the ITU. This situation has been realized through Law no. 24 of 2015 concerning the Table of Allocation of the Indonesian Radio Frequency Spectrum, which states that the frequency allocation in Indonesia refers to the ITU-Radio Regulations. Indonesia is currently in a state of urgency for cyber security or cyber security because of the level of cybercrime or cybercrime in Indonesia. Policy handling cybercrime is different from other crime prevention. However, unlike other crime prevention, cybersecurity requires a comprehensive thought to deal with it. Therefore, the study found two problems: (1) What are the provisions for the use of frequencies in Indonesia, (2) What are the provisions regarding the existence of cyberwarfare, and (3) How are the impacts of cyberwarfare on the frequencies of Indonesian cellular operators based on international information technology law?.

1. Introduction

The frequency spectrum is one of the common human resources (Res Communes) but is also considered a resource belonging to no one) or called *Res Nullius*. Therefore, as res nullius, the frequency does not belong to anyone. Meanwhile, if the frequency spectrum is seen as res communes, its use should not be arbitrary. A licensing mechanism is

needed at the international and national levels. A subject cannot operate the frequency spectrum as an individual 'right', even though it is communal property. However, in reality, it is still common to find cases of illegal use of frequency spectrum due to the complexity and high price of licensing for frequency use. In Indonesia, illegal frequency users are already at an alarming level. In the 2019 frequency order week, 822 unlicensed frequency beams were successfully clarified and stopped.[1] Licensing is needed to ensure effective and efficient use of frequencies and prevent harmful interference. Even though the frequencies are common property, and it can be said that everyone is allowed to use the frequency spectrum, illegal use of frequencies can cause actual harm. The presence of harmful interference may result in repeated damage or interference to the primary public operating system, such as navigation services (GPS), safety services such as distress beacons and others. Therefore, everyone must be aware that the frequency spectrum is an absolute responsibility that must be carried out. [2]

International law regulates the frequency spectrum in the 1992 International Telecommunication Union Convention (ITU Convention). Article 44 paragraph (1) of the Convention stipulates that radio frequencies, geostationary satellite orbits, and other frequencies are included in the category of limited natural resources.[3] However, there is a fundamental difference in the terminology of 'limited natural resources on the frequency spectrum with the category of natural resources. These natural resources are limited to oil, gas, or mineral reserves which. If used massively and not based on effective and efficient use principles, it will run out. While the limitation referred to in the frequency spectrum is based on its nature which can only be used for one frequency transmission in one period of use. This means that other transmissions cannot use the frequency spectrum simultaneously unless the two transmissions are far apart or have weak transmit power.[4]

Illegal frequencies are one type of cybercrime because it has a detrimental and dangerous impact. Frequency disturbances can cause a system's security to be vulnerable to threats of data theft, planting of computer viruses, hacking, and other cybercrimes. Currently, Indonesia is in a state of cyber emergency due to the high level of cybercrime. This is very worrying because, according to data reported by the Central Intelligence Agency (CIA), Indonesia accounts for 1.20% of the world's losses due to cybercrime. Therefore, a mechanism for handling cyber threats is needed through cyber security and cyber defence. Cyber security is an effort to protect the cyber world from harmful sources, while cyber defence is an effort to defend cyber security from potential threats in the future. Both efforts must be carried out at the national and international levels, considering that this type of crime has broad implications (domestic and international).[5]

---

[1] Doly, D. (2021). Peran Negara Dalam Pengelolaan Spektrum Frekuensi Radio Dalam Perspektif Hukum. *Kajian*, *23*(4), 267-283., http://dx.doi.org/10.22212/kajian.v23i4.2115

[2] Budhijanto, D. (2014). Peran Hukum Telekomunikasi terhadap Implikasi Konvergensi Teknologi Informasi dan Komunikasi. *Jurnal Dinamika Hukum*, *14*(1), 134-150. http://dx.doi.org/10.20884/1.jdh.2014.14.1.283.

[3] Article 44 Paragraph 1 of IITU Convention 1992: "*Members shall endeavour to limit the number of frequencies and the spectrum used to the minimum essential to provide a satisfactory manner with the necessary service. To that end, they shall endeavour to apply for the latest advances as soon as possible.*

[4] Budhijanto, D., *loc.cit*.

[5] Moehammad Yuliansyah Saputera (2015), "Pengaruh Cyber Security Strategy Amerika Serikat Menghadapi Ancama Cyber Warfare," *JOM FISIP* 2, no. 2: 1–15.

When viewed at the policy level, cyber crimes have specificities and characteristics so that their handling is different from ordinary crimes. Cybercrimes require comprehensive handling. Furthermore, the vulnerability of a system due to the threat of cybercrimes can have fatal consequences for national security and defence. The nature of the cyber world that is not limited (borderless) will always provide a gap for the entry of threats outside and inside. A country with a weak system will be marked as a country with weak security. Weak state security makes it easy for other countries to enter, control, and damage its system. This can lead to the potential for cyber warfare between countries. In cyberwarfare, the war in question is an attack on objects owned by the state in cyberspace.

One great example of cyberwarfare is Stuxnet, first discovered ten years ago. An employee inside the Iranian nuclear power plant site inserts a USB stick embedded with the Stuxnet worm into a system with an air gap. This is done to exploit some zero-day exploits. This malware looks for specific software running centrifuges and instructs them to spin very fast and then slow for several months without being detected. The centrifuge eventually broke down, and more than 1,000 machines were rendered unusable. The attack has never been blamed on anyone, although it is thought that US and Israeli military entities jointly created this cyber weapon. While no country has disputed the allegations, Stuxnet was also allegedly played as part of a show at the Israeli Defense Force (IDF) retired chief's party. The new cyberwarfare case comes from Russia. Russia is alleged to have carried out numerous and various state-level cyberattacks and carried out several cyber warfare against Ukraine, including the BlackEnergy attack that cut power to 700,000 Ukrainian homes in 2015. In addition, Russia is suspected of carrying out the NotPetya malware, which disguises itself as ransomware but is designed purely to destroy infected systems. These cases show that cyber warfare can be fatal if not taken seriously. Based on the explanation, the writer will discuss three problems in this research, namely (1) What are the provisions for the use of frequencies in Indonesia, (2) What are the provisions regarding the existence of cyberwarfare, and (3) How are the impacts of cyberwarfare on the frequencies of Indonesian cellular operators based on international information technology law?.

2. Metode Penelitian

This type of research is normative research that descriptively examines humans, circumstances, and other phenomena to strengthen old theories and support new theories that are still in the drafting stage.[6] The research uses an approach to the formulation of the problem and research objectives. The data sources used are secondary data sources consisting of primary legal materials, secondary legal materials and tertiary legal materials.[7]

3. Result and Discussion

[6] Soerjono Soekanto (2012), *Pengantar Penelitian Hukum*, Jakarta: Penerbit Universitas Indonesia, p. 50.

[7] Soerjono Soekanto (2012), *Penelitian Hukum Normatif*, Jakarta: PT Raja Grafindo Persada, p. 37.

This study will discuss three problems: a detailed explanation of the use of frequencies in Indonesia, cyberwarfare, and the impact of cyber warfare on the frequency of Indonesian cellular operators based on international information technology law.

A. Frequency Utilization in Indonesia

1) Frequency Utilization and Laws

Frequency is the number of times per second the sound pressure wave repeats. Drumbeats have a much lower frequency than whistles, and frog calls have a lower frequency than crickets. The lower the frequency, the less vibration. High frequency produces more oscillation. The unit of frequency is called hertz (Hz). According to some experts in broadcasting, frequency is considered the primary resource in operating information and telecommunications systems. Frequency serves to convey information from one place to another through the invisible air space (wireless).[8] In the operation of telecommunications, there are several types of radiofrequency spectrum users, namely:[9]

a) Users holding frequency spectrum band allocation license (MNO);
b) The user is not the owner of a frequency spectrum band allocation permit (MVNO);
c) Free frequency users.

Technically, all voice and data telecommunications connections are carried out through wireless networks (copper cables or fibre optic cables) using radio frequencies. Thus, if interpreted literally, the use of the frequency spectrum of an operator who does not have a license to use a frequency is a user of a radio frequency spectrum.[10] International law regulates frequencies in the International Communication Union (ITU Convention) precisely in the ITU Radio Regulations. ITU Radio Regulation" has 4 "volumes" (volumes), which consist of Articles, Appendices, Recommendations and Resolutions and Inclusion by Reference. Volume I of Radio Regulations, namely Articles, has 9 “chapters” (chapters), covering:

a) Terminology and technical characteristics.
b) Frequency allocation
c) Coordination, notification and recording of the determination of frequency and modification of the Plan (Plan).
d) Interference.
e) Administrative Provisions.
f) Provisions for “Services” and “Stations” (radio stations).
g) “Distress and Safety Communications”.
h) “Aeronautical Services” (Aviation Service).

---

8 Rahayu et al. (2015), *Menegakkan Kedaulatan Telekomunikasi dan Penyiaran di Indonesi* (Yogyakarta: PR2Media dan Yayasan TIFA).

9 Doddy Kridasaksana, M Junaidi, and Muhammad Iftar Aryaputra (2017), “Tujuan Negara Dalam Mengatur Frekuensi Radio Komunitas Ditinjau Dari Undang-Undang Nomor 32 Tahun 2002 Tentang Penyiaran (Studi Kasus Di Wilayah Semarang),” *Jurnal Dinamika Sosial Budaya* 17, no. 2: 242, https://doi.org/10.26623/jdsb.v17i2.489.

10 David Flacher and Hugues Jennequin (2018), “Is Telecommunications Regulation Efficient? An International Perspective,” *Telecommunications Policy* 32, no. 5: 364–77, https://doi.org/10.1016/j.telpol.2008.02.005.

i) Maritime Services" (Maritime Service).

Then, volume 2, Appendix, covers almost all the detailed tasks in Radio Regulations contained in 42 Appendixes. The Appendix also contains the planning results at the World Conference on Maritime, Aviation and Satellite Services. While volume 4, Inclusion by Reference, covers several procedures in Radio Regulations which refer to the Recommendation Study Group ITU-R to discuss the details of the mechanism for using data through radio frequencies.

2) Frequency Distribution System

Distribution is distributing goods and services made from producers to consumers so that they are widely distributed. Until now, telecommunications regulations in Indonesia still distinguish between fixed telecommunications operations and mobile telecommunications operations. The cellular telecommunications system in Indonesia is currently used by:[11]

a) Fixed Wireless Access / FWA
b) Cellular Mobile Network Operator.

With the development of technology, the convergence between fixed and mobile technology, the separation between FWA and cellular is already difficult to distinguish. There have been some efforts to review the improvement of regulatory and technical provisions, including licensing issues, the amount of Use Rights Fee, Radio Frequency, interconnection, numbering, etc. The Indonesian cellular system is based on the 2nd generation (digital cellular) technology, namely GSM and CDMA. Both systems can provide 2.5G services. The Cellular Industry Road Map towards 3G can be described as follows:

a) GSM (2G)-GPRS (2.5G)-EDGE (2.5G+) (migrasi)-WCDMA (overlay)-HSPA-LTE
b) cdmaOne (2G)-CDMA2000-1X (2.5G+)-CDMA2000-1xEV-DO/DV (3G)-LTE

The frequency allocation and standards for cellular operations in Indonesia can be briefly described as follows:

a) GSM/GPRS/EDGE (900/1800 MHz)-WCDMA (1.9/2.1 GHz (IMT-2000))
b) CDMA (450/800/1900 MHz).

Before a network operator operates, an anchoring right must be issued by the Ministry of Communication and Information. Landing Right Satellite is the right to use foreign satellites granted to telecommunications operators or broadcasting agencies. The Landing Right can be granted with the following conditions:

a) The satellite to be used does not cause harmful interference to Indonesian satellites or other satellites that have space station permits and radio stations that have licenses; and
b) The opening of equal opportunities for Indonesian satellite operators to compete and operate in the country of origin of the satellite operator.

[11] Diah Arum Maharani and Helena Wirastri Wulandari (2017), "Penggabungan, Peleburan Dan Pengambilalihan Pada Industri Telekomunikasi Di Indonesia," *Jurnal Penelitian Pos Dan Informatika* 5, no. 1: 19, https://doi.org/10.17933/jppi.2015.0501002.

In addition, the cellular network distribution system in Indonesia is divided according to the network allocation in each region. Consequently, no area has a low or unstable network.

3) Frequency Division of Indonesian Cellular Operators and Their Status in International Information Technology Law

Along with the development of technology in Indonesia, the frequency of cellular operators in Indonesia and their allocation no longer uses CDMA but has focused on GSM (*Global System for Mobile Communication*). However, in using a limited spectrum orbit, Indonesia must limit and comply with the allocation to suit the international sphere.

a) GSM Frequency Allocation

The GSM frequency allocation in Indonesia is no different from that in most of the world, especially Europe, namely in the 900 MHz band, otherwise known as GSM900, and in the 1800 MHz band, known as GSM1800 or DCS (Digital Communication System).[12] The bandwidth of the GSM 900 spectrum itself is 25 MHz, and the ARFCN channel numbering starts from 0 onwards; with the bandwidth per GSM channel being 200 kHz (0.2 MHz), then the total number of for GSM900 is 25/0.2=125 channels. However, these channels cannot be used; two channels must be sacrificed as guard band systems at both ends of the spectrum, namely ARFCN 0 at the lower limit and ARFCN 125 at the upper limit. So the effective ARFCN used for GSM900 is ARFCN 1 to 124. Indonesia has 5 GSM operators, namely Telkomsel, Indosat, XL, Axis and Three, each of which has an operating license. Only three operators receive frequency allocation for the GSM900 band, while the GSM1800 band applies to all operators. As explained in the following picture:

Table 1.1.
Frequency Allocation on GSM Operation in Indonesia

OPERATOR GSM	ALOKASI FREKUENSI		
	GSM900 (MHz)	GSM1800 (MHz)	TOTAL (MHz)
TELKOMSEL	7.5	22.5	30
INDOSAT	10	20	30
XL	7.5	7.5	15
AXIS	0	15	15
THREE	0	10	10
TOTAL	**25**	**75**	**100**

b) Indonesia's Status in International Information Technology Law

Through the ratification of ITU, namely Law no. 11 of 1985 concerning Ratification of the International Telecommunications Convention, Nairobi, 1982, Law no. 10 of

[12] Asril Sitompul (2018), "Masalah Hukum Dalam Penggunaan Spektrum Frekuensi Radio Di Indonesia," *Jurnal Hukum Dan Peradilan* 2, no. 3: 405, https://doi.org/10.25216/jhp.2.3.2013.405-426.

1969 concerning Ratification of the International Telecommunication Union Convention, Montreux 1965, and Law no. 11 of 1976 concerning Ratification of the International Telecommunication Convention, Malaga Terremolinos 1973, Indonesia has committed to engage and comply with the policies and regulations provided by the ITU. In fact, as of December 2013, 48 Indonesian satellite filings had been registered with the ITU. The Indonesian filing consists of 42 unplanned band filings and 6 planned band filings.[13] It should be noted that the allocation of the radio frequency spectrum in Indonesia refers to the Radio Regulations, 2012 edition of the International Telecommunication Union, which is also a reference for other countries in the world. This can be seen through the following table:

Table 1.2.[14]
Allocation of Radio Frequency Spectrum in Indonesia

Radio Frequency	Region 3-ITU	Indonesian Allocation
495-505	Maritime Mobile	Maritime Mobile INS36
505-526	Maritime Mobile 5.79 5.79A 5.84 Mobile Aviation Navigation Radio Ground Mobile Aviation	Maritime Mobile 5.79 5.79A 5.84 Mobile Aviation Navigation Radio Ground Mobile Aviation INS36
526,5-535	Mobile Broadcast 5.88	Siaran Bergerak 5,88
535- 1606,5	Broadcast	Broadcast INS01
1606,5-1800	Radiolocation Constant Mobile Radio Navigation 5,91	Radiolocation Constant Mobile Radio Navigation 5,91

Based on the table above, it can be seen that Indonesia adjusts the frequency allocation following those determined by ITU's Radio Regulations.

B. Cyberware Existence: Definition, Types, and Settings

Indonesia is a sovereign country that uses information-technology systems to carry out government based on an online system. Government implementation is also included in the scope of cellular operator frequency in Indonesia. In its development, technology and information cause a lot of impacts, both good and bad. One of the harmful impacts is cyber warfare which is feared to damage the security of cellular operators in Indonesia because it can attack sovereignty through the damage caused by these crimes. The discussion in the following research will discuss the meaning of cyber warfare and its arrangement according to international law.

---

[13] Dwi Cahyanto and Hamzah Hilal (2013), "Analisa Potensi Keunggulan Kompetitif Re-Farming Frekuensi 900 MHz," *IncomTech, Jurnal Telekomunikasi Dan Komputer* 4 (1).

[14] Tengku Ahmad Riza (2018), "Kajian Implementasi Alokasi Frekuensi Komunikasi Untuk Pelayaran Rakyat Di Indonesia," *ELKOMIKA: Jurnal Teknik Energi Elektrik, Teknik Telekomunikasi, & Teknik Elektronika* 4, no. 2 : 197, https://doi.org/10.26760/elkomika.v4i2.197.

1) Cyberwarefare's Definition

Information and communication technology has provided a lot of effectiveness for human life, including government. But behind the positive impact, there is also a harmful impact on state sovereignty, namely cyberwarfare. Information and communication technology has provided a lot of effectiveness for human life, including government. In cyberwarfare, the war in question is an attack on objects owned by the state in cyberspace. Cyberwarfare is a digital entity or can even serve as a diversion from other malicious cyber activity, such as infiltrating a network. Such threats would pose a significant risk to organizations hoping to protect their systems from intruders and allow hackers to directly expose networks to threats or allow groups to steal sensitive data. The types of weapons used in cyber warfare are as follows:[15]

a) Denial-of-Service
   Denial-of-Service or DoS is defined as an attack on the network by sending additional requests until the system becomes slow or completely disconnected. Generally, DoS attacks work by crippling websites or computer network resources and rendering them unusable through many requests for information resulting in an inability to respond to legitimate information and data requests.

b) Malicious Programs
   *Malicious Program*s or malware usually operate by interfering with the functioning of the computer or by opening access so that a remote attacker can take control of the computer.

c) Logic Bombs
   Logic Bombs is a more sophisticated type of programming crime. Its destructive effect occurs when triggered by a particular event that occurs at a predetermined time. A logic bomb can lie dormant for an unexpectedly long time and then activate, so its effects are much more likely to be wider than if the harmful effects were already visible. Once activated, logic bombs can cause severe damage to the infected computer, making it entirely unusable for deleting specific data and activating more complex DOS attacks.

d) *IP Spoofing*
   Also known as IP address spoofing, IP spoofing is a piracy technique that allows a hacking user to operate a computer while appearing as a trusted host. Thus IP Spoofing hides true identity. Hackers can gain access to computer networks and network resources. When opening a network Internet browser, the computer using the browser when entering the URL is taken to a fake web page that reflects the entered web page but was created by the hijacker. When a user interacts with the content of any fake web page, the hijacking user gains the ability to access sensitive network information or basic computer programming features.

[15] Bradley Raboin, "Corresponding Evolution: International Law and the Emergence of Corresponding Evolution: International Law and the Emergence of Cyber Warfare Cyber Warfare Corresponding Evolution: International Law and the Emergence of Cyber Warfare," *Journal of the National Association of Administrative Law Judiciary* 31, no. 2: 10–15, accessed June 14, 2021, https://digitalcommons.pepperdine.edu/naalj.

2) International Regulations on Cyber Warfare: Tallinn Manual on International Law Applicable at Cyber Warfare

Tallinn Manual on International Law Applicable at Cyber Warfare or Tallinn Manual is motivated by several successful conflict cases using cyber operations, such as the Stuxnet worm at Iran's nuclear facilities in 2010. The NATO Cooperative Cyber Defense Center Excellence then conducted a study of international legal arrangements regarding these crimes. The policy also reflects Allied decisions on simplifying cyber defence governance, assistance procedures to Allied countries and integrating Cyberdefense into operational planning (including civil preparedness).[16] In addition, the policy defines ways to promote awareness, education, training and training activities and encourages further progress in various collaborative initiatives, including with partner countries and international organizations. It also foresees increased NATO cooperation with industry, including information sharing and exchanging best practices.[17] Cyber attacks and their consequences are high on the agenda worldwide. The Allies have also committed to increasing information sharing and assisting each other in preventing, mitigating, and recovering from cyber-attacks. As a humanitarian organization, our concern is that military cyber operations are also part of the current armed conflict and may disrupt the functioning of critical infrastructure and vital services for the civilian population.[18] This situation has disastrous consequences. For example, healthcare systems are increasingly digitized and connected but often unprotected and highly vulnerable to cyberattacks. Too often, in armed conflict, water and electricity infrastructure, or hospitals, are damaged by shootings and services function only partially if at all: Imagine an even more significant cyber incident. Civilians caught up in conflict and violence have struggled enough to see their predicament worsen.

The phrase cyber warfare seems to have been used by different people to mean different things. The term is used here to refer to the means and methods of warfare comprising cyber operations which amount to or are carried out in the context of armed conflict within the meaning of International Humanitarian Law. The ICRC is concerned about cyber warfare because of the vulnerability of cyber networks and the potential for humanitarian harm from cyber attacks. When a country's computers or networks are attacked, compromised, or blocked, there may be a risk of civilians losing necessities such as drinking water, medical care and electricity. If the GPS fails, there may be a risk of civilian casualties, for example, through disruption of life-saving rescue helicopter flight operations. Dams, nuclear plants, and aircraft control systems are also vulnerable to cyber-attacks because of their dependence on computers. Networks are interconnected, so it may be challenging to limit the effect of an attack on one part of the system

---

16 "CYBER WARFARE: TALLIN MANUAL 1.0," accessed June 14, 2021, https://business-law.binus.ac.id/2017/10/30/cyber-warfare-tallin-manual-1-0/.

17 "NATO - Cyber Defence," accessed June 14, 2021, https://www.nato.int/cps/en/natohq/topics_78170.htm?selectedLocale=en.

18 Eric Talbot Jensen, "The Tallinn Manual 2.0: Highlights and Insights," *Georgetown Journal of International Law* 48 (2016), https://heinonline.org/HOL/Page?handle=hein.journals/geojintl48&id=743&div=&collection=.

without damaging other parts or disrupting the whole system. The well-being, health, and even the lives of hundreds of thousands of people can be affected. One of the roles of the ICRC is to remind all parties to a conflict that caution must be exercised to save civilians.[19] War has rules and limitations, which apply as much to the use of cyber warfare as rifles, artillery, and missiles.

Tallinn Manual 1.0 is not intended for cyber security as it is generally understood. The Tallinn Manual emphasizes cyber operations such as cyber operations on a country's critical infrastructure or cyberattacks that control target systems from adversaries. The Tallinn manual does not address legal issues relating to cyber-kinetic operations, such as airstrikes bombing cyber control centres, which are regulated in the provisions of armed conflict. Cyber espionage, intellectual property theft and criminal activity in cyberspace, while severe problems for the state, are not included in the regulatory scope of the Tallinn Manual by leveraging agreements, legal cases, and other sources.[20] The Tallinn Manual produces 95 (ninety-five) black letters that can be used as a guide for countries in conditions of cyberwar, including provisions for cyber operations in neutral territories.

According to the Tallinn Manual, currently ratified and entered into force in March 2013 by NATO cyber defence in Estonia, American cyberattacks against Iran are categorized as "use of force". According to The Tallinn Manual on International Law Applicable to the Rules of Cyberwarfare. "Use of Violence" is defined as an act that kills or injures a person or destroys an object or damages an object constitutes the use of force". According to the United Nations Charter, violence is prohibited, except for self-defence. With the use of force by the United States, it can be said that a manual is an act of American hostility towards Iran, which can be said to be the first sign of conflict as stated in international humanitarian law in the 1949 Geneva Conventions.

In 2019 the Indonesian government was discussing cybersecurity to be articulated as law. In addition, the Indonesian Tallinn Manual does not explicitly regulate. In the absence of the rule of law related to cyber attacks or cyber wars, the concept of reference can be interpreted as closely related to cyberspace law.[21] Although to become the underlying law, the Tallinn Manual's regulations must meet several requirements: signed by member countries, ratified, obeyed and implemented by member countries.

C. The Impact of Cyber Warfare on the Frequency of Indonesian Cellular Operators

[19] "Cyberwarfare and International Humanitarian Law: The ICRC's Position What Limits Does the Law of War Impose on Cyber Attacks?," n.d.

[20] Robert E. Barnsby and Shane R. Reeves, "Give Them an Inch, They'll Take a Terabyte: How States May Interpret Tallinn Manual 2.0's International Human Rights Law Chapter," *Texas Law Review* 95 (2016), https://heinonline.org/HOL/Page?handle=hein.journals/tlr95&id=1581&div=&collection=.

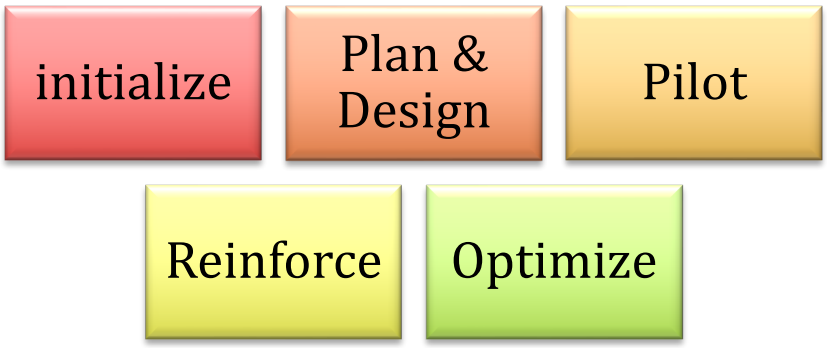
[21] B. Pratama and M. Bamatraf (2021), "Tallinn Manual: Cyber Warfare in Indonesian Regulation," in *IOP Conference Series: Earth and Environmental Science*, vol. 729 (IOP Publishing Ltd.), 12033, https://doi.org/10.1088/1755-1315/729/1/012033.

Since 1998, Indonesia has been a part of cybercrime with other countries. Without having to present physical military strength in the opposing country, attacks through cyberspace have become a new trend in modern warfare in the 21st century. The impact of cyber warfare on the frequency of Indonesian cellular operators is the tapping of civilian victims which can cause advanced losses such as human rights and economic violations. Therefore the minister of defence should pay attention to several things:[22]

1) The need for communication, coordination, and cooperation with the community of information and communication actors such as various telephone operators, Telkom, Indosat, and Excelcomindo, to anticipate cyber attacks in the form of telephone tapping.
2) Coordination and cooperation with the ministry of information and communication to fend off, ward off, and prevent various potential cyber-attacks that attack websites, websites, social media, and communication networks in all banking institutions
3) The Ministry of Defense must cooperate with security forces such as the Indonesian National Police, the State Intelligence Agency, the National Crypto Agency, and other security actors.

Currently, American troops and their coalitions in various countries such as Iraq, Afghanistan, Somalia, Serbia, and Bosnia have not guaranteed the success of the situation or overall control of the situation. Therefore, Indonesia needs extreme cyber resilience. Here is the form of national cyber defence:

Illustration 1.1.
Mechanism of the National Cyber Defense Formation Process in Indonesia



Based on Figure 1.1. It can be seen that the national cyber defence framework in Indonesia is divided into initializing, planning & design, piloting, reinforcing, and optimistic. The explanation of each process is:[23]

1) *Initialize*

[22] Agus Subagyo, "SINERGI DALAM MENGHADAPI ANCAMAN CYBER WARFARE," *Jurnal Pertahanan & Bela Negara* 5, no. 1 (August 6, 2018), https://doi.org/10.33172/jpbh.v5i1.350.

[23] Bagus Artiadi Soewardi, "Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) Yang Tangguh Bagi Indonesia ," 2013, https://www.kemhan.go.id/pothan/wp-content/uploads/migrasi/admin/Cyber Defence.pdf.

Initialize means initiating the formation of a cyber defence work team, mapping national resources, scope, and vision and mission. This stage lasts for 6 months.

2) *Plan & Design*
   Plan & design consists of defensive cyber operation capability. This stage lasts for 12 months.
3) *Pilot*
   The pilot consists of defensive cyber operation capability, which means the implementation stage. This stage lasts for 12 months.
4) *Reinforce*
   The continuation of the pilot is reinforcement or enforcement. In this stage, the mechanism consists of offensive cyber operation capability. This stage lasts for 12 months.
5) *Optimize*
   The last is optimization or optimization, where the stage is carried out continuously for full operational capability.

4. Conclusion

In using the frequency for daily use, Indonesia regulates the frequency allocation to operators in Indonesia, not different from those in international countries. The frequency is divided into two, namely 900Hz and 1800 Hz. There are 5 operators in Indonesia, where only three operators can use 900Hz, namely Telkomsel, Indosat, and XL. Meanwhile, 1800Hz can be used by all three operators plus Axis and Three. Indonesia's frequency allocation position in international law is solid and legal. This is based on the fact that Indonesia has ratified Law no. 11 of 1985 concerning Ratification of the International Telecommunications Convention, No. 10 of 1969 concerning Ratification of the International Telecommunication Union Convention, and Law no. 11 of 1976 concerning Ratification of the International Telecommunication Convention, 1973. This means that Indonesia has complied with every regulation issued by the ITU. This fact is getting stronger because of the provisions of Article 2 of Law no. 24 of 2015 concerning the Table of Allocation of the Indonesian Radio Frequency Spectrum, which states that the allocation of frequencies in Indonesia refers to the ITU-Radio Regulations. The impact of cyber warfare on the frequency of Indonesian cellular operators is the tapping of civilian victims which can cause advanced losses such as human rights and economic violations.

Bibliography / Reference List

A. Journal

Barnsby, Robert E., and Shane R. Reeves. "Give Them an Inch, They'll Take a Terabyte: How States May Interpret Tallinn Manual 2.0's International Human Rights Law Chapter." *Texas Law Review* 95 (2016). https://heinonline.org/HOL/Page?handle=hein.journals/tlr95&id=1581&div=&collection=.

Budhijanto, Danrivanto. "Peran Hukum Telekomunikasi Terhadap Implikasi Konvergensi Teknologi Informasi Dan Komunikasi." *Jurnal Dinamika Hukum*. Vol. 14, January 31, 2014. https://doi.org/10.20884/1.JDH.2014.14.1.283.

Cahyanto, Dwi, and Hamzah Hilal. "Analisa Potensi Keunggulan Kompetitif Re-Farming Frekuensi 900 MHz." *IncomTech, Jurnal Telekomunikasi Dan Komputer* 4,

no. 1 (2013).
"Cyber Warfare: Tallin Manual 1.0." Accessed June 14, 2021. https://business-law.binus.ac.id/2017/10/30/cyber-warfare-tallin-manual-1-0/.
"Cyberwarfare and International Humanitarian Law: The ICRC's Position What Limits Does the Law of War Impose on Cyber Attacks?," n.d.
Flacher, David, and Hugues Jennequin. "Is Telecommunications Regulation Efficient? An International Perspective." *Telecommunications Policy* 32, no. 5 (June 2008): 364–77. https://doi.org/10.1016/j.telpol.2008.02.005.
Jensen, Eric Talbot. "The Tallinn Manual 2.0: Highlights and Insights." *Georgetown Journal of International Law* 48 (2016). https://heinonline.org/HOL/Page?handle=hein.journals/geojintl48&id=743&div=&collection=.
Kridasaksana, Doddy, M Junaidi, and Muhammad Iftar Aryaputra. "Tujuan Negara Dalam Mengatur Frekuensi Radio Komunitas Ditinjau Dari Undang-Undang Nomor 32 Tahun 2002 Tentang Penyiaran (Studi Kasus Di Wilayah Semarang)." *Jurnal Dinamika Sosial Budaya* 17, no. 2 (November 16, 2017): 242. https://doi.org/10.26623/jdsb.v17i2.489.
Maharani, Diah Arum, and Helena Wirastri Wulandari. "Penggabungan, Peleburan Dan Pengambilalihan Pada Industri Telekomunikasi Di Indonesia." *Jurnal Penelitian Pos Dan Informatika* 5, no. 1 (March 6, 2017): 19. https://doi.org/10.17933/jppi.2015.0501002.
"NATO - Cyber Defence." Accessed June 14, 2021. https://www.nato.int/cps/en/natohq/topics_78170.htm?selectedLocale=en.
Nugraha, Rachmat, Neilcy Tjahjamooniarsih, Fitri Imansyah, and Jurusan Teknik Elektro. "Analisis Pengukuran Dan Penilaian Kualitas Penerimaan Siaran Radio Fm Pada Kawasan Perbatasan Kalimantan Barat." *Jurnal Teknik Elektro Universitas Tanjungpura*. Vol. 2, February 3, 2020. https://jurnal.untan.ac.id/index.php/jteuntan/article/view/30065.
Pratama, B., and M. Bamatraf. "Tallinn Manual: Cyber Warfare in Indonesian Regulation." In *IOP Conference Series: Earth and Environmental Science*, 729:12033. IOP Publishing Ltd, 2021. https://doi.org/10.1088/1755-1315/729/1/012033.
Raboin, Bradley. "Corresponding Evolution: International Law and the Emergence of Corresponding Evolution: International Law and the Emergence of Cyber Warfare Cyber Warfare Corresponding Evolution: International Law and the Emergence of Cyber Warfare." *Journal of the National Association of Journal of the National Association of Administrative Law Judiciary* 31, no. 2: 10–15. Accessed June 14, 2021. https://digitalcommons.pepperdine.edu/naalj.
Rahma, Shinta, Diana Peneliti, Pusat Kajian, Kebijakan Penerbangan, Dan Antariksa, Lembaga Penerbangan, and Antariksa Nasional. "Biaya Dan Manfaat Keanggotaan Indonesia Pada Asia-Pacific Space Cooperation Organization (APSCO)," n.d.
RIZA, TENGKU AHMAD. "Kajian Implementasi Alokasi Frekuensi Komunikasi Untuk Pelayaran Rakyat Di Indonesia." *ELKOMIKA: Jurnal Teknik Energi Elektrik, Teknik Telekomunikasi, & Teknik Elektronika* 4, no. 2 (March 14, 2018): 197. https://doi.org/10.26760/elkomika.v4i2.197.
Saputera, Moehammad Yuliansyah. "Pengaruh Cyber Security Strategy Amerika Serikat Menghadapi Ancama Cyber Warfare." *JOM FISIP* 2, no. 2 (2015): 1–15. https://media.neliti.com/media/publications/32726-ID-pengaruh-cyber-

security-strategy-amerika-serikat-menghadapi-ancaman-cyber-warfar.pdf.

Sitompul, Asril. "Masalah Hukum Dalam Penggunaan Spektrum Frekuensi Radio Di Indonesia." *Jurnal Hukum Dan Peradilan* 2, no. 3 (April 23, 2018): 405. https://doi.org/10.25216/jhp.2.3.2013.405-426.

Soewardi, Bagus Artiadi. "Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) Yang Tangguh Bagi Indonesia ," 2013. https://www.kemhan.go.id/pothan/wp-content/uploads/migrasi/admin/Cyber Defence.pdf.

Subagyo, Agus. "Sinergi Dalam Menghadapi Ancaman Cyber Warfare." *Jurnal Pertahanan & Bela Negara* 5, no. 1 (August 6, 2018). https://doi.org/10.33172/jpbh.v5i1.350.

B. Books

Soekanto, Soerjono. 2012. *Pengantar Penelitian Hukum*. Jakarta: Penerbit Universitas Indonesia.

_____. 2012. Penelitian Hukum Normatif. Jakarta: PT Raja Grafindo Persada.