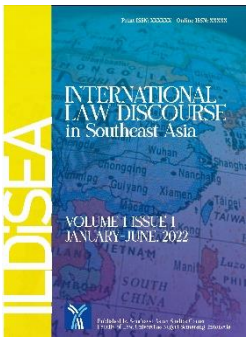
International Law Discourse in Southeast Asia
Volume 1 Issue 1 (January-June 2022), pp. 1-22
ISSN: 2830-0297 (Print) 2829-9655 (Online)
https://doi.org/10.15294/ildisea.v1i1.56874
Published biannually by the Faculty of Law, Universitas Negeri Semarang, Indonesia and managed by Southeast Asian Studies Center, Universitas Negeri Semarang, INDONESIA

Available online since January 31, 2022

Cyber Espionage in National and Global Perspective: How Indonesia Deal with this issue?

Maharani Chandra Dewi*
Malaysia University of Science and Technology
MALAYSIA



ABSTRACT: Indonesia is a legal state, in the execution of a judge is an object that is very important for a trial. In Indonesia alone the practice of fraud and manipulation is still common and often encountered in a trial, the duty of a judge who should be neutral and decide a case with as fair as possible can often be manipulated by the bribery process of a suspect. the power of a judge alone is set in the law of the judicial power law number 48 of 2009. There it has been explained everything about the duties and authority of a judge and how to be a just judge and then can put a suspect into a subject rather than an object. Often in finding a judge complicates a case that is actually trivial and gives a burdensome decision for the little people and even facilitate a big case with a suspect of important people, a concept that is not denied a thing that we often see in law.

KEYWORDS: Cyber Espionage, International Law, National Security, Indonesia, Cybercrime

HOW TO CITE:
Dewi, Maharani Chandra. "Cyber Espionage in National and Global Perspective: How Indonesia Deal with this issue?". *International Law Discourse in Southeast Asia* 1, No. 1 (2022): 1-22. https://doi.org/10.15294/ildisea.v1i1.56874

* *Corresponding author's email: maharanichandradewi@gmail.com*
Submitted: 17/10/2021 Reviewed: 23/10/2021 Revised: 10/12/2021 Accepted: 18/01/2022

I. INTRODUCTION

The development of cybercrime, the beginning of the attack in the Cyber world in 1988, better known as Cyber Attack. At that time there was a student who managed to create a worm or virus that attacks computer programs and kills about 10% of all computers in the world that are connected to the internet. In 1994 a 16 year old music school boy named Richard Pryce, better known as "the hacker" aka "Datastream Cowboy", was arrested for illegally logging into hundreds of secret computer systems including the data centers of the Griffits Air Force, NASA and the Korean Atomic Research Institute or the Korean atomic research agency. During his interrogation with the FBI, he admitted that he learned hacking and cracking from someone he knew through the internet and turned him into a mentor, who has the nickname "*Kuji*". Cybercrime is grouped into several forms according to the existing modus operandi, one of which is "Cyber Espionage" which will be discussed further.

Cyber Crime is the most frightening crime in today's technological developments. Attacks that do not know the target and time for a particular purpose. The privacy of a person or institution can be threatened by cyber crime. Mobile technology and supported by adequate communication network facilities turn a positive image into a dilemma. The development of user knowledge of technology turned out to be misused by some people. For example, by violating access rights to retrieve important data only for certain interests. Various techniques have been developed. Hackers are known as terrible and scary figures in doing cyber crime. They are hired to perform at the behest of institutions or individuals.[1]

---

[1] Evi Dwi Hastri, "Cyber Espionage Sebagai Ancaman Terhadap Pertahanan dan Keamanan Negara Indonesia." *Law & Justice Review Journal* 1, No. 1 (2021):

The technique used by hackers is to insert malware or viruses into the application. Malware itself has many types and continues to grow depending on its needs. The great thing is that malware can change the operating system and even take over the user's computer so that it looks damaged. In addition to the impact of damage to hardware and software, it turns out that there is an impact that causes psychological damage. Belief in something can be drastically reduced. Fear of using technology that can be fatal. Excessive preventive measures backfire very scary. Ethics in the use of technology has no effect.[2]

As a theory says "*crime is a product of society itself*" which can be interpreted that it is society itself that gives birth to a crime. The higher the intellectual level of society (the smarter the human brain), the more sophisticated the crimes that may occur in that society. The borderless network is used as a tool to commit acts that are against the law. Generally, crimes related to technology or cybercrime are crimes involving property and/or intellectual property. The term cybercrime currently refers to an act of crime related to cyberspace and crimes that use computers.

It is further emphasized that the use of the term cyber crime or crime on the internet is more relevant than the term computer crime. Cyber

---

12-25; Alfin Reza Syahputra, and Muhammad Syaroni Rofii. "Vulnerability of Espionage Propaganda by Foreign Citizens (WNA) in Indonesia." *Konfrontasi: Jurnal Kultural, Ekonomi dan Perubahan Sosial* 9, No. 1 (2022): 7-13; Dista Amalia Arifah, "Kasus cybercrime di indonesia." *Jurnal Bisnis dan Ekonomi* 18, No. 2 (2011).

[2] Wadha Abdullah Al-Khater, et al. "Comprehensive review of cybercrime detection techniques." *IEEE Access* 8 (2020): 137293-137311; Damian A. Tamburri Cascavilla Giuseppe, and Willem-Jan Van Den Heuvel. "Cybercrime threat intelligence: A systematic multi-vocal literature review." *Computers & Security* 105 (2021): 102258.

crime that uses communication media and computers, control is in another world in a virtual form but has a very real impact. Deviations and losses have occurred and are felt by people all over the world, including Indonesia. The U.S. The Department of Justice defines computer crime as *"...any illegal act requiring knowledge of computer technology for perpetration, investigation, or prosecution*".[3]

Contrary to the many problems that occur today. Some countries claim to have been the object of espionage by other countries. This is known not to be done in a conventional way, but through cyberspace by utilizing advances in information technology and media. Espionage[4] defined in the Big Indonesian Dictionary is a secret investigation of military data and economic data of other countries; everything to do with the intricacies of mirrors; spying: the arrest of the two deputy military attaches on charges. One of the conventions

---

[3] Adam M. Bossler, "Cybercrime legislation in the United States." *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (2020): 257-280; Andri Winjaya Laksana, "Cybercrime Comparison Under Criminal Law in Some Countries." *Jurnal Pembaharuan Hukum* 5, No. 2 (2018): 217-226.

[4] Although espionage is part of intelligence activities, espionage has a difference from other forms of intelligence gathering in that it can collect information by accessing the place where the information is stored or people who know about the information and will leak it through various pretexts. In general, espionage is considered part of an institutional effort (e.g., government or intelligence services). The term espionage was originally thought of as a condition of spying on a potential or actual enemy, mainly for military purposes, but has now evolved to spying on companies, known specifically as industrial espionage. According to the AIVD (Dutch Intelligence and Security Agency), espionage is the activity of secretly gathering information about the development of other countries. The information collected is related to politics, economy, technology, science and technology, and trade secrets. Cambridge Dictionary, the meaning of espionage is the activity of gathering and reporting classified information, particularly related to the military, politics, business and industry. Espionage is generally carried out using secret agents or spies within an organization or country.

governing this espionage activity is the Hague Convention IV 1907 articles 29 to 31. In simple terms it can be directly included in the type of cyber-espionage, but if it is understood in depth it can enter into other forms and/or types of cybercrime.[5] Not only because it is different from conventional crimes, but the perpetrator also represents a country based on orders and is a proper job.[6] The following are the characteristics or special characteristics of cybercrime that correspond to espionage:

1. Unauthorized access
2. Without violence,
3. Slightly involve physical contact (minimaze of physical contact)
4. Using equipment, technology, and utilizing the global telematics network (telecommunication, media and informatics),
5. These actions result in material and immaterial losses (time, value, services, money, goods, self-esteem, dignity, confidentiality of information) which tend to be greater than conventional crimes.

Cybercrime is a crime with a high-tech dimension, and law enforcement officials do not yet fully understand what cybercrime is. In other words, the condition of human resources, especially law enforcement officers, is still weak. The availability of funds or budget

---

[5] Ilias Bantekas, "The contemporary law of superior responsibility." *American Journal of International Law* 93, No. 3 (1999): 573-595; G. N. Barrie, "Spying-an international law perspective." *Journal of South African Law/Tydskrif vir die Suid-Afrikaanse Reg* 2008, No. 2 (2008): 238-254; Ingrid Delupis, "Foreign warships and immunity for espionage." *American Journal of International Law* 78, No. 1 (1984): 53-75.

[6] Allan Hepburn, *Intrigue: Espionage and Culture*. (Yale University Press, 2008); Kievly Andrew Tambuwun, "Tanggung Jawab Pejabat Diplomatik Yang Melakukan Kegiatan Spionase Menurut Hukum Internasional." *Lex et Societatis* 7, No. 2 (2019); Yosa Bayu Kuswara, "Evaluasi Fungsi Kontra Intelijen Indonesia Dalam Menghadapi Spionase Intelijen Asing." *Jurnal Kajian Stratejik Ketahanan Nasional* 2, No. 2 (2019): 114-128.

for HR training is so minimal that it is difficult for law enforcement institutions to send them to attend training both at home and abroad. The absence of a Computer Forensic Laboratory in Indonesia causes a large amount of time and cost. In the case of Dani Firmansyah who hacked the KPU website, the Police had to bring the hard drive to Australia to investigate the type of damage caused by the hacking. The image of the judiciary has not improved, even though various efforts have been made. This bad image causes people or victims to be reluctant to report their cases to the police.[7] Legal awareness to report cases to the police is low. This is triggered by the image of the judiciary itself, which is not good, another factor is the victim does not want the weakness in his computer system to be known by the public, which means it will affect the performance of the company and its web master. In the Indonesian context, the urgency of this matter is regulated in Law No. 11 of 2008 concerning information and electronic transactions in article 31 paragraph (1): "*Everyone intentionally and without rights or against the law intercepts or intercepts electronic information and/or electronic documents in a computer and/or certain electronic systems belonging to other people*."

II. METHODS

The data used in the preparation of this paper comes from various literature related to the problems discussed. Some of the main types of references used are textbooks of flow and theory in law and technology, print and online editions of national and international

[7] Muhammad Amin Rais, and Phichit Songkarn. "Hacker and the Treat for National Security: Challenges in Law Enforcement". *Indonesian Journal of Counter Terrorism and National Security* 1, No. 1 (2022): 45-66. https://doi.org/10.15294/ijctns.v1i1.56728.

law journals, and also keep referring to the applicable laws. The types of data obtained are varied, qualitative and quantitative. The writing method is literature study. Information obtained from various literatures and compiled based on the results of the study of the information obtained. Writing strives to be related to each other and in accordance with the topics discussed.

The data collected is selected and sorted according to the topic of study. Then do the preparation of the paper based on the data that has been prepared logically and systematically. The data analysis technique is descriptive argumentative. Conclusions are obtained after referring back to the formulation of the problem, the purpose of writing, and discussion. The conclusions drawn represent the subject of the written work and are supported by practical suggestions as further recommendations.

III. CYBER ESPIONAGE: LIMITATIONS & LEGAL ASPECTS

Cyber Espionage is the act or practice of obtaining confidential information without the permission of the holder of information (personal, sensitive, proprietary or confidential nature), from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage. using methods on the internet network, or personal computers through the use of cracking techniques and malicious software including trojan horses and spyware. This can entirely be done online from professional computer desks at bases in faraway countries or it may involve infiltration at home by conventionally trained computer spies and moles or in other cases it may be the criminal work of amateur malicious hackers and software programmers.

Cyber espionage usually involves the use of such access to confidential and confidential information or control of individual

computers or the network as a whole for strategic gain and psychological, political, subversion and physical activities and sabotage. More recently, cyber spying involves the analysis of public activity on social networking sites such as Facebook and Twitter. Such operations, like non-cyber espionage, are usually illegal in the victim country while being fully supported by the highest levels of government in the aggressor country. The ethical situation also depends on one's point of view, especially one's opinion of the government involved. Cyber espionage is one of the crimes of cyber crime that uses the internet network to carry out spying activities against other parties by entering the computer network system of the target party. This crime is usually directed against business rivals whose important documents or data are stored in a computerized system.[8]

There are many types of cyber espionage cases that have occurred in various countries, here are some examples:

1. Theft and use of other people's internet accounts, namely the theft or unauthorized use of other people's IDs and passwords, simply by capturing the ID and Password used by the user on the internet network which will later be used by the thief. As a result of this theft, the user is charged with the cost of using the account.
2. Hijack websites, that is the activity that is often carried out by crackers is changing web pages, which is known as defacement. Piracy can be done by exploiting a security hole. Cracker is a crime by stealing data such as spoofing, etc., unlike hacker crackers

[8] Massulthan Rafi Wijaya, and Ridwan Arifin. "Cyber Crime in International Legal Instrument: How Indonesia and International Deal with This Crime?." *IJCLS (Indonesian Journal of Criminal Law Studies)* 5, No. 1 (2020): 63-74.

which are usually done with bad intentions.

3. Probing and port scanning is one of the steps that crackers take before entering the targeted server is to do reconnaissance. The way to do this is to do "*port scanning*" or "*probing*" to see what services are available on the target server.

The development of the Internet and generally the cyber world does not always produce positive things. One of the negative things which is a side effect, among others, is crime in the cyber world or, cybercrime. The disappearance of the boundaries of space and time on the Internet changed many things. A cracker in Russia was able to break into a server at the Pentagon without permission.

IV. CYBER ESCPIONAGE CASES IN INDONESIA & GLOBAL CONTEXT

Theft and use of other people's Internet accounts. One of the difficulties of an ISP (internet service provider) is that their customer accounts are "stolen" and used illegally. Unlike the theft that is done physically, "theft" account simply captures the "userid" and "password" only. Only stolen information. Meanwhile, the stolen person does not feel the loss of the stolen "thing". Theft only takes effect if this information is used by unauthorized persons. As a result of this theft, the user is charged with the use of the account. This case often occurs in ISPs. However, what has been raised is the use of stolen accounts by two internet cafes in Bandung. Website hijacking. One of the activities that are often carried out by crackers is changing web pages, which is known as defacement. Piracy can be done by exploiting a security hole, and statistics in Indonesia showed one website was hijacked every day.

Probing and port scanning is one of the steps that crackers take before entering the targeted server is to do reconnaissance. The way to do this is to do "port scanning" or "probing" to see what services are available on the target server. For example, scanning results can show that the target server is running the Apache web server program, the Sendmail mail server, and so on. The analogy of this with the real world is to see if your door is locked, the brand of lock used, which window is open, whether the fence is locked (using a firewall or not) and so on. The person concerned has not carried out any theft or attack activities, but the activities carried out are already suspicious. to do probing or portscanning can be obtained for free on the Internet. One of the most popular programs is “nmap” (for systems based on UNIX, Linux) and “Superscan” (for systems based on microsoft windows). In addition to identifying the port, nmap can even identify the type of operating system used. Viruses. As in other places, computer viruses also spread in Indonesia. Deployment is generally done using e-mail. Often people whose email systems are infected with viruses are not aware of this. The virus is then sent elsewhere via email. Denial of Service (DoS) and Distributed DoS (DDos) attacks. DoS attack is an attack that aims to paralyze the target (hang, crash) so that he cannot provide services. This attack does not steal, eavesdrop, or falsify data.

However, with the loss of service, the target cannot provide services so there is a financial loss. What is the status of this DoS attack? Imagine if someone could make a Bank ATM malfunction. As a result, bank customers cannot make transactions and the bank (and customers) can suffer financial losses. DoS attacks can be targeted at servers (computers) and can also be targeted at networks (consuming bandwidth). Tools for doing this are widely available on the Internet. DDoS attacks enhance these attacks by performing them from several

(tens, hundreds, and even thousands) of computers simultaneously. The resulting effect is more powerful than a DoS attack alone. Domain name related crimes. Domain names are used to identify companies and trademarks. But many people try to make a profit by registering the domain name of someone else's company and then trying to sell it at a higher price. This job is similar to ticket brokers. The term is often used is cybersquatting. Another problem is using a rival company's domain name to the detriment of another company. (Case: mustika-ratu.com) Another crime related to domain names is creating a "play domain", which is a domain that is similar to someone else's domain name. (Such as the case ofklikbca.com) The term used today is typosquatting. IDCERT (Indonesian Computer Emergency Response Team). One way to make it easier to handle security issues is to create a unit to report security cases. This security problem abroad began to be recognized with the emergence of the "sendmail worm" which stopped the internet email system at that time. Then a Computer Emergency Response Team (CERT) was formed. Since then, in other countries, CERTs have also been formed to become points of contact for people to report security problems. IDCERT is an Indonesian CERT.

Security device certification. Devices used to address security should have a quality rating. Devices used for personal purposes are certainly different from devices used for military purposes. However, until now there is no institution that handles the problem of evaluating security devices in Indonesia. In Korea this is handled by the Korea Information Security Agency. The following are some examples of approaches to cybercrime (in particular) and security (generally) abroad.

1) The United States has a Computer Crime and Intellectual

Property Section (CCIPS) of the Criminal Division of the U.S. Department of Justice. This institution has a website <http://www.cybercrime.gov> which provides information about cybercrime. However, a lot of information is still focused on computer crime.

2) The National Infrastructure Protection Center (NIPC) is a United States government institution that deals with infrastructure-related issues. This institution identifies parts of infrastructure that are critical (critical) for the country (especially for the United States). Website: <http://www.nipc.gov>. Internet or computer network has been considered as an infrastructure that needs special attention. This institution provides advisory
3) The National Information Infrastructure Protection Act of 1996
4) CERT which provides advisory on the existence of security holes.
5) Korea has a Korea Information Security Agency whose job is to evaluate computer & Internet security devices, especially those that will be used by the government.

Some time ago, the Counter National Executive Office just published a report to Congress presenting frightening images of other countries using cyber espionage to try to obtain business and industry secrets from US companies. The biggest threat in terms of cyber-espionage to American businesses is that China and Russia engage in attempts to acquire sensitive business and information technology. The project reports that China and Russia will "remain aggressive and sensitive to the economy and technology, particularly in cyberspace."

A new US intelligence report says China and Russia are using cyber

espionage to steal US trade and technology secrets to help build their economies. He said Chinese and Russian intelligence had ingested large amounts of high-tech American research and development data, posing a "growing and persistent threat" to US economic security. A report to Congress entitled “Foreign Spies Steal US Economic Secrets in Cyberspace” concluded China and Russia are the “most aggressive collectors” of US economic information and technology. The cyber espionage economy targets key components of the US economy: information technology, military technology, and clean energy and medical technology. A senior intelligence official who spoke on condition of anonymity said it was necessary to dedicate a particular country to dealing with the problem and seek to contain threats that get out of control. The report did not offer many details about the cyber-attacks, but the official said the United States had no evidence. The governments of China and Russia routinely deny involvement in such activities. The US government does not have an accounting of economic losses due to economic cyber espionage. Intelligence officials say the National Science Foundation has put the value of public and private research and development at around $400 billion in 2009. The US International Trade Commission estimates that as much as $50 billion was lost to espionage, cyber-attacks and other fraudulent and trademark crimes.

Cyber espionage is part of the nation state cyber warfare. One of the difficulties in explaining cyber warfare is when defining cyber espionage. Many countries and international bodies define it separately but have difficulty reducing the issue to a single consensus. Factors such as the extent and nature of the damage inflicted from an attack, the identity of the attacker, and how the stolen information is used all influence views on cyber espionage. One of the references that can be used in nation state cyber warfare is

the Tallin Manual which has attempted to explain the definitions, procedures and rules regarding international cyber operations. This manual was published in 2013 as a result of a conference convened by the NATO Cooperatives Cyber Defense Center of Excellence in Tallin, Estonia, defining cyber espionage as "an act undertaken clandestinely or under false pretenses that uses cyber capabilities to gather (or attempt to gather) information with the intention of communicating it to the opposing party" (an action carried out clandestinely (hidden) or with false reasons using cyber capabilities to gather information with the intention of communicating it to the opposing party).

Although most people define cyber espionage specifically targeting confidential information stolen for malicious intent, but that definition does not yet cover the intent of the attack and the nature of the information stolen. The definition of cyber espionage issued in this Tallin Manual is important for countries that are victims of cyber attacks in taking the necessary steps against cyber attacks on a small scale.

V. INDONESIAN LEGAL BASIS FOR CYBER ESPIOPNAGE

The Law that regulates Cyber Espionage Crime Law No 11 of 2008 concerning Information and Transaction Electronic (hereinafter as ITE Law). Article 30 Paragraph 2 ITE Law stated that "*accessing computers and/or electronic systems in any way with the aim of obtaining information and/or electronic documents*" [mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi dan/atau dokumen elektronik]. Article 31 Paragraph 1 "*Every person intentionally and without right or against the law interception or wiretapping of Information and/or Electronic Documents in a certain Computer and/or Electronic System belonging to*

another Person" [Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain]. And the criminal provisions are in: Article 46 Paragraph 2 "*Everyone who fulfills the elements as referred to in Article 30 paragraph (2) shall be sentenced to a maximum imprisonment of 7 (seven) years and/or a maximum fine of Rp. 700,000,000.00 (seven hundred million rupiah)*" [Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah)]. Article 47 "*Everyone who fulfills the elements as referred to in Article 31 paragraph (1) or paragraph (2) shall be sentenced to a maximum imprisonment of 10 (ten) years and/or a maximum fine of Rp.800,000,000.00 (eight hundred million rupiah)*" [Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 31 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah)].

Regulation of Cyber Espionage according to National Law: In national law, the rule of law that contains cyber crime is the Information and Electronic Technology Law. Regarding acts that are prohibited by ITE taking from the Convention on Cyber Crime, however, Indonesia has not ratified the convention. In the Convention on Cyber Crime, cyber espionage is called Illegal Interception, in the ITE Law the cyber crime of Espionage is contained in Article 31 paragraph 1, that is, every person intentionally and without rights or against the law conducts interception or wiretapping of Electronic Information and/or Electronic Documents in a certain Computer and/or Electronic System belonging to another

person.[9]

Regarding the meaning of "interception or wiretapping" it is stated in the explanation of Article 31 paragraph 1, namely: "Activities to listen, record, deflect, change, inhibit, and/or record the transmission of Electronic Information and/or Electronic Documents that are not public, either using a cable network communications or wireless networks, such as electromagnetic or radio frequency beams." Regarding the exceptions to Illegal Interception actions, it is also stated in Article 31 paragraph 3, namely except for interception as referred to in paragraph (1) and paragraph (2), interception carried out in the context of law enforcement at the request of the police, prosecutors, and/or other law enforcement institutions. determined by law. Regarding law enforcement officers who carry out Illegal Interception, there are laws and regulations such as Law No. 17 of 2011 concerning State Intelligence, Law No. 30 of 2002 concerning the Corruption Eradication Commission, Law No. 21 of 2007 concerning the Criminal Act of Trafficking in Persons, and Law No. 35 of 2009 concerning Narcotics. Then the crime of espionage is also regulated in the Criminal Code, one of the forms of crime is an attempt to harm and endanger state security which is contained in Article 124 of the Criminal Code which emphasizes the perpetrators who intentionally notify or hand over to the enemy maps, plans, drawings, or writing about army buildings or being a spy for the enemy or providing accommodation to him, shall be punished with life imprisonment or

---

[9] Rama Halim Nur Azmi, "Indonesian Cyber Law Formulation in The Development of National Laws in 4.0 Era." *Lex Scientia Law Review* 4, No. 1 (2020): 46-58; Dararida Fandra Mahira, Dwi Suci Rohmahwatin, and Nabila Dian Suciningtyas. "Strengthening Multistakeholder Integrated through Shared Responsibility in the face of Cyber Attacks Threat." *Lex Scientia Law Review* 4, No. 1 (2020): 59-69.

be sentenced to a maximum sentence of twenty years.

Law Number 11 of 2008 concerning the Internet & Electronic Transactions (ITE) This law, which was ratified and promulgated on April 21, 2008, although to this day there has not been a Government Regulation stipulating the technical implementation of it, it is hoped that can become a cyber law or cyberlaw to ensnare irresponsible cybercrime actors and become a legal umbrella for the information technology user community in order to achieve legal certainty. Furthermore, it is even emphasized in terms of cyber espionage regulations in the ITE Law, which are as follows:

1. Article 27 of the ITE Law of 2008: Everyone intentionally and without rights distributes and/or transmits and/or makes accessible electronic information and/or electronic documents that have content that violates decency. Criminal threat of article 45(1) of the Criminal Code. Imprisonment for a maximum of 6 (six) years and/or a fine of a maximum of Rp. 1,000,000,000.00 (one billion rupiah). Article 282 of the Criminal Code also regulates crimes against decency.
2. Article 28 of the ITE Law of 2008: Everyone intentionally and without rights spreads false and misleading news that results in consumer losses in electronic transactions.
3. Article 29 of the ITE Law 2008: Everyone intentionally and without rights sends electronic information and/or electronic documents that contain threats of violence or intimidation that are directed personally (Cyber Stalking). Article 45 (3) Any person who fulfills the elements as referred to in Article 29 shall be sentenced to a maximum imprisonment of 12 (twelve) years and/or a maximum fine of Rp. 2,000,000,000.00 (two billion rupiah).

4. Article 30 Paragraph 2 "access computers and/or electronic systems in any way with the aim of obtaining information and/or electronic documents"
5. Article 31 Paragraph 1 "Every person intentionally and without rights or against the law conducts interception or wiretapping of Information and/or Electronic Documents in a certain Computer and/or Electronic System belonging to another Person"

And for the criminal provisions there are:

1. Article 46 Paragraph 2 "Everyone who fulfills the elements as referred to in Article 30 paragraph (1) shall be sentenced to a maximum imprisonment of 6 (six) years and a maximum fine of Rp. 600,000,000 (six hundred million rupiah). Everyone who fulfills the elements as referred to in Article 30 paragraph is sentenced to a maximum imprisonment of 7 (seven) years and/or a maximum fine of Rp. 700,000,000.00 (seven hundred million rupiah). 8 (eight) years and/or a maximum fine of Rp. 800,000,000,- (eight hundred million rupiah).
2. Article 47 Anyone who fulfills the elements as referred to in Article 31 paragraph (1) or paragraph (2) shall be sentenced to a maximum imprisonment of 10 (ten) years and/or a maximum fine of Rp.800,000,000.00 (eight hundred million rupiahs).
3. Article 51 Anyone who fulfills the elements as referred to in Article 35 shall be sentenced to a maximum imprisonment of 12 (twelve) years and a maximum fine of Rp. 12,000,000,000.- (twelve billion rupiahs).

VI. CONCLUSION

Cyber Crime is the most frightening crime in today's technological

developments. Attacks that do not know the target and time for a particular purpose. The privacy of a person or institution can be threatened by cyber crime. Mobile technology and supported by adequate communication network facilities turn a positive image into a dilemma. The ITE Law (Law on Information and Electronic Transactions) which was passed by the DPR on March 25, 2008, is proof that Indonesia is no longer behind other countries in making legal instruments in the field of cyberspace law. This law is cyberlaw in Indonesia, because of its content and wide scope in discussing regulations in cyberspace. The ITE Law which regulates cyber espionage is as follows: Article 30 Paragraph 2, Article 31 Paragraph, Article 46 Paragraph 2, and Article 47.

ACKNOWLEDGMENTS

None.

COMPETING INTERESTS

The Authors declared that they have no competing interests.

REFERENCES

Al-Khater, Wadha Abdullah, et al. "Comprehensive review of cybercrime detection techniques." *IEEE Access* 8 (2020): 137293-137311.

Arifah, Dista Amalia. "Kasus cybercrime di indonesia." *Jurnal Bisnis dan Ekonomi* 18, No. 2 (2011).

Azmi, Rama Halim Nur. "Indonesian Cyber Law Formulation in The Development of National Laws in 4.0 Era." *Lex Scientia Law Review* 4, No. 1 (2020): 46-58.

Bantekas, Ilias. "The contemporary law of superior responsibility." *American Journal of International Law* 93, No. 3 (1999): 573-595.

Barrie, G. N. "Spying-an international law perspective." *Journal of South African Law/Tydskrif vir die Suid-Afrikaanse Reg* 2008, No. 2 (2008): 238-254.

Bossler, Adam M. "Cybercrime legislation in the United States." *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (2020): 257-280.

Delupis, Ingrid. "Foreign warships and immunity for espionage." *American Journal of International Law* 78, No. 1 (1984): 53-75.

Giuseppe, Damian A. Tamburri Cascavilla, and Willem-Jan Van Den Heuvel. "Cybercrime threat intelligence: A systematic multi-vocal literature review." *Computers & Security* 105 (2021): 102258.

Hastri, Evi Dwi. "Cyber Espionage Sebagai Ancaman Terhadap Pertahanan dan Keamanan Negara Indonesia." *Law & Justice Review Journal* 1, No. 1 (2021): 12-25.

Hepburn, Allan. *Intrigue: Espionage and Culture*. (Yale University Press, 2008).

Kuswara, Yosa Bayu. "Evaluasi Fungsi Kontra Intelijen Indonesia Dalam Menghadapi Spionase Intelijen Asing." *Jurnal Kajian Stratejik Ketahanan Nasional* 2, No. 2 (2019): 114-128.

Laksana, Andri Winjaya. "Cybercrime Comparison Under Criminal Law in Some Countries." *Jurnal Pembaharuan Hukum* 5, No. 2 (2018): 217-226.

Mahira, Dararida Fandra, Dwi Suci Rohmahwatin, and Nabila Dian Suciningtyas. "Strengthening Multistakeholder Integrated through Shared Responsibility in the face of Cyber Attacks Threat." *Lex Scientia Law Review* 4, No. 1 (2020): 59-69.

Rais, Muhammad Amin, and Phichit Songkarn. "Hacker and the Treat for National Security: Challenges in Law Enforcement". *Indonesian Journal of Counter Terrorism and*

National Security 1, No. 1 (2022): 45-66. https://doi.org/10.15294/ijctns.v1i1.56728.

Syahputra, Alfin Reza, and Muhammad Syaroni Rofii. "Vulnerability of Espionage Propaganda by Foreign Citizens (WNA) in Indonesia." *Konfrontasi: Jurnal Kultural, Ekonomi dan Perubahan Sosial* 9, No. 1 (2022): 7-13.

Tambuwun, Kievly Andrew. "Tanggung Jawab Pejabat Diplomatik Yang Melakukan Kegiatan Spionase Menurut Hukum Internasional." *Lex et Societatis* 7, No. 2 (2019).

Wijaya, Massulthan Rafi, and Ridwan Arifin. "Cyber Crime in International Legal Instrument: How Indonesia and International Deal with This Crime?." *IJCLS (Indonesian Journal of Criminal Law Studies)* 5, No. 1 (2020): 63-74.

This next president is going to inherit the most sophisticated and persistent cyber espionage cultures the world has ever seen, He needs to surround himself with experts that can expedite the allocation of potent layers of next generation defenses around our targeted critical infrastructure silos.

James Scott
Senior Fellow, Institute for Critical Infrastructure Technology