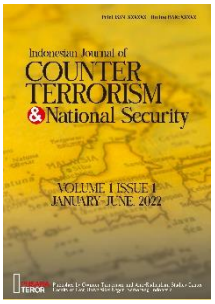
Indonesian Journal of Counter Terrorism and National Security
Volume 1 Issue 1 (January-June 2022), pp. 45-66
ISSN XXXX-XXXX (Print) XXXX-XXXX (Online)
https://doi.org/10.15294/ijctns.v1i1.56728
Published biannually by the Faculty of Law, Universitas Negeri Semarang, Indonesia and managed by Counter Terrorism and Anti Radicalism Studies Center, Universitas Negeri Semarang, INDONESIA
Available online since January 31, 2022

Hacker and the Treat for National Security: Challenges in Law Enforcement

Muhammad Amin Rais*
Cyber Security Forum Jakarta, Indonesia

Phichit Songkarn
Chiang May University, Thailand



ABSTRACT: Globalization has become the driving force behind the birth of the era of information technology development. The development of this technology is very fast and has spread to all corners of the world. The development of information technology is not only felt by developed countries but developing countries also feel the development of information technology, so that information technology gets an important position for the progress of society in this modern era. The need for computer network technology is increasing. Apart from being a medium for providing information, through the internet, commercial community activities are also the largest and growing rapidly and penetrate various national borders. Even through this network market activities in the world can be known for 24 hours. Through the world of the internet or also called cyber space, anything can be done. The positive side of this virtual world of course adds to the trend of world technology development with all forms of human creativity. However, the negative impact cannot be avoided. When pornography is rife on the internet, people can't do much. Along with the development of internet technology, causing the emergence of a crime called cyber crime or crime through the internet network or cyberspace. The emergence of several cases of cyber crime in Indonesia, such as credit card theft, hacking of several sites, tapping other people's data transmissions, such as e-mail and manipulating data by preparing unwanted commands into computer programmers. So that in computer crimes it is possible to have formal offenses and material offenses. Formal offense is the act of someone entering

* *Corresponding author's email: aminrais0211@yahoo.com*
Submitted: 10/11/2021 Reviewed: 10/12/2021 Revised: 11/01/2022 Accepted: 15/01/2022

someone else's computer without permission, while material offense is an act that causes harm to other people. The existence of cyber crime has become a threat to stability, so it is difficult for the government to balance the techniques of crime committed with computer technology, especially in the internet network.

KEYWORDS: Cyber Crime, Cyber Security, National Security, Information Technology

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

I. INTRODUCTION

This rapid development in communication and information technology has resulted in a world that has no boundaries and has led to social change. The development of information technology is seen as a double-edged sword. The purpose of a double-edged sword is that information technology in addition to bringing important benefits for improving welfare and progress of civilization for human life but also brings many negative impacts and harms humans against the law.[1]

[1] H. Kasiyanto Kasemin, *Agresi Perkembangan Teknologi Informasi*. (Jakarta: Prenada Media, 2016); Mohammad Zamroni, "Perkembangan teknologi komunikasi dan dampaknya terhadap kehidupan." *Jurnal Dakwah: Media Komunikasi dan Dakwah* 10, No. 2 (2009): 195-211; I. Gede Ratnaya, "Dampak negatif perkembangan teknologi informatika dan komunikasi dan cara antisifasinya." *Jurnal Pendidikan Teknologi dan Kejuruan* 8, No. 1 (2011); Riska Mayeni, Okviani Syafti, and Sefrinal Sefrinal. "Dampak Perkembangan Teknologi Dikalangan Remaja Dilihat dari Nilai-Nilai Karakter." *Turast: Jurnal Penelitian dan Pengabdian* 7, No. 2 (2019): 239-246.

The perceived impact of the existence of information technology can be in the form of positive impacts or negative impacts. The negative impact as a result of the development of information technology is the emergence of new modes of crime by utilizing information technology generated through computers and internet networks (cybercrime). With the emergence of cyber crime then a new form of legal product emerged, known as cyber law or information technology law. Cyber crimes between these can be said to be all crimes related to the information system itself, and the communication system that creates a means to convey or exchange information with other parties (origator to recipient).[2]

---

[2] Eliasta Ketaren, "Cybercrime, Cyber Space, dan Cyber Law." *Jurnal Times* 5, No. 2 (2016): 35-42; Pooja Aggarwal, P. Arora, and R. Ghai. "Review on cyber crime and security." *International Journal of Research in Engineering and Applied Sciences* 2, No. 1 (2014): 48-51; Anant Jain, and Namit Gupta. "Cyber crime." *National Journal of Cyber Security Law* 2, No. 2 (2020); Darmawan Napitupulu, "Kajian Peran Cyber Law dalam Memperkuat Keamanan Sistem Informasi Nasional." *Deviance Jurnal Kriminologi* 1, No. 1 (2017): 100-113. Furthermore, it is also emphasized that in the context of hacking as crybercrime, hacking is a term used to describe unauthorized access to systems, networks, and data (hereafter target). Hacking may be perpetrated solely to gain access to a target or to gain and/or maintain such access beyond authorization. Examples of national and regional laws criminalizing intentional unauthorized access to a website or information by bypassing security measures are the United Arab Emirates, Article 1 of Federal Law No. 2 of 2006 on the Prevention of Information Technology Crimes, and Article 2 of the Council of Europe's Convention on Cybercrime (Budapest Convention; hereafter Cybercrime Convention). *Please see* Lennon YC Chang, "Legislative Frameworks Against Cybercrime: The Budapest Convention and Asia." in *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (2020): 327-343; Chat Le Nguyen, and Wilfred Golman. "Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action'." *Computer Law & Security Review* 40 (2021): 105521; 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; Yehezkiel Lemuel, "Internet and Crimes: How the Law Responds to Internet Based Crimes? A Book Review of "Aspek Hukum Penipuan Berbasis Internet", Maskun & Wiwik Meilarati, CV Keni Media, Makassar, 2016, 238 Pages, ISBN 978-602-74375-5-5." *JILS (Journal of Indonesian Legal Studies)* 4, No. 2 (2019): 343-350; Robert Brian Smith, "Cybercrime in ASEAN: Anti-Child Pornography Legislation." *JILS (Journal of Indonesian Legal Studies)* 5, No. 2 (2020): 277-294.

This crime is characterized by manipulating data for example espionage, sabotage, provocation, hacking and cracking, software theft and so on. The very fast rate of cybercrime is not accompanied by the ability of the government to keep up with it, so it is difficult to keep up. With the emergence of several cases of cybercrime in Indonesia, it has become a serious threat to the Indonesian government. The government with its legal instruments has not been able to balance the techniques of crimes committed with computer technology, especially on the internet (internet network).[3]

Acts against cyber law are very difficult to overcome by relying on conventional positive law because talking about crime cannot be separated from five interrelated factors, namely perpetrators of crime, victims of crime, mode of crime, perpetrators of crime, social reactions to crime and law. Law is indeed an important instrument in preventing and overcoming crime in addition to other instruments that are no less important.[4]

To create a legal product that becomes a forum for regulating a rapidly changing legal field such as information technology is not an easy thing. Often laws (regulations) seem to quickly become obsolete

---

[3] Prasetiyo Prasetiyo, and Mukhtar Zuhdy. "Penegakan Hukum oleh Aparat Penyidik Cyber Crime dalam Kejahatan Dunia Maya (Cyber Crime) di Wilayah Hukum Polda DIY." *Indonesian Journal of Criminal Law and Criminology (IJCLC)* 1, No. 2 (2020): 79-88; Joshua Oktavianus Siagian, "Cyber Fraud and the Role of Investigators: How They Reveal the Facts (Case of Subnit I Reserse of Cybercrime of West Jakarta Metro Police Department)." *Tanggon Kosala* 10, No. 2 (2021); Giosian Yohanes Sinaga, "Penyelidikan Tindak Pidana Cyber Crime Oleh Sat Reskrim Untuk Meningkatkan Crime Clearance Di Polres Cimahi." *Indonesian Journal of Police Studies* 4, No. 7 (2020).

[4] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*. (Jakarta: Prenada Media, 2018); Indriani Berlian Mewengkang, "Kajian Yuridis Cyber Crime Penanggulangan Dan Penegakan Hukumnya." *Lex Crimen* 10, No. 5 (2021); Dwi Nurahman, "Kebijakan Penegakan Hukum Cybercrime dan Pembuktian Yuridis dalam Sistem Hukum Pidana Nasional." *Keadilan* 17, No. 2 (2019): 145-157; Handrini Ardiyanti, "Cyber-security dan tantangan pengembangannya di indonesia." *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional* 5, No. 1 (2016).

when regulating fields that are undergoing rapid changes, so the situation is like a legal vacuum (*vaccum rechts*) against cybercrime between or cybercrime.

Actually, in cybercrime there is no *legal vacuum*, this happens when legal knowledge is used in the interpretation that should be held by law enforcement officers in dealing with acts of new dimensions that have not been specifically regulated in law. This issue becomes a different matter if the issue of cybercrime is regulated in a law outside the Criminal Code. To overcome this, it is clear that careful legislative action is needed keeping in mind one thing, namely, not to let the legislation become stumped on technological developments so as to make over-legislate regulations, which in turn will have a negative impact both in other legal fields and in the socio-economic field.

In overcoming this, finally in March 2018 a law was passed that covers the community in the cyber field, namely the ITE Law No. 11 of 2018. The law regulates several criminalizations of criminal acts that were previously not criminal acts through several breakthroughs and expansions in its principles and criminal sanctions. In addition to substantive criminal rules, this law also regulates procedures and evidence that has been expanded, namely the inclusion of new evidence related to electronic media.

II. METHODS

This research is normative juridical research. Sampling was carried out not on people but library materials, especially those related to information regulations and electronic transactions. The data used were secondary data. Secondary data were sourced from library materials, and legal materials. Method of Data Collection by means of identification. The method of identification is by collecting library

data in the form of archives, official documents, other library data that are closely related to the research problem. The library data (secondary data) were analyzed using a combination of deductive and inductive thinking patterns. The final result of data processing is qualitative, then analyzed using normative qualitative methods, interpretation methods in legal science, and interpreting data based on theories as mentioned in the literature review.

III. CYBER CRIME IN INDONESIA *&* GLOBAL CONTEXT

In its early days, cybercrime was defined as a computer crime. Regarding the definition of computer crime itself, until now scholars have not agreed on the meaning or definition of computer crime. Even the use of terms in English is still not uniform. Some scholars use the term "*computer fraud*", "*computer-related crime*" or *"computer crime*". However, scholars at that time generally accepted the use of the term "computer crime" because it was considered wider and could be used in international relations.[5] Based on some literature and practice, cybercrime has several characteristics, namely:

1. The act that is carried out illegally, without rights or unethically occurs in cyberspace/cyberspace, so it is not certain which jurisdiction applies to it.[6]

---

[5] Sarah Gordon, and Richard Ford. "On the definition and classification of cybercrime." *Journal in Computer Virology* 2, No. 1 (2006): 13-20; Emilio C. Viano, "Cybercrime: Definition, typology, and criminalization." *Cybercrime, Organized Crime, and Societal Responses*. (Cham: Springer, 2017), pp. 3-22; Nadia Khadam, "Insight to Cybercrime." *Taipei University Law Review* 29, No. 1 (2012): 55-80; Muhammad E. Fuady, "“Cybercrime”: Fenomena Kejahatan melalui Internet di Indonesia." *Mediator: Jurnal Komunikasi* 6, No. 2 (2005): 255-264.

[6] Jennifer Lynch, "Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks." *Berkeley Technology Law Journal* 20, No. 1 (2005): 259-300.

2. The act is carried out using any equipment connected to the internet.[7]
3. 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.[8]
4. The perpetrator is a person who controls the use of the internet and its applications.
5. These acts are often carried out transnationally/across national borders.[9]

In cyber crime (using the internet), Indonesia's position has replaced Ukraine, which previously occupied the first position. Internet crimes (cybercrime) that are rife in Indonesia include credit card fraud, banking fraud, defacing, cracking, hacking, sex transactions, online gambling, terrorism with victims originating from within the country and abroad such as the US, UK, Australia, Germany, Korea, and Singapore, as well as several regions in the country.

According to RM Roy Suryo. Cybercrime cases that often occur in Indonesia are at least grouped into three types of modes[10], namely:

---

7 Raj Singh Deora, and Dhaval Chudasama. "Brief study of cybercrime on an internet." *Journal of Communication Engineering & Systems* 11, No. 1 (2021): 1-6.

8 Ross Anderson, et al. "Measuring the cost of cybercrime." *The economics of information security and privacy*. (Berlin, Heidelberg: Springer, 2013), pp. 265-300; Shreya Kalyani, "Women Safety in Digital World." *National Journal of Cyber Security Law* 3, No. 1 (2020): 47-54; Ali Gholami, and Masoud Pirhadi. "The Challenges of Restoration of Dignity in Cyberspace." *Religion & Communication* 25, No. 1 (2018): 99-128.

9 Rob McCusker, "Transnational organised cyber crime: distinguishing threat from reality." *Crime, Law and Social Change* 46, No. 4 (2006): 257-273; Trong Nguyen, and Hai Thanh Luong. "The structure of cybercrime networks: transnational computer fraud in Vietnam." *Journal of Crime and Justice* 44, No. 4 (2021): 419-440; Barbara Jane Holland, "Transnational cybercrime: The dark web." in *Encyclopedia of Criminal Activities and the Deep Web* (2020): 108-128.

10 Dian Ekawati Ismail, "Cyber Crime di Indonesia." *Jurnal Inovasi* 6, No. 03 (2009); Nandang v "Cyberlaw: Problem dan Prospek Pengaturan Aktivitas Internet." *Jurnal Hukum IUS QUIA IUSTUM* 8, No. 16 (2001): 30-41.

1. Credit Number Theft
   According to Rommy Alkatiry (Deputy Head of Informatics DIN), misuse of credit cards belonging to other people on the internet is the biggest cybercrime case related to the Indonesian internet business world. Misuse of other people's credit cards is not complicated and can be done physically or online. Names and credit cards of other people obtained in various places (restaurants, hotels, or any place that makes payment transactions with credit cards) are entered in the application for purchasing goods via the internet.
2. Attacking the site or e-mail via Virus or Spamming.
   The most common mode is sending the virus via e-mail. According to RM Roy Suryo, overseas crimes like this have been given a fairly heavy sentence. In contrast to Indonesia, which is difficult to overcome because the existing regulations have not yet reached it.
3. Entering or Breaking the Homepage (Hacking)
   According to John. S. Tumiwa in general, the actions of Indonesian hackers are not as bad as those abroad. The behavior of Indonesian hackers is only limited to entering other people's computer sites that are vulnerable to intrusion and telling the owner to be careful. Overseas hackers have entered the banking system and damaged the bank's database.

In the same context, it is further emphasized that the development of cybercrimes in Indonesia is currently more varied, although initially it was dominated by fraudulent crimes using other people's credit cards in transactions via the internet (carding). Cyber crimes that are starting to develop in Indonesia include hacking, cracking such as "deface" the website of the General Election Commission (*Komisi*

Pemilian Umum, KPU) and the Golkar Party, defamation, online prostitution, pornography, online gambling.[11]

The Indonesian state essentially has the skills in this cybersecurity world. Even though Indonesia is in fact still a developing country that is backward in terms of technology, the reality is that what happened was brilliant produced by Indonesian hackers, crackers, and carders. In the United States and Europe, it seems that they are also experiencing "outsourcing" and globalization. In 1986 – 2003, computer virus epicenters were detected mostly from Europe and America and several other countries such as Japan, Australia, and India. However, the research results say that in the next few years Mexico, India and Africa will become the largest virus epicenters in the world, and Indonesia is also included in the top 10. So that it will not be long before Indonesia will be famous but with a name that is not good because the government is less strict in controlling the cyber world.

Hacker and Cracker in terms usually refer to someone who has a great interest in studying computer systems in detail and how to improve their abilities. As for those who often commit acts of destruction on the internet, it is usually called a cracker. It can be said that this cracker is actually a hacker who uses his abilities for negative things. Cracking activities on the internet have a very wide scope, ranging from hijacking other people's accounts, hijacking websites, investigating, spreading viruses, to deactivating targets. The last action is referred to as DoS (Denial of Service). Dos attack is an attack

[11] In another hakicng case, hackers were reported to have disseminated 2.3 million permanent voter list (DPT) data on internet forums. This data is claimed to have been taken from the website of the General Elections Commission (KPU). According to the Founder of Ethical Hackers Indonesia, Teguh Aprianto, the 2.3 million data disseminated in hacker forums are data on permanent voters from the Yogyakarta Special Region (DIY). Among them, the city/regency of Bantul, Gunung Kidul, the city, Kulonprogo and Sleman.

that aims to paralyze the target (hang, crash) so that it cannot provide services.[12]

In carrying out hacker activities there is an activity called defacting. Defacing is a subset of web or application program hacking activities, which focuses on operating changes in the appearance and/or physical configuration of a web program or application without going through the program's source code. While the defacement itself is the end result of cracking activities and the like, the techniques are reading source code (this is specific to the context of web hacking), then replacing images (for example), editing html et al tags and more. Some of the defacing actions are just for fun, to show off their skills, to show off their ability to make programs, but some are to steal data and sell it to other parties. Furthermore, generally hackers can be classified into two other types:

1. White Hat Hacker
   The term in English is White Hat, which focuses its actions on protecting the system, which is in contrast to Black Hat, which focuses more on how to break through the system.[13]
2. Black Hat hackers
   An English term that refers to hackers, namely those who break through security without permission, generally with the intention of accessing computers connected to the internet network.[14]

---

[12] Jean-Loup Richet, "From young hackers to crackers." *International Journal of Technology and Human Interaction (IJTHI)* 9, No. 3 (2013): 53-62; Richard Barber, "Hackers profiled—who are they and what are their motivations?." *Computer Fraud & Security* 2001, No. 2 (2001): 14-17; Eric S. Raymond, "How to become a hacker." *Database and Network Journal* 33, No. 2 (2003): 8-9.

[13] Shivanshi Sinha, and Arora Arora. "Ethical Hacking: The Story of a White Hat Hacker." *International Journal of Innovative Research in Computer Science & Technology (IJIRCST), ISSN* (2020): 2347-5552.

[14] Mario Silic, and Paul Benjamin Lowry. "Breaking bad in cyberspace: Understanding why and how black hat hackers manage their nerves to commit their virtual crimes." *Information Systems Frontiers* 23, No. 2 (2021): 329-341.

In Indonesia, there have been several cases of hacking crimes committed by several people including:

1. KPU site hack

   Several years ago, when Indonesia was holding elections, the KPU website was hacked for the first time. The perpetrator of the hacking of the KPU website is Dani Firmansyah, also known as Xnuxer. After successfully penetrating, Dani left his mark by changing the pictures of the parties participating in the election, such as the Jambu Party, Packaged Drinking Water Party and so on. Of course, this action shocked many parties. The KPU immediately reported this incident to Polda Metro Jaya and hired Jim Geovedi to track down the hacker. After some time of investigation, the police finally managed to arrest Dani in his office. political interests. As a reward for his actions, Dani was sentenced to 6 months and 21 days in prison by the Panel of Judges of the Central Jakarta High Court.

2. Attack on KPAI Site

   Hacking into the website of the Indonesian Child Protection Commission (KPAI) still feels fresh in the minds of many people, especially gamers. The reason is that this attack was motivated by KPAI's support for the blocking of fifteen games. According to KPAI, these games contain violent and sexual content that are not suitable for consumption by minors. Therefore, the government needs to block it. Of course, this immediately faced rejection from many people. Even on social media, a number of parties organized the I Play Games movement to protest against this blocking. The peak was that the KPAI website was hacked by a hacker named Skeptix. The hacker even left cynical message to KPAI. The message reads "*Zuhaha…You're drunk? Fix ur sec first b4 talking about game*." For this attack, the KPAI immediately made a report

to the authorities, but the news of the investigation into the hack is no longer heard.

3. Hacking of Regency Government Sites in East Java by Surabaya Black Hat

   The hacker community 'Surabaya Black Hat' (SBH) claims to have hacked the website of the district government in East Java in 2016. The name of one of the suspected hackers arrested by the police, the initials KSP (21), is in the footer of the display of the hacked site. "We got data that the Surabaya Black Hat hacked the website of the district government in East Java in 2016," as emphaszied by the Head of Sub-Directorate for Cyber Crime, Ditreskrimsus Polda Metro Jaya AKBP Roberto Pasaribu.

IV. POLICIES IN COUNTERING CYBERCRIME HACKING & CRACKING IN INDONESIA

Crime basically grows and develops in society, there is no crime without society. The more advanced and modern people's lives are, the more advanced and modern the types and modus operandi of crimes that occur in society. This seems to justify an adage, that *"where there is society there is crime", ubi societas-ibi jus; ubi jus-ibi crimen*.

1. Motivation

   Motivation is the presence of stimuli in the form of per-group influence factors, whether there is motivation from within the community or group, such as invitations, incitements or praise among colleagues. While external is motivation in the form of competitive spirit between groups, the desire to become famous, and motivational hacktivism. This hacktivism is a reaction that is

motivated by the spirit of hackers to protest against a political/ social condition of their country.[15]

2. Mechanism

   The mechanism in question is the existence of a server or website whose defense mechanism is weak because it is not updated or patched regularly and thoroughly. This is tantamount to paving the way for hackers to ignore their actions to deface them.

3. Moment

   This is also supported by the availability of a secondary mechanism that functions to detect the weakness of a system on the internet, namely in the form of sharing exploit software available on the internet and can be easily used by hackers at the beginner level at once.

4. Misconceptions of Society and Mass Media

   Misconceptions about the existence of hackers with their activities in the community and are often emphasized by the mass media, are often used by hackers to become famous and known. For example, positioning them like a hero and carelessly taking their claim that their defacement activities are based on hacktivism and nationalism is a misconception that generally occurs among us.

In cybercrimes such as hacking and cracking, it is formulated with elements of other criminal acts in accordance with the criminalized acts. information. The law that regulates Information and Electronic Transactions becomes strategic for developing information technology laws that provide rules regarding the use of information technology and possible violations.

---

[15] John Van Beveren, "A conceptual model of hacker development and motivation." *Journal of E-Business* 1, No. 2 (2000): 1-9; Pogrebna, Ganna, and Mark Skilton. "A sneak peek into the motivation of a cybercriminal." *Navigating New Cyber Risks*. (Cham: Palgrave Macmillan, 2019), pp. 31-54.

As in general laws outside the Criminal Code which regulate actions with criminal sanctions, in the ITE Law the formulation of criminal acts and sanctions are also listed separately. All acts prohibited in Articles 27 to 35 above, are threatened with criminal sanctions in Articles 45-52. If one examines the hacking arrangements in the ITE Law, it appears that all actions recommended in the European Convention on Cyber Crime have been regulated in the ITE Law. only on the layout or order of arrangement of the various acts. If the Convention starts with an act that is categorized as hacking in a narrow (pure) sense, then the arrangement in the ITE Law does not follow that pattern. regulates actions that are actually conventional criminal acts (in the Criminal Code), only now they are carried out using computer media and networks. Pay attention to Article 27 which prohibits the actions of people who with intent or no right to distribute, transmit, or make accessible electronic information or electronic documents that have content that violates decency, gambling, defamation, or extortion.[16]

In criminal law laws, the term crime is rarely used. The most popular use of the term crime is only in book II of the Book of the Criminal Code (KUHP). offenses, and criminal acts. Hacking activities if associated with legal products of the Criminal Code will fulfill the formulation of entering or crossing territorial boundaries illegally in accordance with Article 167 of the Criminal Code. What is meant in Article 167 of the Criminal Code is as follows: Whoever enters a house, room or closed yard used by another person against the law and or at the request of the rightful or ordered not to leave

[16] Ismail Koto, "Cyber Crime According to the ITE Law." *International Journal Reglement & Society (IJRS)* 2, No. 2 (2021): 103-110; Dewi Bunga, "Legal Response to Cybercrime in Global and National Dimensions." *Padjadjaran Journal of Law* 6, No. 1 (2019): 69-89; Sefitrios Sefitrios, and Tofik Yanuar Chandra. "The Process and Performance of Combating Cyber Crimes in Indonesia." *SALAM: Jurnal Sosial dan Budaya Syar-i* 8, No. 4 (2021): 975-986.

immediately is threatened with imprisonment for a maximum of nine months or a maximum fine of three hundred rupiahs.

If law enforcers want to carry out investigations and field investigations into crimes against hacking crimes for which in fact there are no clear stipulations, then from the description above, the formulation of the articles of the Criminal Code above, law enforcers should be able to bring hackers to court. While the problem of proving that the perpetrator is guilty or not is another matter, where the problem of proof will be discussed in the next case.

In the Telecommunications Law, hacking activities violate the provisions of Law No. 36 of 1999 concerning Telecommunications. Article 22 of the Law on Telecommunications does not directly mention hacking but with a simple formulation, namely access to networks, communication services are not valid. Then in article 40 of the Telecommunications Law where it is very clear that it is prohibited for everyone to be prohibited from tapping into the information network in any form.[17] If viewed from the elements in the law by coonsidering the object of a criminal act is access to a telecommunications network or service that is carried out without rights, is illegal, manipulates, or is wiretapped, on a computer system. In the case of hacking, these elements have been included.

V. CONCLUSION

This study concludes that the regulation of cybercrimes in Indonesian legislation such as the ITE Law has complemented Indonesia's

[17] Andysah Putera Utama Siahaan, "Pelanggaran cybercrime dan kekuatan yurisdiksi di Indonesia." *Jurnal Teknik dan Informatika* 5, No. 1 (2018): 6-9; Andri Winjaya Laksana, "Pemidanaan Cybercrime dalam Perspektif Hukum Pidana Positif." *Jurnal Hukum* 35, No. 1 (2019): 52-76; M. Syukri Akub, "Pengaturan Tindak Pidana Mayantara (Cyber Crime) dalam Sistem Hukum Indonesia." *Al-Ishlah: Jurnal Ilmiah Hukum* 21, No. 2 (2018): 85-93.

material criminal law which regulates various criminal acts that have developed in line with the development of information and communication technology is an alternative regulation of cybercrime that is possible based on the provisions of Article 103 of the Criminal Code. The regulation of criminal acts outside the Criminal Code can be in the form of a Special Criminal Law or a law in certain fields which regulates criminal sanctions. special. The regulation of cybercrimes in the ITE Law and other legislation has implications for the legal protection of the legal interests of the community, especially in the form of computer data or electronic data, electronic documents, electronic information, and computer systems that are protected and not public, whether privately owned. as well as the State and other interests that are targets of cybercrimes.

ACKNOWLEDGMENTS

None.

COMPETING INTERESTS

The Authors declared that they have no competing interests.

REFERENCES

Aggarwal, Pooja, P. Arora, and R. Ghai. "Review on cyber crime and security." *International Journal of Research in Engineering and Applied Sciences* 2, No. 1 (2014): 48-51.

Akub, M. Syukri. "Pengaturan Tindak Pidana Mayantara (Cyber Crime) dalam Sistem Hukum Indonesia." *Al-Ishlah: Jurnal Ilmiah Hukum* 21, No. 2 (2018): 85-93.

Anderson, Ross, et al. "Measuring the cost of cybercrime." *The economics of information security and privacy*. (Berlin, Heidelberg: Springer, 2013), pp. 265-300.

Ardiyanti, Handrini. "Cyber-security dan tantangan pengembangannya di indonesia." *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional* 5, No. 1 (2016).

Arief, Barda Nawawi. *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*. (Jakarta: Prenada Media, 2018).

Barber, Richard. "Hackers profiled—who are they and what are their motivations?." *Computer Fraud & Security* 2001, No. 2 (2001): 14-17.

Bunga, Dewi. "Legal Response to Cybercrime in Global and National Dimensions." *Padjadjaran Journal of Law* 6, No. 1 (2019): 69-89.

Chang, Lennon YC. "Legislative Frameworks Against Cybercrime: The Budapest Convention and Asia." *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (2020): 327-343.

Deora, Raj Singh, and Dhaval Chudasama. "Brief study of cybercrime on an internet." *Journal of Communication Engineering & Systems* 11, No. 1 (2021): 1-6.

Fuady, Muhammad E. "'"Cybercrime": Fenomena Kejahatan melalui Internet di Indonesia." *Mediator: Jurnal Komunikasi* 6, No. 2 (2005): 255-264.

Gholami, Ali, and Masoud Pirhadi. "The Challenges of Restoration of Dignity in Cyberspace." *Religion & Communication* 25, No. 1 (2018): 99-128.

Gordon, Sarah, and Richard Ford. "On the definition and classification of cybercrime." *Journal in Computer Virology* 2, No. 1 (2006): 13-20.

Holland, Barbara Jane. "Transnational cybercrime: The dark web." *Encyclopedia of Criminal Activities and the Deep Web* (2020): 108-128.

Ismail, Dian Ekawati. "Cyber Crime di Indonesia." *Jurnal Inovasi* 6, No. 03 (2009).

Jain, Anant, and Namit Gupta. "Cyber crime." *National Journal of Cyber Security Law* 2, No. 2 (2020).

Kalyani, Shreya. "Women Safety in Digital World." *National Journal of Cyber Security Law* 3, No. 1 (2020): 47-54.

Kasemin, H. Kasiyanto. *Agresi Perkembangan Teknologi Informasi*. (Jakarta: Prenada Media, 2016).

Ketaren, Eliasta. "Cybercrime, Cyber Space, dan Cyber Law." *Jurnal Times* 5, No. 2 (2016): 35-42.

Khadam, Nadia. "Insight to Cybercrime." *Taipei University Law Review* 29, No. 1 (2012): 55-80.

Koto, Ismail. "Cyber Crime According to the ITE Law." *International Journal Reglement & Society (IJRS)* 2, No. 2 (2021): 103-110.

Laksana, Andri Winjaya. "Pemidanaan Cybercrime dalam Perspektif Hukum Pidana Positif." *Jurnal Hukum* 35, No. 1 (2019): 52-76.

Le Nguyen, Chat, and Wilfred Golman. "Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action'." *Computer Law & Security Review* 40 (2021): 105521.

Lemuel, Yehezkiel. "Internet and Crimes: How the Law Responds to Internet Based Crimes? A Book Review of "Aspek Hukum Penipuan Berbasis Internet", Maskun & Wiwik Meilarati, CV Keni Media, Makassar, 2016, 238 Pages, ISBN 978-602-74375-5-5." *JILS (Journal of Indonesian Legal Studies)* 4, No. 2 (2019): 343-350.

Lynch, Jennifer. "Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks." *Berkeley Technology Law Journal* 20, No. 1 (2005): 259-300.

Mayeni, Riska, Okviani Syafti, and Sefrinal Sefrinal. "Dampak Perkembangan Teknologi Dikalangan Remaja Dilihat dari

Nilai-Nilai Karakter." *Turast: Jurnal Penelitian dan Pengabdian* 7, No. 2 (2019): 239-246.

McCusker, Rob. "Transnational organised cyber crime: distinguishing threat from reality." *Crime, Law and Social Change* 46, No. 4 (2006): 257-273.

Mewengkang, Indriani Berlian. "Kajian Yuridis Cyber Crime Penanggulangan Dan Penegakan Hukumnya." *Lex Crimen* 10, No. 5 (2021).

Napitupulu, Darmawan. "Kajian Peran Cyber Law dalam Memperkuat Keamanan Sistem Informasi Nasional." *Deviance Jurnal Kriminologi* 1, No. 1 (2017): 100-113.

Nguyen, Trong, and Hai Thanh Luong. "The structure of cybercrime networks: transnational computer fraud in Vietnam." *Journal of Crime and Justice* 44, No. 4 (2021): 419-440.

Nurahman, Dwi. "Kebijakan Penegakan Hukum Cybercrime dan Pembuktian Yuridis dalam Sistem Hukum Pidana Nasional." *Keadilan* 17, No. 2 (2019): 145-157.

Pogrebna, Ganna, and Mark Skilton. "A sneak peek into the motivation of a cybercriminal", in *Navigating New Cyber Risks*. (Cham: Palgrave Macmillan, 2019), pp. 31-54.

Prasetiyo, Prasetiyo, and Mukhtar Zuhdy. "Penegakan Hukum oleh Aparat Penyidik Cyber Crime dalam Kejahatan Dunia Maya (Cyber Crime) di Wilayah Hukum Polda DIY." *Indonesian Journal of Criminal Law and Criminology (IJCLC)* 1, No. 2 (2020): 79-88.

Ratnaya, I. Gede. "Dampak negatif perkembangan teknologi informatika dan komunikasi dan cara antisifasinya." *Jurnal Pendidikan Teknologi dan Kejuruan* 8, No. 1 (2011).

Raymond, Eric S. "How to become a hacker." *Database and Network Journal* 33, No. 2 (2003): 8-9.

Richet, Jean-Loup. "From young hackers to crackers." *International Journal of Technology and Human Interaction (IJTHI)* 9, No. 3 (2013): 53-62.

Sefitrios, Sefitrios, and Tofik Yanuar Chandra. "The Process and Performance of Combating Cyber Crimes in Indonesia." *SALAM: Jurnal Sosial dan Budaya Syar-i* 8, No. 4 (2021): 975-986.

Siagian, Joshua Oktavianus. "Cyber Fraud and the Role of Investigators: How They Reveal the Facts (Case of Subnit I Reserse of Cybercrime of West Jakarta Metro Police Department)." *Tanggon Kosala* 10, No. 2 (2021).

Siahaan, Andysah Putera Utama. "Pelanggaran cybercrime dan kekuatan yurisdiksi di Indonesia." *Jurnal Teknik dan Informatika* 5, No. 1 (2018): 6-9.

Silic, Mario, and Paul Benjamin Lowry. "Breaking bad in cyberspace: Understanding why and how black hat hackers manage their nerves to commit their virtual crimes." *Information Systems Frontiers* 23, No. 2 (2021): 329-341.

Sinaga, Giosian Yohanes. "Penyelidikan Tindak Pidana Cyber Crime Oleh Sat Reskrim Untuk Meningkatkan Crime Clearance Di Polres Cimahi." *Indonesian Journal of Police Studies* 4, No. 7 (2020).

Sinha, Shivanshi, and Dr Arora. "Ethical Hacking: The Story of a White Hat Hacker." *International Journal of Innovative Research in Computer Science & Technology (IJIRCST), ISSN* (2020): 2347-5552.

Smith, Robert Brian. "Cybercrime in ASEAN: Anti-Child Pornography Legislation." *JILS (Journal of Indonesian Legal Studies)* 5, No. 2 (2020): 277-294.

Sutrisno, Nandang. "Cyberlaw: Problem dan Prospek Pengaturan Aktivitas Internet." *Jurnal Hukum IUS QUIA IUSTUM* 8, No. 16 (2001): 30-41.

Van Beveren, John. "A conceptual model of hacker development and motivation." *Journal of E-Business* 1, No. 2 (2000): 1-9.

Viano, Emilio C. "Cybercrime: Definition, typology, and criminalization" in *Cybercrime, Organized Crime, and Societal Responses*. (Cham: Springer, 2017), pp. 3-22.

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.

Zamroni, Mohammad. "Perkembangan teknologi komunikasi dan dampaknya terhadap kehidupan." *Jurnal Dakwah: Media Komunikasi dan Dakwah* 10, No. 2 (2009): 195-211.

Hackers are seen as shadowy figures with superhuman powers that threaten civilization.

Mitch Kapor