International Journal of Law, Social Science and Humanities (IJLSH)

Volume 1, Issue 1, 2024

E-ISSN: 3063-7554

https://doi.org/10.70193/ijlsh.v1i1.140

Cybercrime in virtual spaces: An overview of the law in Indonesia

Zulfan

Faculty of Law, Universitas Malikussaleh, Aceh, Indonesia

Submitted: 02 June 2024 *Revised: 28 June 2024* *Published: 09 July 2024*

Abstract:

The Internet has the potential to overcome national barriers and facilitate global dissemination of information. Although its benefits are numerous, it also has detrimental consequences that could disrupt society. Engaging in cybercrime is typically required only to create a substantial number of blogs, accounts, applications, programs, and websites on various social and mass media platforms for illicit purposes. Examples of unlawful activities include, but are not limited to, fraud, data theft, unauthorized use of credit cards, distribution of inappropriate content, online gambling, and prostitution, as well as hate speech and extremist or terrorist activities. To address the issue of virtual space crime, the government enacted Law No. 19 of 2016, which amended Law No. 11 of 2008, with respect to information and electronic transactions. However, it is important to recognize that not all people who use the internet have a comprehensive understanding of the legal framework. Consequently, government, employers, and institutions involved in information and communication technology are responsible for educating the public about the law to reduce the incidence of criminal activity in virtual spaces.

Keywords: Internet; Cyber Crime; ITE Law; Indonesia

INTRODUCTION

The rapid advancement of information technology, particularly in the field of internet communication, has led to substantial social, economic, and cultural transformations. This technology is characterized by systems that can efficiently and expeditiously collect, store, process, generate, and disseminate information to the public. This technology is widely regarded as the primary alternative for facilitating social, economic, and government activities. However, it also has a dual nature or 'double-edged sword', as it can promote welfare, progress, and human development while simultaneously enabling criminal activities (Sanusi, 2005).

Information and communication technology is an electronic system that operates on a computer-based platform, which can only be accessed through virtual means (Tongia et al., 2005). In the virtual world domain, it is challenging to impose constraints on one’s activities due to the affordability and accessibility of information technology from any location in the world (Karina & Mendoza, 2017). Therefore, it is possible for individuals from various backgrounds, including those who use the Internet and those who do not, to engage in criminal activities (Nwizege et al., 2011). People can engage in unauthorized transactions using a person's credit card without consent. Furthermore, through virtual media, individuals can produce photos, status updates, memes, and videos that contain elements of hatred and that target someone's reputation, extremism, and terrorism. Moreover, with ease, someone can become a propaganda specialist by creating blogs, accounts, and websites with false identities (Jewkes, 2010).

*Corresponding Author : Zulfan, Faculty of Law, Universitas Malikussaleh, Aceh, Indonesia, ORCID iD: 0009-0008 1428-9999, E-mail: zulfan@unimal.ac.id

To prevent the use of cyber crime, the government issued Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning the Electronic Information and Transactions Law (hereinafter referred to as the ITE Law). The intention of enacting this legislation is to ensure secure and responsible use of the Internet while preventing its misuse. This law does not impose any restrictions on the democratic freedom enjoyed by Indonesian citizens; instead, it aims to restrict the exercise of free thought and expression in a public forum that could potentially cause harm to individuals, both physically and psychologically.

The Internet should be used in a manner that promotes mutual benefits, ensuring that users and providers of information technology feel secure, justified, and confident in the legal framework governing their actions. Consequently, the implementation of the ITE law aims to ensure, safeguard and uphold the rights and freedoms of individuals according to ethical principles, religious beliefs, security requirements, and the preservation of public order. To achieve this objective, it is imperative that the government conveys to the general public that the presence of the ITE law does not restrict the liberty of democracy; rather, it vests the freedom of democratic society in the hands of the appropriate patron.

METHODS

This study used a qualitative research method. According to McCracken, qualitative methodology typically involves the collection of descriptive data or information through observations, interviews, and examination of relevant documents (Cevilla, 1993; McCracken, 1998). The objective of this study is to comprehensively describe the manner in which the Internet has provided certain hacker groups with an avenue to establish and expand their operations in Indonesia. This study aims to provide an accurate and factual description of this phenomenon, as well as to interpret relevant facts and circumstances.

RESULTS

The rapid advancement of computer technology has resulted in their widespread integration into modern life. Although these technologies are convenient and easy to use, they present security concerns (Solak and Topaloglu, 2015). The cybercriminals appeared to have conducted their operations without hindering. Home computer users are particularly susceptible to attacks by highly skilled geographically dispersed hackers. Unfortunately, the situation has worsened in the smartphone era, and hackers have escalated their attacks of abuse (Renaud et al., 2018). Research initiatives in the field of computer warfare are extensive and include various concerns such as legality, computer weapons, and deterrence. However, a crucial aspect that has often been neglected is restoring peace and security in the aftermath of cyber warfare (Robinson et al., 2018). Computer end-user hygiene often plays an important role in disrupting computer security (Cain et al., 2018). Therefore, we need a deeper understanding of the differences between users related to good or bad intentions.

The advent of information technology and the Internet has facilitated rapid and efficient dissemination of information. The World Wide Web and the devices that support it have effectively reduced geographical barriers and transformed the world into a borderless entity (Finklea, 2012). The development of science and information communication technology has led to various changes in political, economic, social, and cultural fields (United National Office on Drugs and Crime, 2013). Despite the expansion of the scope of state sovereignty, it now includes not only physical territory, such as land, sea, and airspace, but also virtual or cyberspace (Heidegger, 1977). Certain nations in Asia, Africa, and the Middle East have implemented stringent limitations on Internet access because of the belief that the dissemination of information from external sources may prove challenging to regulate (Bernardino, 2017).

The extensive use of the Internet in Indonesia has experienced rapid growth. The number of Internet cafés, commonly referred to as cyber cafés, has increased throughout the country. In particular, remote villages in Indonesia offer affordable access to the Internet, which has contributed to the country's status as a leading Southeast Asian nation in terms of the number of Internet users.

According to the Indonesian Internet Service Providers Association (APJII), the number of Internet users reached 143.26 million in 2017 (Figure 1). Most Internet users in Indonesia are in the age group 25-29 years and 35-39 years. However, the number of age groups that use the Internet is increasing. APJII mentions the age group of teenagers who actively use the Internet from the age group of 15-19 years with as many as 12.5 million users and the age group of 10-15 years with as many as 768 thousand users (APJII, 2016).

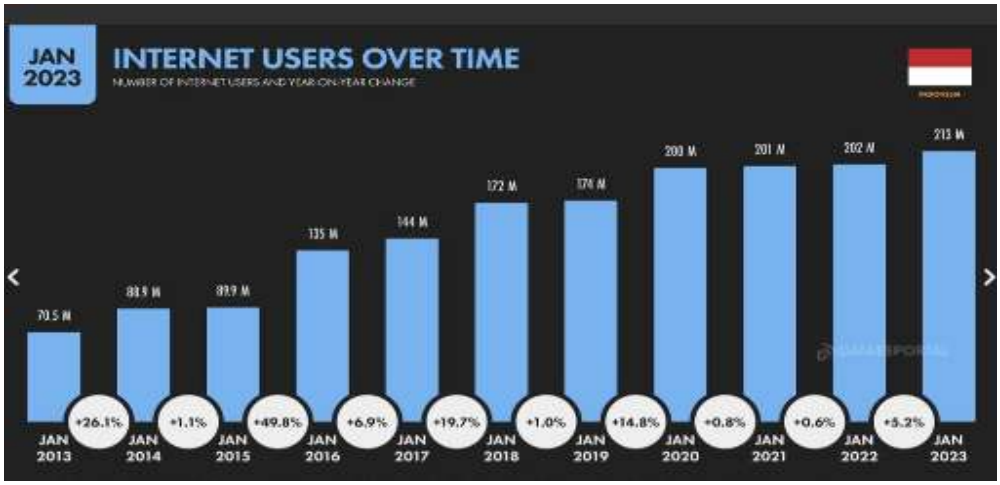

Figure 1. The Internet Users in Indonesia, 2023

The significant population of Internet users in Indonesia, primarily young individuals, presents significant potential for both perpetrators and victims of cybercrime. This inclination towards seeking knowledge, attempting new experiences, and embracing challenges has led to a younger generation of hackers. Indonesia has the highest number of hackers worldwide, with an impressive 38% success rate (Bernardino, 2017). This was followed by China, the United States, Taiwan, Turkey, India, and Russia. The reported increase in the number of hackers in Indonesia is attributed to the widespread availability of hacking learning resources on the Internet, including YouTube, blogs, Facebook and Instagram. In the event of a breach on the www.tiket.com site, it was discovered that Sultan Haikal, a 19-year-old person who had yet to complete high school, was responsible for the incident. As a result of his actions, a financial loss of 4.1 billion was incurred (Andrianyanto, 2017).

Malaysian websites that were hacked in retaliation for the Indonesian flag incident were restored during the SEA Games held in Kuala Lumpur in 2017. Specifically, hackers overturned the images of Malaysian flags on these websites. Furthermore, in 2013, Indonesian hackers engaged in a virtual "war" with Australian hackers. The beginning of the conflict was marked by the unauthorized acquisition of Garuda Indonesian customer credit card information by hackers in Australia. In retaliation, Indonesian hackers targeted and compromised 17 Australian government websites and additional private sector websites. Hecker Indonesia has attracted global attention because of its alleged capacity to infiltrate satellite systems and exert control over international Internet networks (Miftach, 2007).

One of the factors contributing to the increase in cybercrime in Indonesia is the large number of Internet users. Based on data from the Directorate of Cyber Crimes (Dit Tipidsiber), the Criminal Investigation of the Republic of Indonesia Police stated that the number of cyber crimes in 2017 totaled 1,763 cases (Batubara, 2017). According to data from the Identity Theft Resource Center (ITRC), in July 2018, the number of cyber crimes in July 2018 totaled 668 cases, with a total of 22, 408, 258 lost data (Yahya, 2018). From these data, the highest number of cybercrime cases were fraud cases with 767 cases. The second ranking is for handling 528 cases of insult and defamation (Figure 2). Although cybercrime is committed by Indonesian citizens, it is also carried out by foreign citizens in Indonesia using a range of methods.

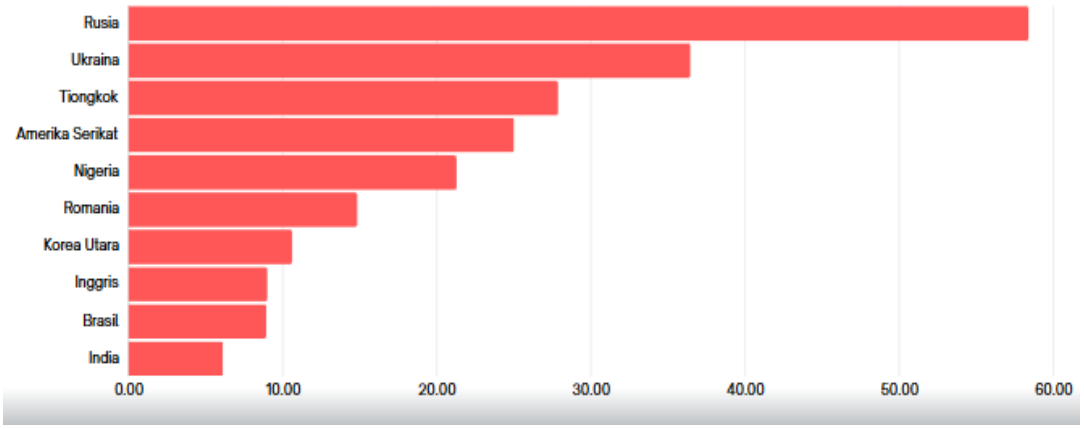

Figure 2. Word Cybercrime Index (ISTR, 2017)

The data shown in Figure 2 indicate the weak state of the security system for information technology and electronic transactions in Indonesia, which has made Indonesia the country most vulnerable to cybercrime attacks by hackers around the globe. Numerous instances of cyberattacks perpetrated by foreign nationals have been reported in Indonesia. For example, a group of Chinese citizens from various organizations carried out fraud and theft through the Internet network in Indonesia. Within a period of only two weeks, this syndicate was able to generate a profit of 2 billion rupiah. Therefore, it is essential that governments and society recognize the increase in criminal activities involving information technology. Cybercrime syndicates not only pose a threat to individual and corporate security systems, but can also breach the government's defense mechanisms.

DISCUSSION

Prevention of cybercrime must begin by providing an understanding to Internet users regarding the limitations of expressing ideas, thoughts, status, statements, pictures, videos, memes and other content on various social media and mass media platforms. The objective of the ITE Law is to govern, supervise, and discipline the utilization of information technology, which is progressively advancing and disrupting the public. The prevalence of fraud, embarrassment, homicide, rape, abduction, and detention has been attributed to the widespread use of the Internet and various social media platforms. Furthermore, the misuse of information technology can lead to criminal activities that target government websites, businesses, financial institutions, and private data. The ITE law is designed to regulate the use of information technology, but it does not guarantee an unrestricted space for individuals to express their thoughts and opinions.

The substance of the ITE law consists of several forms, namely (Arief, 2006)

a. Economic cyber crime;
b. Electronic fund transfer (EFT) crime;
c. Cybank Crime, Internet Banking Crime, Online Business Crime;
d. Cyber/Electronic Money Laundering; 5. Hitech WCC (white collar crime);
e. Internet fraud (bank fraud, credit card fraud, and online fraud)
f. Cyber terrorism;
g. Cyber stalking;
h. Cyber sex, cyber pornography, cyber defamation, cyber (child) criminals.

The ITE Law has been extensively employed by law enforcement agencies to apprehend individuals responsible for offenses, such as pornography, humiliation, and fraud, as well as incidents affecting government sites, businesses, banks, and more since its implementation. For instance, a defamation case allegedly perpetrated by Prita Mulyasari against Omni International Hospital. The situation originated when Prita composed an electronic communication with her acquaintances (e-mail group) detailing the unsatisfactory service provided by Omni International Hospital. The hospital management took legal action against Prita on charges of defamation, as the content of her e-mail had

been widely circulated within the community. The hospital considered her accusations unfounded and biased. The physicians and other medical personnel of the Omni International hospitals consistently provided professional healthcare services. According to these circumstances, Prita Mulyasari was arrested for allegations of violating Article 27 of the ITE Law.

The Prita Mulyasari case presents a significant concern for the community, as it raises the question of whether individuals have the right to express their opinions about people, institutions, or even countries through virtual media, even if their statements may be deemed defamatory. Although Prita Mulyasari successfully won the defamation case against the Omni International Hospital, this issue remains a subject of debate and dispute within the community. However, it is crucial to recognize that expressing this viewpoint must not damage an individual's reputation or integrity because disseminating false or misleading information can result in defamation and harm to one's good name.

Cyberpornography, a form of cybercrime, is frequently found in the virtual world, where it takes the form of written material, visual images, and videos, among other types of explicit content. The most egregious instance of pornography in Indonesia is the dissemination of a video featuring famous band leader Nazril Irham (Ariel Paterpan) along with celebrities Luna Maya and Cut Tari to the general public. During the trial, it was discovered that the repugnant video was saved on a computer at the Grop Band Peterpan studio and propagated via the Internet by Rizaldy, Ariel Paterpan's acquaintance. Ariel Paterpan and Reza Rizaldy were prosecuted under Article 27 paragraph (1) jo. Article 45 paragraph (1) of the ITE Law because both intentionally and without rights distribute and/or transmit and/or access electronic information and/or electronic documents that violate decency. In the trial, the presiding judge determined that Reza Rizaldy had been proven guilty of disseminating a sexually explicit video featuring Ariel Perpan with Luna Maya and Cut Tari through the Internet and consequently sentenced him to a term of imprisonment lasting two years and six months (Supreme Court Decision, No. 68 / Pid / 2011 / PT.Bdg).

The following case was astounding and was conducted by Sultan Haikal M. Aziansyah, a 19-year-old individual who had not yet completed high school. He examined 4,600 websites in various countries. Individuals engaged in malicious activities deliberately gain access to websites belonging to specific persons or organizations with the intention of identifying vulnerabilities. These individuals then extend their assistance in rectifying such deficiencies within the company's website (for example, the website www.tom.com and go-object.com) that may be entered by hackers. However, warnings and offers of cooperation are not acknowledged, which often leads to frustration and results in players targeting the related websites. These websites are not limited to company sites such as PT. Global Network and Tiket.com, but also includes government, police, and military sites, among others. From the results of the various sites, the perpetrators managed to obtain a profit of IDR 4.124.000,982. Haikal allegedly fulfilled the elements of Article 46 paragraphs 1, 2, and 3 in conjunction with Article 30 paragraphs 1, 2, and 3, and/or Article 51 paragraphs 1 and 2 juncto Article 35 and/or Article 36 of the ITE Law, and was sentenced to four years in prison (Alvionitasari, 2017).

Another egregious example is the case of Saracens, an organized group in Indonesia that intentionally disseminates false news, hate speech, and hostile content in cyberspace. The objective of these malicious actions is to provoke political, legal and economic chaos in Indonesia (Shaw, 2011). Saracen has 20 members and nine million followers from 800,000 Facebook accounts from various countries (Syahayani, 2017). They are paid to counter issues related to political contestants in the general elections. Candidates who do not make payments or contributions to Saracens may attempt to disseminate derogatory information that incorporates hateful content related to SARA (ethnicity, religion, race, and group) with the aim of undermining the credibility and standing of political competitors in the eyes of the general public. In contrast, an individual or group who wishes to pay or contribute to the Saracens will likely have a favorable impression, resulting in an increase in their electability (Syahayani, 2017).

Muhammad Harsono Abdullah Saracen Group Admin and its members are prosecuted under Article 45A paragraph 1 & 2 juncto Article 28 paragraph 2 of the ITE Law because these tapering activities are legally and convincingly proven intentionally and without rights to spread false and misleading news aimed at inciting hatred or hostility certain individuals and / or community groups based on

SARA. The judge of the Pekanbaru District Court sentenced the Saracens to guilt with a sentence of two years and eight months in prison (Doly, 2017).

He rapid development of information technology is also realized by perpetrators. Even certain crimes are more effectively carried out through the internet network compared to conventional methods. Someone can become a propaganda expert just by creating a personal blog, account or news site with a fake identity. recruit newImportantlyThe number of internet users in the world is a fertile field for terrorist groups to spread influence and recruit new members to join their groups. Coleman and McCahill said that most terrorist members from Saudi Arabia were recruited through the internet (Kyt et al., 2011).

In an effort to curb the dissemination of false information, hate speech, and extremist content, the government established a dedicated unit known as the National Cyber Agency, tasked with tracking down online platforms, websites, blogs, social media accounts, and other channels that propagate such harmful materials. These include sites that promote hoaxes, radicalism, terrorism ideologies, adult content, and sites that violate the SARA provisions. The government encourages Twitter, Google, YouTube, and other social media platforms to remove content by implementing trusted flagging systems or other appropriate measures (Viva, 2017). According to Baapna and Waimann, the implementation of a sophisticated identification system and the imposition of stricter penalties for cybercriminals can effectively deter cybercrimes, provided that the government strictly enforces relevant laws (Bapna, 2012; Waimann, 1994).

Although the government has developed a system or program aimed at blocking negative websites, it is crucial that the implementation of such measures is consistent and sustainable to effectively disseminate information about the ITE Law to the general public. Research conducted by Abi Bayu indicates that more than 50% of the population remains largely uninformed about the details and significance of the ITE Law (Pranata, 2016). The disregard for the regulations governing the ITE law by certain individuals has led to a situation in which the freedom of opinion afforded by social networks is frequently misused.

Various events, including seminars, workshops, and conferences, can be organized to facilitate socialization among people from diverse cultural, age, and professional backgrounds who use the Internet. While adolescents, students, and young adults utilize various methods to access the Internet, they primarily use current or millennial techniques such as motion graphic animation media, social networking sites, below-the-line media such as posters and pins, and advertisements and documentaries. The primary objective of these media is to educate the public, particularly the younger generation, to express their opinions on social media, and to enhance public literacy regarding the advantages and disadvantages of using an Internet network. Communities must foster a culture of verification when seeking news by procuring information from reputable news sources.

To successfully implement the ITE law, it is essential that the government works closely with a diverse range of stakeholders, including educational institutions, law enforcement agencies, religious leaders, parents and business owners who operate in the digital world. Communities can actively contribute by reporting whether they encounter hoax news, hate speech, or radicalism on news websites and social networks. To this end, the government has established the Content Complaint Ticketing System, which allows the public to file complaints about negative content and monitor the progress of the complaint resolution process (Sa'diyah, 2012). Furthermore, individuals can make use of fake news report features made available on social media platforms, such as the report status function on Facebook, the feedback mechanism on Google, and the report tweet feature on Twitter (Yunita, 2017). Negative news content can also be reported as aduankonten@mail.kominfo.go.id or data.turnbackhoax.id pages.

CONCLUSION

The application of information and communication technology is intended to promote public welfare, improve education, and provide a sense of security and legal clarity to both users and providers of the electronic system. However, when the use of information and communication technology is unrestricted, it can lead to negative consequences such as social, cultural, legal, economic, and

political ramifications. The immediate implementation of the ITE law is crucial and serves as a pioneer in the regulation of information technology and electronic transactions, with the aim of promoting a wise and ethical use that respects moral, religious, security, and public order values in a democratic society while safeguarding the rights and freedoms of all.

The increasing incidence of cybercrime in Indonesia is directly proportional to the rapid advancement of information and communication technology utilizing Internet network facilities. Internet users can easily disseminate and propagate news, images, videos, and other content without verifying the accuracy of the information. Moreover, the use of internet networks for criminal activities has become increasingly prevalent. Such activities include but are not limited to data theft, unauthorized use of credit cards, dissemination of false news, online gambling, online prostitution, distribution of pornographic content, promotion of radical ideologies, and terrorism. The government implemented the ITE law to combat cybercrime and protect individuals from detrimental effects disseminated through digital media, which can have a large impact on society. The government and other relevant organizations must inform the general public about the ITE law, including regulations regarding the dissemination of information via mass media and social media platforms.

Conflict of Interest

All the authors declare that there are no conflicts of interest.

Funding

This study received no external funding.

How to cite:

Zulfan. (2024). Cybercrime in Virtual Spaces: An Overview of the Law in Indonesia. *International Journal of Law, Social Science and Humanities (IJLSH)*, *1*(1), 18-26. https://doi.org/XX.XXXX/ijlsh.XXXX.

REFERENCES

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, *42*, 36–45.

Alvionitasari, R. (2017). *Haikal Tersangka Hacker Ribuan Situs, Polisi: Dia Pemuda Tertutup*. Tempo.

Andrianyanto, D. (2017). *Kawanan Haikal Peretas Ribuan Situs, Siapa Gantengers Crew Ini?* Tempo. https://m.tempo.co/read/863565/kawanan-haikal-peretas-ribuan-situs-siapa-gantengers-crew-ini/full&Paging=Otomatis

APJII, T. (2016). Saatnya jadi pokok perhatian pemerintah dan industri. *Buletin APJII*, 1–7.

Arief, B. N. (2006). *Tindak pidana mayantara perkembangan kajian cyber crime di Indoensia*. PT. Raja Grafindo Persada.

Bapna, J. H. and S. (2012). How can we deter cyber terrorism. *Information Security Journal*, *21*(2), 102–114.

Batubara, P. (2017). *Tahun 2017, Polisi Tangani 1.763 Kasus Kejahatan Siber*. Okezone News.

Bernardino, R. (2017). *Cyber Crime* (Issue November).

Cevilla, C. G. (1993). *Pengantar Metode Penelitian*. Universitas Indonesia Press.

Solak, D., & Topaloglu, M. (2015). The perception analysis of cyber crimes in view of computer science students. *Procedia - Social and Behavioral Sciences*, *182*, 590–595.

Doly, D. (2017). Pengaturan penyebaran ujaran kebencian dan isu sara ditinjau dari hukum konstitusi. *Info Singkat Hukum*, *IX*(17), 1–4.

Finklea, K. M. (2012). The interplay of borders, turf, cyberspace, and jurisdiction: issues confronting U.S. Law enforcement. *Journal of Current Issues in Crime, Law & Law Enforcement*, *5*(1/2), 13–20.

Heidegger, M. (1977). *The Question Concerning Technology, and Other Essays* (W. Lovitt (ed.)). Garland Publishing.

ISTR. (2017). Internet Security Threat Report - ISTR. *Symantec Journal*, *22*(April), 77. https://doi.org/10.1016/S1353-4858(05)00194-7

Jewkes, Y. (2010). *Handbook of Internet Crime*. Willan Publishing.

Renaud, K., Flowerday, S., Warkentin, M., Cockshott, P., & Orgeron, C. (2018). Is the responsibilization of the cyber security risk reasonable and judicious? *Computers & Security*, *78*, 198– 211.

Karina, D., & Mendoza, O. (2017). The vulnerability of cyberspace - The cyber crime. *Journal of Forensic Sciences & Criminal Investigation*, *2*(1), 1–8.

Kyt, E. (2011). Cybersecurity and cyberwarfare: ideas for peace and security. *Center for Strategic and International Studies, July 2010*, 1–34.

Robinson, M., Jones, K., Janicke, H., and Maglaras, L. (2018). An introduction to cyber peacekeeping. *Journal of Network and Computer Applications*, *114*, 70–87.

McCracken, G. . (1998). *The Long Interview*. Sage.

Miftach, F. (2007). Enterprise Hacking: Who Needs Exploit Codes? *Hack In The Box Security Conference*, 1–65.

Nwizege, K. S., Chukwunonso, F., Kpabeb, C., & Mmeah, S. (2011). The impact of ICT on computer applications. *Proceedings - UKSim 5th European Modelling Symposium on Computer Modelling and Simulation, EMS 2011*, *2*(May 2014), 435–439. https://doi.org/10.1109/EMS.2011.45

Pranata, A. B. (2016). *Socialization of ITE Law related to freedom of expression in social media using public service advertisement*. Faculty of Computer Science, DINUS University.

Sa'diyah, N. K. (2012). Modus operandi tindak pidana cracker menurut undang-undang informasi dan transaksi elektronik. *Perspektif*, *17*(2), 78–89.

Sanusi, M. A. (2005). *Hukum dan teknologi informasi* (3rd ed.). Gramedia Pustaka Utama.

Shaw, L. (2011). Hate speech in cyberspace: bitterness without boundaries. *Notre Dame Journal of Law, Ethics and Public Policy*, *25*(1), 279–304. https://doi.org/10.3868/s050-004-015-0003-8

Syahayani, Z. (2017). Saracen: Potret Bisnis Hoax di Indonesia. *Update Indonesia*, *XI*(7), 2–4.

Tongia, R., Subrahmanian, E., & Arunachalam, V. S. (2005). Information and Communications Technology (ICT). In *Information and Communications Technology for Sustainable Development Defining a Global Research Agenda*.

United National Office on Drugs and Crime. (2013). Comprehensive study on cybercrime. *Conference Support Section Organized Crime Branch Division for Treaty Affairs*, *February*, 1–30.

Viva, T. (2017). *Menkominfo Ancam Facebook dan Twitter*. Viva.

Waimann, G. (1994). *The Influential: People who Influnce People*. State University of New York Press.

Yahya, F. (2018). *Hingga Juli 2018, Sudah Ada 668 Kasus Kejahatan Siber*. Okezone News.

Yunita. (2017). *Ini Cara Mengatasi Berita "Hoax" di Dunia Maya*. Kementerian Komunikasi Dan Informatika Republik Indonesia.