

Overseeing Cyber-Neighborhoods: How Far the Indonesian National Police Effort in Handling Cybercrime?

Al Fauzi Rahmat^{1,*}, Dyah Mutiarin², Ulung Pribadi³, Dian
Eka Rahmawati⁴

¹ Master of Government Affairs and Administration, Universitas Muhammadiyah Yogyakarta, Indonesia

² Master of Government Affairs and Administration, Universitas Muhammadiyah Yogyakarta, Indonesia

³ Master of Government Affairs and Administration, Universitas Muhammadiyah Yogyakarta, Indonesia

⁴ Master of Government Affairs and Administration, Universitas Muhammadiyah Yogyakarta, Indonesia

*Corresponding author. Email: fauzirahmata@gmail.com

ABSTRACT

This article explores how far Indonesian National Police (Polri) efforts in handling cybercrime—choosing Indonesia as a case study because it is vulnerable to cybercrime. As a method for collecting data are cybercrime report documents, an official website “patrolisiber.id” and the official social media (Twitter, Facebook, and Instagram) by Polri, and several past kinds of literature to find their efforts. Our findings conclude that cybercrime in Indonesia continues to increase each year. The lack of serious handling by Polri related the cybercrime clearance cases from the total cybercrimes. Nevertheless, Polri has been efforts to handle cybercrime through Dittipidsiber as a division to handling cybercrime, attempting to commit socialization and education, virtual alerts, mediation, and restorative justice. They sent kinds of datasets such as pictures, videos, and tweets to the website and social media; it is a form of socialization and education effort to uphold safe cyber-neighbourhoods. However, other Dittipidsiber efforts as a virtual alert are not well followed up on the official report periodically, only spread in news media; where the total handling is still relatively small from media news coverage when looking at the high number of cybercrimes. Additionally, no factual information on how many accounts have received virtual alerts. Lastly, the meditation and restorative justice efforts has been carried out, but unknown how far the efforts made it; the data and information circulating on online news without official data from Polri.

Keywords: *Cybercrime, Cyber Patrol, Indonesian Police, Police Efforts.*

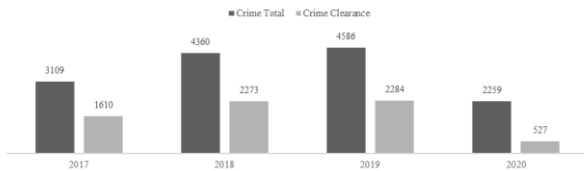
1. INTRODUCTION

This article aims to explore how far the efforts to handle cybercrimes on social media by the Directorate of Cyber Crime (Dittipidsiber) under the police's Criminal Investigation Agency (Bareskrim Polri). Cybercrime has disturbed most government organizations, industries, and the citizen. In Indonesia, the number of cybercrimes continues increasing occur every years (see figure 1.1). If cybercrime continues to occur, then its escalation will potentially threaten the community's safety, to threaten the sovereignty and

safety of the nation and state security [1]. It should be realized that the increase in cybercrime in Indonesia is likely to become a country that continues to be in the index of a country's position that is vulnerable to cybercrimes if no action is taken. Therefore, providing a sense of safety from cybercrime requires an institution tasked with protecting the cyber-neighbourhoods [2].

The National Police Organization (Polri) is the leading party that closely related to its function in the National Police Law that the task of the National Police is to maintain security and order, enforce the law, provide protection and services to community, without exception

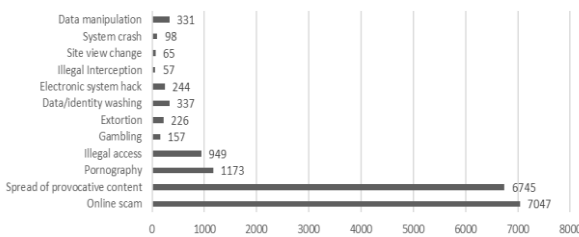
in the cyber-neighbourhoods. Bareskrim Polri is tasked enforcing the law and providing protection against cybercrimes. Therefore, the term cyber police were formed, a team from the Directorate of Cyber Crime (Dittipidsiber). Through official social media, they convey information to the public and detect potential cybercrimes on social media. However, this article aims to look how far the Dittipidsiber efforts in dealing cybercrimes.



Source: patrolisiber.id

Figure 1 Cyber Crime Trends in Indonesia

Based on figure 1.1 above, at a glance, it shows that the total cases of cybercrime continue to increase from 2017-2019, although in 2020, the crime total decreased from the previous year (in 2019) with a difference of 2327 total cases. However, efforts to resolve cases total have unfinished, of which 2020 has decreased cases clearance rather than 2019. As a result, it shows that there has been a decrease in responses related to case reports handled by the National Police in 2020. In sum, it still leaves a space that has not been completed, the National Police's efforts are needed to be able to handle all cases that have been submitted to police reports, the police must be able to cases clearance this because cybercrime is a new phenomenon in the digital era. In which, cybercrime appears simultaneously with the birth of a revolution and transformation of information technology [3] and the rapid penetration of internet networks [4]. Thus, this adds to information security vulnerabilities and increases the escalation of norm violations. Additional, cyber security in Indonesia has not been effective due to the lack of stakeholders in socializing it [1]. To strengthen, according to data obtained based on incoming police reports and the number of completed cases reported all regional police in Indonesia.



Source: patrolisiber.id, * Data above is obtained based on the number of incoming Police Reports and the

number of completed cases reported of all Regional police in Indonesia (Data: January 2016-May 2021)

Figure 2 Number of police reports made by the community*

The data above (figure 1.2) also confirms that fraudulent cybercrime is the highest crime and the spread of provocative content. Moreover, many of them all use telematics access, such as social media platforms, as a space to carry out cybercrimes [5]. Thus, through the Indonesian National Police, the government must provide warnings and prevention in education on social media and provide punishment for cybercriminals such as provocations [6]. On the other hand, cases such as the spread of hoaxes and fake news are also crimes that are often found on social media. Thus, media literacy is very much needed for citizens, so the Police must maximize it so that people cannot access and share invalid content [7]. However, the use of social media by the Police is still not adequate. Limited human resources cause this, so this gives the police delay in responding to social media issues in the community. It contributes to a lack of trust in the Police [8].

2. METHOD

Using qualitative method with library research approaches', it related to explore and collect information relevant to the topic derived from several kind of a literature sources, therefore, it providing a variety of information that is related under the topic. Furthermore, it is related to digging up information about the efforts of Dittipedsiber under the Polri control to deal cybercrimes in Indonesia. Furthermore, the data analysis techniques are undertaken through data collection, reduction, and also conclusion to provide a clearer understanding of the topics raised. To analysis data and visualize, our used the NVivo 12 Plus software. By capturing data through the NCapture and describing it through the dataset on the menus, this study uses for distribution charts and hashtags. On the other hand, collected data also was obtained through portal web <http://patrolisiber.id> and several kind of social media accounts by Dittipedsiber i.e. Twitter (@CCICPolri), Facebook (facebook.com/ccicpolri), and Instagram (@CCICPolri). Moreover, data timeline was taken from January 2016 to May 2021.

3. BASIC THEORY

3.1. Cybercrime: A Crime in The Digital Age

In today's digital era and mobile use, technology has played a perfect role in presenting all information, thus providing convenience in everyday life. However, it's also contributes to an increase in crime [9]. Diverse

distribution of cybercrime issues such as piracy of malicious software and media, fraud, intimidation, victimization and hate speech, and other virtual crime patterns [10]. Therefore, cybercrime victims who have a great opportunity are users with a high frequency of internet users, thus providing a direct opportunity for cybercrime [10]. Cybercrime studies have touched various perspectives, such as management, reporting, disclosure, governance, regulation, and justice [11]. Thus, efforts are needed to create a security system for technology facilities against cybercrime [12], a modelling framework and response to cybercrime [13], the creation of strict laws/ regulations in cyber defence, and punishment efforts [14], [15]. In the context of territorial jurisdiction, cybercrime is a fundamental problem in the digital era, because it is difficult to determine the location where the crime was committed, so cross-country legal considerations are needed to address the boundaries of subjective territorial jurisdiction [16].

3.2. Emerging Police in Cyberspace to Fight Cybercrime

Police organizations face significant challenges from the increasing threat of cybercrime, thereby providing a more substantial workload and complexity at skill and training for cyber-police [17]. To provide a sense of comfort, the National Police is present in creating peace and preventing people from violating norms [18]. It is also emphasized that frontline officers such as the police are expected to encourage public members to report such crimes and investigate them [19]. Just as cybercriminals are uneducated and poor people tend to do so, those aged 20-25 commit many crimes. So the police focus on those who have factors while monitoring social media [20]. Thus, to harmonize efforts to handle cybercrimes, such as hoaxes and fraud and face news, a collaboration between the government and the community is needed [21]. However, it requires the ability of institutions to work collaboratively and participative with high value in investigating the main problems of cybercrime at the national level [22]. Cybercrime perpetrators on the social media, intentionally or unintentionally, will be charged with Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE) [23]. Add, evidence, supporting facilities, and jurisdiction [24].

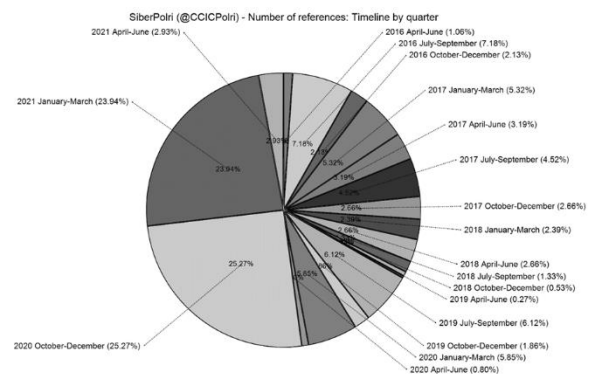
4. FINDING AND DISCUSSION

Cybercrime has become a serious problem globally. Various previous studies have discussed cybercrime from various perspectives, such as management, reporting, disclosure, governance, regulation, and justice [11]. This article contributes to exploring how far the

Indonesian National Police is trying to deal with cybercrime. Cybercrime continues to experience a significant increase throughout the year, as seen from reports and surveys from the patrolsiber.id (see figures 1.1; 1.2), which provides a strong warning for all to be careful in surfing in cyberspace. The public's concern about cybercrime is a frightening phenomenon that the police must immediately follow up. Furthermore, this information technology-based crime is a relatively new criminal crime that emerged along with the birth of the information technology revolution. Thus, there needs to handle efforts such as providing socialization and education to the public, virtual alerts, providing mediation and restorative efforts for cybercriminals.

4.1. Socialize and Educate Efforts by Dittipidsiber Related to Cyber Crime

Through the Dittipidsiber as divisions from Polri that handle cybercrime, it has tried to provide firmness for anyone who commits cybercrimes. This socialization and education effort have been conducted by Dittipidsiber through official social media accounts such as Twitter, Facebook, and Instagram with the @CCICPolri. As shown in the figure below.



Source: NVivo 12 Plus, collected data from official Twitter account's @CCICPolri

Figure 3 The Spread of Tweet on Twitter's @CCICPolri

Based on figure 4. above, Dittipidsiber has spread content from @CCICPolri through the official Twitter account in the form of tweets (total = 341 posts as of May 2021) that are intensive; this is shown from the percentage above (see figure 1.4)—counted in the 2016 April-June period until the 2021 April-June period. The 2020 period October-December has the highest percentage of tweets, namely 25.27% or 95 tweet posts, and the January-March 2021 period with the second-highest percentage of 23.94% or 90 tweet posts. The two periods above have become a concern by Dittipidsiber to conduct socialization and education efforts to deal with cyber-crimes through Twitter. Because that period, there were many cases of cybercrime experienced by Indonesia

citizens on social media. It is also not much different from the socialization and education by the Police through the social media platforms Facebook and Instagram.

On the other hand, Dittipidsiber's efforts in conducting socialization and education for the public can be observed through Facebook with 500 posts and Instagram 366 posts. Various socialization and education efforts undertaken dataset post; such as tweets, short-videos, and also pictures. These various socialization and education efforts were also immediately distributed by official social media account @CCICPolri. It confirms that Indonesian National Police (Dittipidsiber as a division) has made efforts to take preventive measures for the number of cybercrimes through socialization and education on social media [6]. In the moment, there are several efforts by Dittipidsiber in disseminating posts, such as with the support of hashtag distribution in every tweet; there are several vital hashtags that aim to pay attention and disseminate posts about cybercrime, some hashtags shared by @CCICPolri are as follows.

Table 1. Hashtag Distribution as a Form of Support for Socialization and Education

Hashtag	Frequencies	Description
#indonesiamelawanhoax	11.03%	Spreading information that Indonesia is against hoaxes
#indonesianegarahukum	7.59%	Emphasizing that Indonesia is a state of law
#awasketipu	2.76%	Informing that the public should be wary of being deceived
#indonesiantitiputipu	2.76%	Confirming that Indonesia is anti-cheat
#penegakanhukumdemiNKRI	2.76%	Affirming that Indonesia is always ready to uphold the law
#stophoax	2.76%	Convey that the public should stop hoaxes

		(spread)
#amanbermedsos	0.69%	Implying that people should be safe on social media
#bijakberinternet	0.69%	Telling the public that you have to be internet wise
#cerdasbermedsos	0.69%	Prioritizing people to be smart to play social media

The use of hashtags aims to assist a posts that owned to better known by the wider community on social media. The dissemination of hashtags by Dittipedsiber to socialization and education related to cybercrime. The hashtag of #indonesiamelawanhoax as dominates (11.03%) several hashtags echoed by the @CCICPolri Twitter account and spread by retweeting posts by other Twitter accounts. It is in line with the current situation experienced on social media, which often gets hoax news that is disseminated by irresponsible individuals, therefore, it provides its losses for online citizen who are surfing and looking for information in cyber-neighbourhood. The socialization and education efforts by Dittispedsiber are disseminated through the Twitter social media account and disseminated on other social media such as Facebook. Efforts to socialize and educate by disseminating information in the form of datasets as part of providing understanding for the all online citizen on social media, furthermore, they are not easily deceived and trapped in cybercrimes. Because, the spread of hoaxes is an act included in cybercrime [25]. Thus, this also confirms that the Police have given warnings and prevention in the form of education on social media [6].

4.2. Virtual Alert and Meditation Efforts by Dittipidsiber Related to Cyber Crime

Virtual alerts are an Indonesian National Police effort to give a warning to social media accounts that violate the law; it is related to posts containing violations of the law. Experts from the Police who have gone through an in-depth of an arrested post are given virtual alerts. The investigator include experts in criminal law, sociologists, linguists, and ITE experts who analyse posts that can violate the mainstream of cybercrime. So, virtual alerts do not work on their subjectivity. In enforcing cyber security, the Police have succeeded in trying to take virtual alerts to several social media accounts; the Police are more likely to provide virtual alerts to accounts that are indicated to be involved in cybercrimes and prioritize

revision or deletion of posts that are indicated potential to legal channels criminal.

FORM PERSETUJUAN PENGIRIMAN PERINGATAN POLISI VIRTUAL

Dasar: RLJ0715/2021/Dittipidsiber tanggal 23 Februari 2021

Target: [Redacted]

Tangkapan Layar: [Screenshot of Instagram post]

Profil Target: Anonymous

Konten: [Redacted]

Prediksi: Konten akun [Redacted] yang diunggah nissa_sabyan mengandung ujaran kebencian

Pendapat Ahli: 1. Bahasa: Penghinaan terhadap Nisa sabyan dengan melakukan cemohan kasar ditandai dengan penggunaan kata anjing dan dasar jahanam itu penanda cemohan dalam bahasa Indonesia 2. Pidana: Memenuhi unsur pasal 27 ayat (3) UU ITE

Narasi Peringatan I: **VIRTUAL POLICE ALERT** Peringatan I
Komentar Instagram anda pada konten yang diunggah oleh akun nissa_sabyan pada tanggal 22 Februari 2021 pukul 06:50 WIB berpotensi pidana ujaran kebencian.
Guna menghindari proses hukum lebih lanjut, dihimbau untuk segera melakukan koreksi pada konten media sosial setelah pesan ini anda terima.
Salam PRESISI.

Narasi Peringatan Terakhir: **VIRTUAL POLICE ALERT** Peringatan Terakhir
Komentar Instagram anda pada konten yang diunggah oleh akun nissa_sabyan pada tanggal 22 Februari 2021 pukul 06:00 WIB berpotensi pidana ujaran kebencian sebagaimana Pasal 27 ayat (3) UU ITE.
Silaakan melakukan koreksi pada konten media sosial anda maksimal 1x24 jam setelah pesan ini anda terima. Jika peringatan terakhir ini tidak diindahkan, maka proses hukum akan dijalankan sesuai aturan perundangan yang berlaku.
Salam PRESISI.

Waktu Kirim: Tanggal 23 Februari 2021 Metode Pengiriman: DM

Waktu Kirim: Tanggal 24 Februari 2021 Metode Pengiriman: DM

source: detik.com [26]

FORM PERSETUJUAN PENGIRIMAN PERINGATAN POLISI VIRTUAL

Dasar: RLJ0692/2021/Dittipidsiber tanggal 23 Februari 2021

Target: [Redacted]

Tangkapan Layar: [Screenshot of Twitter post]

Profil Target: Anonymous

Konten: [Redacted]

Prediksi: Cuitan akun [Redacted] tidak mendapatkan respon dari pengikutnya, diduga konten tersebut tidak viral.

Pendapat Ahli: 1. Bahasa: Konten tersebut merupakan bentuk penghinaan terhadap SBY. 2. Pidana: Apabila tidak benar, berarti pemberitahuan tersebut adalah merupakan perbuatan memuduh SBY telah melakukan sesuatu hal yang mencemarkan nama baik SBY.

Narasi Peringatan I: **VIRTUAL POLICE ALERT** Peringatan I
Konten Twitter anda yang diunggah pada tanggal 22 Februari 2021 pukul 11:19 WIB berpotensi pidana ujaran kebencian.
Guna menghindari proses hukum lebih lanjut, dihimbau untuk segera melakukan koreksi pada konten media sosial setelah pesan ini anda terima.
Salam PRESISI.

Narasi Peringatan Terakhir: **VIRTUAL POLICE ALERT** Peringatan Terakhir
Konten Twitter anda yang diunggah pada tanggal 22 Februari 2021 pukul 11:19 WIB berpotensi pidana ujaran kebencian sebagaimana Pasal 45 ayat (3) UU ITE.
Silaakan melakukan koreksi pada konten media sosial anda maksimal 1x24 jam setelah pesan ini anda terima. Jika peringatan terakhir ini tidak diindahkan, maka proses hukum akan dijalankan sesuai aturan perundangan yang berlaku.
Salam PRESISI.

Waktu Kirim: Tanggal 23 Februari 2021 Metode Pengiriman: DM

Waktu Kirim: Tanggal 24 Februari 2021 Metode Pengiriman: DM

source: gelora.co [27]

Figure 4. Example of a Virtual Alert Letter by Dittipidsiber

The figure 4.2 above is an example of an approval form for sending a virtual police warning issued by Dittipidsiber to an account that spreads hate speech and hoaxes. In order to avoid further legal imposition, Dittipidsiber warns through Direct Message to correct tweets that are disseminated for 1 x 24 hours, otherwise the legal process is followed up. Therefore, in this regard, the Police prioritizes meditation efforts on cybercriminals, such as the spread of hoaxes and hate speech, if there is a report from the victim concerned. In addition, the virtual alert can bring both parties to meditation and put forward restorative justice efforts [28]. Sending virtual alerts is sent directly by the

Indonesian National Police through the Director of Cyber or a designated official distributed in providing authorization to send directly to a personal account officially via direct message. However, giving this warning is an educational effort for account owners to delete content suspected of being criminalized immediately. If the account owner does not respond to the warning, the police will message as long as no party is harmed; if someone is harmed and makes a police report, the police will facilitate the two parties to make peace through the mediation process.

4.3. Restorative Justice by Dittipidsiber Related to Cyber Crime

Referring to the ITE Law as the legal basis for dealing with cybercrimes, several cases still prioritize restorative justice. The handling of restorative justice can be put forward through Circular Letter SE/2/11/2021 concerning Ethical Cultural Awareness to Realize a Clean, Healthy, and Productive Digital Space for Indonesia. Therefore, this Decree serves as the basis for the Police to put forward restorative justice efforts in resolving cases related to reports of alleged violations of the ITE Law. Except for potentially divisive cases, ethnicity, religion, race, and intergroup, radicalism, and separatism [29]. After restorative justice (no agreement), a new police report. Therefore, not all violations or irregularities in the cyber-neighbourhood are carried out by law enforcement, but suggesting the efforts of restorative justice. Nevertheless, there is not much information on how many cybercrime cases are handled for restorative justice.

Dittipidsiber through the ITE Law Article 27 paragraph 3, Article 207, Article 310 and Article 311, utterances of insults, defamation and slander, there are no detentions, these criminal acts are resolved by means of Restorative Justice. As for criticism of the government or authorities, it is also not detained, criticism is conveyed in a civilized manner. Therefore, restorative justice efforts aim to create a clean, healthy, ethical, productive and diverse cyberspace. However, the problem that the official data of Dittipidsiber does not include how many crimes have been committed by restorative justice efforts, but this does not rule out the possibility that Dittipidsiber's efforts have done.

5. CONCLUSION

Indonesia National Police (Polri) has made various efforts to suppress cybercrime in Indonesia. Through the Directorate of Cyber Crime (Dittipidsiber) as a specific division structure, it has carried out socialization and education for citizens through the official social media channels Twitter with 341 tweets, Facebook with 500 posts, and Instagram 366 posts in which various datasets

such as images, short videos, info graphics, and others. Thus, using hashtags as an effort to disseminate information on socialization and education. In addition, Dittipidsiber have provided a website patrollsiber.id as a report page for citizens who they are victims or looking at cybercrimes on social media; this is an effort to be transparent and responsibility for cybercrimes data. Furthermore, virtual alert and meditation efforts have been carried out for each time, which send virtual alert to social media accounts considered cybercriminals and are included in criminal law. However, restorative justice and meditation efforts are put forward in solving problems, except for cybercrime cases in crimes of ethnicity, religion, race, intergroup, radicalism, and separatism, besides, no knows many crime clearance case handled. It is based on SE/2/11/2021, which prioritizes the realization of a healthy and productive digital space. As a result, this is all to prevent cybercrime attacks and the issue of cyber security must include on policy agenda.

ACKNOWLEDGMENTS

A big thanks to all those who have helped to correct and provide comments on this manuscript, therefore, it deserves to be presented and published.

REFERENCES

- [1] M. Rizal and Y. Yani, "Cybersecurity Policy and Its Implementation in Indonesia," *JAS (Journal ASEAN Stud.*, vol. 4, no. 1, p. 61, 2016, doi: 10.21512/jas.v4i1.967.
- [2] M. I. Alghamdi, "Cybercrime legislation applicable and enforceable," *Mater. Proceeding*, 2021, doi: <https://doi.org/10.1016/j.matpr.2021.04.050>.
- [3] B. K. B. Putra, "Kebijakan Aplikasi Tindak Pidana Siber (Cyber Crime) Di Indonesia," *Pamulang Law Rev.*, vol. 1, no. 1, pp. 1–14, 2018, doi: 10.32493/palrev.v1i1.2842.
- [4] M. J. Islami, "Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index," *Masy. Telemat. Dan Inf. J. Penelit. Teknol. Inf. dan Komun.*, vol. 8, no. 2, p. 137, 2018, doi: 10.17933/mti.v8i2.108.
- [5] S. Singh, V. Thapar, and S. Bagga, "Exploring the hidden patterns of cyberbullying on social media," *Procedia Comput. Sci.*, vol. 167, no. 2019, pp. 1636–1647, 2020, doi: 10.1016/j.procs.2020.03.374.
- [6] M. B. Salam, A. D. Nurlukman, Amiludin, and Irwandi, "Government 's in Role to Reduce Cyberbullying to Youngster on Social Media," *JPPUMA J. Ilmu Pemerintah. dan Sos. Polit. UMA*, vol. 9, no. 1, pp. 65–76, 2021, doi: 10.31289/jppuma.v9i1.4248.
- [7] TanveerKhan, A. Michalasa, and A. Akhunzada, "Fake news outbreak 2021: Can we stop the viral spread?," *J. Netw. Comput. Appl.*, 2021, doi: <https://doi.org/10.1016/j.jnca.2021.103112>.
- [8] O. Shinta and J. M. Logahan, "Social media empowerment in implementing community policing: Study of the cybercrime investigation of the Indonesia national police," *UI Proc. Soc. Sci. ...*, 2019.
- [9] R. Sarre, L. Y. Lau, L. Y. C. Chang, and R. Sarre, "Responding to cybercrime: current trends," *Police Pract. Res.*, vol. 19, no. 6, pp. 515–518, 2018, doi: 10.1080/15614263.2018.1507888.
- [10] E. R. Leukfeldt and M. Yar, "Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis," *Deviant Behav.*, vol. 37, no. 3, pp. 263–280, 2016, doi: 10.1080/01639625.2015.1012409.
- [11] A. Chandra and M. J. Snowe, "A taxonomy of cybercrime: Theory and design," *Int. J. Account. Inf. Syst.*, vol. 38, p. 100467, 2020, doi: 10.1016/j.accinf.2020.100467.
- [12] Y. Zatsarinnaya, A. Logacheva, and M. Grigoreva, "Cybersecurity of Technological Facilities and Industries in the Era of Digital Transformation," *Lect. Notes Electr. Eng. Int. Russ. Autom. Conf.*, vol. 729, pp. 523–532, 2021, doi: https://doi.org/10.1007/978-3-030-71119-1_51.
- [13] D. Mahima, "Cyber threat in public sector: Modeling an incident response framework," *Proc. Int. Conf. Innov. Pract. Technol. Manag.*, pp. 55–60, 2021, doi: 10.1109/ICIPTM52218.2021.9388333.
- [14] K. Babu and M. Ullah, "Cyber legislation and cyber-related legal issues in Bangladesh: Inadequacies and challenges," *Int. J. Electron. Secur. Digit. Forensics*, vol. 13, no. 2, pp. 180–196, 2021, doi: 10.1504/ijesdf.2021.113379.
- [15] H. Manihuruk and D. D. Y. Tarina, "State Defense Efforts through Strengthening Cyber Law in Dealing with Hoax News," *Int. J. Multicult. ...*, pp. 27–36, 2020.

- [16] J. B. Maillart, "The limits of subjective territorial jurisdiction in the context of cybercrime," *ERA Forum*, vol. 19, no. 3, pp. 375–390, 2019, doi: 10.1007/s12027-018-0527-2.
- [17] D. Harkin, C. Whelan, and L. Chang, "The challenges facing specialist police cyber-crime units: an empirical analysis," *Police Pract. Res.*, vol. 19, no. 6, pp. 519–536, 2018, doi: 10.1080/15614263.2018.1507889.
- [18] M. I. Jati, "Manajemen Media sebagai Intervensi dalam Menanggulangi Isu Provokatif di Medsos," *J. Ilmu Kapol.*, vol. 13, no. 2, pp. 16–29, 2019.
- [19] L. Hadlington, K. Lumsden, A. Black, and F. Ferra, "A Qualitative Exploration of Police Officers' Experiences, Challenges, and Perceptions of Cybercrime," *Polic. A J. Policy Pract.*, vol. 15, no. 1, pp. 34–43, 2021, doi: 10.1093/police/pay090.
- [20] A. Almansoori, M. Alshamsi, S. Abdallah, and S. A. Salloum, "Analysis of Cybercrime on Social Media Platforms and Its Challenges," *Hassanien A.E. al. Proc. Int. Conf. Artif. Intell. Comput. Vis. (AICV2021). AICV 2021. Adv. Intell. Syst. Comput.*, vol. 1377, 2021, doi: https://doi.org/10.1007/978-3-030-76346-6_54.
- [21] G. A. Priyanto and M. Sardi, "The Urgency of Protecting Netizen in Freedom of Speech on Social Media," *Media Law Sharia*, vol. 2, no. 1, pp. 76–91, 2021, doi: 10.18196/mls.v2i1.11480.
- [22] D. Johnson, E. Faulkner, G. Meredith, and T. J. Wilson, "Police Functional Adaptation to the Digital or Post Digital Age: Discussions with Cybercrime Experts," *J. Crim. Law*, vol. 84, no. 5, pp. 427–450, 2020, doi: 10.1177/0022018320952559.
- [23] Y. Fitriani and R. Pakpahan, "Analisa Penyalahgunaan Media Sosial untuk Penyebaran Cybercrime di Dunia Maya atau Cyberspace," *CAKRAWALA J. Hum. Bina Sarana Inform.*, vol. 20, no. 1, 2020.
- [24] P. Prasetyo and M. Zuhdy, "Penegakan Hukum Oleh Aparat Penyidik Cyber Crime Dalam Kejahatan Dunia Maya (Cyber Crime) Di Wilayah Hukum Polda Diy," *Indones. J. Crim. Law Criminol.*, vol. 1, no. 2, pp. 79–88, 2020, doi: 10.18196/ijclc.v1i2.9611.
- [25] Y. Nuraeni and A. R. Hidayat, "Tinjauan Yuridis Penanganan Tindak Pidana Hoax Corona Di Media Sosial Oleh Kepolisian Republik Indonesia," *Presumption Law*, vol. 3, no. 1, pp. 72–115, 2019.
- [26] H. Batubara, "Siber Polri Mulai Kirim Peringatan Virtual ke Akun Medsos yang Sebar Hoax," *detikNews*, 2021. .
- [27] Gelora News, "Siber Polri Mulai Kirim Peringatan Virtual ke Akun Medsos yang Sebar Hoax," *Gelora News*, 2021. .
- [28] CNN Indonesia, "Polri: Mayoritas kasus hoaks dari patroli siber tak disidang," *cnnindonesia.com*, 2021.
- [29] Detik News, "Ini Isi Lengkap Surat Edaran Kapolri soal Penanganan Perkara UU ITE," *news.detik.com*, 2021.