Exploring the Cybercrime Prevention Campaign on Twitter: Evidence from the Indonesian Government

Al Fauzi RAHMAT
Universitas Muhammadiyah Yogyakarta, Indonesia
E-mail address: fauzirahmata@gmail.com

Catalin VRABIE
The National University of Political Studies and Public Administration, Romania
E-mail address: catalin.vrabie@snspa.ro

Galih Bagas SOESILO
Universitas Muhammadiyah Purworejo, Indonesia
E-mail address: galihbagas@umpwr.ac.id

Abstract
Cybercrime in Indonesia has recently become a significant problem in line with the increase in internet users, which is a serious issue among online community networks. Therefore, this makes government authorities strive to take preventive measures to prevent the spread of cybercrime. In this case, this article aims to explore the Indonesian government's efforts under the National Cyber and Crypto Agency to run a cybercrime prevention campaign through the @BSSN_RI Twitter account with the tagline Guard Cyberspace. Exploration studies have been initiated and visualized with the code of the NVivo tool. This research has produced several findings, including: Firstly, the Indonesian government has taken current preventive measures, and there has been a call to action to prevent cybercrime during the last two years. Secondly, the Indonesian government has maximized its efforts to prevent cybercrime through various tweets, posters, and the hashtag. Furthermore, Twitter users (outside of public sector accounts) are also contributing to spreading cybercrime prevention campaigns. In addition, there are several words and hashtag frequencies that echo the point of view of the campaign. Moreover, this research also contributes significantly to increasing the richness of literature on how government authorities' use social media as a cybercrime prevention campaign tool, which past studies have limited.

Keywords: Cyber Crime, Prevention Campaign, Advocacy, Social Media, Indonesia.

1. Introduction
In the last few decades, research on the importance of social media for advocacy and campaigning activities has received increasing attention from the organizations and community movement [1]–[6]. But this activity is still limited to government entities' activities. Hence, this activity is crucial in explaining essential issues to support the achievement of information for the wider community [7], [8]. Therefore, the role of government entities in using social media as a channel for information dissemination and advocacy is deemed necessary, bearing in mind that in the current era, the number of social media users is increasing in line with the increase in communication and interaction networks among citizens. However, the availability of social media not only provides space and favorable opportunities, but also results in negative impacts due to its misuse, as an example for internet crimes known as "cybercrime".

Cybercrime refers to an act of abusing online network-based computer technology to illegally gain personal or group benefits and intimidate other users [9]–[12]. As a result, large amounts of personal information and financial transactions become vulnerable to

cybercriminals [13]. In this case, cybercrime currently has become a growing issue as reported by several scholars [14]–[18]. One of the sources of cybercrime attacks is social media is an attack vector for criminal acts because it has a rich data information system, thereby increasing cybercrime. In addition, cybercriminals also target social media because they have the potential to find information about targets easily [19]. Where the targets usually post their activities [20]. On the other hand, several cybercrimes often occur, such as hacking social media, breaking into victims' technology devices, identity theft, phishing, carding, ransomware malware, online fraud, data falsification, spreading illegal content, terrorists, utterances of hatred and contempt, and others [21], [22]. This rise in cybercrimes require a government response to take preventive action so that it does not continue to cause harm.

In this research, Indonesia is used as an case study, in which Indonesia is ranked first for the highest and third largest internet users in Asia [23]. Therefore, this makes it possible to pose a threat of cybercrime disrupting cyberspace activities. Moreover, in 2022, Indonesia is still in sixth position for cyber security in Southeast Asia [24]. As a result, Indonesia has become an easy target for cybercrime in cyberspace, considering that cyber security is relatively low compared to neighboring countries such as Malaysia and Singapore. Therefore, the Indonesian government must increase its attention to educating and promoting cybercrime information to maximize cyber security. In this situation, the main goal is to recognize the characteristics of cybercrime and broaden public understanding of the importance of the cybercrime issue [25]. This has resulted in enormous losses for Indonesian citizens engaging in internet activities.

In this situation, some citizens take collective action to prevent cybercrime. For example, in India, the community has used technology to prevent and raise awareness of cybercrime. In contrast, initiatives from the government entities for cybercrime prevention campaigns are considered to have less influence [26]. Hence, public authorities have a significant role in stimulating cyber-security progress and reducing the vulnerability of cybercrime [25]. Thus, the government has contributed to taking a preventive stance against cybercrime, which is very widespread. On the other hand, several previous studies have been analyzed, such as in Indonesia, where there have been advocacy efforts from the Indonesian Police to prevent the spread of hate speech and hoaxes through the official social media accounts of the Directorate of Cyber Crime, Indonesian police [17]. Moreover, there is a cybercrime prevention campaign launched by the Chinese government to motivate the public authorities to maintain the security of user information from cybercrime, on the other hand, the FBI in the United States, which continues to distribute information through the government's social media accounts via Twitter [27]. In England, there is an effort by the UK government authorities to assist the business sector in controlling cybercrime and efforts to adopt policies similar to those of the government [15]. Finally, government authorities have made many efforts to respond to cybercrime issues [28]–[30].

However, to our knowledge, only a tiny amount of research focuses explicitly on revealing preventive actions and government advocacy efforts through social media for cybercrime from national government authorities in the intelligence and defense agencies for citizens in Indonesia as a case study. Therefore, this research aims to explore Indonesian

government in combating cybercrime with prevention campaign. As pointed out, preventive action is required more than just carrying out duties in law enforcement [31]. In this case, social media as a means to collect data, in which social media is considered part of the way to fulfill the government's goals in cybercrime prevention campaigns [31]. Therefore, this research seeks to produce knowledge about exploring advocacy campaign efforts by the government. This study uses the Indonesian government under the National Cyber and Crypto Agency (Badan Siber dan Sandi Negara) in responding to the rise of cybercrime through Twitter social media. Furthermore, given that an information campaign on cybercrime prevention requires further education to protect citizens [32], and the complexity of cybercrimes is high given the risks they face, there is a need for prevention education from the government [33]. Additionally, the government is considered as a key player in preventing cybercrime and increasing state resilience [34].

Selecting Twitter as a case study, considering that each Twitter user has some followers. Where they communicate with each other through tweets, replies (to other tweets), and mentions (from other retweet) [35]. In the popularity of the Twitter site due to Indonesian Twitter users are ranked fifth in the world and first in Southeast Asia [36]. Others argue, Indonesia, a country in the world, has the fourth most active Twitter social media users and ranks first in Southeast Asia [37]. In this case, this examines the @BSSN_RI Twitter official account by Indonesia's National Cyber and Crypto Agency, which assumed that this account serves as a tool for disseminating information on cybercrime prevention measures and emphasizing the rampant cybercrime experienced. The 'Guard Cyberspace' campaign by BSSN RI aims to increase public awareness and prevent cybercrime. This campaign was made as part of saving the citizens and as a warning to be careful in your activities on internet activities. The spread of this campaign is through the Twitter social media account and several hashtags accompanying the posts. This also rise of hashtag analysis, in order to the existence of hashtags is reliable tracking, which is spread through tweets, thus enabling the Guard Cyberspace campaign to get the attention of many users on Twitter. On the other hand, other argue that hashtags are one of the main tools used by Twitter to detect the number of messages being spread [38]. In this case, adding tweets with hashtags makes finding posts more intuitive [39]. Therefore, the government actors must use hashtags in posts as campaign media and calls to action [40].

2. Literature review

2.1. Cybercrime Urgency Response: The Significant Issue in Worldwide Current Technology Era

Cybercrime has currently created anxiety for all levels of online society, including government organizations, the trade business sector, educational institutions, communities, and others, due to the complexity of the negative impacts it has caused [2[41]. Given the increasing trend of Internet use in the workplace and more Internet-enabled electronic devices, victimization related to cybercrime is likely to occur with increasing frequency [31]. Moreover, the current increase in cybercrime is attributed to an increase in community activity that utilizes information technology systems via the internet network, leading to many types of traditional crimes shift to digital crimes [42]. This indicates that the more people and organizations involved in online activities, the more cybercrimes will increase [9]. Furthermore, additionally, this cybercrime was initiated not only by the perpetrators

alone but carried out simultaneously; this is due to the limited knowledge and IT skills of one another [43], as well as many cyber criminals from across countries [44]. As a result, victims' losses from cybercrimes have become more complex [45], [46]. Therefore, an agile and proactive response to handling losses due to cybercrime is implemented immediately to minimize them [47]. Handling cybercrime activities carried out by transnational actors is crucial, and international-level law is needed to prevent and standardize national rules [48]. The existence of this transnational crime activity occurs because a country has weak cyber-security. Furthermore, perpetrators can use new technology to attack victims [49]. Consequently, there is a need for intense communication with individuals about the potential harm caused by cybercrime. Thus, citizens can motivate themselves to protect themselves better when involved in the online environment [50]. So, in order to raise social awareness of cyber security threats, authorities must be willing to address the protection of information in cyberspace and reduce the threat of cyber-attacks, especially regarding telecommunications spread and content distribution [41].

2.2. Cybercrime Preventive Campaign: How to Combat the Cybercrime?

Law enforcement authorities, such as the police, need to be at the forefront of handling cyber-crimes, where they need to educate the public about how to use cell phones and the internet in a good and correct way [32]. Given this situation, cybercrimes are highly complex, which is in line with the increase in technological systems; the problems caused are also increasing [51]. Thus, cybercrime becomes an increasingly critical threat as media use spreads across all population segments [52]. As a result, public authorities need to strategically manage the handling of cybercrime, which builds their national capacity to fight cybercrime through modernizing the legislative framework, educating and equipping criminal justice actors, strengthening the resilience of the business community, and increasing public awareness [53]. In one of the efforts to reduce cybercrime attacks, the government can inform its citizens about cyber security practices so that they are aware of the dangers of internet activity and how cybercriminals will try to harm them through the system [54], such as by launching a publicity campaign to help people protect themselves from online crimes through the media, television advertisements, and websites [55]. As of this situation, the stakeholders must build a clear and responsible standard regulatory framework in sustainable cyber security efforts and design innovations in mitigating cyber-attacks to raise awareness of cybercrime among all citizens [12]. Thus, education for citizens on securing their online activities and stopping people from committing cybercrimes is necessary [32]. Therefore, user awareness of cybercrime is essential as a solution to avoid cyber-attacks [56]. In addition, a legal system and legal framework are needed [57]. However, cybercrime is not only opposed by law enforcement authorities; civil society must also be involved in building increased awareness of cybercrime attacks [55]. As a result, synergy between public authorities and the community is needed in preventive campaigns to prevent cyber-attacks [58].

3. Material and methods

To present findings and discussion, this study uses the @BSSN_RI Twitter account with the Guard Cyberspace tagline as a prevention campaign on Twitter social media to increase Indonesian public awareness of cybercrimes and how to deal with them by Indonesia's National Cyber and Crypto Agency (*Badan Siber dan Sandi Negara*). Furthermore, the

NVivo software has been used as a visualization instrument that aims to explore data sets through NCapture to Twitter during the first data obtained until March 31, 2023, and it is imported to NVivo software with automatic categorization features called auto coding as a main menu to explore such as tweet and retweet distribution, user networks, word frequency, hashtags echoed, produces an example of tweet-poster-hashtag, and sociogram stream sharpening.

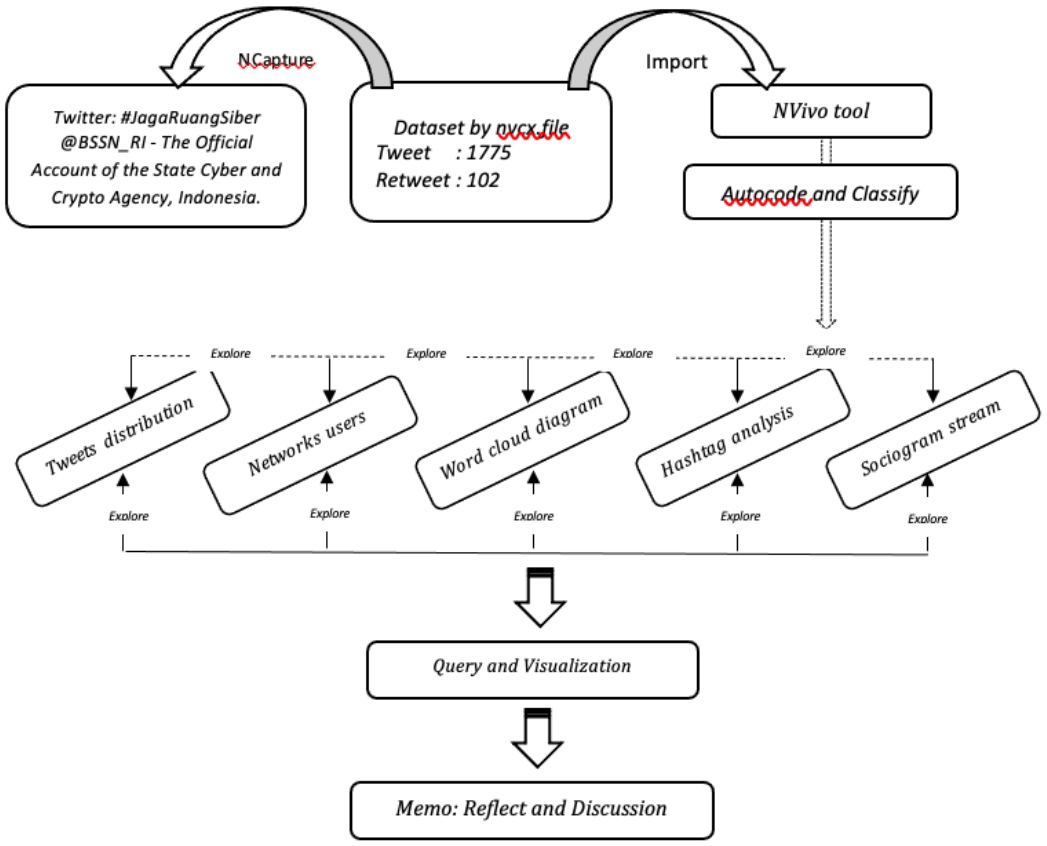

Fig. 1. The dataset workflow processing overview
Source: Authors

4. Finding and discussion

This section contains research findings of the Indonesian government's National Cyber and Crypto Agency's efforts to distribute cybercrime prevention information via @BSSN _RI. Some of the analyses provided include examining the annual and monthly distribution of tweets, followed by a network of connected users, word cloud and hashtag use, instances of posts, and sociogram networks for information diffusion in order to sustain cyberspace.

4.1. Yearly and Monthly Distribution of Tweet of #JagaRuangSiber (BSSN_RI)

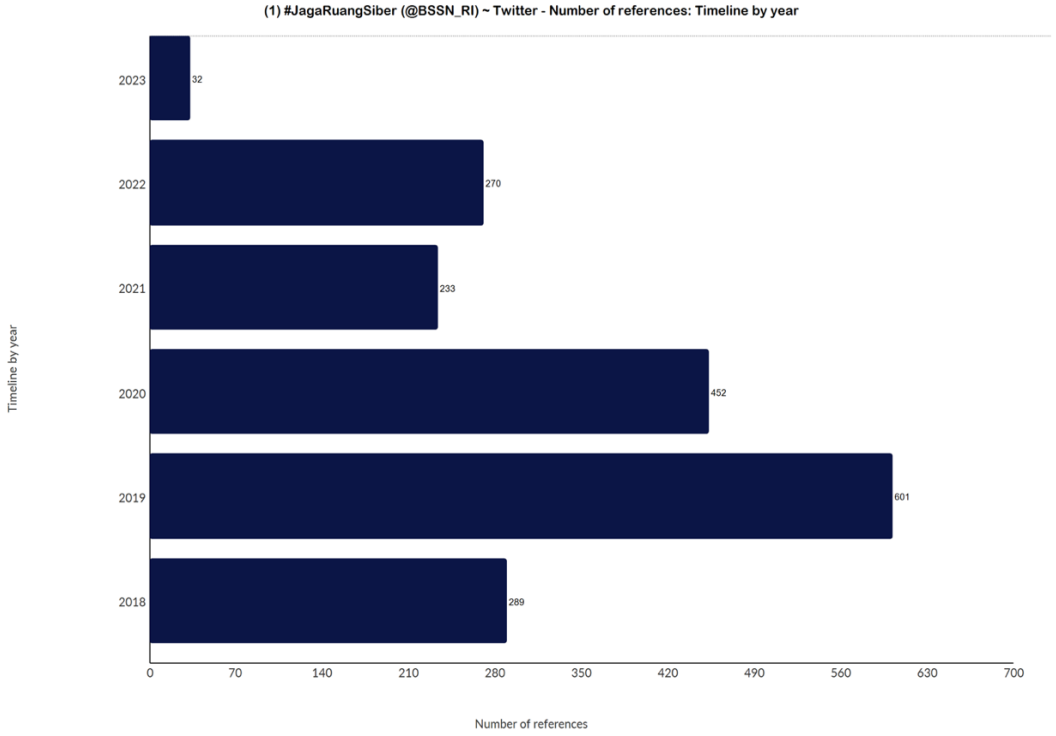

Fig. 2. Spreading reference regarding the cybercrime campaign yearly by @BSSN_RI
Source: NVivo Analysis

Following various tweets yearly, the National Cyber and Crypto Agency of the Republic of Indonesia has undertaken efforts to spread cyberspace protection initiatives. This is consistent with the rising frequency of cybercrime incidents in Indonesian cyberspace. The distribution of information fluctuates detected yearly, with @BSSN_RI Twitter account uploading 289 references posts in 2018 and 601 posts in 2019, as well as a growth of 312 posts in 2019. However, from 2020 to 2021, the ratio dropped from 452 to 233. Indeed, this stands in contrast to the earliest years of the existence of posts to sustain cybersecurity. In addition, there was a rise of 37 references from 2021 to 2022, from 270 to 233. As of 6 April 2023, a total of 32 posts have been published. Additionally, for clarity, the data also examined quarterly, indicating that the agency spreads entries by month to month. Based on Figure 3, there are significant points of view of posts dissemination. In which, October to December 2018 is 15.4%, furthermore, in April to June 2020 it is 10.2% posts. Moreover, July to September 2022 shows a 10.1% posts distribution.

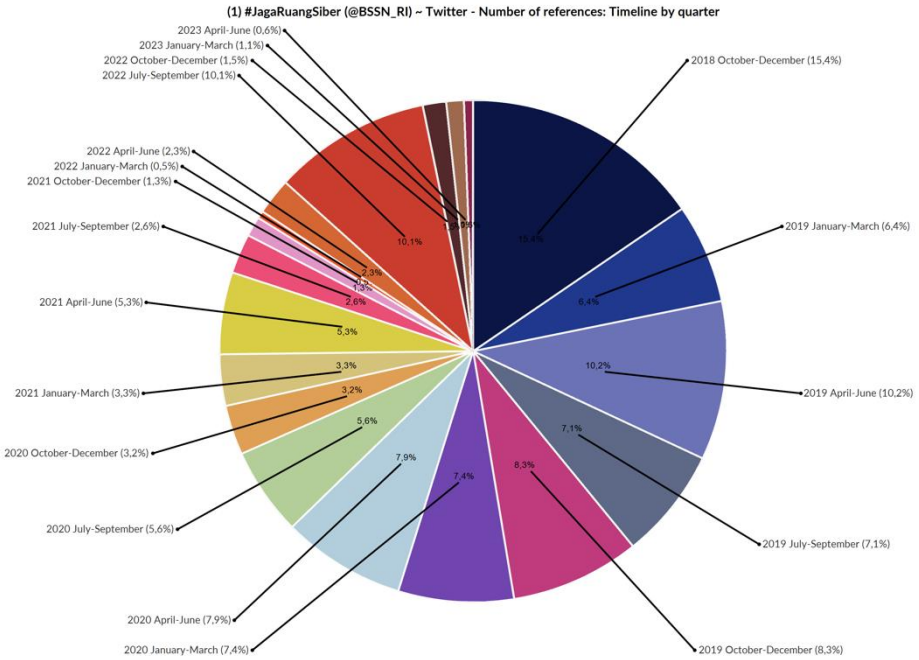

Fig. 3. Monthly Distribution of Tweet of #JagaRuangSiber (BSSN_RI)
Source: NVivo Analysis

4.2. Network-Users of #JagaRuangSiber @BSSN_RI Distribution Information and Outreach

Figure 4 has been visualized the efforts of the Indonesia National Cyber and Crypto Agency in dissemination to cybercrime prevention campaigns through the Twitter account @BSSN_RI. There are a number of Twitter user networks that have caught our attention, including *@setkabgoid*. On the other hand, there are a number of users from Twitter social media by local government, including *@pemprov_gtlo, @PemkabTegal, @diskominfosbali, @kominfodiy, and @diskkominfojabar*. In addition, the involvement of Indonesia national television through the Twitter account, namely *@TVRINasional*, also took part in the campaign against cybercrime. Therefore, this indicates, based on several Twitter user networks distributed by @BSSN_RI, that more government accounts are contributing to efforts to secure cyberspace from cybercrimes. In fact, this preventive measure targets the citizens as an object, which aims to disseminate information about the cybercrimes. Therefore, the Twitter account citizens involvement is not detected much through the @BSSN_RI campaign.

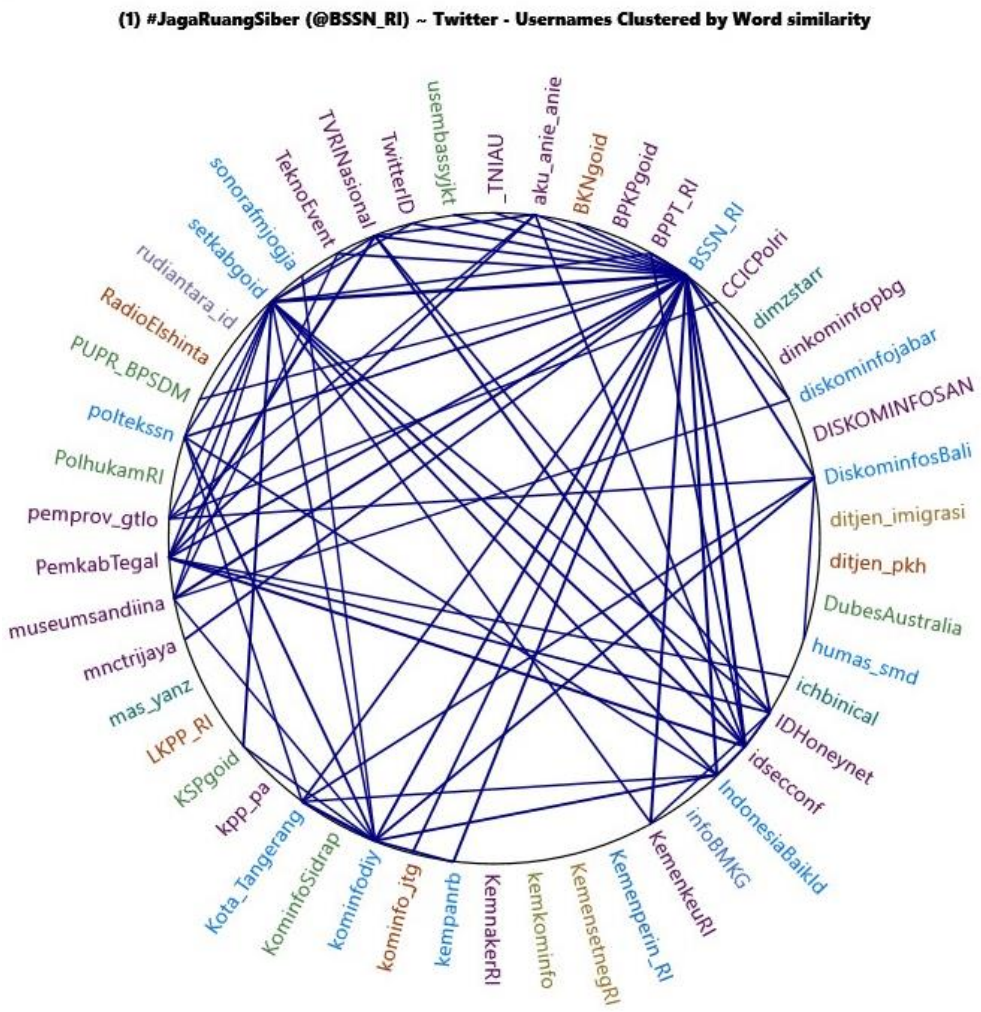

Fig 4. Network Users' Distribution Tweet
Source: NVivo Analysis

4.3. Word Cloud as the Popular Text Distribution

Word frequency analysis is used to identify how often certain values of a variable phenomenon can occur. In this research, word frequency analysis is used as a tool to determine the words spread by @BSSN_RI, especially in relation to cybercrime prevention campaigns. Therefore, this section displayed the word cloud to visualize the dominant text dissemination by @BSSN_RI twitter account. In Figure 5, represented there are 30 prominent words in the word cloud have been captured by NVivo tool. For instance, "*siber*" is cyber, "*bssn*" is the name of agency (*National Cyber and Crypto Agency of the Republic of Indonesia*). On the other hand, "*keamanan*" means security. Following those texts, there are other pivotal term such as "*electronik*" is electronic, digital, "*informasi*" is information, besides, there are other terms such as "*ekonomi"* is economic, "*kesehatan*" is health,

"*kerjasma*" is partnership or cooperation. However, the @BSSN_RI has rich concern to the cybercrime prevention campaign on social media with several issues.

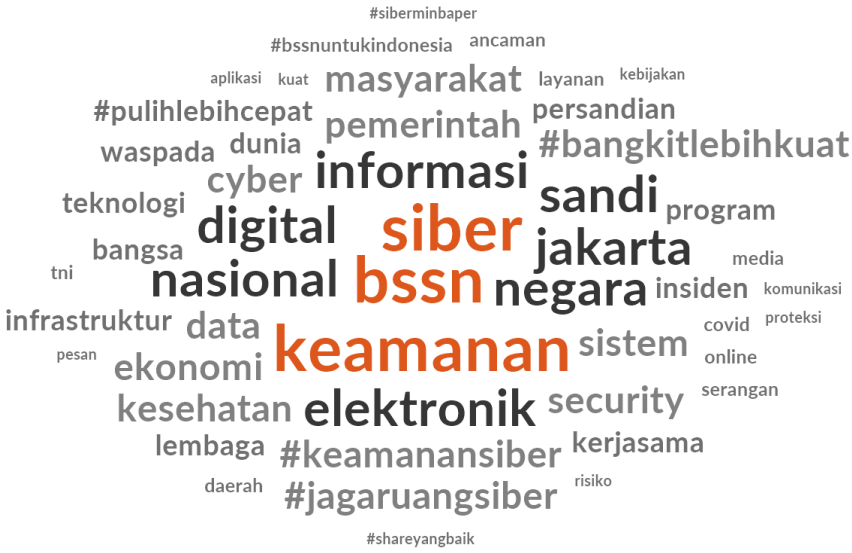

Fig. 5. Word Cloud of Cybercrime Campaign on @BSSN_RI Twitter account
Source: NVivo Analysis

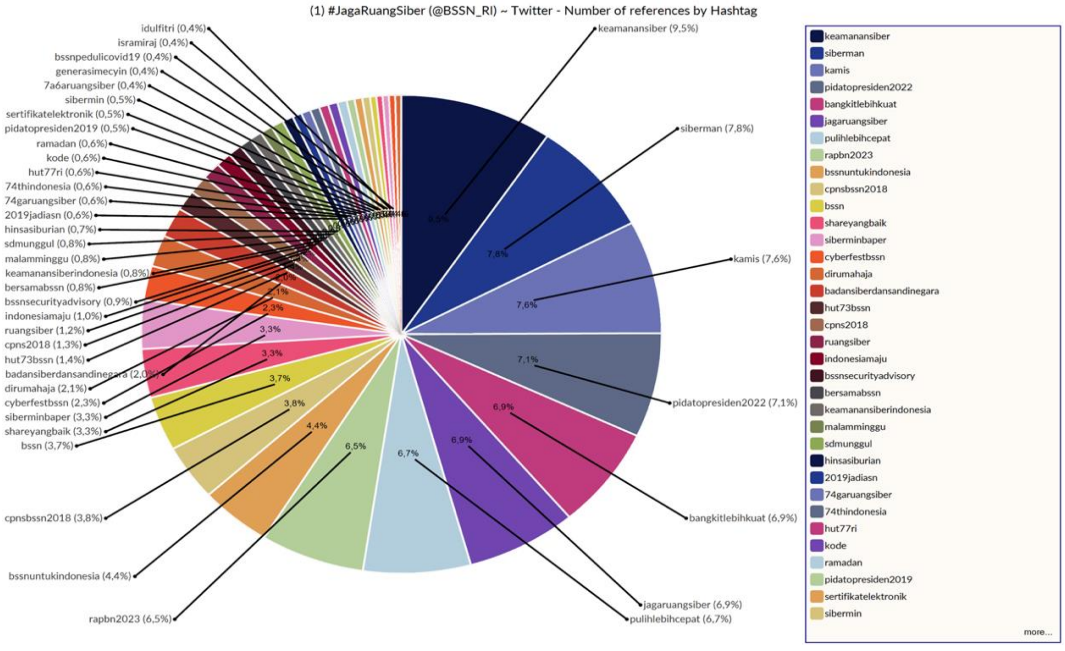

Fig. 6. Supporting Hashtag –along with tweets #JagaRuangSiber (@BSSN_RI)
Source: NVivo Analysis

The spread of the campaign to minimize cybercrime has been carried out by the National Cyber and Crypto Agency via the Twitter account @BSSN_RI, there have been several attempts at tweets, which have also included the use of hashtags. This posts, in turn, circulate more effectively and provide separate concerns for Twitter users to pay attention to. As shown in Figure 6, the use of the hashtag is echoed by the @BSSN_RI Twitter account and also gives the meaning of hashtags such as *#keamanansiber* (9.2%), which is cyber security. Then there is *#siberman* (7.8%), which is the name given by the admin for Twitter users who are concerned about reading and seeing tweets that have been echoed. On the other hand, there are hashtags *#kamis* (7.6%), #pidatoprisiden2022 (7.1%). There is also *#bangkitlebihpulih* (6.9%), which gives confidence to users, and there is also the use of the hashtag *#jagruangsiber* (6.9%), which is an effort to maintain cyberspace in its use and activities. There is a hashtag *#pulihlebihcepat* (6.7%) related to the recovery of the COVID-19 pandemic. And a few other hashtag attempts are also used. On the basis of Figure 7, which showed the National Cyber and Crypto Agency's efforts in the cybercrime prevention campaign on Twitter, posters and tweets with hashtags have been reported. The results of the campaign's information dissemination have been broadcast by hundreds to thousands of users, but few Twitter users retweet and comment on each post.

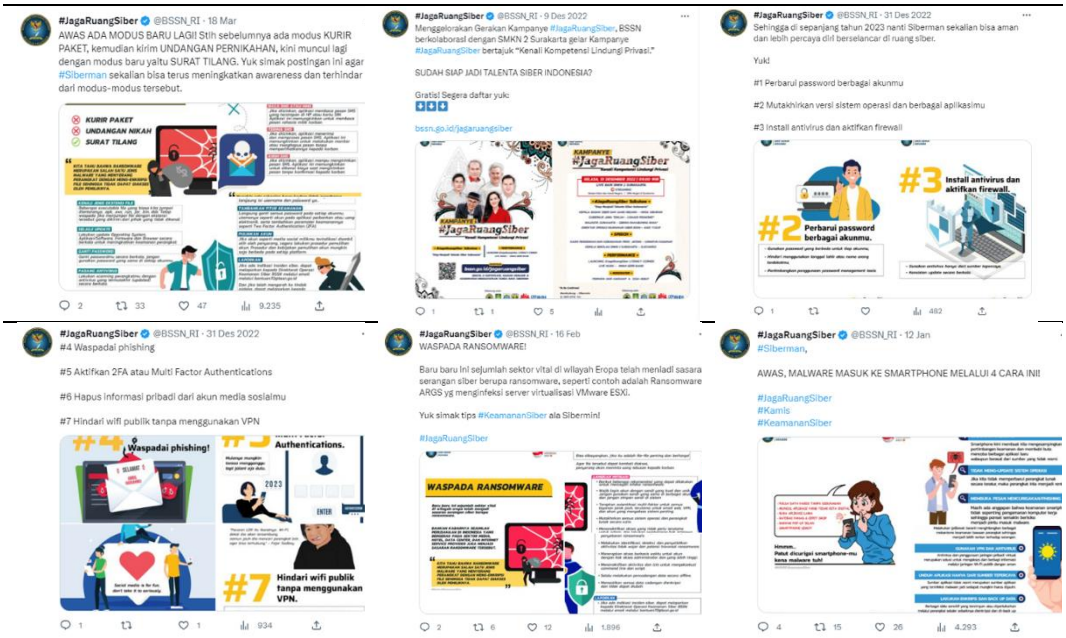

Fig. 7. The Example of Tweets Cybercrime Prevention Campaign Distribution.
Source: @BSSN_RI Twitter Account

4.4. Sociogram Distribution Analysis

Sociometric analysis is one of the efforts to explore network activity from its distribution. Where the sociogram can see the connection between one user and another based on retweets and/or mentions by the user who posted. In this study, one of the efforts to see the distribution network of cyberspace guard campaigns on Twitter can be analyzed. The

campaign to protect cyberspace by the @BSSN_RI has a fairly wide network, and there are efforts to tweets that mention other Twitter users. There are some striking users Tweets from Figure 8, of which *@jokowi* and *@BSrE_ID* are the accounts most mentioned by @BSSN_RI in line with cybercrime prevention campaign efforts. Apart from that, *@musiumsandiina* has been targeted to launch the campaign. Moreover, several accounts of government-owned Twitter social media users, political officials, celebrities, and embassy accounts of other countries (*@DubesAustralia*) have been used as colaborative posts for cybercrime prevention campaigns.

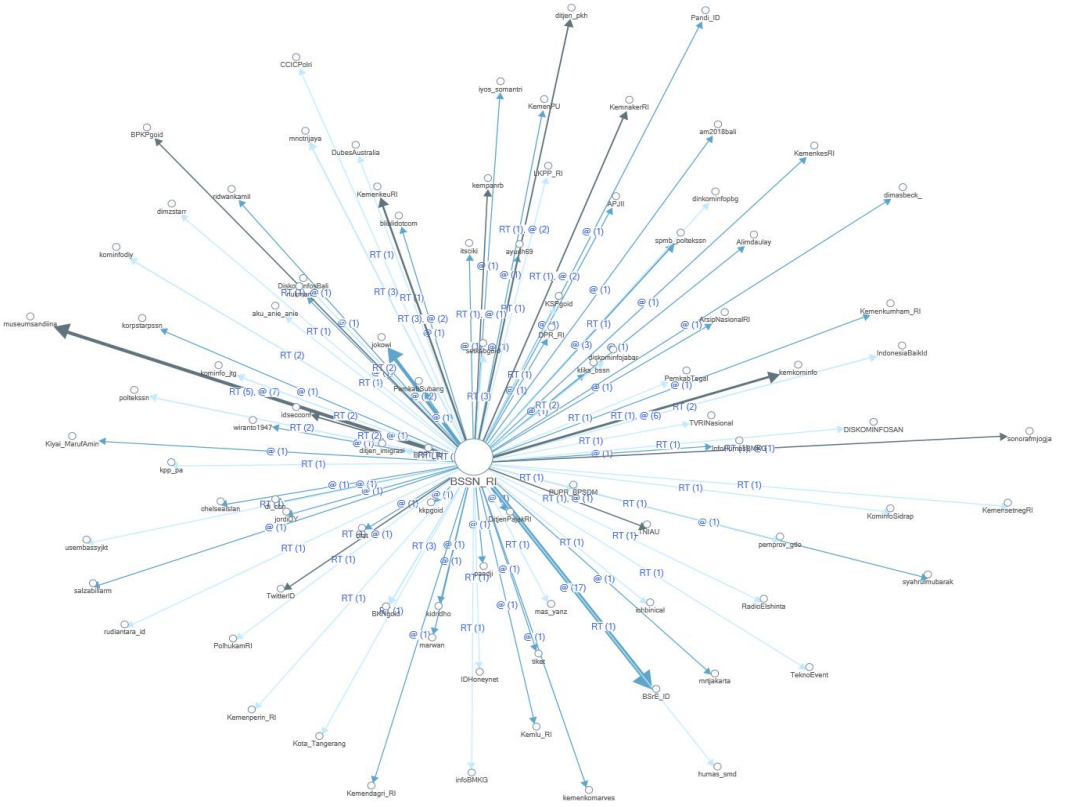

Fig. 8. Twitter Sociogram Analysis from @BSSN_RI Twitter account
Source: NVivo

To begin with, in today's technological era, there are more crimes that threaten users through cybercrime [59]. This is in line with the growing use of the internet as a source of information and communication, which presents an opportunity for cybercrime. Therefore, activities, currently, have shifted to the digital domain as a result of the massive expansion of the use of computers and internet networks; thus, digital societies must increase their awareness of information control and privacy security [6]. In sum, this raises concerns about privacy and the necessary protection of personal data; therefore, the role of government authorities is crucial and needed to increase cyber security awareness. Additionally, in light of the fact that the more citizen activities move (even partially) into cyberspace, the more vulnerabilities are created and more opportunities for malicious cyber

operations, therefore, cyber security should be a central component of every policy, program, initiative, and activity [18]. For instance, in the Indonesian case, the government, through the National Cyber and Crypto Agency (*Badan Siber dan Sandi Negara*), has attempted to carry out an advocacy campaign to protect cyberspace via social media such as Twitter. This campaign aims to increase awareness of the importance of protecting information. In which the importance of protecting personal data is necessary, along with cybercrime attacks that do not only stalk users data; they even have financial implications that can cause loss of life [60]. The large number of cybercrime cases in Indonesia is significant and troubling the citizens [61]. As of this case, the government took more action, resulting in the announcement of Indonesian Law No. 11 of 2008 concerning information and electronic transactions and Law Number 19 of 2016 concerning amendments to Law Number. 11 of 2008 relating to data and electronic commerce. This regulation does not, however, apply to all crimes that take place [62]. In addition, efforts by the government to guarantee improvements in cyber security protection in realizing information stability [63] from all threats [64]. Moreover, the President of the Republic of Indonesia signed Presidential Regulation No. 28 of 2021 concerning the National Cyber and Crypto Agency (BSSN) on April 13, 2021, in the context of realizing national cyber security, protection, and sovereignty and increasing national economic growth [65].

Within the wide variety of cybercrimes, many types are becoming more complicated regarding prosecution and the legal basis. Cybercriminal's package themselves with anonymous accounts, making it difficult to track. In fact, there is a need for cyber law to be necessary; for example, in India, they have called for the availability of cyber law [66]. On the other hand, it is not uncommon for users from different countries to commit cybercrimes, making this crime serious and necessitating cooperation between governments to protect internet users. Thus, taking action can accelerate cybercrime justice [67]. Therefore, every government in every country/state and within a country needs to increase coordination and cooperation as well as capacity-building efforts to fight cybercrime [68]. Besides, there is a need for active campaigns to launch to fight and prevent cybercrime, such as campaigns through social media to make the public aware of cybercrimes, as the National Cyber and Crypto Agency has made efforts to do. However, the @BSSN_RI account is nothing more than an account that disseminates information about campaigns, like other government accounts. Therefore, social media is a tool for information dissemination [69], not a way to make decisions about the pressures and threats experienced by users.

5. Conclusion

In recent years, social media platforms have become an arena for government authorities to disseminate information, as in the case of the National Cyber and Crypto Agency of the Republic of Indonesia, to distribute cyberspace guard campaigns to prevent cybercrime. This study analyzes a collection of tweets and retweets posted on Twitter (@BSSN_RI) in this way. The analysis by NVivo outlines some information dissemination trends that BSSN RI uses, including narratives and images with hashtags. It also emphasizes the existence of other Twitter users, such as central and regional governments, television stations, celebrity influencer, politicians, and politicians campaigning to protect cyberspace. Based on these results, the cyberspace protection campaign has reached users

from diverse backgrounds. It may indicate that Twitter users have retained the disseminated information, thus raising their awareness of the significance of cybercrime prevent.

This study also demonstrates that the @BSSN_RI Twitter account distributes a prevalent set of keywords. In addition to a component of the intensity of information disseminated over the Cyberspace Guard campaign decreasing, many tweets that are unconnected to the campaign are linked to narrative tweets associated with the campaign. Hence, the collection of circulating tweets remains combined with irrelevant posts. Consequently, this has the potential to produce equivocal analyses of the information collected and requires restraint when replying to campaigns that are echoed on social media platforms such as Twitter. Given a shortage of literature on Twitter accounts as an outlet of information and interaction for legislative decision-making, it is recommended that further study be conducted on discursive research in decision-making discourse.

References

[1] Jackson, M., Brennan, L., Parker, L. (2021), *The public health community's use of social media for policy advocacy: a scoping review and suggestions to advance the fiel*d, Public Health, vol. 198, pp. 146–155, doi: https://doi.org/10.1016/j.puhe.2021.07.015.

[2] Choi, M., McKeever, B. (2022), *Social media advocacy and gun violence: Applying the engagement model to nonprofit organizations' communication efforts*, Public Relat. Rev., vol. 48, no. 2, p. 102173, doi: https://doi.org/10.1016/j.pubrev.2022.102173.

[3] Figenschou, T. U., Fredheim, N. A. (2012), *Interest groups on social media: Four forms of networked advocacy*, J. Public Aff., vol. 20, no. 2, 2020, doi: 10.1002/pa.2012.

[4] Ciszek, E. L. (2017), *Advocacy Communication and Social Identity: An Exploration of Social Media Outreach*, J. Homosex., vol. 64, no. 14, pp. 1993–2010, doi: 10.1080/00918369.2017.1293402.

[5] Vrabie, C. (2017), *O operatiune cu stil – The Flame*, Smart Cities Int. Conf. Proc., vol. 5, pp. 161–172.

[6] Vrabie, C. (2021), *Privacy versus Security – scenarios over Smart Societies*, Int. Conf. E-bus. Technol., vol. 1, no. 1, pp. 167–171.

[7] Yuan, Y. P., Dwivedi, Y. K., Tan, G. W. H., Cham, T. H., Ooi, K. B., Aw, E. C. X., & Currie, W. (2023), *Government Digital Transformation: Understanding the Role of Government Social Media*, Government Information Quarterly, 40(1), 101775, doi: 10.1016/j.giq.2022.101775.

[8] Vrabie, C. (2015), *Convergența securității digitale,* Smart Cities Int. Conf. Proceeding, vol. 3, pp. 267–277.

[9] Hawdon, J. (2021), *Cybercrime: Victimization, Perpetration, and Techniques*, Am. J. Crim. Justice, vol. 46, no. 6, pp. 837–842, doi: 10.1007/s12103-021-09652-7.

[10] Ngo, F. T. (2018), *Cybercrime*, in The SAGE Encyclopedia of the Internet, Thousand Oaks,: SAGE Publications, Inc., doi: 10.4135/9781473960367 NV - 3.

[11] Vrabie, C. (2016), *Libertatea ta începe unde se termină intimitatea mea*, Smart Cities Int. Conf. Proc., vol. 4, pp. 135–147.

[12] Tomulescu, C. (2021), *Cyberbiosecurity. A Short Review*, Smart Cities Int. Conf. Proc., vol. 9, pp. 393–410.

[13] Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021), *Phishing Attacks: A Recent Comprehensive Study and a New Anatomy*, Front. Comput. Sci., vol. 3, no. March, pp. 1–23, doi: 10.3389/fcomp.2021.563060.

[14] Back, S., Guerette, R. T. (2021), *Cyber Place Management and Crime Prevention: The Effectiveness of Cybersecurity Awareness Training Against Phishing Attacks*, J. Contemp. Crim. Justice, vol. 37, no. 3, pp. 427–451, doi: 10.1177/10439862211001628.

[15] Kemp, S. (2023), *Exploring public cybercrime prevention campaigns and victimization of businesses: A Bayesian model averaging approach*, Comput. Secur., vol. 127, p. 103089, doi: 10.1016/j.cose.2022.103089.

[16] Curtis, J., Oxburgh, G. (2022), *Understanding cybercrime in 'real world' policing and law enforcement*, *Police J. Theory, Pract. Princ.*, doi: https://doi.org/10.1177/0032258X221107584.

[17] Rahmat, A. F., Mutiarin, D., Pribadi, U., & Rahmawati, E. (2022), *Overseeing Cyber-Neighborhoods:*

How Far the Indonesian National Police Effort in Handling Cybercrime?, in International Conference on Public Organization, vol. 209, no. Iconpo 2021, pp. 549–555.
[18] Codreanu, C. M. (2021), *Digital democracy in Peril . Safeguarding e-democracy by boosting cybersecurity*, Smart Cities Int. Conf. Proc., vol. 9, pp. 461–474, 2021.
[19] Drury, B., Drury, S. M., Rahman, M. A., & Ullah, I. (2022), *A social network of crime: A review of the use of social networks for crime and the detection of crime*, Online Soc. Networks Media, vol. 30, no. April, p. 100211, doi: 10.1016/j.osnem.2022.100211.
[20] Soomro, T. R., Hussain, M. (2019), *Social Media-Related Cybercrimes and Techniques for Their Prevention*, Appl. Comput. Syst., vol. 24, no. 1, pp. 9–17, doi: 10.2478/acss-2019-0002.
[21] Bossler, A. M., Berenblum, T. (2019), *Introduction : new directions in cybercrime research*, J. Crime Justice, vol. 42, no. 5, pp. 495–499, doi: 10.1080/0735648X.2019.1692426.
[22] Baror, S. O., Venter, H. (2019), *A taxonomy for cybercrime attack in the public cloud*, 14th Int. Conf. Cyber Warf. Secur. ICCWS 2019, no. September, pp. 505–515.
[23] Statista, *Countries with the biggest share of internet users in Asia as of July 2022, by country*. New York, United States: Statista Inc., https://www.statista.com/statistics/272358/distribution-of-internet-users-in-asia-pacific-by-country/, date: 2023.
[24] Seasia.co, *Southeast Asian Countries Cybersecurity Index (2022)*, https://seasia.co/2022/09/19/southeast-asian-countries-cybersecurity-index-2022, date: 2023.
[25] Control, J., Galinec, D., Možnik, D., & Guberina, B. (2018), *Cybersecurity and cyber defence : national level strategic approach*, *Automatika*, vol. 1144, doi: 10.1080/00051144.2017.1407022.
[26] Chatterjee, S., Kar, A. K., Dwivedi, Y. K., & Kizgin, H. (2019), *Prevention of cybercrimes in smart cities of India: from a citizen's perspective*, Inf. Technol. People, vol. 32, no. 5, pp. 1153–1183, doi: 10.1108/ITP-05-2018-0251.
[27] Tang, Z., Miller, A. S., Zhou, Z., & Warkentin, M. (2021), *Does government social media promote users' information security behavior towards COVID-19 scams? Cultivation effects and protective motivations*, Gov. Inf. Q., no. January, doi: 10.1016/j.giq.2021.101572.
[28] Nowacki, J., Willits, D. (2020), *An organizational approach to understanding police response to cybercrime*, Policing, vol. 43, no. 1, pp. 63–76, doi: 10.1108/PIJPSM-07-2019-0117.
[29] Tabi, C., Hewage, C., Bakhsh, S. T., Ukwandu, E. (2023), *Contemporary Issues in Child Protection: Police Use of Artificial Intelligence for Online Child Protection in the UK*, in Digital Transformation in Policing: The Promise, Perils and Solutions, R. Montasari, V. Carpenter, and A. J. Masys, Eds. Cham: Springer International Publishing, pp. 85–107. doi: 10.1007/978-3-031-09691-4_5.
[30] Beshears, M. L. (2017), *Effectiveness of Police Social Media Use*, Am. J. Crim. Justice, vol. 42, no. 3, pp. 489–501, doi: 10.1007/s12103-016-9380-4.
[31] Wang, S. Y. K., Hsieh, M. L., Chang, C. K. M., Jiang, P. S., & Dallier, D. J. (2021), *Collaboration between Law Enforcement Agencies in Combating Cybercrime: Implications of a Taiwanese Case Study about ATM Hacking*, Int. J. Offender Ther. Comp. Criminol., vol. 65, no. 4, pp. 390–408, doi: 10.1177/0306624X20952391.
[32] Cross, C. (2021), *Dissent as cybercrime: social media, security and development in Tanzania*, J. East. African Stud., vol. 15, no. 3, pp. 442–463, doi: 10.1080/17531055.2021.1952797.
[33] Dupont, B., Holt, T. (2022), *The Human Factor of Cybercrime*, Soc. Sci. Comput. Rev., vol. 40, no. 4, pp. 860–864, doi: 10.1177/08944393211011584.
[34] Dupont, B., Whelan, C. (2021), *Enhancing relationships between criminology and cybersecurity*, J. Criminol., vol. 54, no. 1, pp. 76–92, doi: 10.1177/00048658211003925.
[35] Yun, G. W., Morin, D., Park, S., Joa, C. Y., Labbe, B., Lim, J., ... & Hyun, D. (2016), *Social media and flu: Media Twitter accounts as agenda setters*, International journal of medical informatics, 91, 67-73, doi: 10.1016/j.ijmedinf.2016.04.009.
[36] Statista, *Leading countries based on number of Twitter users as of January 2022 (in millions)*, https://www.statista.com/statistics/242606/number-of-active-twitter-users-in-selected-countries/, date: 2022.
[37] World Population Review, *Twitter Users by Country 2023*, https://worldpopulationreview.com/country-rankings/twitter-users-by-country, date: 2023.
[38] Anusha, A., Singh, S. (2015), *Is that twitter hashtag worth reading*, in ACM International Conference Proceeding Series, vol. 10-13-Augu, pp. 272–277. doi: 10.1145/2791405.2791526.
[39] Daneshjou, R., Shmuylovich, L., Grada, A., & Horsley, V. (2021), *Research Techniques Made Simple: Scientific Communication using Twitter*, J. Invest. Dermatol., vol. 141, no. 7, pp. 1615-1621.e1, doi:

10.1016/j.jid.2021.03.026.
[40] Depaula, N. (2018), *#Supporting the Cause : An Analysis of How Government Agencies Use Twitter Hashtags*, pp. 788–789, doi: 10.1002/pra2.2018.14505501117.
[41] Tsaruk, O., Korniiets, M. (2020), *Hybrid nature of modern threats for cybersecurity and information security*, Smart Cities Reg. Dev. J., vol. 4, no. 1, pp. 57–78. Available: https://econpapers.repec.org/RePEc:pop:journl:v:4:y:2020:i:1:p:57-78
[42] Weulen Kranenbarg, M., Holt, T. J., van Gelder, J.-L. (2019), *Offending and Victimization in the Digital Age: Comparing Correlates of Cybercrime and Traditional Offending-Only, Victimization-Only and the Victimization-Offending Overlap*, Deviant Behav., vol. 40, no. 1, pp. 40–55, doi: 10.1080/01639625.2017.1411030.
[43] Weulen Kranenbarg, M. (2022), *When do they offend together? Comparing co-offending between different types of cyber-offenses and traditional offense*s, Comput. Human Behav., vol. 130, no. May 2021, p. 107186, doi: 10.1016/j.chb.2022.107186.
[44] Mikkola, M., Ellonen, N., Kaakinen, M., Savolainen, I., Sirola, A., Zych, I., ... & Oksanen, A. (2022), *Cyberharassment victimization on three continents: an integrative approach*, International journal of environmental research and public health, 19(19), 12138., doi: 10.3390/ijerph191912138.
[45] Velasco, C. (2022), *Cybercrime and Artificial Intelligence. An overview of the work of international organizations on criminal justice and the international applicable instruments*, ERA Forum, vol. 23, no. 1, pp. 109–126, doi: 10.1007/s12027-022-00702-z.
[46] Arwana, Y. C. (2022), *Victims of Cyber Crimes in Indonesia: A Criminology and Victimology Perspective*, Semarang State Univ. Undergrad. Law Soc. Rev., vol. 2, no. 2, pp. 181–200, 2022, doi: 10.15294/lsr.v2i2.53754.
[47] Sharma, A., Bhatnagar, D. (2020), *A Study of Need for Police Reforms in India in Cyber Crime Manner*, vol. 10, no. 7, pp. 26800–26804.
[48] Robalo, T. L. A. S., Abdul Rahim, R. B. B. (2023), *Cyber Victimisation, Restorative Justice and Victim-Offender Panels*, Asian J. Criminol., vol. 18, no. 1, pp. 61–74, doi: 10.1007/s11417-023-09396-9.
[49] Kagita, M. K., Thilakarathne, N., Gadekallu, T. R., Maddikunta, P. K. R., & Singh, S. (2021), *A Review on Cyber Crimes on the Internet of Things*, in Deep Learning for Security and Privacy Preservation in IoT, A. Makkar and N. Kumar, Eds. Singapore: Springer Singapore, pp. 83–98. doi: 10.1007/978-981-16-6186-0_4.
[50] Drew, J. M. (2020), *A study of cybercrime victimisation and prevention: exploring the use of online crime prevention behaviours and strategies*, J. Criminol. Res. Policy Pract., vol. 6, no. 1, pp. 17–33, doi: 10.1108/JCRPP-12-2019-0070.
[51] Pepper, I., Rogers, C., Martin, H. (2020), *Evidence based policing: a view on its development within the police service*, J. Work. Manag., vol. 12, no. 1, pp. 91–96, doi: 10.1108/JWAM-01-2020-0001.
[52] Marttila E., Koivula A., Räsänen P. (2021), *Cybercrime Victimization and Problematic Social Media Use: Findings from a Nationally Representative Panel Study*, Am. J. Crim. Justice, vol. 46, no. 6, pp. 862–881, doi: 10.1007/s12103-021-09665-2.
[53] Nosál, J. (2023), *Crime in the Digital Age: A New Frontier*, in The Implications of Emerging Technologies in the Euro-Atlantic Space, J. Berghofer, A. Futter, C. Häusler, M. Hoell, and J. Nosál, Eds. Cham: Springer International Publishing, pp. 177–193. doi: 10.1007/978-3-031-24673-9_11.
[54] Saleous, H., Ismail, M., AlDaajeh, S. H., Madathil, N., Alrabaee, S., Choo, K. K. R., & Al-Qirim, N. (2022), *COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities*, Digital Communications and Networks., doi: https://doi.org/10.1016/j.dcan.2022.06.005.
[55] Buono, L. (2014), *Fighting cybercrime through prevention, outreach and awareness raising*, ERA Forum, vol. 15, no. 1, pp. 1–8, doi: 10.1007/s12027-014-0333-4.
[56] Gupta, R. M.,. Mathur, P, Nanda, R. (2022), *Cyber Security Threat, it's Risks and Susceptibilities, in the Global Perspective*, in Rising Threats in Expert Applications and Solutions, pp. 607–613.
[57] Dutta, N., Jadav, N., Tanwar, S., Sarma, H. K. D., & Pricop, E. (2022), *Importance of Cyberlaw*, in Cyber Security: Issues and Current Trends. Studies in Computational Intelligence, N. Dutta, N. Jadav, S. Tanwar, H. K. D. Sarma, and E. Pricop, Eds. Singapore: Springer Singapore, pp. 159–174. doi: 10.1007/978-981-16-6597-4_9.
[58] Szczepaniuk, E. K., Szczepaniuk, H. (2022), *Analysis of cybersecurity competencies: Recommendations for telecommunications policy*, Telecomm. Policy, vol. 46, no. 3, p. 102282, doi: 10.1016/j.telpol.2021.102282.
[59] Berlian, C., *Kejahatan Siber Yang Menjadi Kekosongan Hukum*, J. equitable, vol. 5, no. 2, pp. 1–20,

2020, doi: https://doi.org/10.37859/jeq.v5i2.2532.
[60] Alzubaidi, A. (2021), *Measuring the level of cyber-security awareness for cybercrime in Saudi Arabi*a, Heliyon, vol. 7, no. 1, p. e06016, doi: 10.1016/j.heliyon.2021.e06016.
[61] Arianto A. R., Anggraini G. (2019), *Membangun Pertahanan Dan Keamanan Siber Nasional Indonesia Guna Menghadapi Ancaman Siber Global Melalui Indonesia Security Incident Response Team On Internet Infrastructure (ID-SIRTII)*, J. Pertahanan Bela Negara, vol. 9, no. 1, pp. 13–30.
[62] Situmeang, A., Girsang, J. (2022), *Efektivitas Undang-Undang Ite Dalam Menangani Ujaran Kebencian Melalui Media Sosial Di Kota Batam*, J. Pendidik. Kewarganegaraan Undiksha, vol. 10, no. 3, pp. 83–100, 2022, doi: https://doi.org/https://doi.org/10.23887/jpku.v10i3.51205.
[63] Suryaningrum, F. (2021), *Efektivitas Penegakan Hukum Patroli Siber di Media Sosial*, LoroNG Media Pengkaj. Sos. Budaya, vol. 10, no. 2, pp. 121–132, doi: 10.18860/lorong.v10i2.966.
[64] Ginanjar, Y. (2022), *Strategi Indonesia Membentuk Cyber Security Dalam Menghadapi Ancaman Cyber Crime Melalui Badan Siber Dan Sandi Negara*, J. Din. Glob., vol. 7, no. 02, pp. 291–312, 2022, doi: 10.36859/jdg.v7i02.1187.
[65] Chotimah, H. C. (2019), *Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara [Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency]*, J. Polit., no. Vol 10, No 2 (2019): Jurnal Politica November 2019, pp. 113–128.
[66] Sen, A., Jena, G., Jena, S., & Devabalan, P. (2022), *A Case Study on Defending against Cyber Crimes*, J. Pharm. Negat. Results, vol. 13, no. 1, pp. 1931–1938, doi: 10.47750/pnr.2022.13.S01.229.
[67] Nugroho A., Chandrawulan A. A. (2022), *Research synthesis of cybercrime laws and COVID-19 in Indonesia: lessons for developed and developing countries*, Secur. J., no. 0123456789, doi: 10.1057/s41284-022-00357-y.
[68] UNODC (2021), *Cybercrime and COVID19 in Southeast Asia: an evolving picture*, United Nations Off. Drugs Crime, no. May 2021, pp. 2–4.
[69] Idris, I. K. (2018), *Government social media in Indonesia: Just another information dissemination tool*, J. Komun. Malaysian J. Commun., vol. 34, no. 4, pp. 337–356, doi: 10.17576/JKMJC-2018-3404-20.