https://doi.org/10.18196/jhi.v11i2.13932

JURNAL HUBUNGAN INTERNASIONAL
VOL. 11, NO. 2 (2023)

Combating Cybercrime and Cyberterrorism in Indonesia

Cynthia Shafira Hartati
Master Program of International Relations, Universitas Muhammadiyah Yogyakarta, Indonesia
cynthia.s.psc20@mail.umy.ac.id
Ali Muhammad
Department of International Relations, Universitas Muhammadiyah Yogyakarta, Indonesia
alimuhammad@umy.ac.id
Submitted: 29 July 2022; Revised: 8 December 2022; Accepted: 17 December 2022

Abstrak

Fenomena kejahatan siber merupakan ancaman keamanan yang semakin nyata bagi Indonesia. Kejahatan siber yang sangat meruyak mengindikasikan bahwa perlunya pengefektifan dari implikasi regulasi dalam menangani cybercrime. Representasi dari tujuan penelitian yang akan dieaborasi oleh peneliti yaitu bagaimana Pihak pemerintah mengefektifkan regulasi yang merujuk kepada problematika terkait dengan menjaga sekuritisasi di bidang siber. Penulis menggunakan metode penelitian deskriptif kualitatif untuk menelaah signifikasi dari peraturan perundang-undangan yang memiliki interkorelasi yang sangat tinggi terhadap dampak dari kejahatan siber yang ada di Indonesia. Fenomena aksi teror baik yang dilakukan secara teritorial maupun yang bermaharajalela di dunia digital meningkat sangat pesat. Dampak dari kemudahan akses atas seluruh data-data yang esensial dalam berbagai lini kehidupan mempunyai berbagai macam motif seperti penyebarluasan propaganda untuk meynyebarluaskan jaringan kejahatan siber.Perlunya tingkat disrupsi yang tinggi untuk menanggulangi fenomena terorisme siber untuk menciptakan kondisi keamanan Indonesia yang kondusif. Adanya kontribusi yang tinggi dan sinergitas dari berbagai lini kenegaraan yaitu pemerintah serta masyarakat akan mempengaruhi keefektifan dari regulasi yang diterapkan di indonesia.
Kata Kunci: Pemerintahan, Penaggulangan, Kejahatan Siber, Indonesia

Abstract

Cybercrime poses a serious risk to national security in Indonesia. The pervasive nature of cybercrime calls into question the efficacy of current regulatory measures. The study objective reflects how the government addresses sustaining securitization in cyberspace. This study employed a descriptive qualitative method to analyze the impact of cybercrime in Indonesia and the regulations with an extremely high intercorrelation. Terrorism, both on the ground and digitally, has been on the rise at an alarming rate in recent years. The influence of universal access to all relevant information has several implications, including the propagation of misinformation and the growth of cybercrime networks. There must be significant disruption to the cyberterrorism industry to foster safe circumstances in Indonesia. The success of Indonesia's regulatory efforts depends on the contribution and synergy between the government and the public.
Keywords: Governance, policy, cybercrime, Indonesia

INTRODUCTION

Today's cyberspace is unlimited by the presence of national borders and time, causing the dependency on modern technology to grow in terms of development statistics. Hence, widespread cybercrime illustrates the relevance of rising trend. Unfortunately, modern civilization still heavily relies on hardware and software developed a century ago; spreading out across vast distances makes it impossible to leave no digital footprints (Svecova & Blazek, 2021). The necessary regulations to predict and prevent cybercrime are tangible steps by policymakers as a catalyst for change in lowering the graph of cybercrime, rather than only focusing on the euphoria of political programs at a specific period as a method to win people's voices in global politics (Dlamini & Mbambo, 2019).

Preventative measures are the driving force in the fight against the global spread of cybercrime, unaffected by geographic or temporal boundaries (Galis & Summerton, 2018). Oversharing in cyberspace can be prevented by various public awareness campaigns and other preventative measures (Leukfeldt et al., 2019).

Society's reliance on the digital world entails several actions in uploading personal data at a more macro level, such as formulating regulations, and large-scale businesses are fundamentally crucial for the efficacy of regulations on cybercrime (Harkin & Whelan, 2019). Cybercrime, of course, is not only an issue of the unseen world but a perfectly reasonable argument (Horgan et al., 2020). The perpetrators of cybercrime have adopted the moral gradation that the regulations covering immoral acts are only pseudo-regulations. Thus, the accumulation of cybercrime cannot be terminated simply by updating regulations; rather, they are more concerned with affirming the follow-up of cybercrime (Millman et al., 2017).

Policymakers should not continue a conservative culture to eradicate cases if cybercrime has happened, and this contradictory aspect of society that cannot be avoided from online activities should be taken into account. Non-optimal execution of cybercrime rules possesses macro-destructive effects in many different areas, including state security, health, finance, education, and even immoral activities (Hull et al., 2018). Explicit narratives cannot halt the negative effects of cyber growth to continue altering regulations without keeping up with the advancement in the digital world and cyber loopholes (Moubayed et al., 2017). Policymakers, as change catalysts, are at the forefront of efforts to eliminate all forms of crime, including those committed online.

A priori, cybercriminals view pseudo-regulation that fails to quickly eradicate cybercrime as encouraging the formation of more extensive crime patterns and the involvement of an increasing number of parties, including those from outside the traditional spheres of politics and business, in pursuit of financial gain (Romanosky et al., 2019). However, it is not solely the role of policymakers to raise public awareness of cybercrime; rather, it is a collaborative effort across communities to vet any news before it is disseminated, rather than allowing themselves to be lulled to sleep by the abundance of social media tools (Nicholson et al., 2012). T-Mobile, a mobile service provider, has been the victim of several hacks. This fact has lessened the company's sense of urgency when dealing with cybercrime. Close to 13,000,000 users' private information is stored on this network. In addition, 40,000,000 users enrolled in 2021, specifically in August. This service has been the target of a string of four separate cyber attacks. More than 2,500,000 users had their information compromised in a single year in 2018. Then, in 2020, there were two other cyber attacks of a similar nature.

The threat of cybercrime evolving into cyberterrorism is a major issue nowadays (Abdullah, 2019). Terrorism in cyberspace and terror in actions such as raising public opinion riots become the forerunner of the outbreak of cyberterrorism in regional domains like the Unitary State of the Republic of Indonesia (NKRI), possessing cultural diversification and political interests. Information on official government sites and personal data are both susceptible to hackers because of cybersecurity flaws (Hovorushchenko et al., 2020). When the economic foundation of a state is breached, it can have far-reaching consequences (Williams et al., 2013).

The purpose of implementing articles 33 and 34 of the 1945 Constitution is to ensure national security based on the security of territory, food and shelter, and the economic system. People should be less likely to give in to provocation and join the offenders if they believe the economy is secure. Cybercrime is motivated by discontent with the effectiveness of official initiatives to address problems of many types. When criminals have easy access to mobilization for the growth of issues with the goal of destroying the unity of a nation, they are more likely to commit acts of cybercrime that lead to a chain reaction of other criminal cases, such as cyberterrorism (Sakban et al., 2019).

The increasing reliance of modern society on digital resources leaves all digital world activities open to hacking by cybercriminals. Data thieves in cyberspace can quickly gain access to sensitive information by targeting a specific location (Sitorus & Tannady, 2021). Micro-destructive phases, such as disagreements between several parties, can easily snowball into macro-destructive stages, threatening national security worldwide (Santhoshi et al., 2019).

The various worldwide initiatives in cyberspace are inseparable from cyberterrorism (Whelan, 2021). As indicated in the analysis inquiry, cybersecurity must be bolstered by rigorous regulations in dealing with cases of cybercrime and cyberterrorism, which is critical for policymakers to consider when formulating effective policies linked to cybercrime handling (Sharma et al., 2016). Numerous studies in this field have demonstrated the critical necessity for cybersecurity-focused regulations of the cybercrime industry.

A book titled "The Global Cybercrime Industry" discusses factors that might initiate terrorist attacks (Kshetri, 2010). The state must carefully consider the digital and physical aspects of national security. Cyberterrorism is a real problem that might destabilize Indonesia. To ensure that the spread of excessive propaganda does not shake the people of a country's sense of national pride, the stability of the state depends on the confidence that its citizens have in their government's ability to enforce effective regulations regarding the investigation and prosecution of criminal offenses (Huey & Rosenberg, 2013).

Cybercrime is rising at 23% annually, as seen by the graph of cumulative growth in cyberterrorism (Beech & Bishop, 2017). The complexity of the digital world is heightened because IP addresses in Indonesia are frequently the target of cyber attacks. Over 6,000 sites have been compromised in the cyber assault, slowing down the real estate and business sectors (Horsman, 2017). This occurrence also depicts that suitable and effective regulations should be enacted with strong synergy with the capacity to identify cybercrime by intelligence agencies to monitor cybercrime that will spread to produce cyberterrorism (Rabadão, 2013).

The Regulations of the Criminal Code Bill detail the execution of preventative measures against cyberterrorism. The proposed Criminal Code Amendments for 2019 contain many enumerated lists of essential requirements for criminal acts directly connected to cyberterrorism.

336: Accessing computers and/or electronic systems in any way without rights, with the intention of obtaining, changing, destroying, or eliminating information on computers and/or electronic systems

337: Accessing computers and/or electronic systems without rights, which causes disturbance or harm to the state and/or relations with international legal subjects

338: Accessing computers and/or electronic systems without the rights to obtain, modify, destroy, or eliminate information belonging to the government which, due to its status, must be kept confidential or protected

339: Accessing computers and/or electronic systems without rights, with the intention of gaining profit or obtaining financial information from the Central Bank, banking institutions or financial institutions, credit card issuers, or payment cards or containing customer report data

Cyber governance in Indonesia is not simply artificial regulation, as seen by the adoption of recent laws on cybercrime, such as (1) the Bali bombing incident on October 12, 2002, which prompted the Indonesian Government to issue Regulation of the Government of the Republic of Indonesia No. 1 of 2002 on the Eradication of Criminal Acts of Terrorism. International cooperation with other countries in the field of intelligence, police, and further technical cooperation related to acts of combating terrorism is carried out by the Indonesian Government in preventing and eradicating criminal acts of terrorism following the provisions of the applicable regulations. (2) Human Rights and Law Enforcement Guidance for the Investigation and Prosecution of Terrorist Crime (Through Revision of Law No. 15 of 2003 concerning Eradication of Criminal Acts of Terrorism).

There is no incompatibility between the execution of intelligence missions and the prosecution of the terrorist-related crime in Indonesia, both of which have been the subject of recent regulatory efforts. Maintaining continuity between the regulations and the parties responsible for enforcing them creates good synergy with each revision to the regulations. It is illustrated by the circumstances surrounding the Bali Bombing I and the Bali Bombing II at the Australian Embassy and Hotel JW Marriott inextricably interrelated.

LITERATURE REVIEW

According to the Understanding Cyberterrorism: The Grounded Theory Method Applied journal, previous studies did not describe specifically and comprehensively the implementation of cyberterrorism regulatory governance (Ahmad et al., 2012). Hence, this research's novelty, often known as the renewal structure, is unique. This study discovered insufficient evidence for a continuous body of regulations to be put in place as a sort of preventative action against the antecedents of cyberterrorism (Galis & Summerton, 2018). Supporters of Ole Waiver and Barry Buzan's notion of securitization theory as a medium, among others, are integral to the interconnectedness of this study. Human security, the focus of this research, significantly impacts Indonesia's massive infrastructure if cybersecurity incidents are not reduced.

Ole Weaver's securitization theory, like Barry Buzan's, has continuity with security theory in fields beyond finance, including ecology, politics, health, and even food (Beech & Bishop, 2017). According to this justification, which shapes the subjectivity of securitization theory, cyberterrorism can be prevented by safeguarding the security and resilience of states, both physically and digitally (Horgan et al., 2020). Security in all aspects of people's lives, which are all interconnected, is at risk from counterproductive or violative cyberterrorism (Dlamini & Mbambo, 2019). Suppose the issue of digital insecurity as a result of cyberterrorism persists. In that case, policymakers should mediate the spread of speech act notions that accelerate efforts to raise cybersecurity awareness at all levels of society (Moubayed et al., 2017).

Government employees can have incomplete or a priori knowledge of cybersecurity concerns from a state's standpoint (Ahmad et al., 2012). Five sporadic or spreading security variables propagate to other state security factors through institutionalized state implementation of regulations, technology, the notion of security, the strength of a major country's policymakers, and the normative concept of state security values (Castillo et al., 2021). Technology that keeps up with the times and facilitates different kinds of information flows is at risk of being compromised by cybercrime, which in turn threatens the security and stability of the state (Moise, 2014).

The main relevant models and theories making up the theoretical framework are summarized and serve as a roadmap for the study. This study's theoretical underpinnings are based on the need for a standardized resource to better explain cybercrime in Indonesia. The idea of securitization is offered as a lens to examine the cybercrime phenomenon related to various notions (Beech & Bishop, 2017). The securitization idea was developed by Jaap de Wilde, Ole Waefer, and Barry Buzan, who looked at a situation involving Indonesia's national defense. This research demonstrates that the reach of cybercrime is global. To further evaluate tactics that the Indonesian Government should adopt in simplifying regulations that help avoid continued cybercrime in Indonesia, the theory of securitization is also enriched by the idea of national security (Martins et al., 2019).

This study elaborates on the idea of national security by describing it as diversification. The etymological significance of the phrase "national security" can be broken down into two parts: the national security function and the described phenomenon. It deals with how national security has evolved to foster a sense of calm and safety for all citizens. Having a feeling of safety is essential to functioning as a community and a nation. When a government fails to adopt the policy changes necessary to establish an effective security infrastructure, the nation's citizens cannot feel safe (Ramadhan, 2020). In light of the fact that technological advancement has brought many benefits with globalization but is still capable of threatening the national security system, both territorially and digitally, a review of the strategic arrangement used to achieve national security in Indonesia is urgently required.

Any nation, organization, or even one person can define the set of parties entitled to security guarantees (Arifah, 2011). As such, it is clear that the state cannot always guarantee the safety of its citizens, even though it is a fundamental human right. Evaluating the efficacy of the national security system is also a civil society right

(Setiawan, 2020). This study further investigates the restrictive definition of national security in the context of cybersecurity.

Cybersecurity, or digital security, integrates offline and online social interactions resulting from technological progress. Any system incorporating long-distance communication potentially threatens a country's national security (Villacampa et al., 2022). The extent of security, which includes the private sector, the government, and public infrastructure, is a cause for worry that necessitates a deeper level of protection in the digital realm. In situations calling for the utmost secrecy, a password or other sort of security system that cybercriminals are unable to crack can be an effective means of preventing the release of sensitive corporate information.

John P. Lovell first proposed the idea of a security strategy as a means for a nation to achieve its objectives through the application of its preexisting power, be it soft power (diplomacy within the purview of this study, such as cyber diplomacy) or hard power (military power employing a war strategy). When designing a security plan to win the cyber war, it is crucial to remember that new technologies can have beneficial and harmful effects on people's daily lives, regardless of where they are developed (Dlamini & Mbambo, 2019). Cyber threats have become a new issue requiring a more robust cybersecurity response with a traditional focus on territorial concerns.

This study's focus is on defending against cybercrime, which can take many forms, including the theft of crucial internal data, the creation of false identities, and the use of these methods by criminals posing not only as terrorists but also as members of the public, government officials, and academics (Cherry, 2005). To assess Indonesia's national security regulatory system, the government's primary aim is to develop a strategic understanding of the constellations or circumstances that lead to state security (Ramadhan, 2020).

Ali Imron, a *da'wah* activist, responded to the current restrictions in Indonesia regarding the Bali bombing case, reminding the people to be vigilant against and prevent acts of extremism, such as using the cover of being a Muslim or a pious Muslim woman to hide one's true intentions (BBC, 2018). On the other side, the attack on the church in Surabaya, East Java, classified as offline terrorism, has been widely condemned by the Indonesian people. Those responsible for terrorist acts often disguise themselves as mothers and children to blend in with the populace. A suicide bomber exploded in the churchyard, wounding 40 people. It accomplished the propaganda goal. As the characteristics of the bomb preparation suggest, the case's assumption has become a heated debate in proving the presence of organized collaboration by ISIS as a terrorist pioneer (Wahyudi, 2018).

People increasingly rely on messaging services to maintain relationships and efficiently complete tasks (Kuk & Randđelović, 2017). However, despite the numerous legitimate uses for messaging apps, some exploit the heightened sophistication these media provide to commit fraud or other forms of cybercrime. Telegram, as a medium for cybercrime, is an example of clandestine or covert motivation for cybercriminals, such as disseminating rumors and recruiting members of cyberterrorist groups (Fiorenza, 2007). Cyberterrorists are increasingly targeting popular messaging platforms like Facebook and Twitter, in addition to more traditional targets like communication networks like Telegram. Telegram, a digital chat software developed by the Russian Government, is a platform that can be geared toward cyberterrorism recruiters. It is a messaging service with a "People Nearby" function to let people connect with those in their immediate area. Hence, cyberterrorist recruiters can easily monitor and hack into seemingly unrelated crime targets (Bloom, 2018).

RESEARCH METHOD

A strategy to account for the variation in complicated regulatory governance should be implemented to eradicate the unfavorable perception of cyberterrorism in Indonesia. This research employed a descriptive qualitative method to examine this idea (Hull et al., 2018). This method creates a systematic, factual, and accurate account of events about the facts, nature, and links between the phenomena researched. Hence, it was

applied to explain the issues arising in this research. This method could provide a full picture of how Indonesia's cybercrime and cyberterrorism regulations have been put into practice.

The method involved several steps, from gathering data to drawing conclusions. It is anticipated that this method would be both involved and modified to contemporary concerns. Qualitative studies dispel the belief that researchers must bend the truth to fit their preconceptions (Romanosky et al., 2019). This study took a descriptive method with a qualitative approach to better understand and address the research problem. This study aims to identify the barriers to cybercrime investigation in Indonesia. Literature was employed as a source of information to provide factual information and a framework for organizing the research method. Books also provided information about cybercrime by studying actual cases and applying cyber law to actual cybercriminals. This study discussed issues directly linked to the cybercrime epidemic.

In Southeast Asian countries, the paradigm of counterterrorism has emerged, consisting of intense collaboration based on monitoring principles. The variety of research into the efficacy of this sequence of close coordination aims to systematically execute intelligence integration. Integrating intelligence efforts, also known as intelligence sharing, is the most effective means of combating the digital terror that threatens national security and prevents it from happening again in the future (Nicholson et al., 2012). State intelligence is a broad discipline with several subfields, but they can be broken down into two main types: inter-state and intra-state intelligence (Harkin & Whelan, 2019). To elaborate, intra-state intelligence performance means that different intelligence agencies inside a country work together to increase the quality of intelligence gathered, as seen in intelligence performance in Indonesia.

There is an internal debate over whether or not collaboration is more important than individual effort when it comes to eliminating cybercrime and cyberterrorism. In Indonesia, the intelligence community is highly competitive and has experienced internal controversy in the form of a trust deficit. Competition is high, and a closed, semi-covert intelligence performance system suggests the environment is not optimal (Saputra, 2016). Existing issue solutions for dealing with terrorism have been significantly impacted by internal rivalries among intelligence agencies (Pradnyana & Rofii, 2020). Therefore, handling this competition phenomenon is necessary. It is best performed through political guidance from the highest stakeholders in the national leadership system to bridge this rivalry.

Intelligence personnel in Indonesia, particularly at the Police Intelligence Agency, the State Intelligence Agency (BIN), and the Strategic Intelligence Agency (BAIS), have been working hard, coordinating the necessary action to destroy current terrorism. The consequences of counterterrorism-based national security are diminished when people fail to cooperate and demonstrate unity. According to the idea of global intelligence, known as intelligence sharing, "knowledge is power", making it difficult to exchange and integrate with other intelligence organizations (Mishra et al., 2021). Since computer criminals can be counted on to carry out acts of terror, ranging from cyber riots to serious terror that can damage many parties, efforts to combat cyberterrorism and cybercrime are urgently required (Kshetri, 2010).

Training terrorists to develop their abilities to fool tracks is the first step in the sequence of events leading to the successful completion of terrorist actions. Intelligence agencies can track the acquisition and distribution of weapons, the maintenance of ongoing cyberterrorism and cybercrime actions, and the recruiting and final execution of members of these groups in cyberspace. The spread of cyberterrorism can be tracked only with the help of appropriate regulations. However, there has not yet been an all-encompassing discussion of the study into the efficacy of these restrictions, particularly those intimately tied to the functioning system of social media and websites, which are the media for digital terror actions. The Ministry of Communication and Informatics took effective measures to monitor and shut down social media accounts associated with disseminating terrorist actions. However, the intelligence agencies that handle this situation do not

play a crucial role (Aliprandi et al., 2022). The stability of essential public infrastructures is jeopardized when intelligence agencies take too long to respond to acts of cyberterrorism and cybercrime. Critical infrastructures such as electrical grids, financial networks, and phone lines are at risk from cyberterrorist attacks. When enforcing effective and well-thought-out regulations, this phenomenon needs collaboration from the nation's leadership.

Cybersecurity and defense are produced due to the union of humans and technology surrounding cyberspace. As a result, cybersecurity and cyber self-defense are covered by many associated terminology and interpretations, both of which have beneficial and harmful effects on daily life in society and the state. It has elevated cybersecurity and self-defense from a purely technological concern to one that threatens national stability. Accordingly, cybersecurity is now considered an element of state security policy. Instead of resorting to using military forces (use of force) as a kind of hard diplomacy, issues can be settled by the effective implication of regulations as a type of soft diplomacy.

RESULT AND ANALYSIS

The Indonesian Constitution has discussed the government's responsibility to protect its citizens from the growing danger of cyberterrorism and cybercrime. Law No. 5 of 2018 concerning the Eradication of Criminal Acts of Terrorism, is only one of several regulations regarding criminal acts of terrorism to protect Indonesia's sovereignty. The Indonesian Army (TNI) plays a crucial role in covering cyberterrorism threats and completing the cyberterrorism track record with its various operation modes. Of course, it synergizes with state intelligence because Indonesia is an extremely large country located at a crossroads between countries from a geopolitical and security standpoint. Therefore, the state's policies and responsibilities in combating cyberterrorism in Indonesia are enshrined in Law No. 5 of 2018 concerning the Eradication of Criminal Acts of Terrorism.

To achieve digital world security in Indonesia, all socioeconomic strata and state and non-state entities require state patronage or full sovereignty from the state. Pseudo-conflict based on unity-shattering religious dogmatism is a common tactic employed by terrorists operating in disguised community settings. Based on people's distrust of government power, this religious-values-based facade is erected to foster national solidarity (Sitorus & Tannady, 2021). Regulations to monitor the spread of cyberterrorism, particularly on social media and websites that support the commission of terrorist activities, have not been extensively explored concerning regional security (Damayanti, 2021). The Ministry of Communication and Informatics has monitored how the social media account deals with terror-related content to shut it down. Critical public infrastructure, including power plants, banks, and telecommunications networks, are at risk due to the intelligence agency's sluggish response to cyberterrorism incidents. It is essential for all parties involved in implementing regulations to work together when dealing with incidents of digital crime (Wahyudi, 2018).

As a result of the coming together of people and technology, new cybersecurity and self-defense domains have emerged. Consequently, the ideas of cybersecurity and self-defense are surrounded by a plethora of jargon and interpretations (Pradnyana & Rofii, 2020). It explains why cybersecurity and self-defense threaten national security, not solely technological security. Hence, cybersecurity strategies must shift away from using the military (hard diplomacy) in favor of non-coercive approaches, such as implementing legislation connected to digital crime in the form of soft diplomacy regulations. Cybersecurity policies are implemented online to protect against many forms of cybercrime, such as financial fraud, identity theft, and even military and terrorist strikes (Saputra, 2016). According to the Copenhagen securitization approach, cybercrime that spreads to other countries is a security concern because it threatens any community or organization that shares its values, way of life, or philosophy. With the new nuclear threat paradigm, radioactive materials are now considered a component of cyberterrorism (Sakban et al., 2019). However, as seen in the recent past with Covid-19, there is a need for more coordinated oversight regarding managing terror cases becoming the basis for assaults in biology (Ma & McKinnon, 2021).

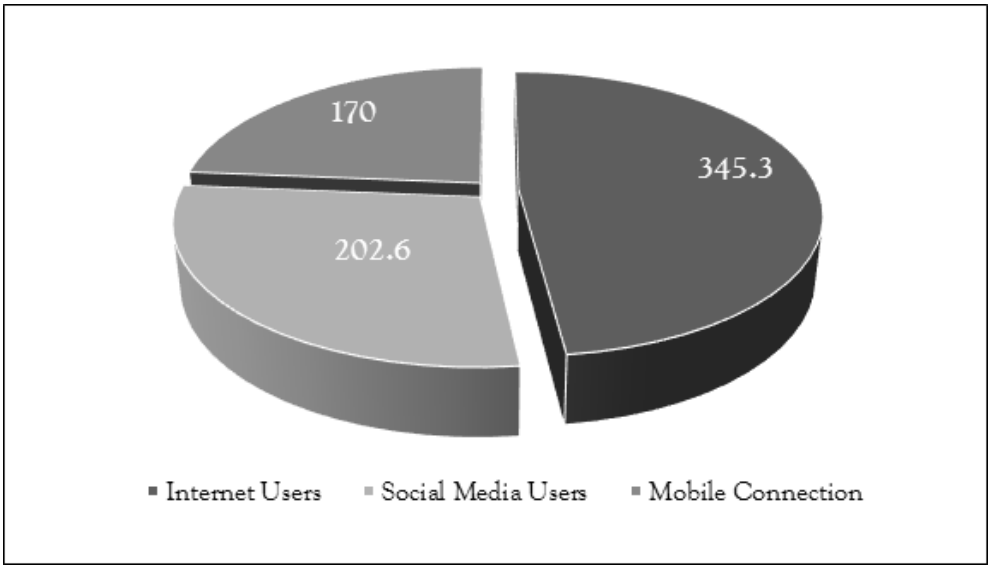

Figure 1. The amount of Indonesian Digital Users in 2021 (in a million)
(Direktorat Tindak Pidana Siber, 2021)

Cybercrime, such as disseminating false news, is one-way cyberterrorists' new methods to make themselves known, as they can distort the public's understanding of events. Naturally, it will cause friction among society at large, which in turn will make it simpler for terrorist strikes to deflect attention away from securing the country as a whole. The Digital Indonesia website revealed that in 2021, there were 2,026,000,000 active internet users in Indonesia, with a further 3,453,000,000 utilizing mobile connections and 170,000,000 using social media (Data Reportal, 2021). The following graph illustrates the relatively high vulnerability of the digital world concerning cybercrime.

These numbers quantify the ineffectiveness of more overarching regulations. Increasingly sophisticated hacking techniques undermine the efficacy of virtual anti-terror regulations and can even increase future counterproductive or dangerous physical terror. The country's authoritarian government has a complete say in improving cybersecurity to the point where it does not facilitate activities like data mining, terrorism-related communication, or the dissemination of propaganda. Consistently expanding cybercriminals orchestrating the recruitment of cyberterrorists are cataloged in the following manner (Kementerian Komunikasi dan Informatika, 2021).

The modus operandi of evil schemes is reflected in the prevalence of cybercrime and the comprehensiveness of cyber detection technologies highly effective in assaulting all victim data. Since this massive cyber attack can wipe out essential state records, it is highly connected with dangers to a nation's politics, ideology, and religion. Cyberterrorists will utilize vulnerable social media accounts to collect sensitive information. An example is the steady trickle of cybercriminal traps that have caught something, like stolen money. By using the money they have stolen to finance further criminal activity online, cybercriminals can spread their terror network and close the circle of their cybercrime chain. The government faces a problem adapting the efficacy of regulations and extending rhythmic patterns in integration to protect the national ecology from the growing threat posed by cybercrime (Data Reportal, 2021). This section provides detailed statistics on the safety of the online environment in 2020, measured by the number of instances of crime.

From January 1, 2020, to April 12, 2020, the National Cyber and Crypto Agency (BSSN) of Indonesia gathered 25,224,811 incidents of cybercrime (BSSN, 2020). An uptick in reported cybercrime incidents was seen in February, with 29,188,645 cases recorded. There were 26,423,989 ongoing cybercrime cases as of the end of

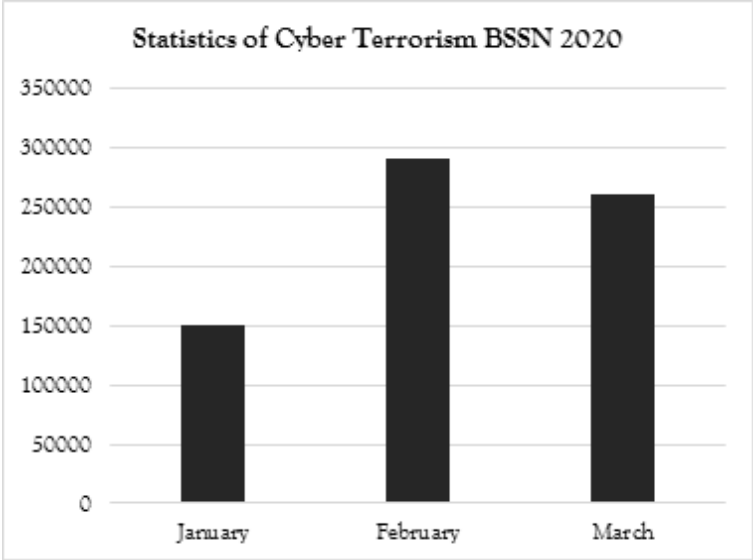

Figure 2. Cyberterrorism Statistics (BSSN, 2020)

March. Moreover, 56% of the stated cyber attacks were related to trojan activity, 43% included collecting personal information, and 1% were web application attacks.

BSSN was created under the Presidential Regulation No. 53 of 2017 to ensure that agencies with front-line access in the field of state security from cybercrime can carry out their responsibility of bolstering online safety in the age of the digital economy, ensure the safety of the public, and hold offenders accountable for their actions. On December 1, 2020, policymakers in Indonesia, including the Coordinating Ministry for Politics, Law, and Security, held the third sub-regional meeting on Counter-Terrorism and Transnational Security (SRM on CTTS) in Jakarta. It became the precursor of the awareness discourse initiative on eradicating digital and physical terrorism. Several integrations from different lines in Indonesia have contributed to the BSSN as part of cooperation integration.

The main facilitator assigned to BSSN also covers other cybersecurity such as the Indonesian National Police (POLRI), the National Counterterrorism Agency (BNPT), the Financial Transaction Reports and Analysis Center (PPATK), the State Intelligence Agency (BIN), the Ministry of Foreign Affairs (Kemlu), Coordinating Ministry for Politics, Law and Security (Kemenkopolhukam), the Ministry of Communication and Informatics (Kemenkominfo), the Ministry of Law and Human Rights (Kemenkumham), and the Ministry of Defence. The prevalence of security organizations in Indonesia is insufficient for determining the true extent of cybercrime. When it comes to preventing the spread of terrorist activities in Indonesia, the best results could be achieved not only at the highest level of government but also through the concerted efforts of the lower level of government. To maximize the strengthening of power, positions, and functions in the leadership positions of the BNPT in 2020, BNPT took an active role in managing illegal activities. One can characterize the overall proportion of cybercrime by the following.

IDR 304,700,000,000 were required in 2021 to fund efforts to combat cyberterrorism and cybercrime. The BNPT's funding in 2021 was IDR 515,900,000,000, as the agency's head planned. Since every aspect of life depends on the internet, measures must be taken to lessen cybercrime. Here, Indonesia has to implement several long-term strategies to reduce cyberterrorism. In addition, there has been little progress in enforcing Indonesia's cybersecurity regulations. The headquarters of BSSN's mission is to counteract cybercrime and other online dangers. Cyberterrorism has not been adequately addressed by the regulations of Law No. 15 of 2003 on

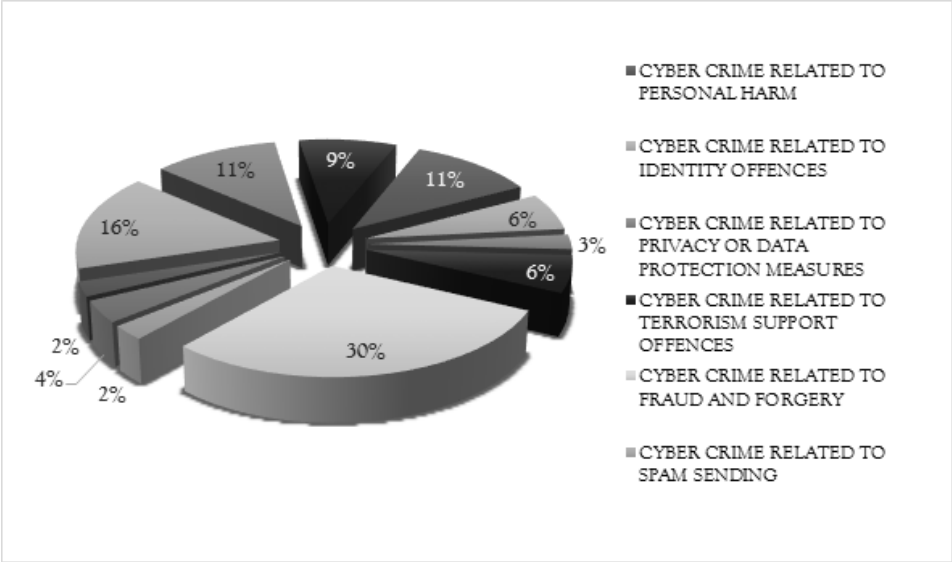

Figure 3. (Statistik Terorisme Siber, 2020)

the Eradication of Criminal Acts of Terrorism and Law No. 11 of 2008 on Information and Electronic Transactions (ITE) (JDIH, 2013).

CONCLUSION

This study utilized the preceding percentages to provide a comprehensive illustration of cybercrime. Personal damage-related cybercrime accounted for 9%, identity theft-related cybercrime accounted for 5%, and privacy or data protection-related cybercrime accounted for 2%. Fraud and identity theft accounted for 24% of all cybercrime, while finance terrorism accounted for 5%. The fact that spamming-related cybercrime accounted for solely 2% of all cybercrime illustrates a diversity across different cybercrime, all of which should see a decline in caseloads in Indonesia. Predictions about the most effective solutions from various sources, such as Nazli Choucri's "Cyber Politics in International Relations," revealed that different chronological sequences of cyberterrorism demonstrate that the defense carried out by the government as a policymaker could maximize the viewpoint of the protagonist (policymaker) viewing security from an ontological perspective. Perspectives on cyberterrorism can offer a way forward regarding technology development beneficial to safeguard against computer crime.

Indonesia's cybercrime legislative framework and policy administration have been in dire need of updating. Once a national security theoretical framework is in place, the government's policy patronage and regulatory power over cybercrime are no longer the sole duty of the state. Existing policy rhetoric should cover the full range of human experience, from the most micro, in the form of individuals, to the most macro, in the form of the Unitary State of the Republic of Indonesia (NKRI), in terms of the psychological, economic, and national security implications of cybercrime.

While the Indonesian Government has enacted several regulations as part of its security plan, additional measures, such as practicing safe and responsible internet use, are also necessary. Furthermore, not all segments of Indonesian society have been educated on the significance of cybersecurity awareness, making it imperative to engage in socialization efforts to expand knowledge of what constitutes cybercrime. Cybercrime is a type of national insecurity in cyberspace. Cybercrime in Indonesia can alter a security system and even erase data from crucial organizations. Using these examples, the Indonesian Government and public can refine their understanding of cybercrime and how it should be dealt with. In addition, the worldwide pandemic has not yet created favorable conditions to be separated from the

digital world, making all aspects of everyday life dependent on the internet.

The government can assist politicized activities in promoting state security in cyberspace using e-governance to connect with the public and the media. The beneficial and harmful effects of the global community's reliance on the digital realm are like two sides of a knife. The government's first line of defense against cybercrime must be to initiate the concept of integrated and cooperative information sharing. By increasing the number of cyber police able to keep a constant vigil over digital data, hackers can be located and dealt with in real-time. This problem remains a focus for the government to tighten security. Still, it can also be a weakness for cybercriminals, leading to the consolidation of power networks and the emergence of even more brazen cybercrime colonies.

REFERENCE

Abdullah, F. M. (2019). Using big data analytics to predict and reduce cyber crimes. *International Journal of Mechanical Engineering and Technology, 10*(1), 1540–1546. h

Ahmad, R., Yunos, Z., & Sahib, S. (2012). *Understanding cyber terrorism: The grounded theory method applied* (pp. 323–328). https://doi.org/10.1109/CyberSec.2012.6246081

Al Moubayed, N., Wall, D., & McGough, A. S. (2017, July). Identifying changes in the cybersecurity threat landscape using the LDA-web topic modelling data search engine. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 287-295). Springer, Cham.

Aliprandi, C., Lotti, L., Neri, F., & Sanna, G. (2022). *Online Police Station, a cutting edge service against cybercrime.* 40, 237–247. https://doi.org/10.2495/DATA080231

Arifah, D. A. (2011). Kasus cybercrime di indonesia. *Jurnal Bisnis dan Ekonomi, 18*(2).

Antunes, M., & Rabadão, C. (2019). *Cybersecurity and Digital Forensics – Course Development in a Higher Education Institution* (Vol. 942, pp. 338–348). https://doi.org/10.1007/978-3-030-17065-3_34

BBC. (2018). *Serangan bom di tiga gereja Surabaya: Pelaku bom bunuh diri "perempuan yang membawa dua anak" - BBC News Indonesia.* Retrieved December 13, 2022, from BBC: https://www.bbc.com/indonesia/indonesia-44097913

Beech, M., & Bishop, J. (2017). Cyber-stalking or just plain talking?: Investigating the linguistic properties of rape-threat messages as compulsive behaviours. In *Violence and Society: Breakthroughs in Research and Practice* (pp. 193–220). https://doi.org/10.4018/978-1-5225-0988-2.ch012

Bloom, M., & Daymon, C. (2018). Assessing the Future Threat: ISIS's Virtual Caliphate. *Orbis, 62*(3), 372–388. https://doi.org/10.1016/j.orbis.2018.05.007

BSSN. (2020). *Statistik Terorisme Siber.* Retriever December 11, 2022 from BSSN: https://bssn.go.id/?s=terorisme+siber+2020

Castillo, I., Munoz, J., Lopez, J. I., Rodriguez, L., Romero, L. D., Gonzalez, M., & Ponce, J. C. (2022). *Helping Students Detecting Cyberbullying Vocabulary in Internet with Web Mining Techniques.* 21–27. https://doi.org/10.1109/CONTIE49246.2019.00014

Cherry, S. (2005). Terror goes online [cyberterrorism]. IEEE Spectrum, 42(1), 72-73.

Damayanti, D. (2021). Implementation of the cyber terrorism prevention, and rehabilitation policy in Polda Metro Jaya Police in Central Jakarta. In *IBIMA Business Review* (Vol. 2021). IBIMA Publishing. https://doi.org/10.5171/2021.695424

Data Reportal. (2021). *Digital in Indonesia: All the Statistics You Need in 2021 — Data Reportal – Global Digital Insights.* https://datareportal.com/reports/digital-2021-indonesia

Dlamini, S., & Mbambo, C. (2019). Understanding policing of cybercrime in South Africa: The phenomena, challenges and effective responses. *Cogent Social Sciences, 5*(1). https://doi.org/10.1080/23311886.2019.1675404

Fiorenza, N. (2007). NATO considers response to cyber warfare following attacks on Estonia. *Jane's International Defence Review, June.*

Galis, V., & Summerton, J. (2018). We are all foreigners in an analogue world: cyber-material alliances in contesting immigration control in Stockholm's metro system. *Social Movement Studies, 17*(3), 299–317. https://doi.org/10.1080/14742837.2017.1383892

Harkin, D., & Whelan, C. (2019). Exploring the implications of 'low visibility' specialist cyber-crime units. *Australian and New Zealand Journal of Criminology, 52*(4), 578–594. https://doi.org/10.1177/0004865819853321

Horgan, S., Collier, B., Jones, R., & Shepherd, L. (2020). Re-territorialising the policing of cybercrime in the post-COVID-19 era: towards a new vision of local democratic cyber policing. *Journal of Criminal Psychology, 11*(3), 222–239. https://doi.org/10.1108/JCP-08-2020-0034

Horsman, G. (2017). Can we continue to effectively police digital crime? *Science and Justice, 57*(6), 448–454. https://doi.org/10.1016/j.scijus.2017.06.001

Hovorushchenko, T., Herts, A., & Pavlova, O. (2020). Method of Forming a Logical Conclusion about Legal Responsibility in the Cybersecurity Domain. In *ICTERI Workshops* (pp. 128-135)

Huey, L., & Rosenberg, R. S. (2013). Reporting and Clearance of Cyberbullying Incidents: Applying "Offline" Theories to Online Victims. *Canadian Journal of Criminology and Criminal Justice , 46*(5), 597–606. https://doi.org/10.3138/cjccj.46.5.597

Hull, M., Eze, T., & Speakman, L. (2018, October). Policing the cyber threat: Exploring the threat from cyber crime and the ability of local law enforcement to respond. In *2018 European Intelligence and Security Informatics Conference (EISIC)* (pp. 15-22). IEEE. https://doi.org/10.1109/EISIC.2018.00011

JDIH. (2013). *UU No. 15 Tahun 2003 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme, Menjadi Undang-Undang.* Retrieved December 13, 2022, from BPK RI: https://peraturan.bpk.go.id/Home/Details/43015/uu-no-15-tahun-2003

Kementerian Komunikasi dan Informatika. (2021). *Statistik Teknologi*

Digital Asia. Retrieved December 13, 2022, from Kominfo: https://www.kominfo.go.id/content/detail/10259/hati-teroris-diteguhkan-melalui-telegram-ungkap-kominfo/0/sorotan_media

Kshetri, N. (2010). *The global cybercrime industry: economic, institutional and strategic perspectives.* Springer Science & Business Media.

Kuk, K., & Ranđelović, D. (2017). *Knowledge discovery in cyberspace: Statistical analysis and predictive modeling* (pp. 1-206).

Leukfeldt, E. R., Notté, R. J., & Malsch, M. (2019). Exploring the Needs of Victims of Cyber-dependent and Cyber-enabled Crimes. *Victims and Offenders, 15*(1), 60–77. https://doi.org/10.1080/15564886.2019.1672229

Ma, K. W. F., & McKinnon, T. (2021). COVID-19 and cyber fraud: emerging threats during the pandemic. *Journal of Financial Crime.* https://doi.org/10.1108/JFC-01-2021-0016

Martins, I., Resende, J. S., Sousa, P. R., Silva, S., Antunes, L., & Gama, J. (2019). The Global Cybercrime Industry: Economic, Institutional) and Strategic Nir Kshetri. *Future Generation Computer Systems, 133*, 95–113. https://doi.org/10.1016/j.future.2022.03.001

Millman, C. M., Winder, B., & Grifths, M. D. (2017). UK-based police officers' perceptions of, and role in investigating, cyber-harassment as a crime. *International Journal of Technoethics, 8*(1), 87–102. https://doi.org/10.4018/IJT.2017010107

Mishra, S., Alowaidi, M. A., & Sharma, S. K. (2021). Impact of security standards and policies on the credibility of e-government. *Journal of Ambient Intelligence and Humanized Computing, 2019* (Naidoo 2020). https://doi.org/10.1007/s12652-020-02767-5

Moise, A. C. (2014). Some considerations on the phenomenon of cybercrime. *Journal of Advanced Research in Law and Economics, 5*(1), 38–43. https://doi.org/10.14505/jarle.v5.1(9).04

Nicholson, A., Watson, T., Norris, P., Duffy, A., & Isbell, R. (2012, July). A taxonomy of technical attribution techniques for cyber attacks. In *European conference on information warfare and security* (p. 188). Academic Conferences International Limited.

Pradnyana, I. P., & Rofii, M. S. (2020). Cyberterrorism Threats in Indonesia and State Responses. *Literatus Journal, 2*(2), 181-192.

Ramadhan, I. (2020). Cyber-Terrorism in the Context of Proselytizing, Coordination, Security, and Mobility. *International Relations Department of Universitas Pertamina, Islamic World and Politics, 4*(2).

Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: How do carriers price cyber risk? *Journal of Cybersecurity, 5*(1). https://doi.org/10.1093/cybsec/tyz002

Sakban, A., Sahrul, Kasmawati, A., & Tahir, H. (2019). Police preventative against cyber-bullying crimes in indonesia. *International Journal of Scientific and Technology Research, 8*(12), 1532–1534.

Santhoshi, N., Chandra Sekharaiah, K., Madan Mohan, K., Ravi Kumar, S., & Malathi, B. (2019). Cyber Intelligence Alternatives to Offset Online Sedition by in-Website Image Analysis Through WebCrawler Cyberforensics. *In Soft Computing and Signal Processing* (pp. 187-199). Springer, Singapore.

Saputra, R. W. (2016). A survey of cyber crime in Indonesia. *2016 International Conference on ICT for Smart Society, ICISS 2016* , July, 1–5. https://doi.org/10.1109/ICTSS.2016.7792846

Setiawan, D. A. (2020). Cyber Terrorism and its Prevention in Indonesia. *Jurnal Media Hukum, 27*(2), 267–283. https://doi.org/10.18196/jmh.20200156

Sharma, P., Doshi, D., & Prajapati, M. M. (2016). Cybercrime: Internal security threat. In *2016 international conference on ICT in business industry & government (ICTBIG)* (pp. 1-4). IEEE.

Sitorus, T., & Tannady, H. (2021). Synergy, System IT. Risk Management and The Influence on Cyber Terrorism and Hoax News Action. *Journal of Theoretical and Applied Information Technology, 99*(8), 1802-1814.

Svecova, H., & Blazek, P. (2021). *The Impact of Cybersecurity on the Rescue System of Regional Governments in SmartCities: Vol. 1371 CCIS* (pp. 365–375). https://doi.org/10.1007/978-981-16-1685-3_30

Villacampa, C., Torres, C., & Miranda, X. (2022). Institutional Response to Trafficking in Human Beings in Spain: Are All Victims Equally Protected? *European Journal on Criminal Policy and Research, 0123456789.* https://doi.org/10.1007/s10610-022-09506-w

Wahyudi, S. T. (2018). Hubbul Waton Minal Iman as Reinforcement Theorem of State Defense in the Context of Terrorism Prevention in Indonesia. *SHS Web of Conferences, 54*, 08019. https://doi.org/10.1051/shsconf/20185408019

Williams, M. L., Edwards, A., Housley, W., Burnap, P., Rana, O., Avis, N., & Sloan, L. (2013). Policing cyber-neighbourhoods: tension monitoring and social media networks. *Policing and society, 23*(4), 461-481.