Politeia : Journal of Public Administration and Political Science and International Relations
E-ISSN : 3031-3929
Volume. 2 Issue 2 April 2024
Page No: 62-82

Indonesia's Digital Security Strategy: Countering the Threats of Cybercrime and Cyberterrorism

Khoirunnisa Khoirunnisa[1], Didi Jubaidi[2]
Universita 17 Agustus 1945 Jakarta, Indonesia[1,2]
Correspondent: khoirunnisa@uta45jakarta.ac.id [1]

Received : Maret 28, 2024
Accepted : April 06, 2024
Published : April 27, 2024

Citation: Khoirunnisa, K., & Jubaidi, D. (2024). Indonesia's Digital Security Strategy: Countering the Threats of Cybercrime and Cyberterrorism. Politeia: Journal of Public Administration and Political Science and International Relations, 2(2), 62-82. https://doi.org/10.61978/politeia.v2i1

ABSTRACT: Cybercrime is becoming a very serious threat to Indonesia's national security. The pervasive nature of cyberattacks raises questions about the effectiveness of current regulatory measures. This research aims to analyze how the government addresses security challenges in cyberspace in a sustainable manner. A descriptive qualitative method was used to evaluate the impact of cybercrime in Indonesia and its relationship with highly interrelated regulations. The results show that the threat of cybercrime and cyber-terrorism, in both physical and digital forms, has increased alarmingly in recent years. The impact of universal access to all relevant information has several consequences, such as identity theft, malware attacks, disclosure of confidential information, theft of intellectual property, coordinated attacks, compromise of critical systems, dissemination of disinformation, manipulation of public opinion and financial crimes including dissemination of false information and development of cybercrime networks. Significant measures are needed to disrupt the cyber terrorism industry to create a safe environment in Indonesia. The success of regulatory measures in Indonesia relies on a holistic approach involving the active participation of the government, society, and the private sector.

Keywords: Crime, Cybercrime, Cyberterrorists, Digital

INTRODUCTION

Cyberspace, or the internet, has changed the way we interact and communicate around the world. The internet enables the exchange of information regardless of geographical or time boundaries. Some significant impacts of this phenomenon involve the development of statistics as a tool to understand and measure various aspects of life that occur in cyberspace (Yuniarto, 2015). Hence, the rise of cybercrime reflects the relevance of the ever-growing trend. Unfortunately, however,

modern society still relies heavily on hardware and software technologies built more than a century ago. The dissemination of information involving huge distances makes it difficult to avoid leaving a digital footprint (Machmiyah et al., 2017).

The need for regulation to detect and prevent cybercrime reflects the real efforts of policymakers as drivers of change in reducing the level of cybercrime (Loqman & Rahman, 2020). It should not only focus on the euphoria of political programs in a particular period as a method to win public support in the global political arena (Jerry Indrawan, 2019).

Preventive is a driving factor in countering the international spread of cybercrime, which is not limited by geographic or time constraints (Supanto et al., 2023). Preventing information oversharing online can be done through various public awareness campaigns and other preventive measures, as exemplified by (Aditiawarman, Mac, 2019). Reliance on modern technology opens up opportunities for cybercriminals to conduct more sophisticated and widespread attacks. Cyber-attacks can include data theft, malware attacks, phishing attacks, and more, the digital society demands the adoption of several macro-level measures, including the establishment of regulations and the crucial role of large-scale businesses in supporting the effectiveness of regulations against cybercrime (Hapsari & Pambayun, 2023). Cybercrime, clearly, is not only a supernatural problem, but also a rational argument (Djanggih & Qamar, 2018). The perpetrators of cybercrime have taken the attitude that the regulations governing indecent acts are merely fake rules. Therefore, stopping the accumulation of cybercrime cannot be achieved through regulatory reform alone, but rather through enforcement of cybercrime follow-ups (Millman, C. M., Winder, B., & Griffiths, 2017)It is important that policymakers do not continue to adopt a conservative stance when dealing with cybercrime cases that have occurred. They need to be aware of the contradictory aspects of society that cannot be avoided when dealing with online activities. Hence, there is a need for a paradigm shift towards a more proactive and responsive approach to cybersecurity challenges.

Some steps that can be taken include: (Rahmawati, 2019)

1. **Proactive Prevention**: Focus on preventing cybercrime before it happens by promoting cybersecurity, public education about online risks, and awareness campaigns.
2. **Public and Private Cooperation**: Encourage cooperation between the government, private sector, and other institutions to exchange information and jointly confront cybersecurity threats.
3. **Effective Law Enforcement**: Ensure an effective law enforcement system and prompt follow-up against cyber criminals to provide a deterrent effect and demonstrate the consequences of their actions.
4. **Policy and Regulatory Updates**: Continuously update policies and regulations to keep up with technological developments and cybercrime dynamics, while increasing vigilance against new challenges.
5. **International Collaboration**: Participate in international collaboration efforts to tackle cybercrime that crosses national borders.
6. **Cybersecurity Education**: Include cybersecurity education in school curricula and training programs to increase the public's understanding of the risks and precautions that can be taken.

By adopting a more proactive and holistic approach, policymakers can help protect the public from the impact of cybercrime and build a safer and more trusted online environment.

Inadequacies in the implementation of cybercrime rules have far-reaching damaging impacts across multiple sectors, involving stability of the country's security, including unethical health, finance, and education. Creating an explicit narrative is not enough to address the negative impacts of cyber growth. Regulatory changes without keeping up with the digital world and cyber loopholes are unable to stop the negative effects, as expressed by (Moubayed et al., 2017) .

Through their role as catalysts of change, policymakers can take the initiative to: (Muhammad et al., 2023).

1. **Establishment and Updating of Regulations**: Creating and updating regulations that are relevant to technological developments and cybercrime. This involves constant adjustments to address new and evolving threats.
2. **Public Awareness Campaign**: Initiate a public awareness campaign to increase public understanding of the risks of cybercrime and the importance of digital security. This awareness can help engage the public in protecting themselves online.
3. **International Collaboration**: Encourage cooperation between countries in fighting cybercrime. Criminal activities on the internet transcend national boundaries, underscoring the imperative of international collaboration in addressing cyberattacks with cross-regional implications.
4. **Law Enforcement and Investigations**: Ensure effective law enforcement against cyber criminals. This involves careful investigation and legal prosecution to provide effective sanctions.
5. **Education and Training**: Support education and training programs to improve cybersecurity skills in various walks of life. This includes training for industry workers, students, and even ordinary individuals to recognize and protect themselves from cyberattacks.
6. **Security Technology Investment**: Encourage investment in innovative security technologies to improve defenses against evolving cyber threats.

By taking these steps, policymakers can play an important role in creating a safer online environment that is resistant to cybercrime. Collaboration between the public, private and civil society sectors is also key in effectively addressing this challenge.

In hindsight, cyber criminals see the perceived ineffectiveness of regulation in quickly tackling cybercrime as a factor that could encourage a wider pattern of crime. This may result in the involvement of more parties, including those operating outside the realm of conventional politics and business, with the aim of financial gain. (Muhammad et al., 2023). In addition to the role of policymakers, the importance of public awareness of cybercrime also necessitates collaborative efforts from the entire community. This involves proactive measures, such as checking the veracity of news before spreading it, rather than allowing oneself to be lulled by the vast amount of information on social media (Nurlatun et al., 2021). The evolving threat from cybercrime to cyberterrorism has become a major issue today, as expressed by (Abdullah, 2019). Cyber-terrorism, which involves actions such as mobilizing public opinion, is the main trigger for the spread of cyber-terrorism in areas with cultural diversity and political interests, such as the Unitary State of

the Republic of Indonesia (NKRI). Information contained on official government websites and personal data is now increasingly vulnerable to hacking due to weaknesses in cybersecurity (Hapsari & Pambayun, 2023). Disruptions to a country's economic foundation can have far-reaching impacts, involving important aspects of economic and social life. Acts of cybercrime mobilized by criminals with the aim of undermining the unity of a nation can create widespread and sustained impacts. Some possible consequences and chain reaction mechanisms involve:

1. **Polarization of Society**: Mobilized issues can trigger polarization among communities, fragmenting inter-group relations and creating social disagreements.
2. **Cyber Terrorism Mobilization**: Criminals who successfully capitalize on these issues can design cyber terrorism attacks aimed at damaging critical infrastructure or exploiting vulnerabilities in national security systems.
3. **Spreading Desinformation**: Criminals can use cybercrime expertise to spread disinformation, create information chaos, and undermine public trust in legitimate sources of information.
4. **Coordinated Attacks**: By utilizing sophisticated techniques, criminals can launch coordinated attacks involving a large number of cybercriminal acts to achieve their goals.
5. **National Security Crisis**: Cyber terrorism and coordinated attacks can create a national security crisis, forcing governments to face serious challenges related to the nation's security and resilience.
6. **Impact on the Economy**: Attacks on critical infrastructure and businesses can have a serious impact on economic stability, resulting in significant financial losses and undermining business confidence.

Therefore, the prevention and protection of cybercrime is not only the responsibility of the government, but also involves active participation from the community, business sector, and other related parties. Cross- sector collaboration and sustainability of cyber protection efforts are key in dealing with increasingly complex threats in this digital era.

The increasing reliance on digital resources among modern society opens up the entire spectrum of activities in the digital world to potential hacks by cybercriminals. As the use of technology intensifies, so do digital security risks. The impact of cybercriminal involvement may include: ((Soesanto et al., 2023).

1. **Identity Theft**: Cybercriminals can steal and misuse personal information, including identity data, for criminal purposes such as fraud and financial theft.
2. **Malware Attacks**: Intrusion of devices with malware, such as viruses and ransomware, can cause damage to data and operating systems, even harming the operational sustainability of an organization or individual.
3. **Disclosure of Confidential Information**: Unauthorized access may result in the disclosure of confidential information, including company data, business plans, or employee personal data.
4. **Intellectual Property Theft**: Cybercriminals can steal intellectual property, such as product designs or algorithms, which can negatively impact innovation and business sustainability.

5. **Coordinated Attacks and Infiltration of Critical Systems**: Coordinated attacks or infiltration into critical systems, such as electrical infrastructure or healthcare, can have a serious impact on national security and society.
6. **Spread of Disinformation and Manipulation of Public Opinion**: Cybercriminals may utilize digital platforms to spread disinformation, change public opinion, or create social and political instability.
7. **Financial Crimes**: Through phishing attacks or financial data theft, cybercriminals can steal money or financial information that can be used for fraud or other financial crime activities.

Prevention and protection against cybercrime attacks involves measures such as strong cybersecurity, digital risk awareness education, and compliance with relevant security practices and regulations (Budi et al., 2021).

Several studies in this area have emphasized the urgency of the need for regulations focused on cybersecurity, particularly in the context of the cybercrime industry. Cyber terrorism is a real threat that could destabilize Indonesia. To ensure that the excessive spread of propaganda does not destabilize a country's people's sense of national pride, a country's stability depends largely on its citizens' confidence in its government's ability to enforce effective regulations regarding the investigation and prosecution of criminal offenses, as highlighted by (Rozika, 2017). Cybercrime has increased by 23% per year, as seen in the cumulative growth graph of cyber terrorism. The complexity of the digital world is increasing as IP addresses in Indonesia are often the target of cyberattacks. More than 6,000 websites have been compromised in cyberattacks, which has resulted in a slowdown in the real estate and business sectors (Hapsari & Pambayun, 2023).

This incident also highlights the need for appropriate and effective regulations, which should be implemented in synergy with the capacity of intelligence agencies to identify cybercrime, this is necessary to monitor the potential spread of cybercrime that could lead to cyber terrorism (Arianto & Anggraini, 2019).

Cybersecurity management in Indonesia is not only focused on making regulations, this can be seen from the implementation of several recent laws related to cybercrime. For example, the Bali Bombing incident on October 12, 2002 prompted the Government of Indonesia to issue Government Regulation of the Republic of Indonesia No. 1 of 2002 on the Eradication of the Criminal Acts of Terrorism (Hammam Riza et al., 2016). The Indonesian government has conducted international cooperation with other countries in terms of intelligence, policing, and further technical cooperation, especially related to the eradication of criminal acts of terrorism. (Kementerian Pertahanan Republik Indonesia, 2015). This effort is part of the strategy to prevent and counter terrorism, in line with the prevailing laws and regulations.

The coherence between the implementation of intelligence missions and prosecution of terrorism crimes in Indonesia shows effective integration in order to prevent and counter terrorism threats. (Sanur, 2016)The fact that both have been the subject of current regulatory efforts reflects the commitment of the Indonesian government to face security challenges with a holistic approach. As such, the integration between intelligence and law enforcement is an important cornerstone in the effort to protect the public and ensure national security.

Maintaining continuity between regulations and the parties responsible for enforcing them is a crucial step that can create good synergy, especially in the context of regulatory revisions. By ensuring that all parties involved have a good understanding of the applicable regulations, effective cooperation for consistent implementation and enforcement can be strengthened. This synergy can help improve the effectiveness of regulations and ensure better compliance from the various parties involved (Santoyo, 2008).

Illustrations of the circumstances surrounding Bali Bombing I and Bali Bombing II at the Australian Embassy and the JW Marriott Hotel are closely intertwined, reflecting the complexity and interconnectedness of the threat of terrorism. Both events show that the threat of terrorism can involve various locations and parties, highlighting the importance of a comprehensive understanding and collaborative efforts in preventing and countering acts of terrorism across various sectors and regions.

According to the journal (Muhammad Mumtaaz et al., 2021) in his journal entitled "Anti Cyber Terrorism as a Strategic Effort in Combating Cyber Terrorism in Indonesia", previous research did not specifically and comprehensively explain the implementation of regulatory governance related to cyberterrorism. Therefore, this research has its own uniqueness, which is often referred to as structural renewal. The findings of this study show a lack of sufficient evidence to support the implementation of sustainable regulation as a preventive measure against the enabling factors of cyberterrorism.

In this context, maintaining state security and resilience, both in the physical and digital worlds, is considered a crucial step to prevent cyber terrorism. This justification indicates that through a holistic approach to security, including digital aspects, the state can reduce the potential threat of cyber terrorism. Therefore, cyber terrorism prevention and counterterrorism strategies should include policies and actions that support national resilience, creating a strong layer of defense against potential attacks in cyberspace.

Security in all aspects of people's lives, which are interconnected, is potentially subject to adverse impacts or cyber breaches (Dlamini & Mbambo, 2019). For example, the problem of digital insecurity stemming from cyber terrorism continues to grow. In this context, the intermediation of policymakers is needed to disseminate ideas and actions that can accelerate cybersecurity awareness-raising efforts at all levels of society (Moubayed et al., 2017).

The ongoing development of technology that supports various types of information flows can be vulnerable to cybercrime infiltration, which in turn can threaten the security and stability of a country (Pansariadi & Soekorini, 2023). As such, there is a need for a holistic approach that includes strong regulation, prudent technological development and international cooperation to address security threats that can propagate from these diverse security variables.

By referring to relevant models and key theories, this theoretical framework forms a strong basis for directing the research. The theoretical foundation of this study stems from the need for a standardized resource that can provide a better understanding of cybercrime in Indonesia. As such, this study aims to develop a detailed and contextualized analysis of the cybercrime phenomenon in the Indonesian context, utilizing the previously established theoretical basis.

Through the lens of the idea of securitization, this research aims to investigate and analyze the phenomenon of cybercrime in the context of various ideas and concepts. This approach allows

researchers to understand how cybercrime is viewed as a security threat that requires emergency responses and special measures. As such, the concept of securitization provides a solid basis for analyzing the dynamics and impact of cybercrime, as well as for formulating appropriate policies and strategies in the face of this challenge.

The idea of securitization, introduced by Jaap de Wilde, Ole Waever and Barry Buzan, is the focus in looking at situations involving Indonesia's national defense. This research illustrates that cybercrime is not limited to a national scale, but has a global scope that affects various aspects of security around the world. Thus, engaging the securitization framework in this research helps deepen the understanding of the global dimension of the cybercrime threat faced by Indonesia (Raharjo et al., 2022).

In order to further evaluate the tactics that the Indonesian Government should adopt to simplify regulations that help prevent the continuation of cybercrime in Indonesia, the securitization theory is enriched with the concept of national security (Raharjo et al., 2022).

In this context, the concept of national security is described as a form of diversification that involves two main aspects. Firstly, there are national security functions that encompass a range of tasks and responsibilities aimed at keeping the country safe. Secondly, there are the phenomena described, referring to the various events or conditions that come into focus when discussing national security. This etymological understanding helps to detail the meaning and scope of the concept of "national security" in the context of this study.

The existence of national security is linked to the evolution of national security means to foster a sense of calm and security for all citizens. The existence of a sense of security is critical to the functioning of a community and a state. When governments are unable to adopt the necessary policy changes to build an effective security infrastructure, citizens cannot feel safe (Ramadhan, 2020).

It is important to conduct a review of the strategic arrangements used to achieve national security in Indonesia, given the technological advances that bring the benefits of globalization but also pose threats to the national security system, both in the territorial and digital aspects. This review is crucial due to the dynamic changes in the security landscape, where new challenges are emerging rapidly and involve more complex dimensions.

Adopting responsive and innovative strategies in the face of technological change and digital security- related threats can help ensure the effectiveness of national security systems. Therefore, iterations and adjustments to national security regulations, policies and infrastructure are crucial to protect the country from various forms of evolving threats.

The integration of offline and online social interactions, introduced by technological advances, is a key feature of cybersecurity or digital security. Systems that involve remote communication carry potential threats to a country's national security, as asserted by (Arvianto, 2021) This highlights the importance of understanding and addressing cybersecurity challenges arising from digital transformation in social interactions and communications.

The protection of security levels involving the private sector, government, and public infrastructure is a focus of concern that requires a more intensive level of protection in the digital world. In situations that require maximum confidentiality, the use of passwords or other security

systems that can resist hacking attempts by cybercriminals can be considered an effective way to prevent the disclosure of sensitive corporate information. This emphasizes the importance of developing a robust security strategy in the face of increasingly complex cybersecurity threats in the digital environment.

The notion of security strategy first proposed by John P. Lovell refers to an approach in which a state seeks to achieve its objectives through the application of pre-existing power. This force can include soft power, such as diplomacy (including cyber diplomacy in the context of this research), or hard power involving a war strategy using military force. This approach reflects the importance of utilizing existing security resources to design strategies that can effectively achieve state objectives, both in the diplomatic and military realms.

In this research, the main focus is on defense against cybercrime, which can take many forms. These include the theft of vital internal data, the creation of false identities, and the utilization of such methods by criminals posing not only as terrorists, but also as members of the public, government officials, and academics (Sri Yunanto, Angel Damayanti, 2017). The focus on protecting against these threats reflects the importance of developing a comprehensive security strategy in the face of increasingly complex vulnerabilities in the cyber world.

In assessing Indonesia's national security regulatory system, the government has the main objective of developing a strategic understanding of the constellations or circumstances that can affect the country's security (Ramadhan, 2020). This reflects an effort to have a deeper insight into the factors that can affect national security, as well as identify the measures needed to maintain and improve it.

It is important to note that Ali Fuzi, a da'wah activist, has responded to the restrictions in Indonesia regarding the Bali bombing case. Fuazi reminded the public to be vigilant and prevent acts of extremism, particularly by paying attention to the possibility of disguise. He highlighted the risk that someone could use the guise of being a pious Muslim or Muslimah to hide their true intentions (Endang Nurdin, 2020). The statement shows the urgency of raising public awareness of the potential threat of extremism and the need to involve all parties in prevention efforts.

Cyber terrorists are increasingly aiming their attacks at popular messaging platforms such as Facebook and Twitter, in addition to more traditional targets such as communication networks like Telegram. Telegram, which is a digital chat software developed by the Russian Government, is one of the platforms used to recruit cyber terrorist recruiters. This change reflects cyber terrorists' adaptation to trends and developments in the use of social media and messaging platforms to spread propaganda and recruit members.

Telegram is a messaging service with a feature called "People Nearby," which allows people to connect with individuals around them. This feature can provide an opportunity for cyberterrorist recruiters to easily monitor and hack crime targets that may seem unrelated (Bloom, 2018). The existence of such features highlights how technology can be leveraged for the benefit of cyber terrorists, emphasizing the need for security and regulatory measures to protect users and prevent potential exploitation by irresponsible parties.

Based on the description and explanation, the author formulates the problem, namely how is Indonesia's digital security strategy to overcome and fight the increasing threat of cybercrime and cyber terrorism?

METHOD

This research applied descriptive qualitative methods to test this idea, as expressed by (Creswell, 2015). A descriptive qualitative approach allows researchers to describe and understand the context, variables, and dynamics involved in the governance of cyber terrorism-related regulations in Indonesia, and consider their impact on public perception. This method involves a series of steps, starting with the collection of comprehensive data related to the patterns of cybercrime attacks and cyber terrorism in Indonesia. Next, the data will be analyzed using various relevant analytical techniques and tools to identify possible patterns and trends. Once the analysis is complete, the next step is to formulate an appropriate digital security strategy, including the implementation of technologies and policies that are appropriate to the Indonesian context. Finally, conclusions will be drawn to evaluate the effectiveness of the proposed strategy and determine the next steps needed to improve the country's digital security.

The data collection techniques used are document analysis and direct observation of trends and events related to cybercrime. Apart from that, data collection techniques also involve the use of open data sources (open source) in the context of digital security involving utilizing publicly available information from various online sources which can be used for analysis of cybercrime and cyber terrorism in Indonesia including:

1. Cybercrime Reports: International organizations, research institutions, and governments frequently publish reports on cybercrime trends and incidents. Examples of these sources include reports from Interpol, Europol, CERT (Computer Emergency Response Team) Indonesia, Association of Indonesian Internet Service Providers (APJII) and cyber security research institutions.
2. News Websites and Blogs: News and analysis published on news websites and blogs that specialize in coverage of cybercrime and cyberterrorism can be a valuable source of information.
3. Government Public Releases: The government often releases public information about cybercrime incidents and countermeasures. This may include press releases, official statements, or related policy documents.
4. Online Public Data: Publicly available data, such as internet traffic data or financial transaction data published by financial institutions, can provide insight into suspicious or unusual activity related to cybercrime.

RESULT AND DISCUSSION

Cyber Crime Threats

The 1945 Constitution has stated that the Government is responsible for safeguarding and protecting its citizens from the threat of cyber terrorism and the increase in cybercrime. Law No. 5/2018 on the Eradication of the Criminal Acts of Terrorism is one of the regulations established to tackle criminal acts of terrorism and protect Indonesia's sovereignty (Josianto Adam, 2014).

Such regulatory efforts reflect the government's seriousness in facing cybersecurity challenges and creating a legal basis to eradicate terrorism crimes involving the digital domain.

Such regulatory measures not only reflect the government's responsibility in protecting its citizens from the threat of cybercrime, but also demonstrate a response to technological developments and evolving security challenges. The law provides a legal basis for tackling criminal acts of terrorism, including those related to cyberspace, and helps maintain Indonesia's sovereignty in the digital age.

The importance of the law is as a form of prevention and action against cyber threats that can harm not only national security, but also society in general. Thus, this kind of regulation becomes a critical instrument in responding to complex and evolving security challenges in cyberspace.

The role of the Indonesian National Army (TNI) in tackling the threat of cyber terrorism and completing the track record of cyber terrorism with its various modus operandi shows the active involvement of the military sector in maintaining national security, including in the digital realm. The TNI has an important role in protecting Indonesia from domestic and foreign threats, including those from cyberspace (Marimin, 2021).

TNI can play a role in various aspects, such as cyber security capacity building, training personnel to deal with cyber threats, and coordinating with relevant government and private institutions. In the era of evolving information technology, involving the military in countering cyber terrorism can increase the government's responsiveness and effectiveness in dealing with this threat (Marimin, 2021).

The importance of TNI's role in the context of cybersecurity reflects the complexity of modern security challenges involving digital aspects. Inter-agency cooperation, including the role of the TNI, is key to achieving optimal cybersecurity at the national level.

The synergy between the Indonesian National Army (TNI) and state intelligence is very important considering Indonesia's vast position, located at the crossroads between countries with various geopolitics and security. The presence of the TNI in handling the threat of cyber terrorism can complement the role of state intelligence in monitoring and identifying potential threats.

Indonesia as a strategic and geopolitically diverse country requires close collaboration between various security agencies, including the TNI and intelligence, to address complex security challenges. Involving state intelligence can provide in-depth insight into cyber threats that may involve elements from abroad or involve certain geopolitical aspects (Kementerian Pertahanan Republik Indonesia, 2015)

Thus, cooperation between TNI and state intelligence is strategic in creating a strong and responsive cyber security environment amidst changing geopolitical dynamics.

Law No. 5/2018 on the Eradication of the Criminal Acts of Terrorism is a legal foundation that covers state policies and responsibilities in addressing the threat of cyber terrorism in Indonesia. This law provides a legal basis for the eradication of criminal acts of terrorism in all its forms, including those related to the cyber domain.

In the context of cybersecurity, the law may cover aspects such as the definition of cyber terrorism, preventive measures, handling perpetrators, and inter-agency collaboration to counter the threat. Therefore, the Law on the Eradication of Terrorism is an important instrument in the state's

efforts to protect society and infrastructure from the threat of terrorism, including cyber terrorism (Astuti, 2015).

The implementation and enforcement of this law involves cooperation across sectors and security agencies to create an effective and responsive legal environment to the threat of cyber terrorism in Indonesia. In addition to the Act, other legal and policy frameworks may also be required to address the evolving dynamics in the cyber domain (Fitriati, 2016).

Achieving digital security in Indonesia requires strong collaboration from various social strata, state and non-state entities. In this context, several steps and approaches can be part of a joint strategy to improve digital security

Tactics that utilize pseudo-conflicts based on religious dogmatism are indeed often used by terrorists to create divisions in society, they may use religion as a catalyst to create tensions and conflicts among different groups (Mukhammad Ilyasin et al., 2016). Some aspects and impacts of this tactic include:

1. **Breaking Unity**: Terrorists often try to utilize religious differences to break down unity in society. They may stimulate conflict between religious groups with the aim of creating instability and chaos.
2. **Provocation and Provocation**: Terrorists may use provocative religious rhetoric to create tension and stimulate emotional responses from certain groups. This can lead to greater conflict and violence.
3. **Utilization of Social Gaps**: Terrorists may take advantage of social and economic disparities among religious groups to attract support and recruit sympathizers. They may promise to correct existing inequalities or injustices.
4. **Manipulation of Religious Issues**: Terrorists tend to manipulate religious issues for their own benefit. They may use radical or deviant interpretations of religion to justify their violent acts.
5. **Creating Fear and Suspicion**: This tactic can create an atmosphere of fear and suspicion among different religious communities. It can hinder interfaith dialog and worsen intergroup relations.

Religious value-based façades built to foster national solidarity may reflect people's distrust of government power or a desire to utilize religious values as a tool to create social cohesion. When people feel distrustful or dissatisfied with the government, certain parties may try to build facades that emphasize religious values to strengthen unity.

Regulations to monitor the spread of cyber terrorism, especially on social media and websites that support terrorism activities, have become an increasingly urgent need. Social media and online platforms have become the main channels for propaganda, recruitment, and coordination of terrorism activities.

The Ministry of Communication and Information Technology has been monitoring the response of social media accounts to terrorism content with the aim of shutting them down. It is important to note that critical public infrastructure, such as power plants, banks, and telecommunication networks, are vulnerable to cyber terrorism attacks (Nuruzzaman, 2018). Collaboration between

various parties can be the key to success in tackling the threat of cybercrime, with close cooperation among all stakeholders, it can be expected that the response to cybercrime will be more effective and efficient. This will help protect digital infrastructure and overall national security.

The coming together of people and technology has created a new domain of cybersecurity and self-defense. In this context, the notion of cybersecurity and self-defense has become surrounded by various jargons and interpretations (Pradnyana & Rofii, 2020). This phenomenon reflects the complexity and dynamics involved in protecting information and digital infrastructure from the threat of cybercrime, as cybersecurity challenges are not only technological in nature, but also cover broader aspects, including national security. As such, cybersecurity approaches need to include strategies that involve legal and diplomatic aspects, not just military aspects.

The implementation of an online cybersecurity policy is a step to protect against various types of cybercrime, including financial fraud, identity theft, and even the threat of military and terrorist attacks (Saputra, 2016). The Copenhagen securitization approach emphasizes that an issue, in this case cybercrime, is considered a security issue when it is labeled as a threat to the existence of a community or organization with shared values, way of life, or philosophy. Thus, cybersecurity policies can be implemented online to protect against various forms of cybercrime, such as financial fraud, identity theft, military attacks, and terrorism. (Saputra, 2016).

It is important to note that this securitization approach views cybercrime as a threat that can disrupt the stability and sustainability of a social or political entity. Cybersecurity policy therefore includes not only technical efforts to protect digital infrastructure, but also involves legal, diplomatic and collaborative measures to address the threat as a serious security issue. As such, it may include measures such as international cooperation, legislation, and global law enforcement to mitigate the impact of cybercrime.

Misunderstandings or disinformation resulting from the spread of fake news can undermine stability and public trust in institutions and authorities. Therefore, efforts to prevent and counter cybercrime need to be directed not only at technical aspects, but also at digital literacy and public awareness to identify reliable information.

According to Association of Indonesian Internet Service Providers (APJII), in 2023, the number of internet users in Indonesia reached 215.63 million people and there were a total of 167 million social media users, while according to the Central Statistics Agency (BPS) data, the number of smartphone users in Indonesia reached 278.69 million (APJII, 2023). This information reflects the significant growth in internet penetration in Indonesia, indicating that more and more Indonesians are connected to cyberspace. The growth in the number of internet users can lead to various positive impacts, such as increased access to information and communication. However, it can also increase cybersecurity challenges, as more people engage in online activities. Special attention is needed in the development of cybersecurity policies and strategies to anticipate potential risks that may arise along with the growth of internet users. This data shows a high level of vulnerability in the digital world related to cybercrime.

The data also reflects that more comprehensive regulations are less effective. The advancement of more sophisticated hacking techniques opens the door for anti-terror regulations to fail in cyberspace and may even increase the risk of counterproductive or harmful physical terror in the future.

In this context, authoritarian governments in the country have policies that give them full authority to enhance cybersecurity to the extent that they can stop activities such as data mining, terrorism-related communications, or propaganda dissemination. Cyber criminals who continuously expand cyber terrorist recruitment are classified as follows (Kominfo, 2023).

Malicious schemes are reflected in the prevalence of cybercrime and the effectiveness of sophisticated cyber detection technologies in targeting all victim data. Massive cyberattacks can wipe out a country's critical data, creating a serious threat to the political, ideological, and religious aspects of a country (Loqman & Rahman, 2020). Cyber terrorists tend to utilize vulnerable social media accounts to collect sensitive information. For example, they may use the trap of a successful cybercriminal capturing something, such as stolen money. By using funds obtained from criminal activities, cyber criminals have the ability to support additional criminal activities online. This gives them the opportunity to expand their terror networks and complete their cybercrime cycle (A. Adang Supriyadi, 2023).

Such activities can include spreading terror propaganda, mobilizing public opinion, and even carrying out more sophisticated cyberattacks. Therefore, engaging in cybercrime not only provides financial benefits for the perpetrators, but also gives them the power to plan and execute acts of cyber terrorism that can harm the stability and security of a country. In this context, the protection of cybersecurity is crucial to prevent the escalation of cybercrime that could lead to a greater threat of cyber terrorism.

The data obtained is from January 1, 2023 to the third week of November 2023 and is expected to provide an overview of cybercrime incidents in Indonesia in 2023.

Online Buying and Selling Fraud

Online buying and selling became the most frequently reported activity and the main focus of cybercrime, dominating 1st place with 53,793 incidents, accounting for 45.87% of the total reports. While scamming ranked 3rd with 12,472 incidents, or about 10.63% of the total reports, unreal online investments or fraudulent practices in online freelance work, which harmed many job seekers, ranked 3rd with 9,810 reports or 8.36%. This crime involves a fraud mode in which the perpetrators deceive victims by offering promises of large profits, then asking victims to transfer a certain amount of money to the fraudsters. In the next rank, there were reports related to online gambling activities totaling 9,618 or 7.13% of the total reports (Tanujaya, 2023).

Fictitious online investment or online freelance work scams that are very much taking victims of job seekers and then deceiving their victims to deposit money to fraudsters with the lure of large profits ranked 3rd with 9,810 reports or 8.36% followed by reports on Online Gambling activities of 9,618 or 7.13% of the total reports, the presence of Online Gambling which is a source of concern among the public, reports related to Online Extortion also reached a fairly high number, as many as 8,368 reports or 7.13%. In fact, this figure exceeds the number of reports related to Online Loan incidents, such as threats from debt collectors or data misappropriation in the context of Online Loans which reached 4,573 reports or 3.90%, Web Phishing ranked ninth with a total of 2,539 reports or 2.16%, which is often used as a fraudulent method to steal important credentials such as login information, passwords, and mobile banking PINs. In the tenth position, there were reports of Online Prostitution totaling 1,851 or 1.58% (Tanujaya, 2023).

WhatsApp Most Reported

If you are curious about what media is most often used to commit crimes in 2023, then Whatsapp, Instagram, and Facebook (Meta group) dominate 71.35% of the total reports, TikTok, with the popularity of the number of users not inferior to Instagram, only ranks 10th with 176 reports or only about 0.15% of the total. The most used social media for criminal acts is Whatsapp, dominating the first rank with 50,218 reports or around 42.89%, followed by Instagram which ranks second with 20,631 reports or around 17.62%, while Telegram comes in 3rd after Instagram, with a total of 12,817 reports or around 10.95% of the total social media reports most often used to commit crimes in Indonesia in 2023. Outside of platforms from the Meta group and Telegram, other platforms used to commit crimes include Website with 3,678 reports or around 3.14%, Michat with 1,345 reports or around 1.15%, Twitter or X which is in 9th place with 1,100 reports or around 0.94%, and TikTok in 10th place (Arradian, 2023).

The government faces the challenge of optimizing the effectiveness of regulations and designing an integrated regulatory pattern to maintain the security of the national environment from various threats coming from cybercrime. Better alignment and design of regulations, as well as harmonious integration within the cybersecurity framework, play an important role in maintaining national security and resilience from various forms of threats originating from cybercrime.

Cyber Terrorism Threat

The establishment of the National Cyber and Crypto Agency (BSSN) under Presidential Regulation No. 53/2017 aims to improve Indonesia's capability to respond to and counter increasingly complex cybercrime threats. With BSSN, the government seeks to harmonize efforts and resources to maintain security in cyberspace, including in protecting the country's critical infrastructure and important data. BSSN focuses on improving security in the digital environment in the digital economy era, protecting public safety, and holding cybercriminals accountable for their actions (Sudarmadi et al., 2019).

The development of BSSN also reflects an awareness of the importance of coordination and collaboration at the national level in facing cybersecurity challenges. With the authority granted to BSSN, it is expected to create effective synergy between relevant parties in formulating policies, conducting early detection, and providing rapid responses to cybercrime threats that may threaten national sovereignty and stability (Sudarmadi et al., 2019)

On December 1, 2020, the third sub-regional meeting took place in Jakarta, involving Indonesian policymakers, including the Coordinating Ministry for Political, Legal and Security Affairs. The meeting focused on the issue of Counter-Terrorism and Transnational Security (SRM on CTTS) (Rifawan & Wibawa, 2021). The meeting aimed to discuss strategies and cooperation between countries in facing transnational security challenges, especially terrorism and cybercrime. Participants discussed concrete steps to strengthen regional cooperation and improve responses to threats involving technology and cyberspace. In addition, the meeting served as a platform to exchange intelligence information and coordinate efforts to combat terrorism and cybercrime at the sub-regional level. This meeting is the beginning of an awareness effort to eradicate terrorism both digitally and physically. Various lines in Indonesia integrate and contribute to BSSN as part of enhanced cooperation.

In this context, awareness and collaboration are key in building a solid defense against the threat of terrorism, including in the digital realm. The involvement of various sectors and government agencies reflects a shared commitment to creating a safe and secure environment from various types of security threats.

BSSN has engaged a number of key facilitators in its efforts to address cybersecurity, including agencies such as the Indonesian National Police (POLRI), the National Counterterrorism Agency (BNPT), the Financial Transaction Reports and Analysis Center (PPATK), the National Intelligence Agency (BIN), the Ministry of Foreign Affairs (MoFA), the Coordinating Ministry for Political, Legal and Security Affairs (Kemenkopolhukam), the Ministry of Communication and Information Technology (Kemenkominfo), the Ministry of Law and Human Rights (Kemenkumham), and the Ministry of Defense(BSSN, 2023). The existence and involvement of these institutions reflect the Indonesian government's serious commitment to addressing cybersecurity challenges holistically.

In this context, inter-agency cooperation is very important to deal with the threat of cyber terrorism. BSSN's collaboration with various government agencies covers aspects of cybersecurity, ranging from policing, counter-terrorism, financial analysis, to international relations and defense. By involving these various sectors, the Indonesian government seeks to address the threat of cybercrime in a comprehensive and effective manner.

Involving various ministries and agencies in cybersecurity efforts shows the seriousness of the Indonesian government in responding to the complex challenges that arise in the digital world. This increased cross- sectoral cooperation is expected to provide a fast and efficient response to the evolving threats in the cyber domain.

Measuring the prevalence of security organizations in Indonesia does not directly reflect the actual level of cybercrime. Preventing the spread of terrorist activities in Indonesia requires synergy between higher and lower levels of government. Success in preventing terrorism, including cyber terrorism, is not only the responsibility of the central government, but also involves the participation and cooperation of local governments, local communities, and the private sector (Sudarmadi et al., 2019).

Joint efforts from different levels of government and sectors can create a strong ecosystem to fight cybercrime. Empowering local authorities, educating the public, and involving the private sector in improving cybersecurity can be key to success. In this context, inter-agency collaboration and active participation from all levels of society are important to create a safer and more resilient environment against terrorism threats, including those from the cyber domain.

In order to maximize the strengthening of the powers, positions, and functions of the leadership of the National Counterterrorism Agency (BNPT) in 2020, BNPT took an active role in managing illegal activities. The overall proportion of cybercrime can be described as follows. In 2021, IDR 304,700,000,000 is required to fund efforts to combat cyber terrorism and cybercrime. Funding allocated to the National Counterterrorism Agency (BNPT) in the same year reached IDR 515,900,000,000, in accordance with the plan prepared by the head of BNPT. The funding plan of IDR 515,900,000,000 aims to strengthen efforts to counter terrorism and cybercrime. With a significant allocation of funds, BNPT hopes to increase efficiency and effectiveness in countering

the threat of terrorism, especially in the cyber domain. This financial support is expected to strengthen the country's capacity to address security challenges that develop in the digital world.

In the face of internet dependency and the growing threat of cyber terrorism, Indonesia needs to implement a long-term strategy. This could include strengthening the regulatory framework, enhancing international cooperation, and increasing cybersecurity capacity across all sectors. In addition, a holistic approach involving the government, private and civil society sectors can help create a more resilient cybersecurity ecosystem. In addition, increasing public awareness of cyber risks is also key in prevention efforts. Through these measures, it is hoped that Indonesia can reduce the risk of cyber terrorism and protect its digital infrastructure.

At the same time, enforcement of cybersecurity regulations in Indonesia has made limited progress. BSSN, as the lead agency in this effort, has a specific mission to address cybercrime and other online risks. As such, improving the capacity and effectiveness of BSSN is key in enforcing cybersecurity regulations. Proactive measures in detecting, preventing and responding to cyber threats should be continuously improved to mitigate the risks that Indonesia may face in the digital realm.

Preventive measures against cyber terrorism in Indonesia still show shortcomings in the existing regulatory framework, especially in Law No. 15 Year 2003 on Eradication of Criminal Acts of Terrorism and Law No. 11 Year 2008 on Electronic Information and Transactions (ITE) (JDIH, 2003). Further review and updating of these regulations is required in order to address the current challenges related to cyber terrorism.

Despite updates in countering cyber terrorism, such as the establishment of the National Cyber and Crypto Agency (BSSN) and the sub-regional meeting on Counter-Terrorism and Transnational Security in December 2020, further improvements in the regulatory aspects are still needed to address the dynamic developments in the realm of cyber terrorism. Enhanced cooperation and coordination between various agencies, such as the Coordinating Ministry for Political, Legal and Security Affairs, the Indonesian National Police (POLRI), the National Counterterrorism Agency (BNPT), and BSSN, needs to be strengthened to achieve optimal effectiveness in preventing cyber terrorism in Indonesia.

CONCLUSION

A holistic approach to cybersecurity involves more than just government regulations. Raising awareness and safe internet practices at the community level is crucial. Initiatives to educate about cybersecurity risks, teach digital safety practices, and encourage responsible use of technology can help engage communities in protecting against cyber terrorism. Thus, collaboration between the government, the private sector, and the community can be key to effectively addressing cybersecurity challenges.

Cybersecurity awareness is key in engaging the public in protection against cybercrime. Socialization efforts that involve a broader segment of society will help increase understanding of potential risks and how to protect themselves from cyberattacks. Training, seminars and educational campaigns can help educate the public on good digital security practices. With this

increased awareness, it is hoped that people can be more proactive in keeping their information and data safe.

Cybercrime is indeed a form of national insecurity in cyberspace. Indonesia, like other countries, is vulnerable to cyberattacks that can be detrimental to national security. These attacks can include the theft of sensitive data, sabotage against critical infrastructure, or even cyber activities related to terrorism.

It is important to continue to increase efforts to improve cybersecurity, including strengthening regulations, increasing public awareness, and improving response capabilities to cybersecurity incidents. These proactive measures arie expected to minimize the impact of potential cyberattacks on national security.

Meanwhile, cyber terrorism is a serious threat that needs to be addressed seriously by the Indonesian government. Although there have been efforts and regulations implemented, such as the establishment of the National Cyber and Crypto Agency (BSSN) and sub-regional meetings on Counter-Terrorism and Transnational Security, there are still some challenges and shortcomings in handling cyber terrorism.

Some of the obstacles involve the mismatch between the implementation of intelligence missions and the prosecution of terrorism crimes, the lack of coordination and cooperation between agencies, and the expansion of cyber terrorist modus operandi that continues to grow. In addition, existing regulations may not be fully adequate to address the dynamic developments in the cyber terrorism domain.

In facing this challenge, further improvements in regulatory aspects, increased cross-agency cooperation, and efforts to continue to understand and anticipate new methods that may be used by perpetrators of cyber terrorism are needed. Only with these measures, Indonesia can increase its effectiveness in preventing and countering cyber terrorism, maintaining national security in an increasingly complex digital world.

REFERENCE

A. Adang Supriyadi. (2023). *CYBERTERRORISM* (Issue November). Badan Nasional Penanggulangan Terorisme.

Abdullah, F. M. (2019). Menggunakan analisis data besar untuk memprediksi dan mengurangi kejahatan dunia maya. *Jurnal Internasional Teknik Dan Teknologi Mesin*, *10*(1), 1540–1546.

Aditiawarman, Mac, D. (2019). Hoax dan Hate Speech di Dunia Maya. In *Lemabaga Kajian Aset Budaya Indonesia Tonggak Tuo*. LEMBAGA KAJIAN ASET BUDAYA INDONESIA.

APJII. (2023). *Survei APJII Pengguna Internet di Indonesia Tembus 215 Juta Orang*. Asosiasi Penyelenggara Jasa Internet Indonesia. https://apjii.or.id/berita/d/survei-apjii-pengguna-internet-di-indonesia-tembus-215-juta-orang

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 INFRASTRUC. *Jurnal Pertahanan & Bela Negara*, *9*(1), 13–30.

Arradian, D. (2023). *WhatsApp, Instagram, dan Facebook Jadi Media Sosial Favorit Penjahat Siber di Indonesia*. Sindo News. https://tekno.sindonews.com/read/1259453/207/whatsapp-instagram-dan-facebook-jadi-media-sosial-favorit-penjahat-siber-di-indonesia-1700791863

Arvianto, A. (2021). *Cyber Security, Mitigasi Risiko dan Eksploitasi Teknologi*. Kementerian Keuangan Republik Indonesia. https://www.djkn.kemenkeu.go.id/kpknl-ambon/baca-artikel/14014/Cyber-Security-Mitigasi-Risiko-dan-Eksploitasi-Teknologi.html

Astuti, S. A. (2015). Law Enforcement of Cyber Terorism in Indonesia. *Rechtsidee*, *2*(2), 157–178. https://doi.org/10.21070/jihr.v2i2.82

BSSN. (2023). *BSSN Bersama Kementerian/Lembaga Terkait Sepakati Finalisasi Pembahasan Rencana Aksi Nasional Keamanan Siber Tahun 2023*. BSSN.Go.Id. https://www.bssn.go.id/bssn-bersama-kementerian-lembaga-terkait-sepakati-finalisasi-pembahasan-rencana-aksi-nasional-keamanan-siber-tahun-2023/

Budi, E., Wira, D., & Infantono, A. (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional. *Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia P-ISSN 2086-5805 Akademi Angkatan Udara*, *3*(November), 24–25. https://doi.org/10.54706/senastindo.v3.2021.141

Creswell, J. W. (2015). *Penelitian kualitatif & desain riset*. Pustaka Pelajar.

Djanggih, H., & Qamar, N. (2018). Penerapan Teori-Teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime). *Pandecta: Research Law Journal*, *13*(1), 10–23. https://doi.org/10.15294/pandecta.v13i1.14020

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

Endang Nurdin. (2020). *Perang melawan radikalisasi: "Mereka menuduh kami lebih kafir dari polisi", kata adik trio Bom Bali I terkait upaya "membina mantan napiter."* BBC News Ndonesia. https://www.bbc.com/indonesia/indonesia-50408540

Fitriati, R. (2016). *Membangun Model Kebijakan Nasional Keamanan Siber Dalam Sistem Pertahanan Negara*.

Hammam Riza, David Darmawan, Indra Utoyo, Thomas Lahey, Jamalul Izza, Edwin Lim, Rohit Kumar, & Wendi usino. (2016). *Data and Cyber Security: technology, use cases and Governance* (Dr. Rudi Rusdiah, Ed.; Vol. 4, Issue 1). Perkempulan Basis Data Indonesia.

Hapsari, R. D., & Pambayun, K. G. (2023). ANCAMAN CYBERCRIME DI INDONESIA: Sebuah Tinjauan Pustaka Sistematis. *Jurnal Konstituen*, *5*(1), 1–17. https://doi.org/10.33701/jk.v5i1.3208

JDIH. (2003). *UU No. 15 Tahun 2003 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme, Menjadi Undang-Undang.*

Jerry Indrawan. (2019). Cyberpolitics sebagai Perspektif Baru Memahami Politik di Era Siber. *Jurnal Politika*, *10*(1), 1–15.

Josianto Adam, A. (2014). Tindak Pidana Cyber Terrorism Dalam Transaksi Elektronik. *Lex Administratum*, *2*(3), 164–173.

Kementerian Pertahanan Republik Indonesia. (2015). *Buku Putih Pertahanan Indonesia 2015*.

Kominfo. (2023). *Pemerintahan Digital Ditopang Keamanan Siber*. Menkominfo. https://www.kominfo.go.id/content/detail/49533/pemerintahan-digital-ditopang-keamanan-siber/0/berita

Loqman, L., & Rahman, A. (2020). Implikasi Diplomasi Pertahanan terhadap Keamanan Siber dalam Konteks Politik Keamanan. *Jurnal Diplomasi Pertahanan*, *6*(2), 1–93.

Machmiyah, S., A'yuni, R. Q., Putri, V. Z. E., Dewangga, A. S., Dewi, Q. P., Fatharani, R. B., Gunawan, N. R., Putri, N. A. P., Afifah, N. Z., Pamadya, E. V., Yoga, A. A., Agus, K. W., Khairunnisa, D. A., Yasa, Lestari, P., & Rakasiw, G. A. A. (2017). From Citizen To Netizen. In *Laboratorium Penelitian dan Pengembangan FARMAKA TROPIS Fakultas Farmasi Universitas Mualawarman, Samarinda, Kalimantan Timur* (Issue September).

Marimin, M. (2021). Politik Kriminal Peran Tentara Nasional Indonesia (TNI) Dalam Penanganan Pemberantasan Terorisme Di Indonesia. *Jurnal Hukum Progresif*, *9*(1), 74–86. https://doi.org/10.14710/jhp.9.1.74-86

Millman, C. M., Winder, B., & Griffiths, M. D. (2017). UK-Based Police Officers' Perceptions of, and Role in Investigating, Cyber-Harassment as a Crime. *International Journal of Technoethics (IJT)*, *8*(1), 87–102. https://doi.org/http://doi.org/10.4018/IJT.2017010107

Moubayed, N. Al, Wall, D., & McGough, A. S. (2017). Identifying changes in the cybersecurity threat landscape using the LDA-web topic modelling data search engine. *Conference: International Conference on Human Aspects of Information Security, Privacy, and Trust*, *10292 LNCS*(January 2018), 287–295. https://doi.org/10.1007/978-3-319-58460-7_19

Muhammad, K., Firdaus, S. U., Hasrul, M., & Aci, L. (2023). Kebijakan Publik dan Politik Hukum: Membangun Demokrasi Berkelanjutan untuk Masyarakat. *Souvereignty*, *2*(4), 354–368.

Muhammad Mumtaaz, G., Rafif Wardhana, T., & Harnung Diastutui, F. (2021). ANTI CYBER TERORISM SEBAGAI UPAYA STRATEGIS DALAM MENANGGULANGI CYBER TERORISM DI INDONESIA. *Al-Hakam Islamic Law & Contemporary Issues*, *2*(2), 48–59.

Mukhammad Ilyasin, M. Abzar D, & Mohammad Kamaluddin. (2016). *Teroris Dan Agama*.

Nurlatun, R., Nayoan, H., & Pangemanan, F. (2021). Upaya Pemerintah Dalam Mengatasi Penyebaran Berita Palsu (Hoax) di Media Sosial (Studi Kasus Dinas Kominfo Kota Manado). *JURNAL GOVERNANCE*, *1*(2), 1–8.

Nuruzzaman, M. (2018). TERORISME DAN MEDIA SOSIAL SISI GELAP BERKEMBANGNYA TEKNOLOGI INFORMASI KOMUNIKASI. *Syntax Literate : Jurnal Ilmiah Indonesia*, *3*(9), 61–76.

Pansariadi, R. S. B., & Soekorini, N. (2023). Tindak Pidana Cyber Crime dan Penegakan Hukumnya. *Binamulia Hukum*, *12*(2), 287–298. https://doi.org/10.37893/jbh.v12i2.605

Pradnyana, I. P. H., & Rofii, M. S. (2020). Ancaman Cyberterrorism di Indonesia dan Respons Negara. *Literatus*, *2*(2), 181–191. https://doi.org/10.37010/lit.v2i2.92

Raharjo, A., Bintoro, R. W., Ajeng, N., & Utami, T. (2022). The Legal Policy of Criminal Justice Bureaucracy Cybercrime. *Bestuur*, *10*(2), 105–122.

Rahmawati, C. (2019). Tantangan Dan Ancaman Keamanan Siber. *SENASTINDO AAU*, *1*(1), 299–306.

Ramadhan, I. (2020). Cyber-Terrorism in the Context of Proselytizing, Coordination, Security, and Mobility. *Islamic World and Politics*, *4*(2), 180–197.

Rifawan, A., & Wibawa, S. (2021). Perlindungan Warga Negara Indonesia di Luar Negeri dari Keterlibatan Pendanaan Terorisme. *Jurnal Majelis, Media Aspirasi Konstitusi*, *3*.

Rozika, W. (2017). Propaganda dan Penyebaran Ideologi Terorisme Melalui Media Internet (Studi Kasus Pelaku Cyber Terorisme oleh Bahrun Naim). *Jurnal Ilmu Kepolisian*, *89*(2005), 122–134.

Santoyo. (2008). Penegakan Hukum di Indonesia. *Jurnal Dinamika Hukum*, *8*(3), 199–204.

Sanur, D. (2016). Upaya Penanggulangan Terorisme ISIS di Indonesia Dalam Melindungi Keamanan Nasional. *Jurnal Politica*, *07*(1), 25–47.

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

Soesanto, E., Romadhon, A., Dwi Mardika, B., & Fahmi Setiawan, M. (2023). Analisis dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital Untuk Mengamankan Objek Vital dan File. *SAMMAJIVA : Jurnal Penelitian Bisnisdan Manajemen*, *1*(2), 186.

Sri Yunanto, Angel Damayanti, I. N. (2017). Ancaman Dan Strategi Penanggulangan Terorisme Di Dunia Dan Indonesia. In *Pertumbuhan Asuransi Syariah Di Dunia Dan Indonesia: Vol. III. No.1.* (Issue PERTUMBUHAN ASURANSI SYARIAH DI DUNIA DAN INDONESIA).

Sudarmadi, D. A., Josias, A., & Runturambi, S. (2019). Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional*, *2*(2).

Supanto, Ismunarno, Parwitasari, T. A., & Budyatmojo, W. (2023). Pencegahan dan Penanggulangan Kejahatan Teknologi Informasi Di Wilayah Pdm Kabupaten Klaten Melalui Metode Sosialisasi Interaktif. *Jurnal Gema Keadilan*, *10*(3), 170–182.

Tanujaya, A. (2023). *Statistik Kejahatan Siber di Indonesia Selama 2023*. DetikInet. https://inet.detik.com/security/d-7054249/statistik-kejahatan-siber-di-indonesia-selama-2023

Yuniarto, P. R. (2015). Masalah Globalisasi di Indonesia: Antara Kepentingan, Kebijakan, dan Tantangan. *Jurnal Kajian Wilayah*, *5*(1), 67–95.