Sortuz. Oñati Journal of Emergent Socio-legal Studies
Volume 16, Issue 1 (2026), 5-24
ISSN 1988-0847
DOI link: https://doi.org/10.35295/sz.iisl.2409

Law enforcement of cyber terrorism crimes in strengthening national data security from the perspective of Indonesian positive law

Karina Frity Rahmasari[1]
Al Pink Saputra Napitupulu[2]
Anida Nadyana Novauzyah[3]
Sahat Maruli Tua Situmeang[4]

Abstract:

Cyberterrorism constitutes an advanced and rapidly evolving form of transnational crime that exploits information and communication technologies to compromise national data security, disrupt digital infrastructures, and endanger public welfare. This study examines the adequacy of Indonesian positive law in responding to cyberterrorism, especially its implications for vital sectors such as transportation, energy, finance, and public services, all of which rely heavily on interconnected digital systems and are increasingly vulnerable to extensive operational failures. Using a descriptive-analytical method grounded in a normative legal approach, the research reviews statutory regulations to identify weaknesses within the current legal framework. The findings indicate that Indonesia lacks specific legislation governing cyberterrorism, creating legal uncertainty, evidentiary challenges, jurisdictional conflicts, and difficulties in attributing liability to anonymous perpetrators. Existing laws—including the ITE Law, Anti-Terrorism Law, and the Cybersecurity and Resilience Bill—remain fragmented. Strengthening Indonesia's legal architecture through specialized legislation and improved institutional coordination is therefore essential.

[1] Karina Frity Rahmasari, Fakultas Hukum Universitas Komputer Indonesia, Jl. Dipatiukur No. 102-118, Kota Bandung, Jawa Barat 40132- Email: karina.31622007@mahasiswa.unikom.ac.id
[2] Al Pink Saputra Napitupulu, Fakultas Hukum Universitas Komputer Indonesia. Email: alpink.31622012@mahasiswa.unikom.ac.id
[3] Anida Nadyana Novauzyah, Fakultas Hukum Universitas Komputer Indonesia. Email: anida.31622015@mahasiswa.unikom.co.id
[4] Sahat Maruli Tua Situmeang, Fakultas Hukum Universitas Komputer Indonesia. Email: sahat@email.unikom.ac.id , https://orcid.org/0009-0003-6893-3958

Keywords:

Cyber terrorism, Indonesian positive law, law enforcement, national data security, regulations

Resumen:

El ciberterrorismo constituye una forma avanzada y en rápida evolución de la delincuencia transnacional que aprovecha las tecnologías de la información y la comunicación para comprometer la seguridad de los datos nacionales, perturbar las infraestructuras digitales y poner en peligro el bienestar público. Este estudio examina la idoneidad del derecho positivo indonesio para responder al ciberterrorismo, especialmente sus implicaciones para sectores vitales como el transporte, la energía, las finanzas y los servicios públicos, todos los cuales dependen en gran medida de sistemas digitales interconectados y son cada vez más vulnerables a fallos operativos de gran alcance. Utilizando un método descriptivo-analítico basado en un enfoque jurídico normativo, la investigación revisa las regulaciones legales para identificar las debilidades del marco jurídico actual. Las conclusiones indican que Indonesia carece de una legislación específica que regule el ciberterrorismo, lo que genera incertidumbre jurídica, dificultades probatorias, conflictos jurisdiccionales y dificultades para atribuir la responsabilidad a los autores anónimos. Las leyes existentes, entre ellas la Ley ITE, la Ley Antiterrorista y el Proyecto de Ley de Ciberseguridad y Resiliencia, siguen siendo fragmentadas. Por lo tanto, es esencial reforzar la arquitectura jurídica de Indonesia mediante una legislación especializada y una mejor coordinación institucional.

Palabras clave:

Ciberterrorismo, derecho positivo indonesio, aplicación de la ley, seguridad nacional de los datos, normativa

TABLE OF CONTENTS

1. INTRODUCTION

The Internet refers to a vast network of interconnected computer systems comprising numerous smaller networks with diverse structures and protocols. It originated from a visionary scientific initiative aimed at developing a unified global platform capable of enabling seamless information exchange across geographical boundaries. Over time, this concept evolved into what is now recognized as the modern Internet, operating through standardized communication protocols — most notably the Transmission Control Protocol/Internet Protocol (TCP/IP) — which ensure accurate and reliable data transmission between digital systems worldwide. Initially designed for academic and governmental communication needs, the Internet later expanded into a global public infrastructure that fundamentally transformed how individuals interact, access information, and conduct economic as well as commercial activities (Goni *et al.* 2022).

In Indonesia, commercial Internet services became publicly accessible around 1994, marking the beginning of nationwide connectivity and the rapid expansion of digital infrastructure (Goni *et al.* 2022). Since then, Internet usage has grown exponentially, supported by the increasing availability of digital services and the expansion of information networks (Lewis 2024). According to recent national digital-use reports, Indonesia has one of the largest and fastest-growing Internet user populations in Southeast Asia, contributing significantly to the development of the country's digital economy (Lesmana *et al.* 2023). This advancement has provided substantial benefits, including improved access to information, enhanced communication, and the acceleration of economic and public-service innovation (Fahriza *et al.* 2024). However, rapid digital development has also introduced new security threats, most notably cyber terrorism, which involves the use of digital technologies by individuals or groups to instill fear, disrupt public order, or compromise national security systems (Astuti 2015). As Indonesia's digital connectivity continues to expand, the risk of cyberattacks targeting critical sectors—such as financial institutions, transportation networks, and governmental databases—also increases, creating vulnerabilities that may lead to severe operational and economic disruptions (Bakry *et al.* 2021). These conditions underscore the urgent need for robust cybersecurity frameworks, strengthened law-enforcement capacity, and enhanced interagency and international cooperation to protect national digital infrastructure (Hartati and Muhammad 2023).

Recent digital-use reports show that Indonesia has one of the largest and fastest-growing Internet user populations in Southeast Asia, with Internet penetration continuing to rise annually in line with the expansion of digital infrastructure and public reliance on online services (Lesmana *et al.* 2023). Within this rapidly expanding digital ecosystem, cyberterrorism has emerged as a contemporary form of crime that exploits information technology to threaten national data security and societal stability (Astuti 2015). This study aims to evaluate the effectiveness of Indonesia's positive legal system in addressing cyberterrorism and to examine the implications of cyber-based attacks on critical national infrastructure, including transportation, energy, and public service systems, which are highly vulnerable to disruptions and may incur substantial economic losses (Bakry *et al.* 2021). Methodologically, this research adopts a descriptive-analytical approach grounded in normative legal analysis, relying on statutory laws and regulations as primary data sources (Pati *et al.* 2023). The findings indicate that Indonesia still lacks explicit legal provisions specifically regulating cyberterrorism, resulting in legal uncertainty and enforcement

challenges (Hartati and Muhammad 2023). These circumstances underscore the urgent need to reinforce Indonesia's legal framework and to strengthen international cooperation to address the increasingly complex threat of cyberterrorism more effectively (Billow 2024).

In recent years, terrorism—including cyberterrorism—has become a central focus of public attention across both print and electronic media (Astuti 2015). One significant case of cyberterrorism in Indonesia is the Brain Cipher ransomware attack targeting the National Data Center (PDN), which encrypted and restricted access to essential government data managed by ministries and various state agencies (Buana 2024). The incident severely disrupted public services and resulted in operational disturbances across approximately 239 government institutions (Buana 2024).

As a state responsible for safeguarding human dignity and national security, Indonesia has enacted several legal instruments to address the growing threat of terrorism. The government strengthened its counterterrorism framework through Law of the Republic of Indonesia Number 5 of 2018, which amended Law Number 15 of 2003 that previously ratified Government Regulation in Lieu of Law Number 1 of 2002 on Terrorism Crimes. The reinforcement of this legal framework is essential, as terrorism—particularly in its evolving cyber form—is recognized as an extraordinary crime requiring comprehensive and extraordinary measures for its prevention and eradication (Astuti 2015, Bakry *et al.* 2021, Hartati and Muhammad 2023).

However, to date, Indonesia does not yet have specific legislation that explicitly regulates cyberterrorism. This legal vacuum creates significant uncertainty regarding the legal basis for investigating and prosecuting cyber-terror offenses. Recent legal analyses emphasize that although existing instruments—such as the Electronic Information and Transactions Law (ITE Law) and Law No. 5 of 2018 on the Eradication of Terrorism—provide partial authority for handling cyber-based threats, they still do not define "cyberterrorism" or provide a tailored regulatory framework for digital-based terror acts (Paminto 2022). Therefore, it is essential to conduct a comprehensive study evaluating the effectiveness of Indonesia's current legal instruments in addressing cyberterrorism and their impact on the protection of critical national infrastructure. A comprehensive study in this context includes examining (1) legal clarity and definitional precision; (2) substantive and procedural adequacy of existing laws; (3) enforcement capability, including digital forensics and inter-agency coordination; (4) judicial outcomes related to cyber-based terrorism cases; and (5) national cyber-resilience, particularly preventive and protective measures for critical infrastructure.

2. LITERATURE REVIEW

Cyberterrorism constitutes a criminal offense perpetrated by individuals or groups driven by ideological or political motives (Holt and Bossler 2022). These acts typically involve cyberattacks, the destruction of digital information, disruption of computer networks, and interference with technological infrastructure (Weimann 2015). Radical groups increasingly utilize social media platforms to disseminate propaganda, recruit members, and broaden their operational influence (Aly *et al.* 2017). As Margaret Thatcher famously stated, "publicity is the oxygen of terrorism," underscoring how media exposure amplifies the psychological impact of terror acts on domestic and global audiences (Thatcher 1985).

Cyberterrorism comprises two core dimensions. First, it functions as a communication and coordination channel for extremist networks, enabling propaganda dissemination, recruitment, fundraising, money laundering, and online training (Conway 2017). Second, it operates as a direct attack vector in which terrorist groups exploit cyber vulnerabilities to conduct espionage, data theft, sabotage, or disruptions targeting governmental and civilian digital infrastructure (Weimann 2020). This dual nature of cyberterrorism enables extremist actors to circumvent traditional security mechanisms and expand their global operational footprint with minimal physical presence (Holt and Bossler 2021).

Cyberterrorism refers to two core activities, namely, as a means of communication and coordination related to the use of cyberspace, particularly the internet, to spread propaganda, conduct recruitment, raise funds, launder money, and train members. The second core is a direct target, as it involves the exploitation, theft, and destruction of facilities related to the cyber field owned by the government or civil society (Pradnyana and Rofii 2020). The rapid advancement of information and communication technology has enabled terrorist organizations to expand their operational reach. Cyberspace is used not only as a means of communication but also as a direct target for cyber-attacks. These attacks aim to instill fear, cause economic disruption, and weaken national security. Cyberterrorism has become a growing concern globally due to its ability to bypass traditional security measures and cause widespread harm to national infrastructures without direct physical violence (Pradnyana and Rofii 2020).

The accuracy of the universally accepted working definition of cybercrime is still debated in academic literature (Phillips *et al.* 2022). Cyberterrorism operates through two primary mechanisms that enable extremist actors to exploit digital ecosystems for ideological or political purposes (Weimann 2020). First, it serves as a medium for communication and coordination among terrorist networks, utilizing digital platforms to disseminate propaganda, recruit members, raise funds, and conduct operational planning (Conway 2017). Terrorist groups increasingly leverage encrypted messaging applications and decentralized online networks to evade detection and monitoring by law enforcement authorities (Aly *et al.* 2017). Second, cyberterrorism directly targets critical infrastructure by exploiting security vulnerabilities within digital systems (Holt and Bossler 2021). This includes cyber espionage, data theft, intrusions into government databases, and the deployment of ransomware attacks against essential governmental and civilian services (Weimann 2020). A prominent example is the Brain Cipher ransomware attack on Indonesia's National Data Center (PDN), which encrypted vital government data and disrupted the operations of approximately 239 government institutions, significantly impairing public service delivery (Muhammad Sukardi 2024).

A recent development in cyberterrorism is the rise of leaderless resistance, commonly referred to as "lone wolf" terrorism (Spaaij 2012). This phenomenon involves individuals or small groups acting independently of formal terrorist organizations and typically becoming radicalized through online extremist content (Gill *et al.* 2014). Although the scale of such attacks is often smaller, their anonymity and unpredictability create significant challenges for law enforcement agencies attempting to detect and prevent them (Hoffman *et al.* 2020). The increasing proliferation of actors who are recruited, influenced, and mobilized via digital platforms contributes to a "domino effect" that reinforces and disseminates ideological violence across networks (Weimann 2020).

As a country committed to maintaining national security, Indonesia has established various legal frameworks to combat terrorism. One of the key regulations is Law Number 5 of 2018, which revises Law Number 15 of 2003 and affirms Government Regulation in Lieu of Law Number 1 of 2002 on Terrorism Crimes. According to Article 1 of Law Number 5 of 2018, terrorism is defined as any act of violence or threat of violence that creates a widespread atmosphere of terror or fear, potentially resulting in mass casualties and/or causing damage or destruction to strategic vital objects, the environment, public facilities, or international facilities, with ideological, political, or security disruption motives. Although Indonesia has enacted general counter-terrorism legislation, academic analyses show that current laws do not explicitly define or criminalize "cyberterrorism," leaving a regulatory gap in handling cyber-based terror offenses (Astuti 2015, Bakry *et al.* 2021). The absence of a clear legal framework raises uncertainty regarding the prosecution of cyber-based terrorist activities and highlights the need for legal reform.

Internet technology, on the one hand, provides progress, but on the other hand, it also hurts human civilization (Carthy *et al.* 2020). It is a common understanding that something can be good or bad depending on the user. The increasing sophistication of cyberterrorism presents substantial challenges for law enforcement and national cybersecurity governance (Weimann 2020). One major challenge is the lack of legal clarity in defining and prosecuting cyberterrorism offenses within Indonesia's current regulatory framework (Astuti 2015). In the absence of a dedicated cyberterrorism statute, authorities continue to rely on general cybercrime provisions under Law Number 11 of 2008 on Electronic Information and Transactions (ITE Law), which are often insufficient to address the complex, ideological, and transnational nature of cyberterrorism cases (Bakry *et al.* 2021). Another challenge lies in the rapid technological adaptation of terrorist networks, as these groups continually enhance their cyber capabilities, making it difficult for security agencies to anticipate, prevent, and mitigate evolving cyber-based threats (Holt and Bossler 2021). Additionally, cyber terrorism often involves transnational elements, requiring stronger international cooperation in intelligence sharing, cyber defense strategies, and legal harmonization with global cybersecurity frameworks. The ITE Law provides a sufficient legal basis, but regulatory updates are still needed to be more responsive to technological developments (Fahriza *et al.* 2024).

To effectively counter cyberterrorism, Indonesia must enhance its cybersecurity infrastructure and legal mechanisms to comprehensively address digital threats. This includes enacting a specialized cyber terrorism law, strengthening digital forensic capabilities, and integrating artificial intelligence (AI) and big data analytics to detect potential cyber threats. Furthermore, Indonesia should consider ratifying international agreements, such as the Budapest Convention on Cybercrime, which provides a legal framework for cross-border cooperation on cybercrime. Without a clear and comprehensive regulatory framework, Indonesia remains vulnerable to cyber-terrorism threats, as empirical studies have shown that the sophistication and frequency of cyber-based attacks continue to escalate globally and regionally, exposing countries with inadequate legal protections to heightened security risks (Weimann 2020). Research on Indonesia's counter-terrorism and cybercrime governance further demonstrates that gaps in statutory regulation—particularly the absence of explicit provisions addressing cyberterrorism—significantly weaken the state's ability to prevent and respond to digital attacks targeting critical national systems (Astuti 2015, Bakry *et al.* 2021). These vulnerabilities not only endanger national security but also carry the potential to disrupt economic stability and erode public confidence in digital governance, especially as terrorist

groups increasingly integrate advanced cyber techniques into their operations (Holt and Bossler 2021).

3. RESEARCH METHODOLOGY

This research employs a descriptive-analytical methodology and adopts a normative juridical approach to examine the legal norms and frameworks related to cyberterrorism in Indonesia. The study is conducted through a comprehensive literature review focusing on statutory regulations, legal doctrines, academic publications, and expert opinions. A qualitative juridical analysis is employed to assess how existing legal instruments address cyberterrorism and to identify normative gaps that may hinder effective law enforcement. The analysis includes an assessment of the clarity, consistency, and adequacy of Indonesia's legal provisions related to cyber terrorism. To measure the effectiveness of current legislation, a qualitative evaluation is conducted based on case studies involving relevant laws and regulations, such as the Criminal Code (KUHP), Law Number 5 of 2018 (amending Law Number 15 of 2003), and Law Number 19 of 2016 (amending Law Number 11 of 2008 on Information and Electronic Transactions or ITE Law). The analysis examines whether these legal instruments provide explicit definitions and comprehensive regulatory mechanisms or if further legislative enhancement is required. Furthermore, the study evaluates how these laws are implemented by law enforcement agencies and assesses their practical effectiveness in prosecuting cyber terrorism cases and ensuring legal certainty. The research also undertakes a comparative analysis by juxtaposing Indonesia's legal framework with international standards—particularly the Budapest Convention on Cybercrime—to evaluate the degree of alignment between national regulations and globally recognized best practices. This comparative assessment employs doctrinal legal analysis, focusing on similarities and gaps in substantive offenses, procedural powers, and international cooperation mechanisms. A case study methodology is applied to examine the real-world implications of regulatory shortcomings, with explicit reference to the Brain Cipher ransomware attack as an empirical illustration of how legal gaps contribute to systemic vulnerabilities. The Indonesian legal response to this incident is analyzed through a normative-evaluative approach to identify specific provisions requiring reform. Additionally, the study incorporates an empirical legal perspective by examining how existing statutory norms shape institutional performance, inter-agency coordination, and societal resilience against cyber threats. Data derived from the examination of legal texts, regulatory instruments, and documented governmental responses are analyzed using content analysis techniques to assess the regulatory impact on society and the state's overall capacity to safeguard national cybersecurity.

4. RESULTS AND DISCUSSION

4.1. EFFECTIVENESS OF EXISTING LEGISLATION AGAINST CYBER TERRORISM CRIMES

The evolving landscape of cyberterrorism necessitates advanced digital forensic capabilities to ensure that investigators can effectively trace, identify, and prosecute perpetrators (Holt and Bossler 2021). Modern cyberterrorism incidents frequently employ sophisticated attack vectors—such as encryption, anonymization technologies, and multi-layered intrusion techniques—that pose significant challenges for traditional investigative approaches

(Weimann 2020). As a result, law enforcement agencies require specialized technical expertise and structured investigative methodologies to respond adequately to these increasingly complex and technologically advanced threats (Bakry *et al.* 2021). Law enforcement agencies must develop comprehensive digital forensics units equipped with cutting-edge tools and trained personnel capable of handling complex cybercrime scenarios (Asasfeh *et al.* 2023). The integration of artificial intelligence (AI) and machine learning (ML) algorithms in forensic analysis has proven instrumental in identifying attack patterns, tracing digital footprints, and establishing evidentiary chains capable of withstanding judicial scrutiny (Dunsin *et al.* 2024). Digital evidence preservation and analysis present unique challenges in cyberterrorism cases, particularly when dealing with encrypted communications, anonymization technologies, and transnational data flows conditions under which conventional forensic techniques often fall short (Riskiyadi 2020). The implementation of standardized digital forensics protocols ensures consistency in evidence collection and maintains the integrity of investigative processes. Furthermore, real-time monitoring systems and threat intelligence platforms enable the proactive identification of potential cyberterrorism activities before they materialize into full-scale attacks (Nayak 2024).

Article 1 of Law Number 5 of 2018 states that terrorism is an act that uses violence or threats of violence that creates a climate of terror or widespread fear, which can result in mass casualties and/or cause damage or destruction to vital strategic objects, the environment, public facilities, or international facilities with ideological, political, or security disturbance motives. The threat of terrorism is exacerbated by technology and parently; this threat has not received appropriate space in the legal regulations in Indonesia (Bakry *et al.* 2021).

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 (Hartati and Muhammad 2023). The rapid development of information technology in Indonesia increases the risk of cyber terrorism, which poses a serious threat to the nation's critical infrastructure. Cyber terrorism attacks can generate impacts far more destructive than conventional terrorism because they are capable of paralyzing essential public systems such as power grids, transportation networks, financial systems, and government service platforms. Such disruptions may trigger widespread economic losses, chaos in public services, erosion of public trust in state institutions, and even compromise national security. Therefore, the law must function as a preventive and repressive mechanism to address cyber terrorism effectively, ensuring that national development proceeds in a stable and secure environment. In this context, evaluating the effectiveness of existing legislation and understanding the specific impacts of cyber terrorism attacks on critical infrastructure becomes an urgent necessity. Cyberterrorism, as a crime in cyberspace, needs to be firmly regulated in Indonesian National Law, so that anyone or any group that intentionally commits crimes in cyberspace, disrupting the security of others, can be prosecuted based on existing electronic evidence (Astuti 2015).

Cyberterrorism's transnational nature demands harmonized legal frameworks and enhanced international cooperation mechanisms. The disparity in national cybercrime legislation creates jurisdictional gaps that cyber terrorists exploit to evade prosecution. For example, while Indonesia regulates cybercrime under Law Number 11 of 2008 on Electronic Information and Transactions (ITE Law), other countries such as the United

States have broader statutes covering computer fraud, identity theft, and critical infrastructure attacks under the Computer Fraud and Abuse Act (CFAA), whereas European countries, guided by the Budapest Convention on Cybercrime, emphasize harmonized definitions of cyber offenses and international cooperation mechanisms (Clough 2014, Le Nguyen and Golman 2021). These differences in scope, procedural powers, and penalties often allow cybercriminals to operate across borders with reduced risk of legal consequences. Although international legal instruments like the Budapest Convention provide foundational frameworks for cross-border collaboration, continuous updates are essential to address emerging threats, new technologies, and the evolving tactics of cyberterrorists (Clough 2014).

The positive legal instruments in Indonesia that regulate cyberterrorism offenses have not yet been set out in legislation in an expressive manner, which creates problems and uncertainty in efforts to accommodate cyberterrorism crimes (Argastya and Supano 2022). This presents a unique challenge in law enforcement because the unclear definition of cyberterrorism in the applicable laws results in difficulties for law enforcement officers in imposing sanctions on perpetrators of cyberterrorism crimes. Currently, Indonesia lacks a specific law that explicitly defines and regulates cyberterrorism crimes, resulting in legal uncertainties and enforcement challenges (Mansur and Gultom 2005). Effective cyberterrorism prevention requires robust collaboration between government agencies and private sector entities that manage critical infrastructure. Public-private partnerships (PPPs) in cybersecurity create comprehensive defense mechanisms that leverage both regulatory authority and technical innovation. Private companies often possess advanced cybersecurity technologies and expertise that complement government resources, while regulatory bodies provide legal frameworks and enforcement capabilities (Pala and Zhuang 2019).

The absence of a clear legal definition complicates law enforcement efforts, making it difficult to prosecute perpetrators effectively. Law enforcement also experiences ambiguity because there is no instrument that clearly and unequivocally regulates it. In this context, Indonesia must utilize criminal law to formulate and address cyber-terrorism crimes (Argastya 2024). The Indonesian Penal Code (KUHP) does not explicitly regulate cyberterrorism, although specific provisions can be used to prosecute related offenses. The conventional nature of the KUHP limits its ability to address modern cybercrimes, including cyberterrorism (Argastya and Supano 2022). Some relevant articles in the KUHP include Article 168 on public order offenses, Article 340 on crimes against life, Article 363 on theft, and Article 368 on extortion and threats. However, these articles do not fully meet the qualifications of cyber terrorism crimes, highlighting the need for further legal clarification and adaptation.

Law enforcement in Indonesia terrorism has encountered enormous difficult when it comes to combating financing (Pati *et al.* 2023). The primary legal framework addressing terrorism in Indonesia is Law No. 5 of 2018, which amended Law No. 15 of 2003 on the Eradication of Terrorism Crimes. Several provisions within this law, such as Articles 6, 7, 9, 11, and 12, could potentially be applied to cyber terrorism. Article 6 covers the use of violence or threats to create widespread fear, while Article 7 addresses corporate liability for acts that support terrorism, including failure to protect user data. Article 9 criminalizes funding activities related to terrorism, including cyber-attacks that harm the public. Additionally, Articles 11 and 12 regulate preparatory actions for terrorism and additional penalties for perpetrators. However, these provisions lack specific references to

cyberterrorism and do not adequately reflect the complexities of cyber-based terrorist activities.

In addition to the anti-terrorism law, Law No. 1 of 2024, which amends Law No. 19 of 2016, and amends Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law), contains provisions that can be used to address cyberterrorism. Articles 30, 32, and 33 of the ITE Law criminalize unauthorized access, data breaches, and disruptions to electronic systems. Article 30 criminalizes unauthorized access to electronic systems, while Articles 32 and 33 provide protections for confidential electronic information and documents. These provisions aim to address cybercrimes, including hacking and data breaches, but they do not explicitly define or categorize cyberterrorism. The latest amendment, Law No. 1 of 2024, which revises the ITE Law, still does not specifically regulate cyber terrorism. Although it introduces new provisions on technology-related crimes, cyberterrorism remains unaddressed. The relevant articles in the updated ITE Law, such as Article 28 on the prohibition of spreading hateful or threatening content, Article 30 on unlawful access to electronic systems, and Article 33 on misuse of access, provide some legal basis for prosecuting cyberterrorism-related crimes.

A comprehensive approach to combating cyber terrorism requires collaboration between the ITE Law and the Anti-Terrorism Law. While the ITE Law establishes a legal framework for cybercrimes, broader legal enforcement is necessary to address cyberterrorism effectively. As cyberterrorism is a transnational crime, Indonesia must cooperate with international organizations and legal frameworks. Mutual legal assistance treaties (MLATs) and extradition agreements specifically tailored for cybercrime cases facilitate international prosecution efforts. The development of standardized legal definitions for cyberterrorism across different jurisdictions eliminates ambiguities that hinder international cooperation. Additionally, joint training programs for law enforcement personnel from different countries enhance operational coordination and ensure consistent application of international legal standards (Peters and Jordan 2019).

The emerging issue of cybersecurity has made it a relevant concern for all UN organizations, whether they utilize the internet or are responsible for ensuring access and protecting state interests (Myers 2020). One of the key international legal instruments addressing cybercrime is the Budapest Convention on Cybercrime, signed on November 23, 2001, in Budapest, Hungary. Over 60 countries have adopted this convention, including Indonesia, which ratified it in 2009 as part of its commitment to combating cybercrime globally. The convention provides guidelines for developing national laws and procedures for handling cybercrime cases. Although the Budapest Convention does not explicitly regulate cyberterrorism, discussions on cyberterrorism are ongoing at the international level. The United Nations and other international bodies may develop more comprehensive legal instruments to address this evolving threat. The mechanism of 'state socialization' combined with incentives, e.g., assistance in building law enforcement capacity, the diffusion of the Budapest Convention has had a profound influence on the development of cybercrime legislation in a number of Pacific Island Countries (PIC) (Le Nguyen and Golman 2021).

Crimes that are not extraordinary and can destroy Indonesia instantly or in a relatively short period, namely cyber terrorism (Bakry *et al.* 2021). This form of crime poses a serious threat because it targets vital sectors such as government systems, military infrastructure,

financial institutions, and public utilities by exploiting weaknesses in digital networks. Unlike conventional crimes, cyberterrorism can be carried out remotely and anonymously, making it difficult to detect and prevent. The damage caused can be extensive, from paralyzing national communication systems to leaking sensitive information or inciting mass panic. In a country like Indonesia, where digital transformation is progressing rapidly, the risk becomes even more significant if adequate cybersecurity measures are not implemented. Therefore, it is crucial for the government and society to strengthen digital resilience, raise awareness, and build a strong cyber defense system to prevent such destructive attacks.

One of the most significant cyberterrorism incidents in Indonesia occurred in June 2024, when the Brain Cipher ransomware attack targeted the National Data Center (PDNS). This attack disrupted critical national infrastructure; however, no legal proceedings were initiated against the perpetrators. Instead, the government's response focused on post-incident recovery and reinforcing cybersecurity protocols to mitigate future risks. The incident underscored the legal system's deficiencies, particularly the lack of explicit statutory provisions governing cyberterrorism. The effectiveness of current regulations is constrained by several factors, including the absence of a clear and comprehensive legal definition of cyberterrorism and the rapid evolution of digital technologies. These deficiencies contribute to inconsistencies in determining which acts qualify as criminal offenses across different legal jurisdictions, thereby exacerbating the complexity and severity of cyber terrorism threats (Mumtaaz *et al.* 2021)

In conclusion, Indonesia lacks specific and detailed legal provisions addressing cyber terrorism in its existing laws. The Anti-Terrorism Law (Law No. 5 of 2018) and the ITE Law (Law No. 19 of 2016 and its 2024 amendment) provide some legal grounds for addressing cyberterrorism-related activities, but they do not comprehensively regulate this issue. This legal gap weakens law enforcement efforts, allowing perpetrators to exploit regulatory uncertainties. While Indonesia has a legal framework to address cyberterrorism, there is an urgent need to develop clearer and more detailed legislation that aligns with international standards. Although cybercrime has been regulated in the positive law in force in Indonesia, the regulation and implementation of security can still be said to be inadequate (Lesmana *et al.* 2023). The rapid advancement of emerging technologies, including quantum computing, artificial intelligence, and Internet of Things (IoT) devices, presents new vulnerabilities that cyber terrorists may exploit. Quantum computing capabilities could potentially render current encryption methods obsolete, necessitating the development of quantum-resistant security protocols. Similarly, AI-powered cyberattacks demonstrate increasing sophistication in bypassing traditional security measures, requiring adaptive defense strategies (Al Zaidy 2024).

Therefore, continuous efforts are needed to improve regulations, enhance law enforcement capabilities, and strengthen international cooperation. These measures could include drafting new legislation specifically addressing cyberterrorism and adopting preventive strategies to mitigate emerging threats. Law enforcement cooperation is an operational necessity for national agencies in investigations, and specialized international law enforcement organizations assist in bridging divides in everything from geopolitical affairs to capacities and capabilities, which can be so prevalent, especially in the cyber field (Billow 2024).

4.2. The Impact of cyber terrorism attacks on national critical infrastructure

Cyberterrorism has emerged as one of the most significant threats to global security, economy, and social stability. The Impact of these digitally orchestrated attacks extends far beyond traditional warfare boundaries, affecting critical infrastructure, financial systems, and public safety on an unprecedented scale (Lewis 2024). Cyber terrorism, or terrorist attacks based on network technology, is a distinct form of crime with unique characteristics. Cyberterrorism is considered a violation of cyber laws that specifically targets critical territorial infrastructure with national importance, posing threats to civilians and government officials (Mumtaaz *et al.* 2021). The increasing misuse of network technology has raised concerns among nations, prompting them to formulate and establish appropriate legal regulations to address potential cyber threats. Each country has its own network regulations, and initially, cybercrime laws did not attract much attention. Critical infrastructure represents another primary target for cyberterrorists. Energy grids, transportation systems, healthcare facilities, and communication networks face constant threats from malicious actors. Attacks on critical infrastructure were rampant in 2024, with manufacturing, finance, energy, utilities, retail, and healthcare sectors experiencing the most significant breaches. These attacks disrupt supply chains, affect production and delivery systems, and compromise essential services that millions depend upon daily.

The rapid development of information and communication technology has brought significant benefits to various aspects of life, but it also presents new threats, particularly in the form of cyberterrorismm. This phenomenon has emerged as a serious challenge to national and global security, demanding legal and institutional responses that are both adaptive and collaborative. However, over time, the growing number of cyber-related incidents has made society aware of the need for legal frameworks to regulate illegal or deviant behavior in cyberspace. As outlined in the EU Convention on Cyber Crime, given the global nature of cyberterrorism crimes, investigation agencies must cooperate and have international relations so that the investigation process can be carried out quickly, effectively and accurately. This is important, because the solution to cyberterrorism can only be done at the international level and not relying only on each country (Mumtaaz *et al.* 2021). The international community also recognizes the necessity of cooperation between countries and industries to combat cybercrime, ensuring the protection of technological development and users' interests.

Cyber terrorism is a type of crime closely related to terrorists who use advanced technology as a means and target of terrorist attacks (Asri *et al.* 2024). With technological advancements, cyber terrorism continues to escalate daily, including in Indonesia. Cyber threats can manifest in various forms, including cyber terrorism targeting national critical infrastructure. National critical infrastructure refers to essential facilities and systems that are vital for the country's survival and security. It encompasses a wide range of assets, systems, and networks that are crucial for supporting the national economy, public health and safety, and national security. Critical infrastructure plays a key role in protecting national assets and can be found in various national systems, such as Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems. A cyber attack targeting industrial systems like SCADA or ICS could lead to a severe crisis, resulting in extensive damage to essential national systems, including transportation, oil supply, military distribution, energy networks, and various industries.

On June 20, 2024, Indonesia experienced a cybercrime attack carried out by a group known as Brain Cipher. The attack involved ransomware targeting the National Data Center (PDNS), causing critical data from ministries and various government agencies to be locked and inaccessible. This led to significant disruptions in public services, affecting 239 government institutions, including the immigration system at Soekarno-Hatta International Airport, which resulted in long queues and travel delays (Buana 2024). The incident not only exposed vulnerabilities in the country's cybersecurity infrastructure but also highlighted the urgent need for a more robust and coordinated national response to cyber threats, as the breach compromised essential services and raised concerns about the protection of sensitive state data.

Severe cyber threats targeting industrial control systems carry profound financial implications. A report by Tempo estimates that disruptions within Indonesia's travel and tourism sector may incur losses of up to IDR 2.19 billion per minute. Cybercriminals are increasingly aware of their capacity to extort substantial ransoms from targeted institutions, while states may also deploy cyber warfare strategically as a means to assert geopolitical influence. The ransomware attack on the National Data Center (PDNS), orchestrated by the Brain Cipher group, included a ransom demand of USD 8 million (approximately IDR 131 billion), clearly illustrating the economic magnitude of cyber terrorism and its potential to paralyze national industries and public infrastructure within a short timeframe. This incident underscores how cyberterrorism not only threatens national security but also has the potential to paralyze key sectors of the economy within minutes. The enormous financial losses resulting from halted operations, disrupted services, and the cost of recovery reflect the devastating consequences of such attacks. Moreover, the demand for a multimillion-dollar ransom illustrates how cybercriminals strategically exploit the high dependency of modern industries on digital infrastructure.

According to data from Kumparan, cyber attacks in Indonesia reached 2,499,486,085 in 2024, marking an increase of 347,172,666 attacks from the previous year. This equates to an average of 13,733,440 cyber attacks per day, or 158 cyber attacks per second, raising public concerns about Indonesia's cybersecurity resilience. This alarming surge in cyber attacks highlights the pressing need for Indonesia to enhance its cybersecurity infrastructure, implement stronger regulatory frameworks, and invest in cybersecurity education to build a more resilient digital ecosystem capable of withstanding increasingly sophisticated threats.

In Indonesia, cyber terrorism is addressed through the application of positive law. Before the enactment of the Electronic Information and Transactions Law (ITE Law), the Indonesian Penal Code (KUHP) was used as the legal basis for prosecuting cyber-related offenses. However, both laws are now applied together to address cyber terrorism cases. The legal provisions regarding cyber terrorism in the KUHP (2019 version, Articles 336–339) serve as the legal foundation for prosecuting cyber terrorism acts:

1. Article 336 regulates offenses that disrupt public order. Cyber attacks that block access to public networks can be considered a violation of public order under this provision, even though it does not explicitly mention cyberterrorism.
2. Article 337 oversees actions that cause harm to others. In the context of cyber terrorism, this article applies if a cyber attack results in material or non-material losses, such as stolen data or blocked systems.

3. Article 338 governs acts that cause reputational damage or embarrassment. Cyber attacks may tarnish a victim's reputation or cause psychological distress.
4. Article 339 addresses offenses that endanger public safety. In the context of cyber terrorism, this provision applies if a cyber attack threatens critical infrastructure or poses significant risks to society.

In addition to the KUHP, the ITE Law also plays a crucial role in combating cyber terrorism, particularly through Articles 30, 31, and 32:

1. Article 30 regulates and prohibits unauthorized access to computer systems, which is applicable in prosecuting hackers.
2. Article 31 addresses hacking activities, including those that damage information systems.
3. Article 32 regulates the misuse of access to computer systems and electronic services.

Based on these provisions, criminal procedural law (Hukum Acara Pidana) can be considered lex generalis, while the regulations under the ITE Law serve as lex specialis. There is also a Criminal Code (Kitab Undang-Undang Hukum Pidana/KUHP) and a Civil Code (Kitab Undang-Undang Hukum Perdata/KUHPer). The two laws have explained orders, prohibitions, and punishments to every party and institution that harms other parties, primarily when it occurs in cyberspace (Iswardhana 2021).

This distinction clarifies that the ITE Law provides more specific legal guidelines for handling cyberterrorism cases compared to the broader criminal code provisions. The success of regulatory measures in Indonesia relies on a holistic approach involving the active participation of the goverment, society, and the private sector (Khoirunnisa and Jubaidi 2024). Based on this, cyber terrorism is included in the type of cyber crime. Existing cyber crimes and privacy issues that target Cyber Crime, a comprehensive framework was developed that provides an overview of potential security and privacy threats along with attack methods and countermeasures (Goni *et al.* 2022).

Cyberattacks on national infrastructure are increasingly frequent, targeting not only specific organizations but also the broader public that depends on digital information services (Lewis 2024, Buana 2024). The consequences of such attacks are multifaceted: economically, disruptions to digital systems can hinder business operations, reduce national productivity, and impose substantial costs for data recovery and cybersecurity measures (Lewis 2024). From a national security perspective, compromised infrastructure can trigger social instability and weaken the state's capacity to safeguard sovereignty and maintain public order (Bakry *et al.* 2021).

Cyber attacks on national infrastructure will have an impact on public trust in the government to ensure the security and welfare of the wider community. When cyber attacks succeed in thwarting public system disruptions, public trust in the government as a provider of protection and security for its people will also decrease. The decline in public trust will potentially decrease participation in digital public services in the future. And this can also be a new threat because if the public refuses to participate, it can hinder national development and development in the future.

Therefore, by looking at all forms of impacts that will be a threat to the security of national infrastructure and the welfare of the wider community, it is deemed necessary to take strategic steps to prevent and overcome them. Intelligent security can be defined as a next-generation security information analysis technology that analyses the correlations between the data and security events happening in key IT infra network systems and application services in order to respond to unknown critical attacks such as an APT attack (Chun and Cho 2022). One step that can protect this national critical infrastructure is the development of stronger and more comprehensive cybersecurity policies. Policies like this need to be developed to analyze risks and implement other strategic steps. And also requires cooperation between various stakeholders including the government, private companies and international organizations, by continuing to coordinate responsively and adaptively in dealing with evolving threats.

5. Conclusion

Cyberterrorism in Indonesia poses a serious threat to critical national infrastructure, including transportation systems, energy networks, government services, and national data centers. Existing legal instruments, such as the Electronic Information and Transactions Law (ITE Law) and the Law on the Eradication of Terrorism Crimes, provide partial regulation but lack clear definitions and comprehensive provisions for cyberterrorism, resulting in legal uncertainty and inconsistent enforcement. Incidents like the Brain Cipher ransomware attack highlight operational, economic, and security vulnerabilities. Addressing these challenges requires a strengthened legal framework with explicit definitions and dedicated provisions for cyberterrorism offenses. In parallel, enhancing cybersecurity measures, safeguarding national data, and fostering international cooperation aligned with global standards, such as the Budapest Convention on Cybercrime, are essential. Comprehensive regulatory reform combined with strategic collaboration with global cybersecurity partners is necessary to ensure the resilience, security, and reliability of Indonesia's digital infrastructure.

References

Al Zaidy, A., 2024. Digital Crimes and Digital Terrorism: The New Frontier of Threats in Cyberspace. *Journal of Information Technology, Cybersecurity, and Artificial Intelligence* [online], 1(1). Available at: https://doi.org/10.70715/jitcai.2024.v1.i1.00

Aly, A., Macdonald, S., and Jarvis, L., 2017. *Introduction to the Special Issue: Terrorist Online Propaganda and Radicalization.* Studies in Conflict & Terrorism [online], 40(1), 1–9. Available at: https://doi.org/10.1080/1057610X.2016.1157402

Argastya, A.Y., 2024. Penanggulangan Terhadap Kejahatan Cyber-Terrorism Melalui Politik Hukum Pidana. *Jurist-Diction* [online], 7(2). Available at: https://doi.org/10.20473/jd.v7i2.44633

Argastya, A. Y., and Supano, 2022. Penerapan Hukum Pidana Pada Penyidikan Kepolisian Untuk Menanggulangi Kejahatan Cyber Terrorism. *Recidive* [online], 11(1), 14. Available at: https://doi.org/10.20961/recidive.v11i1.67425

Asasfeh, A., *et al.*, 2023. Exploring Cyber Investigators: An In-Depth Examination of the Field of Digital Forensics. *2023 IEEE DASC/PiCom/CBDCom/CyberSciTech Conference* [online], pp. 0084–0088. IEEE. Available at: https://doi.org/10.1109/DASC/PiCom/CBDCom/Cy59711.2023.10361449

Asri, A., *et al.*, 2024. ANTI TERORISME SIBER: Upaya Antisipatif Penanggulangan Terorisme Siber di Indonesia. *Jurnal Ilmiah Hukum Dirgantara* [online], 15(1), 1–13. Available at: https://journal.universitassuryadarma.ac.id/index.php/jihd/article/view/1369

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

Bakry, M., *et al.*, 2021. Strengthening the Cyber Terrorism Law Enforcement in Indonesia: Assimilation from Islamic Jurisdiction. *International Journal of Criminology and Sociology* [online], 10, 1267–1276. Available at: https://doi.org/10.6000/1929-4409.2021.10.146

Billow, J., 2024. No Country Is an Island: Embracing International Law Enforcement Cooperation to Reduce the Impact of Cybercrime. *Journal of Cyber Policy* [online], 9(2), 149–158. Available at: https://doi.org/10.1080/23738871.2023.2245417

Buana, G., 2024. Kronologi Serangan Ransomware ke PDNS. *Media Indonesia* [online]. Available at: https://mediaindonesia.com/teknologi/682359/kronologi-serangan-ransomware-ke-pdns

Carthy, S. L., *et al.*, 2020. Counter-Narratives for the Prevention of Violent Radicalisation: A Systematic Review. *Campbell Systematic Reviews* [online], 16(3), e1106. Available at: https://doi.org/10.1002/cl2.1106

Chun, Y. H., and Cho, M. K., 2022. An Empirical Study of Intelligent Security Analysis Methods Utilizing Big Data. *Journal of Logistics, Informatics and Service Science* [online], 9(1), 26–35. Available at: https://doi.org/10.33168/liss.2022.0103

Clough, J., 2014. A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation. *Monash University Law Review*, 40(3), 698–736.

Conway, M., 2017. Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research. *Studies in Conflict & Terrorism* [online], 40(1), 77–98. Available at: https://doi.org/10.1080/1057610X.2016.1157408

Dunsin, D., *et al.*, 2024. A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. *Forensic Science International: Digital Investigation* [online], 48, 301675. Available at: https://doi.org/10.1016/j.fsidi.2023.301675

Fahriza, W., Sahlepi, M. A., and Rahmayanti, R., 2024. Effectiveness of Law Enforcement Against Cybercrime in Indonesia. *Law Sinergy Conference*, 1(1), 179–185.

Gill, P., Horgan, J., and Deckert, P., 2014. Bombing Alone: Tracing the Motivations and Antecedent Behaviors of Lone-Actor Terrorists. *Journal of Forensic Sciences* [online], 59(2), 425–435. Available at: https://doi.org/10.1111/1556-4029.12312

Goni, O., *et al.*, 2022. The basic concept of cybercrime. Journal of Technology Innovations and Energy [online], 1(2), 16-24. Available at: https://doi.org/10.56556/jtie.v1i2.113

Hartati, C. S., and Muhammad, A., 2023. Combating Cybercrime and Cyberterrorism in Indonesia. *Jurnal Hubungan Internasional*, 11(2).

Hoffman, B., Ware, J., and Shapiro, E., 2020. Assessing the Threat of Incel Violence. *Studies in Conflict & Terrorism* [online], 43(7), 565–587. Available at: https://doi.org/10.1080/1057610x.2020.1751459

Holt, T. J., and Bossler, A. M., 2022. *Cybercrime and Digital Forensics: An Introduction.* 3rd ed. London: Routledge.

Horgan, J., 2014. *The Psychology of Terrorism.* 2nd ed. London: Routledge.

Iswardhana, M. R., 2021. Cyber Diplomacy and Protection Measures Against ICT Threats in Indonesia. *Journal of Islamic World and Politics* [online], 5(2). Available at: https://doi.org/10.18196/jiwp.v5i2.12242

Khoirunnisa, K., and Jubaidi, D., 2024. Indonesia's Digital Security Strategy: Countering the Threats of Cybercrime and Cyberterrorism. *Journal of Public Administration and Political Science and International Relations* [online], 2(2). Available at: https://doi.org/10.61978/politeia.v2i2.211

Kitab Undang-Undang Hukum Pidana (KUHP).

Le Nguyen, C., and Golman, W., 2021. Diffusion of the Budapest Convention on Cybercrime. *Computer Law & Security Review* [online], 40, 105521. Available at: https://doi.org/10.1016/j.clsr.2020.105521

Lesmana, S. J., Latif, I. S., and Felina, F., 2023. Law Enforcement in Efforts to Combat Cyber Crime in Indonesia. *The International Journal of Law Review and State*

Administration [online], 1, 120–128. Available at: https://www.ijems.id/index.php/ijlrsa/article/view/90

Lewis, J.A., 2024. Economic Impact of Cybercrime. *Center for Strategic and International Studies* [online]. Available at: https://www.csis.org/analysis/economic-impact-cybercrime

Mansur, D. M. A., and Gultom, E., 2005. *Cyber Law: Aspek Hukum Teknologi Informasi*. PT Refika Aditama.

Muhammad Sukardi, 2024. 239 Data Instansi Pemerintah Terdampak Serangan Ransomware. *SindoNews* [online], 27 June. https://nasional.sindonews.com/read/1404713/15/239-data-instansi-pemerintah-terdampak-serangan-ransomware-1719489981

Mumtaaz, G. M., Wardhana, T. R., and Diastuti, F. H., 2021. Anti Cyber Terrorism sebagai Upaya Penanggulangan di Indonesia. *Al-Hakam Islamic Law & Contemporary Issues*, 2(2).

Myers, N., 2020. Cyber Security: Cyber Crime, Attacks and Terrorism. *ODU UN Day Issue* [online], 1–13. Available at: https://www.odu.edu/sites/default/files/documents/1st-cyber-attacks.pdf

Nayak, M., 2024. AI-Enhanced Digital Forensics. *Journal of Electrical Systems* [online], 20(1s), 211–229. Available at: https://doi.org/10.52783/jes.766

Pala, A., and Zhuang, J., 2019. Information Sharing in Cybersecurity: A Review. *Decision Analysis* [online], 16(3), 172–196. Available at: https://doi.org/10.1287/deca.2018.0387

Paminto, S. R., 2022. Cyber Terrorism Countermeasures in Indonesia. *Jurnal Wawasan Yuridika* [online], 6(2). Available at: https://doi.org/10.25072/jwy.v6i2.464

Pati, N. V., *et al.*, 2023. The Implementation of Law Enforcement in Combating Terrorist Financing in Indonesia. *Indonesian Journal of International Law* [online], 21(2), 5. Available at: https://doi.org/10.17304/ijil.vol21.2.6

Peters, A., and Jordan, A., 2019. Countering the Cyber Enforcement Gap. *Journal of National Security Law & Policy* [online], 10, 487. Available at: https://jnslp.com/2020/02/13/countering-the-cyber-enforcement-gap-strengthening-global-capacity-on-cybercrime/

Phillips, K., *et al.*, 2022. Conceptualizing Cybercrime. *Forensic Sciences* [online], 2(2), 379–398. Available at: https://doi.org/10.3390/forensicsci2020028

Pradnyana, I. P. H., and Rofii, M. S., 2020. Ancaman Cyberterrorism di Indonesia dan Respons Negara. *Literatus* [online], 2(2), 185. Available at: https://doi.org/10.37010/lit.v2i2.92

Riskiyadi, M., 2020. Investigasi forensik terhadap bukti digital dalam mengungkap cybercrime. *Cyber Security dan Forensik Digital* [online], 3(2), 12–21. https://doi.org/10.14421/csecurity.2020.3.2.2144

Spaaij, R., 2012. *Understanding Lone Wolf Terrorism: Global Patterns, Motivations and Prevention*. Dordrecht: Springer.

Thatcher, M., 1985. *Speech to American Bar Association ("We must try to find ways to starve the terrorist and the hijacker of the oxygen of publicity on which they depend")*. 15 July. American Bar Association, London.

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU ITE.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas UU ITE.

Undang-Undang Nomor 5 Tahun 2018 tentang Pemberantasan Tindak Pidana Terorisme.

Weimann, G., 2015. *Terrorism in Cyberspace: The Next Generation*. Woodrow Wilson Center Press/Columbia University Press.