JURNAL AL-DUSTUR
Volume IX No. 1, June 2026
E ISSN: 2686-6498 II P ISSN: 2622-5964
Published by: Department of Constitutional Law, Postgraduate Program of IAIN Bone
Addres: Jln. HOS Cokroaminoto, Watampone, South Sulawesi - Indonesia
Email: jurnal.aldustur@gmail.com / jurnal.aldustur@iain-bone.ac.id

FROM KINETIC VIOLENCE TO DIGITAL FEAR: PARADIGM SHIFTS IN NATIONAL LEGAL RESPONSES TO CYBERTERRORISM IN INDONESIA AND UNITED STATES

Nadiah Khaeriah Kadir[1], Judhariksawan[1], Syamsuddin Muhammad Noor[1], Maskun[1], Imelda Hermilinda Abas[2]
[1]Faculty of Law, Universitas Hasanuddin, Makassar, Indonesia
[1]Academy of Arts and Philosophy, Shinawatra University, Thailand

Corresponding Author: nadiahkhaeriah@unhas.ac.id

Keywords:
Cyberterrorism; National Legal Systems; State Jurisdiction; Indonesia; United States.

Received:
December 22, 2025
Accepted:
May 19, 2026
Published:
June 5, 2026

ABSTRACT
The evolution of terrorism from conventional physical violence to the mass production of digital fear has redefined cyberspace as a critical arena for contemporary security threats. Cyberterrorism, characterized by borderless operations and transnational impacts, poses profound challenges to national legal systems that remain predominantly grounded in territorial sovereignty paradigms. This article aims to analyze the reorientation of national legal frameworks in response to the qualitative shift from traditional counterterrorism models toward regulatory architectures capable of addressing digital disruption. Utilizing a normative-doctrinal legal research method with a comparative approach between Indonesia and the United States, this study evaluates the coherence, adequacy, and effectiveness of national cyber regulations in confronting transnational threats. The findings reveal a significant divergence in legal approaches. the United States has integrated the effects doctrine and the protective principle to extend extraterritorial jurisdiction, whereas the Indonesian legal landscape remains sectoral and fragmented, resulting in enforcement lacunae and conceptual ambiguity. This study asserts that regulatory disparities and the absence of a harmonized statutory definition undermine cross-border cooperation and international legal certainty. The novelty of this research lies in its reframing of cyberterrorism as a qualitative transformation—shifting from acts of physical violence to the generation of digital fear—and offers insights for transitioning toward a more cohesive, technologically neutral legal model.

How to cite:
Kadir, N. K., J., J., Noor, S. M., M., M., Abas, I., H. (2026). FROM KINETIC VIOLENCE TO DIGITAL FEAR: PARADIGM SHIFTS IN NATIONAL LEGAL RESPONSES TO

CYBERTERRORISM IN INDONESIA AND UNITED STATES. Jurnal Al-Dustur, 9(1). doi:https://doi.org/10.30863/aldustur.v9i1.11107

INTRODUCTION

Cyberterrorism has become a critical contemporary threat that demands sustained and rigorous scholarly attention. The accelerated advancement of digital technologies, along with the increasing scale, frequency, and sophistication of cyberattacks, requires continuous adaptation of data and information system security mechanisms. As cyber threats evolve in complexity, existing countermeasures often fail to provide adequate protection, revealing substantial shortcomings within prevailing security frameworks. This situation underscores the urgency of systematically identifying structural and operational vulnerabilities while simultaneously formulating more resilient, dynamic, and forward-looking strategies to enhance defenses against cyberterrorism.[1]

The concept of cyberterrorism began to take shape in the early 1990s, parallel to the swift growth of the Internet and the development of a highly interconnected information society.[2] Terrorist organizations increasingly leverage internet-based networks to support and expand their operational capabilities, a practice widely recognized in the literature as the exploitation of digital technologies by terrorist actors. In many respects, this engagement parallels the behavior of conventional internet users, as extremist groups utilize online platforms for communication, operational coordination, and the dissemination of ideological narratives through websites and digital media channels. Cyberspace also functions as a key conduit for the distribution and retrieval of operational resources, including visual, audio, and audiovisual materials, software applications, and other forms of information pertinent to terrorist activities.

Intelligence reports have consistently demonstrated that organizations such as Hezbollah, Hamas, and Al-Qaeda have long incorporated digital instruments—ranging from computerized databases and electronic mail to encryption technologies—into their organizational infrastructures. Beyond communication and propaganda, online environments facilitate financial transactions, fundraising mechanisms, and various cyber-enabled illicit activities that sustain and reinforce terrorist networks. The employment of digital technologies by individuals or groups to conduct or support terrorist acts is commonly conceptualized as cyberterrorism.

Within international legal discourse, cyberterrorism is frequently understood as a particular manifestation of cybercrime, distinguished by its ideological objectives and the nature of its intended societal and political impact. The anonymity and inherently transnational character of cyberspace substantially reduce operational barriers, thereby complicating the attribution and identification of perpetrators. In contrast to traditional forms of terrorism that rely on physical violence, cyberterrorism provides strategic advantages by enabling remote execution without physical proximity to the target. Collectively, these features illustrate the transformation of terrorism in the digital era and underscore the growing significance of

[1] Kakimzhan Bishmanov et al., "Analysis of Modern Types of Cyberterrorism and Methods for Countering Them," *IDP. Revista d'Internet ...*, no. 41 (2024): 1–14.

[2] Dian Alan Setiawan, "Cyberterrorism and Its Prevention in Indonesia," *Jurnal Media Hukum* 27, no. 2 (2020): 267–83.

cyberspace as a critical domain of terrorist activity.[3]

As cyberterrorism poses a growing threat to international security and necessitates collective responses, it has assumed increasing significance within the field of international relations. A comprehensive understanding of this evolving form of terrorism is essential for accurately assessing the contemporary international security landscape. While terrorist actors progressively exploit cyberspace as an effective instrument for generating widespread fear and disruption, both states and international organizations have incorporated counter-cyberterrorism measures into their respective security frameworks.

Although the underlying motivations driving cyberterrorism remain consistent with those of conventional terrorism, the operational means employed are fundamentally different and less familiar. The convergence of advanced technologies with terrorist objectives introduces a higher degree of complexity compared to traditional manifestations of terrorism. Moreover, digital technologies not only facilitate coordination and scale but also enable cyber-attacks to be conducted at lower cost, with greater speed, ease, and transnational reach, thereby amplifying their potential impact.[4]

The adoption of clear national legal frameworks on cyberterrorism is crucial to ensure effective prevention, enforcement, and international cooperation. In the absence of specific domestic regulations, legal gaps may emerge, undermining deterrence and complicating cross-border investigations. Well-defined national rules provide legal certainty, strengthen institutional coordination, and support harmonization with international norms in addressing the transnational nature of cyberterrorism. This article aims to examine how national legal systems are being reoriented to address the evolving threat of cyberterrorism, shifting from frameworks traditionally designed to counter physical violence toward regulatory models capable of responding to digitally mediated fear and disruption. By comparatively analyzing the legal approaches of Indonesia and the United States, the article seeks to assess the adequacy, coherence, and adaptability of existing national regulations in confronting cyberterrorism.

Despite facing similar risks from cyber-enabled terrorist activities, Indonesia and the United States adopt markedly different legal and regulatory approaches in addressing cyberterrorism. Indonesia, operating within a civil law system, regulates cyberterrorism through fragmented provisions dispersed across counter-terrorism and cyber-related legislation, particularly the Anti-Terrorism Law and the Law on Electronic Information and Transactions, without explicitly formulating cyberterrorism as a distinct criminal offense.[5] In contrast, the United States, grounded in a common law tradition, approaches cyberterrorism through a security-driven framework that integrates counter-terrorism statutes, cybersecurity policies, and an expansive application of extraterritorial jurisdiction, emphasizing national security imperatives. A cornerstone of U.S. cybercrime regulation is the Computer Fraud and Abuse Act (CFAA) 18 U.S.C. § 1030, which criminalizes unauthorized access to computers, transmission of malware, cyber extortion, and related conduct that could be leveraged for

[3] Yasniar Rachmawati Madjid, "Cyberterrorism Challenges: The Need for Global Mutual Legal Assistance for Universal Criminal Jurisdiction," *Yustisia Jurnal Hukum* 10, no. 3 (2021): 388–414.

[4] Mucahit Ergun and Gulsen Seker Aydin, "Evolution of Cyberterrorism: Challenges and Solutions," *Journal of Internasional Relations Studies* 4, no. 2 (2024): 64–73.

[5] Arvid Gema Indrawan et al., "Penanggulangan Tindak Pidana Cyber Terrorism Dalam Perspektif Kepastian Hukum," *Jurnal Hukum Jurisdictie* 3, no. 2 (2021): 35–63, https://doi.org/10.34005/jhj.v3i2.47.

terrorist purposes, and has been amended multiple times, including through the USA PATRIOT Act to extend jurisdiction and enhance investigative authority for terrorism-related cyber offenses. This divergence raises critical legal issues concerning definitional clarity, jurisdictional reach, and the balance between state security and the protection of fundamental rights. Therefore, a comparative examination of cyberterrorism regulation in Indonesia and the United States is essential not only to assess the effectiveness of each legal system but also to contribute to the broader discourse on harmonizing legal responses to cyberterrorism as a transnational crime under international law.

The novelty of this article lies in its reframing of cyberterrorism as a qualitative transformation of terrorism, from acts of physical violence to the production of digital fear, rather than treating it merely as a subset of cybercrime or conventional terrorism. In the context of cyberterrorism, *digital fear* refers to the deliberate creation of collective anxiety, psychological intimidation, and a pervasive sense of insecurity generated through cyberattacks targeting digital systems that underpin essential societal functions. Unlike conventional terrorism, which relies on physical violence to instill fear, cyberterrorism exploits the invisibility, unpredictability, and transnational characteristics of cyberspace to produce sustained public uncertainty and perceived vulnerability, particularly when attacks threaten critical infrastructures such as energy grids, financial systems, healthcare services, and communication networks.[6] This fear is further intensified by the use of online propaganda, symbolic cyber operations, and the rapid dissemination of information and disinformation through digital platforms, often amplifying the psychological impact beyond the actual technical damage inflicted.[7] Consequently, *digital fear* constitutes a defining element that distinguishes cyberterrorism from ordinary cybercrime, as the primary objective lies not merely in unlawful system interference but in intimidating populations and coercing states, thereby aligning cyberterrorism with the core rationale of terrorism within criminal law and international security discourse. Earlier studies on cyberterrorism have predominantly concentrated on conceptual definitions and typologies[8], or on the technical and operational dimensions of cyber threats, including critical infrastructure vulnerabilities and online propaganda mechanisms.[9] From a legal perspective, existing scholarship has largely examined cyberterrorism within the broader frameworks of international law, cybercrime conventions, and state responsibility, often focusing on jurisdictional challenges and attribution issues in cyberspace.[10]

However, these studies tend to address cyberterrorism either through isolated legal instruments or as an extension of pre-existing counterterrorism and cybercrime regimes, without sufficiently analyzing how national legal systems recalibrate their normative and institutional structures in response to the shift from physical violence to digitally mediated fear. Departing from this body of literature, the present article offers a comparative legal analysis that

---

[6] Maura Conway, "Determining The Role of the Internet in Violent Extremism and Terrorism," *Studies in Conflict & Terrorism* 40, no. 1 (2017): 77–98.

[7] Dorothy E. Denning, ed., "Cyber Conflict as an Emergent Social Phenomenon," in *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (IGI Global, 2011), https://doi.org/10.4018/978-1-61692-805-6.

[8] Maura Conway, "Terrorism and the Internet: New Media—New Threat?," *Parliamentary Affairs* 59, no. 2 (2006): 283–98.

[9] Gabriel Weimann, *Terrorism in Cyberspace: The Next Generation* (Columbia University Press, 2015).

[10] J. Kulezsa, *Due Diligence in International Law* (Brill Nijhoff, 2016).

integrates counterterrorism law, cyber regulation, and international legal considerations within a unified analytical framework. By juxtaposing Indonesia and the United States, two jurisdictions characterized by distinct legal traditions, institutional capacities, and security priorities, this study generates original insights into how national legal systems adapt to cyberterrorism and explores the broader implications of divergent regulatory models for legal harmonization and international cooperation.

The urgency of examining cyberterrorism regulations in Indonesia stems from the rapid expansion of digital infrastructure and the corresponding increase in cyber-enabled threats targeting national security, public order, and critical information systems. Indonesia has established a legal framework through instruments such as the Electronic Information and Transactions Law; however, these regulations remain fragmented and are not yet specifically designed to comprehensively address cyberterrorism as a distinct transnational crime. The absence of a clear legal definition and jurisdictional framework creates challenges in law enforcement, particularly in attribution, evidence gathering, and cross-border cooperation. As cyberterrorism often transcends national boundaries, strengthening regulatory clarity and coherence is essential to ensure effective prevention and prosecution while safeguarding state sovereignty.[11]

In comparison, the United States has developed a more advanced and integrated legal regime to address cyberterrorism, supported by statutes such as the USA PATRIOT Act and the Computer Fraud and Abuse Act, as well as institutional coordination among federal agencies. The U.S. approach emphasizes not only criminalization but also preventive measures, intelligence integration, and international collaboration, reflecting a comprehensive national security strategy. Analyzing the regulatory frameworks of both Indonesia and the United States is therefore crucial to identify normative gaps, best practices, and potential models for legal reform. Such comparative analysis contributes to the development of a more robust and adaptive legal system capable of responding to the evolving nature of cyberterrorism threats in the global context.[12]

METHODS

The research method is always dependent on the type of data required. To answer the issues formulated in the problem statement above, this study examining the comparative jurisdiction of states in international law concerning the handling of cyberterrorism actors as transnational crimes employs a normative juridical legal research method. This method emphasizes library-based research activities, in which the study is conducted by examining legal literature such as statutory regulations, books, papers, articles, journals, magazines, and other legal materials relevant to the object of the research. As this study constitutes normative juridical research, the approaches used include the conceptual approach, the statute approach, and the comparative approach. The conceptual approach is carried out by examining the views and doctrines that have developed within the field of legal science, through which the researcher

[11] S. W. Brenner, *At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare*, 97, no. 2 (2007): 379–475.

[12] P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford University Press, 2014).

identifies ideas that give rise to legal definitions, legal concepts, and legal principles relevant to the legal issues under study. An understanding of these views and doctrines ultimately serves as a foundation for constructing legal reasoning and formulating arguments to resolve the issues at hand.[13] The statute approach is conducted by reviewing all laws and regulations related to the legal issues under examination, with close attention to their respective characteristics.[14] This approach focuses on analyzing statutory provisions as the primary source of law, emphasizing the systematic examination of legal norms, their hierarchy, and their consistency within the legal system. Within this analytical framework, comparison constitutes a fundamental instrument of inquiry. It enhances descriptive precision and plays a central role in concept formation by bringing into focus significant similarities and differences across legal systems, norms, or cases. Furthermore, comparison is systematically employed in testing hypotheses and contributes to the inductive development of new hypotheses, ultimately supporting broader processes of theory-building and reinforcing the rigor of legal analysis.[15]

In applying this approach, the researcher considers potential conflicts between different legal norms, including vertical conflicts guided by the principle *lex superior derogat legi inferiori*, whereby higher-level legislation overrides lower-level legislation and horizontal conflicts, guided by the principle *lex specialis derogat legi generali,* whereby specific legislation prevails over general legislation, as well as the principle *lex posterior derogat legi priori,* meaning that newer legislation supersedes older legislation governing the same subject matter. The comparative approach is undertaken by comparing the laws of one country with those of one or more other countries concerning the same issues. Additionally, judicial decisions from multiple jurisdictions may also be compared where they involve similar cases. This approach enables the researcher to identify similarities and differences between the legal norms or judicial rulings examined. Consequently, the researcher gains insight into the legal philosophies underlying the various statutes being compared, as well as the judicial reasoning reflected in court decisions addressing similar matters.

RESULTS AND DISCUSSION

Paradigm Shift in Terrorist Networks

In the early 2000s, cyberspace gained prominence as a critical domain of international security and conflict. Concurrently, the September 11 attacks intensified concerns regarding the potential emergence of cyberterrorism, prompting the development of numerous national policies aimed at both countering and conceptualizing this anticipated threat. Early academic engagement with cyberterrorism largely originated within United States policy environments, where scholarly inquiry intersected with national defense, intelligence, and law enforcement institutions.

The widely circulated images of the September 11, 2001, attacks illustrate the centrality of spectacle in acts of terrorism. Scenes depicting fear-stricken civilians fleeing the collapse of the

[13] T. Hutchinson and N. Duncan, *Defining and Describing What We Do: Doctrinal Legal Research*, 17, no. 1 (2012): 83–119.

[14] Tunggul Ansari Setia Negara, *Normative Legal Research in Indonesia: Its Origins and Approaches*, 4, no. 1 (2023): 1–9.

[15] David Collier, "The Comparative Method," in *Political Science: The State of the Discipline II* (American Political Science Association, 1993).

towers, as well as individuals falling from burning buildings, were repeatedly broadcast across national and global media outlets. These visual representations have become deeply embedded in collective memory and have exerted a lasting influence on United States security policy. Beyond such large-scale events, more localized acts of terrorism, such as car bombings, executions, and suicide attacks, also function as performative displays designed to maximize visibility and psychological impact.[16] In the digital era, these acts are increasingly mediated through real time or recorded online dissemination. Visual content portraying beheadings, as demonstrated in the work of Simone Molin Friis, possesses a heightened capacity to generate fear, especially among audiences who identify with the victims.[17]

Within the broader transformation of terrorism into the digital domain, it is essential to situate cyberterrorism within contemporary academic debates on terrorism and the misinterpretation of Islam. A growing body of international scholarship emphasizes that Islam, as a religion, fundamentally promotes peace, justice, and social harmony, and therefore cannot be inherently associated with acts of terrorism. Noor Haidi Hasan demonstrates that radical movements, particularly in Southeast Asia, are shaped primarily by socio-political dynamics, identity struggles, and ideological contestation rather than by authentic Islamic teachings. In the context of cyberterrorism, this distinction becomes increasingly significant, as digital platforms are frequently exploited to disseminate extremist narratives that selectively manipulate religious doctrines to justify violence.[18]

The migration of terrorism into cyberspace has further intensified the instrumentalization of religious narratives as part of digital propaganda strategies. Cyberterrorist actors utilize the speed, anonymity, and global reach of the internet to construct persuasive ideological messages, often framing their actions within distorted interpretations of Islam. However, Khaled Abou El Fadl argues that such narratives constitute a profound theological distortion that departs from the normative foundations of Islamic law, which emphasize justice, mercy, and the protection of human dignity. This perspective reinforces the understanding that cyberterrorism should not be viewed solely as a technological or security issue, but also as an ideological phenomenon operating within the contested space of digital communication.[19]

Conventional terrorism relies on kinetic means, such as suicide attacks and improvised explosive devices, to inflict death, injury, and material destruction, thereby generating fear and anxiety within targeted civilian populations. Through such acts, terrorism seeks to demoralize society and exert pressure on governments to adopt or abandon particular political objectives. While this strategy has proven effective in certain contexts, it is fundamentally shaped by the physical nature of violence and the organizational capacities required to execute such attacks. In contrast, cyberterrorism operates through malicious digital technologies rather than physical force, yet it retains the same underlying intent of advancing political, religious, or ideological objectives by causing physical or, more frequently, psychological harm to civilian populations. This functional continuity distinguishes cyberterrorism from cyberwarfare, which predominantly

[16] Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (2013): 365–404.

[17] S. M. Friis, "Behead, Burn, Crucify, Crush": Theorizing the Islamic State's Public Displays of Violence," *European Journal of International Relations* 24, no. 2 (2018): 243–67.

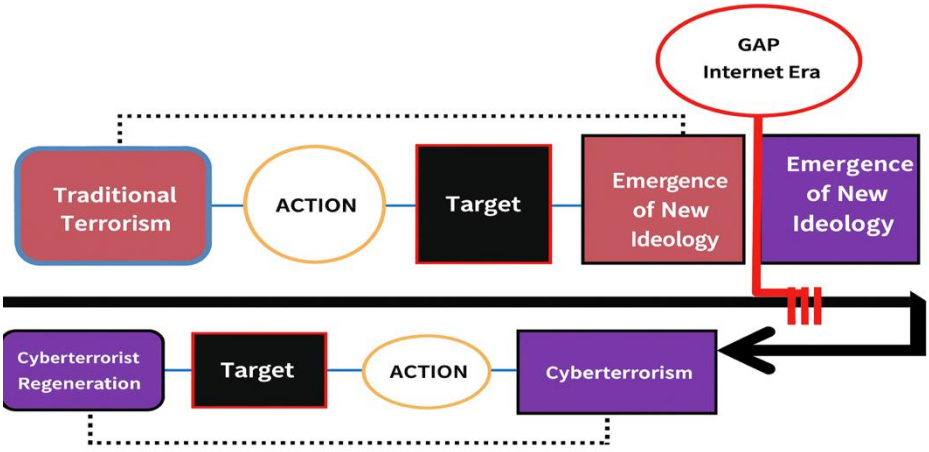
[18] Noorhaidi Hasan, "Violent Activism, Islamist Ideology, and the Conquest of Public Space Among Youth in Indonesia," in *Youth Identities and Social Transformations in Modern Indonesia* (Brill, 2016), https://doi.org/10.1163/9789004307445_011.

[19] Khaled Abou El Fadl, *The Great Theft: Wrestling Islam From the Extremists* (HarperOne, 2007).

targets military systems, and from cybercrime, which is generally motivated by financial gain or personal objectives unrelated to political conflict.[20] Nevertheless, in practice, the boundaries between cyberterrorism, cyberwarfare, cybercrime, and hacktivism are increasingly blurred, as terrorist groups, state actors, and non-state entities may employ overlapping tactics such as data theft, financial exploitation, identity manipulation, or distributed denial of service attacks to disrupt critical systems.

This evolution in methods is closely linked to a broader transformation in the organizational structures of terrorist actors. Conventional forms of terrorism have traditionally been associated with well-defined organizations characterized by hierarchical command structures, centralized planning, and coordinated execution, with responsibility for attacks often publicly claimed. Such organizational models were prevalent prior to the intensification of global counterterrorism efforts following the September 11, 2001 attacks on the World Trade Center. In Indonesia, this pattern was reflected in major incidents such as the Bali Bombings I and II and the first and second J.W. Marriott Hotel bombings, which involved extensive organizational coordination, financing, and logistical preparation and resulted in large-scale casualties and destruction. However, as sustained counterterrorism measures progressively dismantled terrorist networks, cells, and key operatives, the operational environment for organized violence became increasingly constrained. In response, terrorist actors adapted by shifting toward more decentralized and individualized modes of operation, characterized by minimal organizational structure, limited coordination, and independently executed attacks, thereby laying the groundwork for more flexible and technologically mediated forms of terrorism, including cyberterrorism.

Figure 1. The cycle of transformation from traditional terrorism to the era of cyberterrorism.[21]



As illustrated in the figure, terrorist actions conducted within a traditional organizational framework are typically episodic and conclusive, lacking systematic post-attack evaluation mechanisms. Such attacks are often conceived as decisive acts rather than components of a

[20] Michael L. Gross et al., "Cyberterrorism: Its Effects on Psychological Well-Being, Public Confidence and Political Attitudes," *Journal of Cybersecurity* 3, no. 1 (2017): 49–58.

[21] Dipak K. Gupta, *The Roots of Terrorism: Who Are the Terrorists?* (Chelsea House, 2006).

sustained long-term strategy aimed at organizational survival or intergenerational ideological transmission. Consequently, when these operations fail to achieve their intended objectives and are met with effective countermeasures, traditional terrorist groups tend to experience structural and ideological disintegration. Nevertheless, this characterization remains partly inferential, as the continued existence and internal dynamics of traditional terrorist organizations are not fully verifiable. The diversity of motives, identities, and attack modalities observed over time further indicates an absence of coherent ideological continuity, reinforcing perceptions of organizational fragmentation or decline.[22]

In contrast to conventional terrorist operations, groups that integrate internet technologies into their activities tend to exhibit more durable and systematically organized characteristics. These groups are often guided by clearer strategic objectives and supported by structured processes of recruitment and ideological transmission, enabling sustained regeneration over time. This dynamic helps explain why, despite the arrest and prosecution of individual perpetrators under national legal systems, subsequent attacks may still occur, carried out by actors sharing similar affiliations and ideological commitments.

Although cyberterrorist networks generally operate on a smaller numerical scale than traditional terrorist organizations, they benefit from highly decentralized and geographically dispersed structures, coupled with efficient mechanisms of ideological dissemination and cadre formation. Moreover, their extensive use of digital platforms allows them to exert significant influence over public opinion and collective perceptions. Within this framework, the destructive potential of cyberterrorism may, in certain respects, surpass that of traditional terrorism, as it simultaneously exploits psychological vulnerabilities, social dynamics, and the fragility of digital infrastructures.[23]

Scholars of cyberterrorism have long observed that cyberattacks generally lack the visual spectacle that characterizes conventional terrorist violence, thereby challenging their capacity to generate immediate and recognizable fear. The frequently invoked worst-case scenario, a large-scale power outage, does not involve visible destruction or dramatic imagery, and even a completely darkened city often leaves observers uncertain as to whether the disruption results from an intentional attack or a technical malfunction. This ambiguity stands in stark contrast to acts of physical terrorism, such as the September 11 attacks, which were deliberately designed to eliminate uncertainty through spectacular violence that could not be mistaken for an accident.[24]

From the perspective of fear production, this distinction underscores the difference between physical spectacle and digital fear. While physical terrorism relies on visual shock and instant media recognition, cyberterrorism operates through less visible, delayed, and often ambiguous effects. Power outages, for example, restrict real-time information flows and inhibit live media coverage, thereby limiting their immediate terror inducing potential. As Michael Stohl's analysis of the 2003 northeastern United States power outage illustrates, even when an incident is initially suspected to be an act of cyberterrorism, the absence of clear visual markers and attribution tends to result in public irritation rather than widespread fear or security mobilization. This contrast suggests that cyberterrorism produces fear not through spectacular

[22] A. Adang Supriyadi, *Cyberterrorism* (Badan Nasional Penanggulangan Terorisme, 2020).
[23] Maskun, *Kejahatan Siber (Cyber Crime): Suatu Pengantar* (Prenada Media Group, 2013).
[24] E. Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back down to Earth," *International Security* 38, no. 2 (2013): 41–73.

imagery but through sustained uncertainty, systemic disruption, and the erosion of trust in digital and critical infrastructures, thereby constituting a qualitatively different modality of terror in the digital age.[25]

While terrorism constitutes a grave criminal offense, cyberterrorism represents an intensified threat due to its exploitation of global technological dependence as a means of generating widespread disruption. By leveraging digital infrastructures, cyberterrorism seeks to destabilize social, economic, and political order in pursuit of ideologically motivated objectives. This form of terrorism is characterized by novel methods, unconventional instruments, and dispersed operational environments, often involving unidentified perpetrators operating from indeterminate locations with the intent to cause harm.[26] Terrorist organizations have experienced significant transformations in both their network structures and the selection of attack targets. Among these developments, the most notable is a paradigmatic shift driven by the necessity for terrorist networks to adapt to changing technological and socio-political contexts. This evolution is closely linked to a broader transformation in operational modalities, reflecting a transition from conventional methods of terrorism toward more modern and technologically mediated forms of activity.

The Existence of Cyberterrorism as a Form of Modern Terrorism

Globalization has had significant impacts on the development of communication technologies, ultimately giving rise to computer-based communication in the form of the internet. The internet is formed by interconnected computer networks that span countries and continents, creating a global information ecosystem. Technically, it consists of a collection of smaller computer networks with different systems yet integrated with one another. Every device connected to the internet has the potential to function as a printing press, a broadcasting station, and a content production hub. The internet's ability to transmit words, images, and sound makes it an extremely powerful tool for disseminating information, opening spaces for discussion, and spreading propaganda, disinformation, and even hate speech on a massive and borderless scale. Gary R. Bunt emphasizes that globalization facilitates the emergence of new forms of terrorism. In this context, the internet has become a strategic medium for terrorist groups to pursue their agendas globally. Philip Seib and Dana M. Janbek describe this phenomenon as *global terrorism through new media*, an evolution of the post–Al-Qaeda era. Terrorism is no longer dependent on the strength of individual networks but increasingly relies on media networks that reach all corners of the world. Through these new media, messages of terror are not only delivered at the local, national, or regional level; they can reach global audiences in a very short time.[27]

The existence of cyberterrorism as a form of modern terrorism illustrates the adaptive evolution of terrorist strategies in response to rapid digitalization and the increasing dependence of contemporary societies on cyberspace. Unlike conventional terrorism, which primarily relies on physical violence, cyberterrorism utilizes cyberattacks to instill fear, disrupt critical digital

[25] Jeppe T. Jacobsen, "Cyberterrorism: Four Reasons for Its Absence-So Far," *Perspective on Terrorism* 16, no. 5 (2022): 62–72.

[26] Himanshu Agarwal and Sarfraj Ahmed, "Cyber Terrorism: Threatful Purposes," paper presented at 2nd International Conference on the Emerging Technologies in Computing, 2022.

[27] Philip Seib and Dana M. Janbek, *Global Terrorism and New Media: The Post–Al Qaeda Generation* (Routledge, 2007).

infrastructures, and coerce governments through the exploitation of information and communication technologies, thereby achieving terroristic objectives without direct physical harm.[28] The capacity of cyber operations to generate extensive psychological effects, systemic disruption, and transnational consequences indicates that terrorism has extended beyond territorial and physical constraints into a digitally mediated threat environment.[29] Consequently, cyberterrorism should be conceptualized not merely as an extension of cybercrime but as a distinct manifestation of modern terrorism, given that its primary objective remains the production of fear and intimidation to influence public behavior and state decision-making, thereby posing significant challenges to existing legal and security frameworks.

In general, the term *cyberterrorism* still lacks a single, clear definition and remains a subject of debate. Differences in definition arise because each country, institution, or legal system has its own perspective in formulating the concept. This supports Emerald Archer's view that "There is no universally agreed upon definition of terrorism broadly, or cyber terrorism specifically," meaning that to this day there is no global consensus on a definitive definition either for terrorism in general or for cyberterrorism in particular. Lee Jarvis and Stuart Macdonald argue that the difficulty in understanding cyberterrorism stems from two main questions. First, what exactly is meant by cyberterrorism what kinds of acts fall within this category? Second, is cyberterrorism truly a distinct form of violence, different from other types of violence? Does it have unique characteristics, or is it simply part of the broader and already diverse category of terrorism? The understanding of cyberterrorism depends heavily on who is providing the definition. Following the 11 September 2001 terrorist attacks, the U.S. Federal Bureau of Investigation (FBI) formulated an initial, relatively broad definition as the use of cyber technology to disable critical national infrastructures such as energy, transportation, or government sectors—with the aim of pressuring or intimidating the government or the public.[30]

However, this definition raises problems because it could also encompass acts more properly classified as *cyberwarfare* between states. This has become a major point of critique in discussions of cyberterrorism, as the term is often used subjectively and influenced by political perspectives and national interests.[31] Over time, the FBI refined its definition with a more specific approach, describing cyberterrorism as premeditated, politically motivated attacks against information, computer systems, programs, or data that result in violence against civilian targets and are carried out by subnational groups or clandestine agents. Through this definition, the FBI emphasizes that cyberterrorism is committed by non-state actors rather than states. Even so, the principal challenge in identifying cyberterrorism remains the anonymity of cyberspace. In many cases, law enforcement agencies face serious difficulties in determining who the perpetrators really are and whether they are acting individually, as part of a terrorist organization, or even on behalf of a state within the framework of cyberattacks that resemble acts of war.[32] This attribution problem significantly complicates the legal qualification of cyber incidents, blurring the boundaries between cybercrime, cyberterrorism, and cyber warfare, and creating uncertainty

[28] Weimann, *Terrorism in Cyberspace: The Next Generation*.

[29] Conway, "Determining The Role of the Internet in Violent Extremism and Terrorism."

[30] Emerald Archer, "Crossing the Rubicon: Understanding Cyber Terrorism in the European Context," *The European Legacy: Toward New Paradigms* 14, no. 7 (2009): 605–22.

[31] Lee Jarvis and Stuart Macdonald, "What Is Cyberterrorism and Why Does It Matter? Findings from a Survey of Researchers," *Terrorism and Political Violence* 27, no. 3 (2015): 1–20.

[32] Roland Heickerö, "Cyberterrorism: Electronic Jihad," *Strategic Analysis* 38, no. 4 (2014): 554–65.

regarding the applicable legal regime and jurisdictional authority.[33] In transnational settings, where cyberattacks may simultaneously affect multiple states, the lack of reliable attribution further hinders effective law enforcement cooperation and raises complex questions concerning state responsibility under international law. Consequently, anonymity in cyberspace not only undermines accountability but also increases the risk of legal fragmentation and strategic miscalculation, underscoring the urgent need for clearer normative frameworks and coordinated international responses to address cyberterrorism effectively.

This dynamic is reflected in Denning's influential definition of cyberterrorism, articulated during a policy briefing before the U.S. House of Representatives in 2000, which exemplifies how national policy debates played a pivotal role in shaping and disseminating the concept of cyberterrorism across both academic discourse and public narratives. Even prior to this, in October 1999, the U.S. Naval Postgraduate School produced what has been widely regarded as the first and most comprehensive study on "cyber terror" for the Defense Intelligence Agency. Notably, the study drew a clear conceptual boundary between "pure" cyberterrorism and other forms of terrorist engagement with digital technologies, emphasizing that the use of information technology solely to support terrorist activities does not, in itself, constitute cyberterrorism.

Since then, her definition has been extensively used in academic articles and interviews. Denning understands cyberterrorism as:[34]

> "The convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear."

Denning further argues that attacks resulting in death, physical injury, explosions, or significant economic loss may be categorized as cyberterrorism. She also stresses that attacks on critical infrastructure, if they have substantial impact, may satisfy the elements of cyberterrorism. Conversely, attacks that merely disrupt non-essential services or cause financial loss without meaningful strategic effects are generally not classified as cyberterrorism. Gabriel Weimann, a leading scholar in this field, defines cyberterrorism as the use of computer network tools to damage or disrupt the functioning of critical infrastructure of a state, such as energy, transportation, and government services.[35] This definition differs from Dorothy Denning's in several respects:

1. Denning does not specify that attacks must be carried out *through* computers, only that they are directed *against* computers, networks, or the information contained in them. Weimann, by contrast, explicitly states that computers are both the tools and targets of the attack.

---

[33] Jay P. Kesan and Carol M. Hayes, "Mitigative Counterstriking: Self-Defence and Deterrence in Cyberspace," *Harvard Journal of Law & Technology* 25, no. 2 (2012): 429–75.

[34] Dorothy Denning, "Cyberterrorism: Testimony Before the Special Oversight Panel on Terrorism Committee on Armed Service U.S. House of Representatives," 2002, https://faculty.nps.edu/dedennin/publications/Testimony-Cyberterrorism2000.htm.

[35] Gabriel Weimann, "Cyberterrorism: The Sum of All Fears?," *Studies in Conflict and Terrorism* 28 (2005): 130.

2. Weimann does not mention the motives behind the attack, whereas Denning emphasizes that political or social motives are essential elements of cyberterrorism.
3. For Weimann, cyberterrorism only includes attacks targeting vital networks supporting national infrastructure and carried out with the aid of computer technology.
4. Unlike Denning, who requires serious consequences such as physical violence or major economic loss for an attack to be considered cyberterrorism Weimann's definition does not explicitly require such impacts.

Despite their differences, Denning's and Weimann's definitions share a common impact-based approach: both emphasize the outcomes that must result from an attack in order for it to qualify as cyberterrorism. Neither focuses on the identity of the actors involved. This contrasts with Roland Heickerö's view that cyberterrorism is not limited to organizations or individuals; states may also be involved under certain circumstances.[36]

An important contribution toward refining the conceptual boundaries of cyberterrorism is the distinction between *cyberterrorism* in a broad sense and the narrower concept of *pure cyberterrorism*. Gordon and Ford explain that pure cyberterrorism refers specifically to attacks carried out directly through computer systems with the aim of damaging, disrupting, or destroying computer networks.[37] In contrast, cyberterrorism in the broader sense encompasses all forms of utilizing online technologies and features by terrorists to support and facilitate their actions. Within this framework, for example, the online purchase of airline tickets by the perpetrators of the 11 September 2001 attacks falls under cyberterrorism, as it evidences the use of digital technology as part of a terror strategy. This is often referred to as *traditional cyberterrorism*, where perpetrators exploit the internet as a medium of communication, identity concealment, or as a target of attack, as in Distributed Denial of Service (DDoS) attacks against government websites.[38]

In this context, pure cyberterrorism can be divided into two main forms, destructive cyberterrorism and disruptive cyberterrorism. Destructive cyberterrorism involves manipulating and damaging information systems in ways that destroy both virtual and physical assets. Such attacks often employ malicious software such as viruses, worms, Trojans, or ransomware. Their main objective is to produce physical or digital destruction and to instill fear in society, consistent with the core nature of terrorism. Disruptive cyberterrorism, by contrast, focuses on halting critical digital activities, such as disabling vital websites or disrupting online infrastructure that forms part of everyday life. Techniques used include web defacement, DDoS attacks, unauthorized access, and the modification or deletion of confidential information. Considering the diverse forms and impacts of cyberterrorism, it is clear that pure cyberterrorism constitutes a real threat capable of targeting critical elements of modern society. Such threats are not only posed by terrorist actors but can also be perpetrated by ordinary cybercriminals, and they may result in serious consequences such as identity theft, fraud, theft of sensitive data, espionage, sabotage, symbolic attacks, and extortion—all of which can undermine social order and national security.

---

[36] Heickerö, "Cyberterrorism: Electronic Jihad."

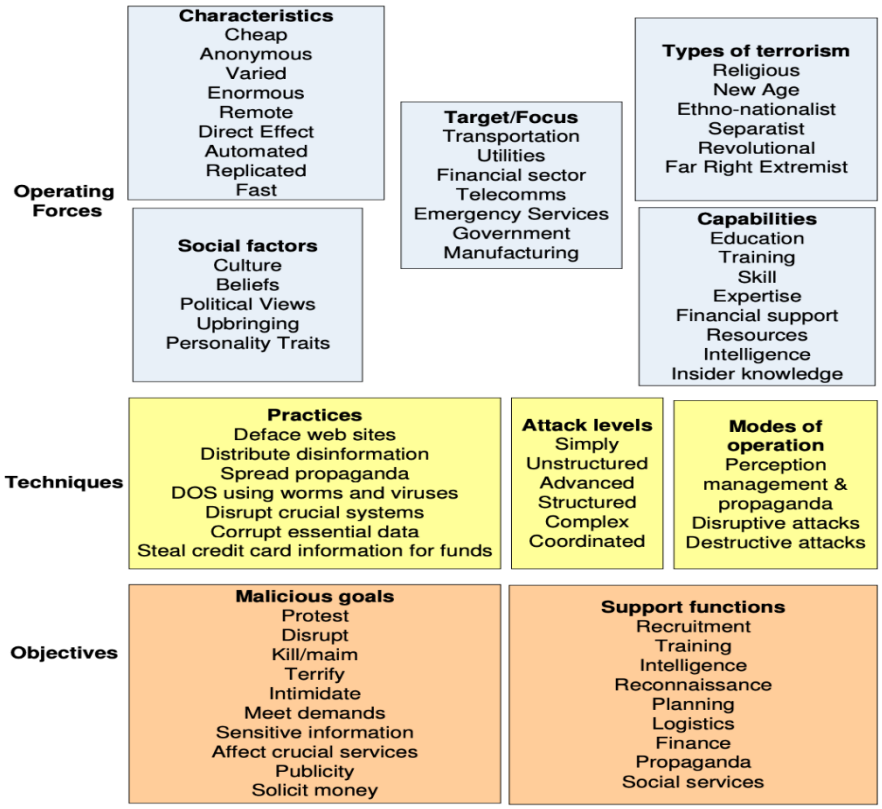
[37] Sarah Gordon and Richard Ford, *Cyberterrorism?* (Symantec, 2003).

[38] Silvia Michielin, "Cyberterrorism: A Study of the Issue in the Framework of the Council of Europe" (Università Ca' Foscari Venezia, 2019).

Meanwhile, John Rollins and Clay Wilson offer a comprehensive definitional approach to cyberterrorism through two main perspectives: an intent-based approach and an effect-based approach.[39] The intent-based approach emphasizes the political, ideological, or religious motives of perpetrators in carrying out cyberattacks, with the primary goal of generating fear, pressuring state authorities, or influencing public policy. In this sense, cyberterrorism involves the use of information technology and networked systems by non-state actors motivated by terrorist purposes. The effect-based approach, on the other hand, focuses on the consequences of the attack: an act is classified as cyberterrorism if it results in significant impact such as damage to critical infrastructure, loss of life, or social disorder, regardless of the perpetrator's motives. Together, these approaches underscore that cyberterrorism is a convergence of digital technology and terrorist action, and it can be understood both from the perspective of the actor's intention and the scale and nature of the harm caused.[40]

To facilitate a clearer understanding of the characteristics of cyberterrorism as an emerging form of terrorism distinct from conventional manifestations, Namosha Veerasamy, an academic researcher at the Council of Scientific and Industrial Research (CSIR) in South Africa, developed a conceptual framework for analyzing cyberterrorism, as outlined below.[41]

Figure 2. Cyberterrorism's Concept



[39] John Rollins and Clay Wilson, *Terrorist Capabilities for Cyberattack: Overview and Policy Issues*, Congressional Research Service Report for Congres (2007), 3.

[40] Pardis Moslemzadeh Tehrani, *Cyberterrorism: The Legal and Enforcement Issues.* (World Scientific Publishing Europe Ltd, 2017).

[41] Namoosha Veerasamy and Marthie Grobler, "Countermeasures to Consider in the Combat Against Cyberterrorism," paper presented at Conference Paper Workshop on ICT Uses in Walfare and Safeguarding if Peace, 2010.

The framework outlined above addresses both the technical and psychological dimensions of cyberterrorism. The capacity to conduct attacks rapidly, directly, anonymously, and remotely provides significant strategic advantages when compared to the financial costs and extensive planning required for conventional attacks such as bombings. Nevertheless, the nature of the attacks and the practices employed are largely shaped by the intensity of the underlying motivations that drive broader ideological or strategic objectives.

National Security and Law Enforcement of Cyberterrorism in Indonesia and United States

Cyberterrorism remains a conceptually ambiguous phenomenon. Most existing definitions distinguish between, on the one hand, politically motivated violent acts, or threats thereofcarried out through the use of the internet, and, on the other hand, the preparatory and supportive activities conducted online or via digital platforms, including recruitment, communication, and financing.[42] While governments primarily perceive violent cyber-enabled terrorist acts as the most severe threat, the absence of fully realized instances of so-called "pure" cyberterrorism has led policy responses to concentrate largely on disrupting the preparatory and facilitative digital activities of suspected terrorists and radicalized individuals. Given the "low probability, high impact" nature of terrorism, counterterrorism policies have increasingly been characterized by heightened political and legal exceptionalism, particularly in the aftermath of the September 11 attacks and the subsequent global "war on terror."[43]

As cyberterrorism is inherently embedded within the digital domain, efforts to counter it have increasingly converged with a broader trend in national security and law enforcement: the expansion of the digital surveillance state. The pursuit of enhanced security through online surveillance has become a prominent feature of international security practices, foreign intelligence operations, and both domestic and transnational law enforcement regimes.[44]

This development has generated extensive debate concerning the proportionality and effectiveness of digital surveillance measures, as well as their compatibility with fundamental rights, including privacy and freedom of expression. Additional concerns have been raised regarding discriminatory outcomes arising from algorithmic or hard-coded biases within surveillance technologies, alongside growing tensions with procedural safeguards such as the presumption of innocence, given the increasingly preemptive nature of contemporary surveillance practices.[45]

In the Indonesian context, cyberterrorism is commonly referred to as *"terorisme mayantara,"* with the term *mayantara* serving as the Indonesian linguistic equivalent of "cyber," thereby corresponding terminologically to cyberterrorism in English.[46] By contrast, events such as the Bali Bombings I exemplify conventional terrorism, as they involved clearly defined command structures and identifiable perpetrators. However, the increasing integration of digital

---

[42] Dennis Broeders et al., "Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy," *Studies in Conflict & Terrorism* 46, no. 12 (2023): 2426–53.

[43] Harold H. Koh, "On American Exceptionalism," *Stanford Law Review* 55, no. 5 (2003): 1479–527.

[44] Dennis Broeders et al., "Big Data and Security Policies: Towards a Framework for Regulatingthe Phases of Analytics and Use of Big Data," *Computer Law & Security Review* 33, no. 3 (2017): 309–23.

[45] Palasinski Marek and Lorraine Bowman Grieve, "Tackling Cyber-Terrorism: Balancing Surveillance with Counter-Communication," *Security Journal* 30, no. 2 (2017): 556–68.

[46] Muhammad Nadjib and Hafied Cangara, "Cyber Terrorism Handling in Indonesia," *The Business and Management Review* 9, no. 2 (2017): 274–83.

technologies across multiple sectors of social, economic, and political life has created new opportunities for criminal and terrorist actors to exploit technological infrastructures in the execution of their activities.

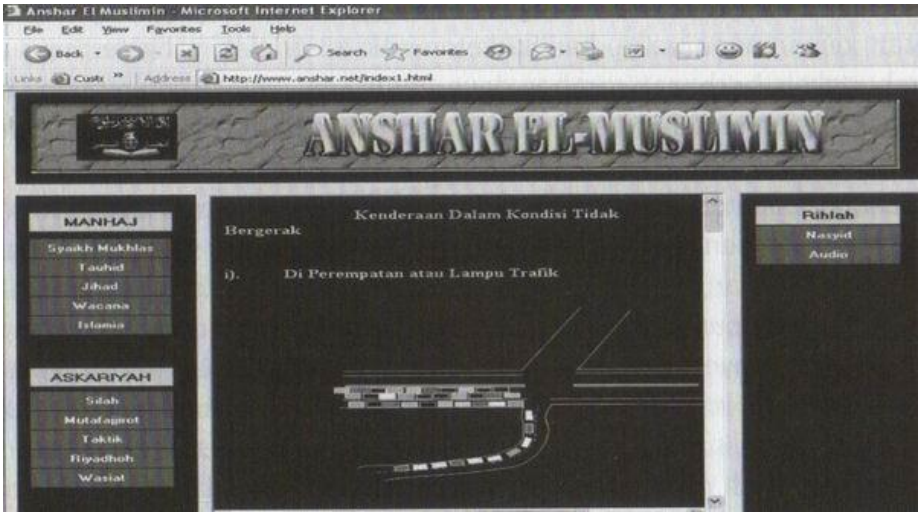
The phenomenon of cyberterrorism in Indonesia began to be identified in the aftermath of the Bali Bombings I on 12 October 2002, which remains one of the most destructive terrorist attacks in the country's history. Two years later, in 2004, the Indonesian National Police uncovered digitally mediated activities linked to terrorist networks, marked by the arrest of individuals operating internet websites for the purpose of terrorist propaganda. Subsequent investigations revealed that Imam Samudra, one of the principal perpetrators of the Bali Bombings I, who was later sentenced to death, continued to coordinate terrorist networks through digital means while in detention. Using a notebook computer smuggled into Krobokan Prison in Denpasar, Bali, he reportedly engaged in online activities for several months prior to the attacks. These activities took place between July 2005 and the lead-up to the Bali Bombings II on 1 October 2005, before his transfer to Nusakambangan Prison.

Law enforcement authorities successfully apprehended two individuals implicated in cyberterrorism-related activities, namely Agung Setyadi, a lecturer at a higher education institution in Semarang, and Mohammad Agung Prabowo, also known as Max Fiderman, a university student in Semarang, Central Java. In his testimony, Agung Setyadi stated that he neither knew nor had ever met Imam Samudra in person. The arrests led to the seizure of various items of digital evidence, including a laptop computer, two mobile phones, three SIM cards, a flash drive, a USB Bluetooth device, two external hard drives, a CD case, and several related documents. Investigations revealed that Max Fiderman possessed advanced expertise in information technology, particularly in carding, cracking, and hacking techniques, and had provided technical training to both Agung Setyadi and Imam Samudra. In cyberspace, Imam Samudra operated under the pseudonym "Al-Irhab" and communicated with Max through online chat platforms, specifically via Islamic-themed channels on the MiRC chat network.[47]

Although Imam Samudra reportedly attempted to ideologically recruit Max into his network through a process of *bai'at* (oath of allegiance), Max declined due to the absence of strong ideological or religious motivations, being driven instead by personal gratification derived from digital engineering activities. In his technical capacity, Max nonetheless contributed to the development of the propaganda website *www.anshar.net* at the request of Noordin M. Top, who at the time was a central figure within terrorist networks in Indonesia. For this purpose, Max registered web-hosting services through *www.openhosting.co.uk*, a United Kingdom–based provider, at an approximate cost of £300, and secured the domain name via the DNS server *www.joker.com* in Germany for approximately USD 60. The financial resources used to support these activities were obtained through carding-related cybercrime, which Max also employed to fund his educational expenses and other operational needs.

[47] Supriyadi, *Cyberterrorism*.

Figure 3. The List of Public Vulnerability Points and Potential Targets[48]



The content of the website *www.anshar.net* contained information outlining attack techniques that exploited vulnerabilities in public spaces, including toll road entry points, traffic congestion areas, office building entrances and exits, shopping centers, entertainment venues, sports facilities, hotels, and exhibition sites. The website also listed several potential terrorism targets in Indonesia, such as Ancol, Planet Hollywood, the Senayan Golf Driving Range, and the Jakarta Convention Center. According to investigators, the website was developed between June and August 2005 by Qital, also known as Abdul Azis—later identified as a suspect in the Bali Bombings II—acting under the direction of Noordin M. Top, who was a fugitive at the time. During the development process, Qital sought assistance from Agung Setyadi, who subsequently involved an individual named Max due to his expertise in information technology. Through online communication channels, Qital coordinated with Max, ultimately leading to the successful creation of the *www.anshar.net* website.[49] Max was recorded as using the internet service provider Matri, with identified IP address ranges including 202.152.162.x and 202.93.x, which were linked to the Matrix service—namely, a postpaid GSM telephone card operated by PT Indosat. Although strong indications were found regarding the involvement of cybercrime techniques in financing terrorist activities, to date there has been no definitive quantitative data available to estimate the total amount of funds generated through such methods.[50]

A notable case of cyberterrorism in the United States emerged in August 2020, when the U.S. government, through the Department of Justice, the Department of Homeland Security, and the Department of the Treasury, officially announced the disruption of three cyberterrorism campaigns conducted by three distinct terrorist organizations. These groups were the Al-Qassam Brigades, Al-Qaeda, and the Islamic State of Iraq and Syria (ISIS). The campaigns were carried out online and were aimed at mobilizing support for terrorist activities within the territory of the United States. The three organizations employed sophisticated cyber technologies in executing

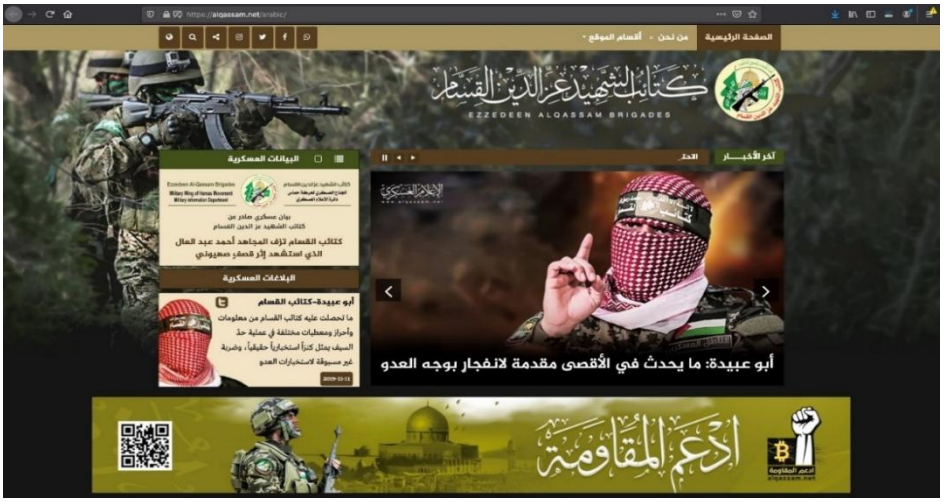
[48] Sam Ardi, "Cyberterrorism," *Cyberterrorism*, n.d., accessed January 3, 2026, https://samardi.wordpress.com/2012/07/02/cyberterrorism/.

[49] Antara, *Pengacara TPM Dampingi Tersangka Pembuat Laman Www.Anshar.Net.*, 2006, https://www.antaranews.com/berita/40759/pengacara-tpm-dampingi-tersangka-pembuat-laman-wwwansharnet.

[50] Ida Rochmawati, "Cyber Terorisme Dan Eksistensi Gerakan Terorisme Kelompok Islam Radikal Di Indonesia," *INOVATIF: Jurnal Penelitian Pendidikan, Agama Dan Kebudayaan* 2, no. 1 (2016): 33–53.

their operations, including fundraising activities that successfully generated millions of U.S. dollars. The funds were collected through approximately 300 cryptocurrency accounts, three websites, and four Facebook accounts, all of which were subsequently seized by U.S. authorities. Although the groups pursued similar objectives, each implemented distinct campaign strategies and fundraising mechanisms, operating anonymously within the digital environment.[51]

Figure 4. Al-Qassam Brigades[52]



The first enforcement action concerned the Al-Qassam Brigades and their efforts to raise funds online through cryptocurrency. In early 2019, the Al-Qassam Brigades disseminated appeals on their social media platforms calling for donations in the form of Bitcoin to finance their terrorist campaigns.[53] These appeals were subsequently redirected to their official websites, namely *alqassam.net*, *alqassam.ps*, and *qassam.ps*. The organization asserted that Bitcoin donations were untraceable and would be used to support terrorist operations. Their websites provided instructional videos explaining how to donate anonymously, including the use of uniquely generated Bitcoin addresses for each individual donation. However, contrary to these claims, the donations were not entirely anonymous. Through coordinated efforts involving the Internal Revenue Service (IRS), Homeland Security Investigations (HSI), and the Federal Bureau of Investigation (FBI), law enforcement authorities successfully traced and seized all 150 cryptocurrency accounts used to launder funds flowing into and out of Al-Qassam Brigades–controlled accounts. Simultaneously, criminal search warrants were executed against individuals residing in the United States who were identified as having contributed donations to the terrorist fundraising campaign.

The second cyberterrorism financing campaign was conducted by Al-Qaeda. As outlined in the asset forfeiture complaints, the organization operated a Bitcoin-based money laundering network through Telegram channels and various other social media platforms to

[51] Halida Azalea Iffa Dina, "Aksi Cyber-Terrorism Di Amerika Serikat Dalam Perspektif Keamanan Global," *Global & Policy* 9, no. 2 (n.d.): 131.

[52] U.S. Department of Justice, "Global Disruption of Three Terror Finance Cyber-Enabled Campaigns," accessed December 22, 2025, https://www.justice.gov/archives/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns.

[53] Congress.Gov, "Terrorist Financing: Hamas and Cryptocurrency Fundraising," legislation, accessed January 3, 2026, https://www.congress.gov/crs-product/IF12537.

solicit cryptocurrency donations in support of its terrorist objectives. In several instances, Al-Qaeda actors masqueraded as charitable organizations, while in reality they openly and explicitly solicited funds to finance violent terrorist attacks. One such example involved an online post by a purported charity that called for donations to equip terrorists operating in Syria.[54]

The third case involved ISIS during the COVID-19 pandemic. Murat Cakar, an ISIS facilitator responsible for managing several of the group's hacking operations, exploited the website *FaceMaskCenter.com* as a front for trading counterfeit personal protective equipment (PPE). This scheme not only generated financial resources for terrorist activities but also demonstrated how cyberterrorist actors opportunistically exploited global crises and digital marketplaces to sustain their operations.[55]

These two cases occurring respectively in Indonesia and the United States demonstrate that cyberterrorism should not be understood solely as cyberattacks targeting digital infrastructure, but rather as the strategic use of cyberspace as a core enabling environment for terrorist activities, including propaganda dissemination, recruitment, communication, and financial mobilization. In the Indonesian context, the cases involving Imam Samudra, Agung Setyadi, and Max Fiderman illustrate how information and communication technologies were employed to construct terrorist networks that transcended individual actors and national borders without requiring direct physical interaction. The use of propaganda websites, online chat platforms, and cyber-enabled financial crimes such as carding reflects the adaptive transformation of terrorist practices in response to digital technological developments, rendering contemporary threats more covert, decentralized, and difficult to detect. By contrast, the United States case reflects a more advanced and systematized manifestation of cyberterrorism, particularly through the exploitation of cryptocurrencies and global digital platforms. Online fundraising campaigns conducted by the Al-Qassam Brigades, Al-Qaeda, and ISIS reveal the capacity of terrorist organizations to leverage the relative anonymity of cyberspace, social media ecosystems, and blockchain technologies to generate substantial financial resources across multiple jurisdictions. This operational shift underscores that cyberterrorism is increasingly detached from traditional hierarchical terrorist structures and instead relies on technical expertise, dispersed digital networks, and the psychological manipulation of a transnational support base.

Indonesia and the United States represent two jurisdictions with fundamentally different legal systems and socio-legal cultures, yet both confront comparable challenges in addressing cyber-related threats, including cyberterrorism. In Indonesia, although several statutory instruments regulate cybercrime, their practical implementation continues to face substantial obstacles, particularly in terms of enforcement capacity, inter-agency coordination, and technological expertise. Despite the enactment of Law No. 5 of 2018 on the Eradication of Terrorism Crimes and the most recent amendment to the Information and Electronic Transactions Law (Law No. 1 of 2024)[56], the regulation of cyberterrorism in Indonesia remains largely implicit and sectoral. The absence of an explicit statutory definition of cyberterrorism

[54] Chainalysis, "Chainalysis in Action: Department of Justice Announces Takedown of Two Terrorism Financing Campaigns with Help from Blockchain Analysis," Chainalysis, accessed January 3, 2026, https://www.chainalysis.com/blog/cryptocurrency-terrorism-financing-al-qaeda-al-qassam-brigades-bitcointransfer/.

[55] David Choi, "Fake N95 Face Masks Were Being Sold on This ISIS-Linked Website — and It Shows How Terror Groups Are Using COVID-19 as a Propaganda Tool," Business Insider, accessed January 3, 2026, https://www.businessinsider.com/fake-face-mask-website-isis-2020-8.

[56] Law No. 1 of 2024 on Information and Electronic Transactions.

generates legal uncertainty, especially with regard to offense classification, evidentiary thresholds, and prosecutorial consistency. Nevertheless, the ITE Law continues to function as a functional legal basis for prosecuting cyber-enabled terrorist conduct, insofar as such acts involve the use of electronic systems to access, manipulate, or exploit data in furtherance of terrorist objectives.

From a doctrinal perspective, cybercrime under Indonesian law may be understood as encompassing two broad categories. The first comprises offenses in which electronic information or digital platforms serve as instruments for committing substantive crimes, such as online fraud, digital extortion, dissemination of false information, and cyberterrorism-related propaganda or coordination. The second category consists of offenses that directly target electronic information systems and networks themselves, including illegal access, system interference, unlawful interception, and electronic data theft.[57] While this interpretative framework affords a degree of flexibility, it simultaneously reveals the fragmented and non-codified nature of Indonesia's current regulatory approach to cyberterrorism.[58]

In addition to the ITE Law, Indonesia's counterterrorism framework is primarily governed by Law No. 5 of 2018 on the Eradication of Terrorism Crimes, which amended Law No. 15 of 2003.[59] Although this statute does not explicitly employ the term *cyberterrorism*, it provides a legal basis for addressing cyber-enabled terrorist conduct through provisions criminalizing acts of terrorism, conspiracy, assistance, training, incitement, and the dissemination of terrorist ideology. Several of these offenses are formulated in a technologically neutral manner, allowing their application to activities conducted through digital and electronic means, including online propaganda, recruitment, coordination, and financing. Moreover, Law No. 5 of 2018 expands the scope of criminal liability to include preparatory acts (*early stage criminalization*), such as planning, mobilization, and support for terrorism, which are highly relevant in the context of cyberterrorism. The law also strengthens preventive measures by authorizing surveillance, interception of communications, and financial monitoring, subject to judicial oversight. When read in conjunction with Law No. 1 of 2024 on Information and Electronic Transactions, Indonesia's legal framework enables law enforcement authorities to prosecute cyberterrorism through a combination of substantive terrorism offenses and cybercrime-related provisions. Nevertheless, the absence of an explicit statutory definition of cyberterrorism continues to pose challenges in terms of legal certainty, doctrinal coherence, and consistent enforcement.

By contrast, the United States does not regulate cyberterrorism through a single statute that explicitly employs the term *cyberterrorism*. Instead, it adopts a comprehensive, flexible, and multi-layered legal framework that integrates cybercrime law, counterterrorism legislation, financial regulation, and national security and intelligence regimes. The Computer Fraud and Abuse Act (CFAA)[60] serves as a central instrument for addressing attacks against computer systems and networks, while provisions contained in the USA PATRIOT Act[61], and statutes

[57] Sofwan Rizko Ramadoni et al., "Sejarah Undang-Undang ITE: Periodisasi Regulasi Peran Negara Dalam Ruang Digital," *Langgong: Jurnal Ilmu Sosial Dan Humaniora* 3, no. 2 (2023): 4158.

[58] Jecky Tamora Lumban Tobing, "Cyber-Terrorism Dari Sudut Pandang Hukum Pidana Indonesia," *Jurnal Lex Dirgantara* 1, no. 2 (2024): 9.

[59] Law No. 5 of 2018 on the Eradication of Terrorism Crimes.

[60] The Computer Fraud and Abuse Act (CFAA).

[61] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act.

criminalizing material support to terrorism are employed to prosecute digitally facilitated terrorist financing, propaganda dissemination, and logistical support.

In addition to criminal prosecution, the United States actively deploys non-penal legal mechanisms, most notably asset forfeiture and the seizure of digital assets, including cryptocurrencies, as both preventive and repressive tools to disrupt cyberterrorism financing networks. This regulatory architecture is reinforced by the extensive authority of law enforcement and intelligence agencies, including the Federal Bureau of Investigation (FBI), the Department of Homeland Security (DHS), the Department of Justice (DOJ), and the Department of the Treasury, all of which possess mandates to conduct digital surveillance, trace financial transactions, and carry out cross-border operations. This approach reflects a legal orientation that prioritizes pre-emptive enforcement, national security protection, and regulatory adaptability in response to rapidly evolving digital technologies, while simultaneously generating ongoing debates concerning proportionality, privacy rights, and the permissible scope of state power.

In sum, this comparative analysis reveals that although Indonesia and the United States face analogous cyberterrorism challenges, their legal responses differ markedly in terms of normative clarity, institutional integration, and enforcement strategy. Indonesia's approach is characterized by an implicit and fragmented regulatory framework that relies on the combined application of cybercrime and counterterrorism legislation, offering doctrinal flexibility but simultaneously generating legal uncertainty and uneven enforcement. Conversely, the United States adopts a comprehensive and multi-layered legal architecture that systematically integrates cybercrime law, counterterrorism statutes, financial regulation, and national security regimes, reinforced by strong inter-agency coordination and the strategic use of both penal and non-penal measures. These findings suggest that the effectiveness of cyberterrorism regulation is contingent not merely upon the existence of substantive criminal norms, but also upon regulatory coherence, institutional capacity, and the ability of legal systems to adapt to rapidly evolving digital threats while maintaining proportionality and respect for fundamental rights.

CONCLUSION

The metamorphosis of terrorism from conventional physical manifestations to the production of pervasive digital fear necessitates a rigorous normative recalibration of national legal architectures to address the inherent translucency and borderless nature of cyberspace. This comparative inquiry demonstrates that while the United States employs a multi-layered regulatory framework, leveraging the effects doctrine and protective principle to extend jurisdiction over extraterritorial threats, the Indonesian legal landscape remains characterized by fragmented, implicit, and sectoral regulations that engender enforcement lacunae and conceptual ambiguity. The absence of a harmonized statutory definition and the persistent reliance on territorial-based sovereignty paradigms significantly undermine international legal certainty and the efficacy of cross-border counterterrorism cooperation. Ultimately, the study posits that mitigating the low probability, high impact risks of cyberterrorism require a transition toward a more cohesive, technologically neutral, and internationally integrated legal model capable of safeguarding critical infrastructure against the sophisticated, decentralized, and ideologically driven modalities of modern digital terror.

REFERENCES

Abou El Fadl, Khaled. *The Great Theft: Wrestling Islam From the Extremists*. HarperOne, 2007.

Antara. *Pengacara TPM Dampingi Tersangka Pembuat Laman Www.Anshar.Net.* 2006. https://www.antaranews.com/berita/40759/pengacara-tpm-dampingi-tersangka-pembuat-laman-wwwansharnet.

Archer, Emerald. "Crossing the Rubicon: Understanding Cyber Terrorism in the European Context." *The European Legacy: Toward New Paradigms* 14, no. 7 (2009): 605–22.

Ardi, Sam. "Cyberterrorism." *Cyberterrorism*, n.d. Accessed January 3, 2026. https://samardi.wordpress.com/2012/07/02/cyberterrorism/.

Bishmanov, Kakimzhan, Zarina Muratzhan, Zhanat Dilbarkhanova, and Viktoriya Lyutsik. "Analysis of Modern Types of Cyberterrorism and Methods for Countering Them." *IDP. Revista d'Internet ...*, no. 41 (2024): 1–14.

Brenner, S. W. *At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare*. 97, no. 2 (2007): 379–475.

Broeders, Dennis, Fabio Cristiano, and Daan Weggemans. "Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy." *Studies in Conflict & Terrorism* 46, no. 12 (2023): 2426–53.

Broeders, Dennis, Erik Schrijvers, Bart van der Sloot, Rosamunde van Brakel, Josta de Hoog, and Ernst Hirsch Ballin. "Big Data and Security Policies: Towards a Framework for Regulatingthe Phases of Analytics and Use of Big Data." *Computer Law & Security Review* 33, no. 3 (2017): 309–23.

Chainalysis. "Chainalysis in Action: Department of Justice Announces Takedown of Two Terrorism Financing Campaigns with Help from Blockchain Analysis." Chainalysis. Accessed January 3, 2026. https://www.chainalysis.com/blog/cryptocurrency-terrorism-financing-al-qaeda-al-qassam-brigades-bitcointransfer/.

Choi, David. "Fake N95 Face Masks Were Being Sold on This ISIS-Linked Website — and It Shows How Terror Groups Are Using COVID-19 as a Propaganda Tool." Business Insider. Accessed January 3, 2026. https://www.businessinsider.com/fake-face-mask-website-isis-2020-8.

Collier, David. "The Comparative Method." In *Political Science: The State of the Discipline II*. American Political Science Association, 1993.

Congress.Gov. "Terrorist Financing: Hamas and Cryptocurrency Fundraising." Legislation. Accessed January 3, 2026. https://www.congress.gov/crs-product/IF12537.

Conway, Maura. "Determining The Role of the Internet in Violent Extremism and Terrorism." *Studies in Conflict & Terrorism* 40, no. 1 (2017): 77–98.

Conway, Maura. "Terrorism and the Internet: New Media—New Threat?" *Parliamentary Affairs* 59, no. 2 (2006): 283–98.

Denning, Dorothy. "Cyberterrorism: Testimony Before the Special Oversight Panel on Terrorism Committee on Armed Service U.S. House of Representatives." 2002. https://faculty.nps.edu/dedennin/publications/Testimony-Cyberterrorism2000.htm.

Denning, Dorothy E., ed. "Cyber Conflict as an Emergent Social Phenomenon." In *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*. IGI Global, 2011. https://doi.org/10.4018/978-1-61692-805-6.

Dina, Halida Azalea Iffa. "Aksi Cyber-Terrorism Di Amerika Serikat Dalam Perspektif Keamanan Global." *Global & Policy* 9, no. 2 (n.d.): 131.

Ergun, Mucahit, and Gulsen Seker Aydin. "Evolution of Cyberterrorism: Challenges and Solutions." *Journal of Internasional Relations Studies* 4, no. 2 (2024): 64–73.

Friis, S. M. "Behead, Burn, Crucify, Crush": Theorizing the Islamic State's Public Displays of Violence." *European Journal of International Relations* 24, no. 2 (2018): 243–67.

Gartzke, E. "The Myth of Cyberwar: Bringing War in Cyberspace Back down to Earth." *International Security* 38, no. 2 (2013): 41–73.

Gordon, Sarah, and Richard Ford. *Cyberterrorism?* Symantec, 2003.

Gross, Michael L., Daphna Canetti, and Dana R. Vashdi. "Cyberterrorism: Its Effects on Psychological Well-Being, Public Confidence and Political Attitudes." *Journal of Cybersecurity* 3, no. 1 (2017): 49–58.

Gupta, Dipak K. *The Roots of Terrorism: Who Are the Terrorists?* Chelsea House, 2006.

Hasan, Noorhaidi. "Violent Activism, Islamist Ideology, and the Conquest of Public Space Among Youth in Indonesia." In *Youth Identities and Social Transformations in Modern Indonesia*. Brill, 2016. https://doi.org/10.1163/9789004307445_011.

Heickerö, Roland. "Cyberterrorism: Electronic Jihad." *Strategic Analysis* 38, no. 4 (2014): 554–65.

Hutchinson, T., and N. Duncan. *Defining and Describing What We Do: Doctrinal Legal Research*. 17, no. 1 (2012): 83–119.

Indrawan, Arvid Gema, Abdul Harris Semendawai, and Wiryanto Wiryanto. "Penanggulangan Tindak Pidana Cyber Terrorism Dalam Perspektif Kepastian Hukum." *Jurnal Hukum Jurisdictie* 3, no. 2 (2021): 35–63. https://doi.org/10.34005/jhj.v3i2.47.

Jacobsen, Jeppe T. "Cyberterrorism: Four Reasons for Its Absence-So Far." *Perspective on Terrorism* 16, no. 5 (2022): 62–72.

Jarvis, Lee, and Stuart Macdonald. "What Is Cyberterrorism and Why Does It Matter? Findings from a Survey of Researchers." *Terrorism and Political Violence* 27, no. 3 (2015): 1–20.

Kesan, Jay P., and Carol M. Hayes. "Mitigative Counterstriking: Self-Defence and Deterrence in Cyberspace." *Harvard Journal of Law & Technology* 25, no. 2 (2012): 429–75.

Koh, Harold H. "On American Exceptionalism." *Stanford Law Review* 55, no. 5 (2003): 1479–527.

Kulezsa, J. *Due Diligence in International Law*. Brill Nijhoff, 2016.

Law No. 1 of 2024 on Information and Electronic Transactions.

Law No. 5 of 2018 on the Eradication of Terrorism Crimes.

Lindsay, Jon R. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* 22, no. 3 (2013): 365–404.

Madjid, Yasniar Rachmawati. "Cyberterrorism Challenges: The Need for Global Mutual Legal Assistance for Universal Criminal Jurisdiction." *Yustisia Jurnal Hukum* 10, no. 3 (2021): 388–414.

Marek, Palasinski, and Lorraine Bowman Grieve. "Tackling Cyber-Terrorism: Balancing Surveillance with Counter-Communication." *Security Journal* 30, no. 2 (2017): 556–68.

Maskun. *Kejahatan Siber (Cyber Crime): Suatu Pengantar*. Prenada Media Group, 2013.

Michielin, Silvia. "Cyberterrorism: A Study of the Issue in the Framework of the Council of Europe." Università Ca' Foscari Venezia, 2019.

Nadjib, Muhammad, and Hafied Cangara. "Cyber Terrorism Handling in Indonesia." *The Business and Management Review* 9, no. 2 (2017): 274–83.

Negara, Tunggul Ansari Setia. *Normative Legal Research in Indonesia: Its Origins and Approaches*. 4, no. 1 (2023): 1–9.

Ramadoni, Sofwan Rizko, Reza Pramasta Gegana, and Kalen Sanata. "Sejarah Undang-Undang ITE: Periodisasi Regulasi Peran Negara Dalam Ruang Digital." *Langgong: Jurnal Ilmu Sosial Dan Humaniora* 3, no. 2 (2023): 4158.

Rochmawati, Ida. "Cyber Terorisme Dan Eksistensi Gerakan Terorisme Kelompok Islam Radikal Di Indonesia." *INOVATIF: Jurnal Penelitian Pendidikan, Agama Dan Kebudayaan* 2, no. 1 (2016): 33–53.

Rollins, John, and Clay Wilson. *Terrorist Capabilities for Cyberattack: Overview and Policy Issues*. Congressional Research Service Report for Congres. 2007.

Seib, Philip, and Dana M. Janbek. *Global Terrorism and New Media: The Post–Al Qaeda Generation*. Routledge, 2007.

Setiawan, Dian Alan. "Cyberterrorism and Its Prevention in Indonesia." *Jurnal Media Hukum* 27, no. 2 (2020): 267–83.

Singer, P. W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press, 2014.

Supriyadi, A. Adang. *Cyberterrorism*. Badan Nasional Penanggulangan Terorisme, 2020.

Tehrani, Pardis Moslemzadeh. *Cyberterrorism: The Legal and Enforcement Issues.* World Scientific Publishing Europe Ltd, 2017.

The Computer Fraud and Abuse Act (CFAA).

Tobing, Jecky Tamora Lumban. "Cyber-Terrorism Dari Sudut Pandang Hukum Pidana Indonesia." *Jurnal Lex Dirgantara* 1, no. 2 (2024): 9.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act.

U.S. Department of Justice. "Global Disruption of Three Terror Finance Cyber-Enabled Campaigns." Accessed December 22, 2025. https://www.justice.gov/archives/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns.

Weimann, Gabriel. "Cyberterrorism: The Sum of All Fears?" *Studies in Conflict and Terrorism* 28 (2005): 130.

Weimann, Gabriel. *Terrorism in Cyberspace: The Next Generation*. Columbia University Press, 2015.