Journal of Human Rights, Culture and Legal System
Vol. 3, No. 3, November 2023, pp. 625-655
ISSN 2807-2812

Techno-Prevention in Counterterrorism: Between Countering Crime and Human Rights Protection

Ali Masyhar [a*] Silaas Oghenemaro Emovwodo [b]

[a] Faculty of Law, Universitas Negeri Semarang, Semarang, Indonesia.
[b] Faculty of Art and Social Science, Universiti Brunei Darussalam.

* corresponding author: ali_masyhar@mail.unnes.ac.id

ARTICLE INFO

Article history
Received: July 13, 2023
Revised: October 30, 2023
Accepted: November 2, 2023

Keywords
Counter;
Cyber Terrorism;
Cyber Security;
Governance;

ABSTRACT

Terrorism has become a significant concern throughout the world. This concern is supported by the increasing use of the internet, which has triggered an increase in cyberattacks. This research aims to determine the role of governance in counter-cyber terrorism. The normative legal methodology utilized in this study results from an exhaustive literature evaluation. This research shows that the government's role is needed to counter cyber terrorism. Although the Indonesian government has initiated a national cybersecurity strategy and implemented short-term and long-term programs, some obstacles and challenges hinder its implementation. The ITE Law has encouraged Indonesia to establish policies and regulations regarding information security. There have yet to be any regulations regarding cyber-attacks to counter cyber terrorism. Various institutions with common interests in national defense and security, including the cyber domain, must collaborate with BSSN. Other government agencies that depend on each other include the *TNI*, *Polri*, Ministry of Defense, *BIN*, and Ministry of Communication and Information. Apart from that, governance is also needed, including international organizations, several non-governmental organizations (NGOs), government and private governance, and several other components.

1. Introduction

In recent years, terrorism has emerged as a prominent global issue. Defense and deterrence concepts are subject to transformation in light of evolving concerns and asymmetric threats. Consequently, each nation will confront a multifaceted array of challenges and priorities. As the emphasis shifts to perceived adversaries of peace—including mercenary terrorists, religious fundamentalists, and

organized criminals who are becoming more adept at utilizing modern technology and capitalizing on economic alienation or radical religious misalignments—perceptions of security threats are undergoing a paradigm shift. Nevertheless, the current global schism transcends economic inequalities and religious divergences. Additional elements contributing to this phenomenon encompass resistance towards dual-use technologies, inequities in armaments export policies, prejudices in trade practices, and intense rivalry in defense modernization, technological advancement, and economic development. Public facilities that rely on information and electronic technology may serve as incubators for terrorist activities, which are particularly susceptible to transpiring in Indonesia and also utilize such facilities.

At the same time, the internet is continuously influencing people's lifestyles and becoming an ever-expanding component of their social lives. Constraints of globalization are progressively reinforcing the Internet's position in society. The number of Internet users is projected to increase from 3.9 billion (51% of the world population) in 2018 to 5.3 billion (66% of the world population) by 2023. In addition, the quantity of devices connected to IP networks is projected to surpass three times the global population. In addition, networked devices are projected to increase significantly from 18.4 billion in 2018 to 29.3 billion in 2019. Furthermore, establishing 14.7B Machine-to-Machine (M2M) connections will be completed.[1] Internet integration is permeating governments' critical infrastructures, and the Internet is increasingly recognized as a significant driver of socioeconomic development. The ever-expanding and profound architecture of the Internet renders us susceptible to an ever-growing array of novel threats. Detecting these hazards in network traffic is one of the most critical concerns in contemporary cyber security.[2]

Cybersecurity safeguards network data, software, and physical structures against illicit access or modification. Two components comprise the security of a network: the network security system and the host protection system.[3] Cybersecurity is a technological advancement designed to safeguard a network's software, data, and physical infrastructure from unauthorized intrusion or

[1] Morteza Safaei Pour and others, 'A Comprehensive Survey of Recent Internet Measurement Techniques for Cyber Security', *Computers & Security*, 128 (2023), 103123 https://doi.org/10.1016/j.cose.2023.103123

[2] Rian Saputra and others, 'Artificial Intelligence and Intellectual Property Protection in Indonesia and Japan', *Journal of Human Rights, Culture and Legal System*, 3.2 (2023), 210–35 https://doi.org/10.53955/jhcls.v3i2.69

[3] Huseyin Ahmetoglu and Resul Das, 'A Comprehensive Review on Detection of Cyber-Attacks: Data Sets, Methods, Challenges, and Future Research Directions', *Internet of Things*, 20 (2022), 100615 https://doi.org/10.1016/j.iot.2022.100615

alteration. The network protection system and the network security system are the two components that comprise the security of a network. The intrusion detection systems (IDS), antivirus software, and firewalls of these systems assist cyber-security professionals in identifying unauthorized network transactions.[4] Cyberattacks on a global scale are expanding at an alarming rate of magnitude. The assaults above are frequently associated with the widely recognized and publicized menace of cyber terrorism.[5] Cyberterrorism is a new type of terrorism that exploits or uses information technology.

Critical components of the direct action strategy against terrorism include the confiscation of terrorist training facilities, reprisals against state sponsors, the collection of intelligence, and the blocking of terrorist bank accounts. Preventative measures, such as bolstering border security and implementing technological barriers (e.g., metal and explosives detectors), are frequently the foundation of defensive strategies. Specific policies implemented by the counter-terrorism division are inclined toward a direct action strategy. Terrorism eradication efforts must critically address its fundamental causes, with the ultimate objective of preventing terrorist acts.[6] Convincing nations to enforce more severe sanctions for individuals who exploit this technology poses a formidable obstacle, alongside galvanizing international support in the struggle for this objective. National governments must maintain their efforts to combat terrorism.

Indonesia has been implicated in several recent occurrences as one of the nations with inadequate cyber security. Several recent incidents, including the ransomware-induced breach of user or bank customer data, provide evidence in support of this claim. Ransomware is a malevolent assault targeting software to restrict user file access, encrypt files, turn off the user's screen, or demand a ransom.[7] In Indonesian cyberspace, all illicit activities are governed by Law No. 19 of 2016, an amendment to Law No. 8 of 2011 on Electronic and Information Transactions. As a preventative measure against criminal acts, the *ITE* Law is the legal foundation for addressing offenses committed through computers and other

[4] Mokhtar Mohammadi and others, 'A Comprehensive Survey and Taxonomy of the SVM-Based Intrusion Detection Systems', *Journal of Network and Computer Applications*, 178 (2021), 102983 https://doi.org/10.1016/j.jnca.2021.102983

[5] Jordan J. Plotnek and Jill Slay, 'Cyber Terrorism: A Homogenized Taxonomy and Definition', *Computers & Security*, 102 (2021), 102145 https://doi.org/10.1016/j.cose.2020.102145

[6] Sheraz Ahmad Choudhary and others, 'Role of Information and Communication Technologies on the War against Terrorism and on the Development of Tourism: Evidence from a Panel of 28 Countries', *Technology in Society*, 62 (2020), 101296 https://doi.org/10.1016/j.techsoc.2020.101296

[7] Ryan Randy Suryono, Indra Budi, and Betty Purwandari, 'Detection of Fintech P2P Lending Issues in Indonesia', *Heliyon*, 7.4 (2021), e06782 https://doi.org/10.1016/j.heliyon.2021.e06782

electronic means.[8] Ongoing dialogues are encouraged regarding the critical role of academics and practitioners in the field, coordination, and collaboration across all instruments for eradicating terrorism due to revising the Anti-Terrorism Law in Indonesia. Drifts and incoherence among counterterrorism components constitute challenges encountered within the counterterrorism domain. Undoubtedly, in response to such circumstances, patterns and methods of counterterrorism must also evolve. Initially focused solely on physical/personal surveillance, particularly physical movement between locations, counterterrorism can no longer be its primary concern. By implementing information technology, the assailants no longer rely on visual perception to execute their schemes. Anything is possible so long as they have an internet or cyber connection.[9]

Legislation No. 19 of 2016 amending Law No. 11 of 2008 on Information and Electronic Transactions, Law No. 36 of 1999 on Telecommunications, and Minister of Communication and Information Regulation No. 5 of 2017 on the Fourth Amendment to Securing the Use of Internet Protocol-Based Telecommunication Networks are just a few of the cyber security policies and regulations that Indonesia has already established. The development of information and communication technology (ICT) is growing along with the increase in cybercrime. However, until now, comprehensive policies and regulations related to cyber security still need to be explained.[10] Law Number 5 of 2018, which amends Law Number 15 of 2003 regarding Criminal Acts of Terrorism and broadens the definition of terrorism to include crimes, is an additional regulatory measure implemented by the government to combat cyber terrorism. Terrorism is conducted online. This enables law enforcement to combat terrorist activities associated with internet and technological usage proactively.[11] Apart from that, Government Regulation (PP) Number 71 of 2019 concerning Supervision of the Implementation of Electronic Systems and Transactions is also regulated. Involving relevant ministries or institutions and all sectors of the country in national preparedness, counter-radicalization, and deradicalization initiatives coordinated by the National Agency Countering Terrorism ensures optimal

[8] Dita Septasari, 'The Cyber Security and The Challenge of Society 5.0 Era in Indonesia', *Aisyah Journal Of Informatics and Electrical Engineering (A.J.I.E.E)*, 5.2 (2023), 227–33 https://doi.org/10.30604/jti.v5i2.231

[9] Ali Masyhar and others, 'Digital Transformation of Youth Movement for Counter Radicalism', 2022, p. 030010 https://doi.org/10.1063/5.0109808

[10] Abdul Kadir Jaelani and Resti Dian Luthviati, 'The Crime Of Damage After the Constitutional Court's Decision Number 76/PUU-XV/2017', *Journal of Human Rights, Culture and Legal System*, 1.1 (2021) https://doi.org/10.53955/jhcls.v1i1.5

[11] Reza Octavia Kusumaningtyas and James Kalimanzila, 'The Impact of Tax Incentive on Increase Foreign Direct Investment', *Journal of Sustainable Development and Regulatory Issues (JSDERI)*, 1.2 (2023), 51–63 https://doi.org/10.53955/jsderi.v1i2.7

prevention. To maximize the efficacy of efforts to eradicate terrorist-related crimes, it is critical to bolster institutional operations, particularly those that are coordinated with the National Agency Countering Terrorism.[12]

It is noteworthy to mention, according to available data, that the National Counter-Terrorism Agency (BNPT) intends to conduct deradicalization initiatives for 1,192 formerly convicted terrorists in 2022. Remarkably, among the deradicalized population, 1,036 individuals continue to be identified as maintaining radical ideologies. These findings highlight the difficulties and limitations of current deradicalization efforts in altering an individual's extremist ideology. This report emphasizes the significance of ongoing and comprehensive support, including confronting social, economic, and ideological factors contributing to radicalization and providing continuous monitoring, psychological counseling, education, vocational training, and community reintegration.[13]

Although the Indonesian government has initiated a national cyber security strategy and executed both short-term and long-term programs, obstacles and challenges impede its implementation. The state of law enforcement in Indonesia can be characterized by three aspects of the legal system, namely structure, substance, and legal culture, as viewed through the lens of Lawrence M. Friedman. Improving cyber security policies is complicated from a legal structure standpoint by the multifaceted character of cyber threats. Consequently, managing this matter extends beyond the purview of the *TNI* or *Polri*. It encompasses multiple ministries, including the Ministry of Defense and Communication and Information. The lack of resolute measures taken by law enforcement agencies in addressing instances of cyber terrorism that infringe upon human rights may exacerbate the crisis and create avenues for future criminal activities. However, these endeavors have proven to be ineffective in preventing cyberterrorism attacks. For this failure, numerous conflicts of interest and a lack of cooperation serve as scapegoats.[14]

Consequently, Indonesian laws and regulations about cyber terrorism offenses lack clarity and consistency about their legal substance. In particular, as stipulated in Law No. 5 of 2018, amending Law No. 15 of 2003 regarding eradicating criminal

[12] Harryadin Mahardika, Juliana French, and Agung Sembada, 'Keep Calm and Eat Satay: Indonesia's Consumption-Themed Signals of Defiance against Terrorism', *Australasian Marketing Journal*, 26.3 (2018), 231–38 https://doi.org/10.1016/j.ausmj.2018.06.002

[13] Ali Masyhar, Ali Murtadho, and Ahmad Zaharuddin Sani Ahmad Sabri, 'The Driving Factors for Recidivism of Former Terrorism Convicts in Socio-Legal Perspective', *Journal of Indonesian Legal Studies*, 8.1 (2023) https://doi.org/10.15294/jils.v8i1.69445

[14] Christiaan Röell and others, 'Managing Socio-Political Risk at the Subnational Level: Lessons from MNE Subsidiaries in Indonesia', *Journal of World Business*, 57.3 (2022), 101312 https://doi.org/10.1016/j.jwb.2022.101312

acts of terrorism, and Law No. 19 of 2016, amending Law No. 11 of 2008 regarding electronic transactions and information. Despite this, law enforcement officials are still permitted to utilize extant legal provisions, given the protracted procedure that goes into formulating statutory regulations. Favorable legislation in Indonesia remains inadequate in its ability to apprehend cyber terrorists. The intent here is to establish a concrete and precise rule concerning cyber terrorism, as the omission and omission of the term "cyber terrorism" in these two statutes creates legal ambiguity and a lacuna. Priority consideration should be given to including a bill concerning special cyberterrorism regulations.

The scope of the ITE Law is restricted to unlawful content, illegal access, illegal wiretapping, data interference, system interference, device misuse, and computer fraud; it does not address other types of cybercrime.[15] Currently, cyber attacks that potentially disrupt the integrity of Indonesia's security and defense are not regulated under the ITE Law.[16] From the perspective of legal culture, cyberterrorism preys on individuals' anxieties. Internet-based propaganda dissemination can be more effective and rapid. Organized groups utilize wiretapping. And can inflict tremendous damage by amassing information to instill fear in the public via secure and efficient communication channels. Insufficient knowledge regarding human rights not only contributes to cyber terrorism but also to human rights violations. Those who fail to recognize the significance of human rights may engage in criminal activities that inflict injury upon others.[17]

Table 1. Cyber Crime Policy in 6 ASEAN Countries

	Openness of the Platform	**Cybercrime Prevention**	**Privacy**
Indonesia	Judicial System	No specific cybersecurity laws; Information and Electronic Transaction Act (Law of the Republic of Indonesia No. 19 of 2016)	Law (UU) Number 27 of 2022 concerning Protection of Personal Data.
Malaysia	Notice and takedown	Computer Crime Act	Personal Data

[15] J.O. Akanni, 'A Non-Linear Optimal Control Model for Illicit Drug Use and Terrorism Dynamics in Developing Countries with Time-Dependent Control Variables', *Decision Analytics Journal*, 8 (2023), 100281 https://doi.org/10.1016/j.dajour.2023.100281

[16] Muammar Bakry and others, 'Strengthening the Cyber Terrorism Law Enforcement in Indonesia: Assimilation from Islamic Jurisdiction', *International Journal of Criminology and Sociology*, 10 (2021), 1267–76 https://doi.org/10.6000/1929-4409.2021.10.146

[17] Jane A. Bullock, George D. Haddow, and Damon P. Coppola, 'Cybersecurity and Critical Infrastructure Protection', in *Introduction to Homeland Security* (Elsevier, 2021), pp. 425–97 https://doi.org/10.1016/B978-0-12-817137-0.00008-0

		1997	Protection Act 2010 (PDPA)
Philippines	Judicial System	Cybercrime Prevention Act (2012)	Data Privacy Act (2012)
Singapore	Notice and takedown	COMPUTER MISUSE ACT (1993, amended 2017)	The Data Privacy Act of 2012
Thailand	Judicial System	Computer-Related Crime Bill (2007, amended 2017)	Sector-specific approaches such as the National Health Service Act-Personal Information Protection Act (Draft)
Vietnam	Judicial System	Law on Cyber Information Security (Law No. 86/2015/QH13)	Law on Cyber Information Security (Law No.86/2015/qh13).

Source: Processed from various sources based on researcher analysis

It is evident from this table that the functions of the regulations implemented by each country vary according to their level of development. Notice and takedown procedures about platform openness are exclusively implemented in Singapore and Malaysia. In contrast, Thailand, Vietnam, Indonesia, and the Philippines lack regulations permitting rights holders (reporters) to exercise direct legal enforcement by safeguarding their copyrights via the Notice and Takedown mechanism. In this regard, the "Judicial System" refers to the legal recourse copyright holders must utilize to protect their rights. Only Indonesia, among the ASEAN member states that have been identified, needs to possess an undeniable sense of urgency.

Vadim et al. researched terrorism and proposed a counterterrorism model that organically integrates the dynamics of competing interest groups. As a result of research findings, the intended model relaxation incorporates optimal control problems with suitable phase constraints to eradicate several model inconsistencies and develop new numerical algorithms to design counter-terrorism strategies—additionally, M.K.D. Cross conducted research, which revealed that trans governmental networks of knowledge and best practices could fortify the foundation of European intelligence through informal channels. Concurrently, areas of intelligence sharing that are highly classified and whose dynamics could be more manageable to comprehend continue. Consequently, a disparity arises between the dissemination of intelligence among experts and the implemented community governance practices.[18] Furthermore, Sheraz et al.

[18] M.K.D. Cross, 'Counter-Terrorism & the Intelligence Network in Europe', *International Journal of Law, Crime and Justice*, 72 (2023), 100368 https://doi.org/10.1016/j.ijlcj.2019.100368

conducted research indicating that information and communication technology significantly contributes to advancing cross-border tourism and the fight against terrorism.[19]

The legislation and regulations about information technology in Indonesia must comprehensively address all forms of cybercrime. As a result, several cybercrimes threaten national sovereignty and security yet remain unregulated internationally. Indonesia requires specific regulations about cybercrime. This specialized regulation establishes overarching principles that govern all offenses committed in information and communication technology. These principles shall extend to criminal activities that compromise the confidentiality, availability, or integrity of data or electronic systems or computer systems, as well as criminal guidelines and procedural laws governing investigations and investigations in the domain above, including the seizure and search of digital evidence. This is owing to the susceptibility of Indonesia to cyber-attacks and legal vulnerabilities about their mitigation. As a result, it is imperative to research the government's function in combating cyberterrorism.

2. Research Method

The normative legal methodology utilized in this study results from an exhaustive literature evaluation. Legislation, books, and periodicals are a few of the primary and secondary legal sources consulted for this article. Legislative methodology was utilized in this research study to identify a legal foundation and assess regulations about cyber terrorism policies in Indonesia and other nations. To establish cyberspace defense and security, concepts associated with cybersecurity are uncovered using a conceptual approach.[20] In the interim, a comparative methodology is employed to assess the differences in cyber security policies between Indonesia and other nations.

3. Results and Discussion

Governance in Countering Cyber Terrorism

The Internet has emerged as an indispensable tool for worldwide communication. It has become an ever-more-integrated component of individuals' daily existence for over two decades. Innovations and cost reductions in this domain have substantially enhanced the accessibility, functionality, and usability of the Internet; consequently, it now boasts an estimated global user base of three

[19] Choudhary and others.

[20] Al Fadilla Yoga Brata and Rakotoarisoa Maminiaina Heritiana Sedera, 'The Implementing a Carbon Tax as a Means of Increasing Investment Value in Indonesia', *Journal of Sustainable Development and Regulatory Issues (JSDERI)*, 1.2 (2023), 39–50 https://doi.org/10.53955/jsderi.v1i2.6

billion.[21] Cyberspace is the primary platform for nations to conduct their economic, commercial, cultural, social, and governmental interactions and activities. These interactions involve entities at all levels, including individuals, non-governmental organizations, and government and governmental institutions.[22]

The administration of counterterrorism can be conceptualized as consisting of two interconnected dynamics. Responses continue to be dominated by "top-down" state-led strategies that include arrest and detention, stop-and-search, surveillance, and other police and security methods. This is in addition to the resilience of infrastructure and technology.[23] Community participation in the eradication of terrorism is frequently contingent on a variety of government-related issues. For instance, trust is necessary for public members to provide information to law enforcement, security, or other legal institutions. This is due to the perception among the general public that giving information to authorities results in a loss of control over the data and its subsequent utilization.[24]

Community involvement is a crucial method for establishing and preserving trust. Nevertheless, the following factors may impede the establishment of trust: In the absence of information-sharing protocols, when community members perceive community involvement solely as a means to disseminate information rather than as a means to empower and support the community; when policies and practices that stigmatize and potentially harm members of society place a strain on established trust; and when police and other professional units/divisions experience high staff turnover.[25] Concurrently, the difficulty of eradicating terrorism effectively necessitates increased community governance, including the involvement of non-governmental organizations and civil society groups. Nevertheless, within the strictly controlled domain of the government, community involvement is severely restricted, which undermines the effectiveness of policies designed to avert radicalization and terrorism recruitment.[26]

---

[21] Sen Tan and others, 'Attack Detection Design for Dc Microgrid Using Eigenvalue Assignment Approach', *Energy Reports*, 7 (2021), 469–76 https://doi.org/10.1016/j.egyr.2021.01.045
[22] Gholamreza Aghajani and Noradin Ghadimi, 'Multi-Objective Energy Management in a Micro-Grid', *Energy Reports*, 4 (2018), 218–25 https://doi.org/10.1016/j.egyr.2017.10.002
[23] Basia Spalek and Salwa El-Awa, 'Governance and Counter-Terrorism: Engaging Moderate and Non-Violent Extremist Movements in Combatting Jihadist-Linked Terrorism', *International Journal of Law, Crime and Justice*, 72 (2023), 100367 https://doi.org/10.1016/j.ijlcj.2019.100367
[24] Azhmyakov and others.
[25] Tali Seger Guttmann, Shaked Gilboa, and Judith Partouche-Sebban, '"I Live with Terror inside Me": Exploring Customers' Instinctive Reactions to Terror', *International Journal of Hospitality Management*, 92 (2021), 102734 https://doi.org/10.1016/j.ijhm.2020.102734
[26] Cross.

Global governance, also known as world governance, comprises many formal and informal institutions and individuals worldwide, including public and private entities, collaborating to address a complex issue that may involve competing or even antagonistic interests. Global governance is comprised of a wide variety of components. These components include international organizations, both state-owned and non-state, international organizations with a regional or global focus, as well as several non-governmental organizations (NGOs), international law (including multilateral agreements, customary law, judicial decisions, and international standards), United Nations resolutions, declarations, government and private governance, and several other components. Regional and international endeavors to establish comprehensive cyber security have been undertaken thus far; however, their progress appears stagnant. Indonesia is actively engaged in combating terrorism via AMMTC; however, no dedicated endeavors have been initiated to address cyberterrorism. As AMMTC is only concerned with conventionally resolving terrorism cases, progress toward overcoming this obstacle appears to be sluggish, particularly in light of the technological advancements made by terrorist organizations.

Commercial enterprises frequently establish specialized cyber-security departments in response to the ever-changing and ubiquitous risks posed by data breaches and other dangerous security incidents.[27] The recognition that cybersecurity practice encompasses more than mere technological implementation is growing. Applying sociological and political perspectives to such practices is increasingly prevalent, especially in organizations.[28] Cyber norms offer states direction regarding implementing, interpreting, and using their legal responsibilities in the digital realm. Furthermore, they reflect potential, present, and widely accepted interpretations of international law, so they are not legally insignificant.[29] Additionally, international organizations have made contributions towards the safeguarding of critical infrastructures. While most of these measures lack global legal force, they still serve as significant components of state policy and potentially reflect a consensus among nations. Following this, the 2015 OAS Declaration for the Protection of Critical Infrastructure from Emerging Threats provides an expanded definition of critical infrastructures in the context of terrorism. The Declaration explicitly increases the potentially severe consequences

[27] Joseph Da Silva, 'Cyber Security and the Leviathan', *Computers & Security*, 116 (2022), 102674 https://doi.org/10.1016/j.cose.2022.102674

[28] Mark Burdon and Lizzie Coles-Kemp, 'The Significance of Securing as a Critical Component of Information Security: An Australian Narrative', *Computers & Security*, 87 (2019), 101601 https://doi.org/10.1016/j.cose.2019.101601

[29] Triantafyllos Kouloufakos, 'Untangling the Cyber Norm to Protect Critical Infrastructures', *Computer Law & Security Review*, 49 (2023), 105809 https://doi.org/10.1016/j.clsr.2023.105809

that may arise from the disruption of those infrastructures. These consequences extend beyond the efficient operation of the Member States and include the flow of essential services and the functioning of supply chains. While ratifying the African Union Convention on Cyber Security and Personal Data Protection, the African Union focused on defining critical cyber/ICT infrastructure. This infrastructure is indispensable for safeguarding national and public safety, economic stability, national and international stability, and critical cyberspace's long-term viability and restoration. One potential approach is to examine the Global Commission on the Stability of Cyberspace (GCSC) endeavors, an initiative involving multiple stakeholders that fosters comprehension and mutual consciousness among the diverse cyberspace communities engaged in matters about global cybersecurity. The Paris Call for Trust, issued by French President Emmanuel Macron in 2018 at the UNESCO Internet Governance Forum, will also be examined. This call urges nations to unite in opposition to the emerging risks that imperil infrastructure and citizens.[30]

These cyberattacks, known as "cyber warfare," can wreak havoc on government and civilian infrastructure and disrupt a country's essential systems.[31] An examination of cyber security in Indonesia reveals that the country has been the target of numerous cyber attacks and cyber conflicts fought against other entities. In 1998, cyberspace witnessed ethnic unrest, specifically in Indonesia, which was embroiled in a battle with hackers suspected of originating from China and Taiwan. Then, according to research conducted in August 2010 by Symantec, the developer of Norton Antivirus, Indonesia ranked second among the ten countries affected by the Stuxnet malware, behind Iran. Furthermore, the Sydney Morning Herald reported on October 31, 2013, that Australia had conducted wiretapping of the Indonesian government via its diplomatic representative facility located in Jakarta. Simultaneously, the magnitude of cyber assaults is escalating on a global scale, as evidenced by a sequence of cyber assaults documented by The Telegraph UK: in May 2017, the WanaCrypt0r 2.0 cyber attack, more commonly known as the WannaCry virus, proliferated at an unprecedented rate across the globe. The virus initially increased in Ukraine before rapidly spreading to ten additional countries, including Indonesia, in less than two hours.[32]

---

[30] Petros Chatzis and Eliana Stavrou, 'Cyber-Threat Landscape of Border Control Infrastructures', *International Journal of Critical Infrastructure Protection*, 36 (2022), 100503 https://doi.org/10.1016/j.ijcip.2021.100503

[31] Shu Tian, Bo Zhao, and Resi Ong Olivares, 'Cybersecurity Risks and Central Banks' Sentiment on Central Bank Digital Currency: Evidence from Global Cyberattacks', *Finance Research Letters*, 53 (2023), 103609 https://doi.org/10.1016/j.frl.2022.103609

[32] Gabriele Lattanzio and Yue Ma, 'Cybersecurity Risk and Corporate Innovation', *Journal of Corporate Finance*, 82 (2023), 102445 https://doi.org/10.1016/j.jcorpfin.2023.102445

The attributes of cyberspace, its low barrier to entry, anonymity, unpredictability regarding the threatening geographical region, profound consequences, and absence of public disclosure, have attracted formidable and feeble entities, such as governments, organized and terrorist organizations, and individuals. Threats to cyberspace include cyber warfare, cybercrime, cyber terrorism, and cyber espionage.[33] The absence of a precise and all-encompassing definition not only obfuscates established legal pathways but also generates many interpretations and applications, ultimately leading to occasionally contradictory legal conclusions.[34]

Cyberattacks are deliberate activities executed by nations to infiltrate the computer systems or networks of another country to cause harm or disturbance.[35] Foreign intelligence agencies employ cyber tools to carry out a variety of espionage and intelligence collection operations. As a result of the misuse and devastation of a nation's information infrastructure consisting of computer systems, Internet information networks, and processors and controllers embedded in critical industries, numerous analogous incidents have been documented globally. An additional source of cyber attacks is profit-driven organizations that target cyber systems; the number of attacks from these groups is growing. Additionally, other organizations (hackers) occasionally gain access to the network for self-expression. Presently, it is feasible to compromise the network with minimal expertise and knowledge by downloading the required programs and protocols from the Internet and utilizing them to launch attacks against other websites. Meanwhile, another group (Hacktivism) attacks a website or host of popular emails with political motivations. Typically, these organizations cause an increase in the volume of email traffic for the hosts, and they spread political messages through website infiltration.[36]

The International Telecommunication Union (ITU) ranks the 193 member countries of the Global Cybersecurity Index (GCI) to increase international commitment to cyber security. The five pillars of the GCI framework, legal,

[33] K.S. Niraja and Sabbineni Srinivasa Rao, 'WITHDRAWN: A Hybrid Algorithm Design for near Real Time Detection Cyber Attacks from Compromised Devices to Enhance IoT Security', *Materials Today: Proceedings*, 2021 https://doi.org/10.1016/j.matpr.2021.01.751

[34] Bilal Alhayani and others, 'WITHDRAWN: Best Ways Computation Intelligent of Face Cyber Attacks', *Materials Today: Proceedings*, 2021 https://doi.org/10.1016/j.matpr.2021.02.557

[35] William Motsch and others, 'Approach for Dynamic Price-Based Demand Side Management in Cyber-Physical Production Systems', *Procedia Manufacturing*, 51 (2020), 1748–54 https://doi.org/10.1016/j.promfg.2020.10.243

[36] Matthew Beechey, Konstantinos G. Kyriakopoulos, and Sangarapillai Lambotharan, 'Evidential Classification and Feature Selection for Cyber-Threat Hunting', *Knowledge-Based Systems*, 226 (2021), 107120 https://doi.org/10.1016/j.knosys.2021.107120

technical and procedure, organizational, capacity development, and international cooperation, form the basis of this evaluation. Merely emphasizing technological components to surmount challenges related to cyber information security needs to be improved. Effective cybersecurity requires an ecosystem where regulations, institutions, expertise, collaboration, and technical execution operate unison. In addition to being the government's obligation, this also demands the participation of the private sector and consumers.[37] As a result, cultivating a culture of cybersecurity is of the utmost importance so that members of the public can recognize and assess the potential dangers associated with utilizing electronic networks.[38]

Government agencies and public officials in Indonesia have already implemented systems and strategies for cyber security and resilience governance.[39] The coordination of cyber security and resilience policies has been undertaken by the *Kominfo*, which is the Ministry of Communication and Information. The Indonesian cyber security and resilience system and strategy involve the participation of three government organizations: the Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII), the Information Security Coordination Team, and the Information Security Directorate. International cooperation has been executed thus far on a sectoral level by organizations, communities, and entities by their respective functions. Collaboration with ASEAN to address cyber security and resilience is one of Indonesia's alliance strategies in cyber security and resilience policy at the international level. Then, on July 3, 2018, a cyber agreement was signed between the Ministry of Foreign Affairs of the Kingdom of the Netherlands and Indonesia's National Cyber and Crypto Agency (BSSN).

In August 2018, Indonesia signed cyber cooperation agreements with Australia and the United Kingdom.[40] The contents of the bilateral partnership with Australia are cyber economy and cybersecurity. In the interim, collaboration with the Netherlands encompasses the exchange of insights regarding management policy

[37] Claire Seungeun Lee and Ji Hye Kim, 'Latent Groups of Cybersecurity Preparedness in Europe: Sociodemographic Factors and Country-Level Contexts', *Computers & Security*, 97 (2020), 101995 https://doi.org/10.1016/j.cose.2020.101995

[38] Mayra Macas, Chunming Wu, and Walter Fuertes, 'Adversarial Examples: A Survey of Attacks and Defenses in Deep Learning-Enabled Cybersecurity Systems', *Expert Systems with Applications*, 238 (2024), 122223 https://doi.org/10.1016/j.eswa.2023.122223

[39] Barr-Kumarakulasinghe Cheryl, Boon-Kwee Ng, and Chan-Yuan Wong, 'Governing the Progress of Internet-of-Things: Ambivalence in the Quest of Technology Exploitation and User Rights Protection', *Technology in Society*, 64 (2021), 101463 https://doi.org/10.1016/j.techsoc.2020.101463

[40] Victor Bolbot and others, 'Developments and Research Directions in Maritime Cybersecurity: A Systematic Literature Review and Bibliometric Analysis', *International Journal of Critical Infrastructure Protection*, 39 (2022), 100571 https://doi.org/10.1016/j.ijcip.2022.100571

strategies, legislation, cyber law, and legislation; bolstering institutional capabilities and aid; and advancing technological advancements in the realm of cyber security via educational and networking initiatives; conferences and seminars; and the participation of high-ranking officials, analysts, and field implementers in exchange for knowledge.[41] The Indonesian government engaged in a collaborative effort with the United States government on September 28, 2018, alongside bilateral partnerships with multiple nations, to promote cyberspace capacity building and cooperation and advance national strategy development, incident management capabilities, cybercrime prevention capabilities, and collaboration, partnerships with various stakeholders, and capacity and cooperation in the realm of cyberspace. Indonesian cyber diplomacy is implemented within the framework of multilateral cooperation through the ASEAN Political-Security Community (APSC) in Subchapter B.4.1 of the ASEAN Regional Forum (ARF). To safeguard Indonesia's cyber security and sovereignty, these diplomatic endeavors incorporated the involvement of BSSN, a national cyber institution.[42]

ASEAN nations' progress appears to be sluggish for several reasons. To begin with, they continue to employ traditional approaches in their battle against cyber terrorism, which in this case involves the dissemination of black propaganda via social media platforms. Second, no special efforts have been made to address the challenges posed by the dissemination of black propaganda on social media as part of cyberterrorism. Thirdly, the involvement of an excessive number of institutions hinders the effectiveness of resolving cyberterrorism as a transnational crime due to the absence of structured subordination among the pertinent institutions. Awareness, support from upper management, and adherence to policies and procedures are all crucial components in fostering a cyber security culture.

Collaborative Governance, which seeks to implement public policy, is a regulatory framework that oversees one or more public institutions through the active participation of non-public stakeholders in a formal, consensus-driven, and deliberative collective decision-making process—Administering public assets and programs. Stakeholders can identify prospects for reciprocal advantage, foster greater comprehension and confidence among themselves, amass knowledge and

[41] Gunawan A. Tauda, Andy Omara, and Gioia Arnone, 'Cryptocurrency: Highlighting the Approach, Regulations, and Protection in Indonesia and European Union', *BESTUUR*, 11.1 (August) (2023), 1 https://doi.org/10.20961/bestuur.v11i1.67125

[42] Moon QMN-Nguyen, 'Media Presentations of Vietnam's Cybersecurity Law: A Comparative Approach with Corpus-Based Critical Discourse Analysis', *Computer Law & Security Review*, 50 (2023), 105835 https://doi.org/10.1016/j.clsr.2023.105835

data, improve coordination efficiency and effectiveness, and bolster decisions' credibility. Collaborative governance arose as a response to cross-sectoral policy challenges that necessitated administrative modifications for resolution.[43]

Organizational and governmental governance significantly influenced the development of an appropriate cyber security culture model, as evidenced by the commonalities among several frameworks examined.[44] Every national and private institution and agency in Indonesia has implemented cyber defense to safeguard the network systems supporting their critical infrastructure. In contrast, legislation must still be enacted to mandate national protection within the national cyber policy framework. Although the ITE Law has prompted Indonesia to establish policies and regulations about information security, constructing a national defense through cyber security can only be accomplished partially based on this legislation. Limiting cyberattacks against companies and governments requires effective exchange of information and coordination during incident resolution. Because known methods for preventing cyber attacks are insufficient, information sharing and analysis centers (ISACs) and cyber security incident response teams (CSIRTs) develop innovative techniques for reporting and coordinating an incident. The government must prepare dynamic ways to fight cyber threats because technology proliferates.[45]

Role of Government Agencies and Cybersecurity Legislation Policies

Due to the far-reaching consequences of a cyber attack, which extend beyond economic losses to the infringement of individual rights and the compromise of a nation's sovereignty, Indonesia must prioritize defense development and cybersecurity to preserve its national security.[46] The large number of cases of cyber threats in Indonesia shows that the technological capacity and expertise in the cyber field possessed by the Indonesian government are still lacking compared to the power owned by the perpetrators of these cyber threats. Technological developments that are becoming increasingly sophisticated also cause the dangers that exist in cyberspace to become more sophisticated. This shows that BSSN, as a national cyber security institution, must always increase cyber security capacity in

[43] Diaz Valdivia.
[44] Betsy Uchendu and others, 'Developing a Cyber Security Culture: Current Practices and Future Needs', *Computers & Security*, 109 (2021), 102387 https://doi.org/10.1016/j.cose.2021.102387
[45] Daniel A. Sepúlveda Estay and others, 'A Systematic Review of Cyber-Resilience Assessment Frameworks', *Computers & Security*, 97 (2020), 101996 https://doi.org/10.1016/j.cose.2020.101996
[46] Ogobuchi Daniel Okey and others, 'Investigating ChatGPT and Cybersecurity: A Perspective on Topic Modeling and Sentiment Analysis', *Computers & Security*, 135 (2023), 103476 https://doi.org/10.1016/j.cose.2023.103476

Indonesia and increase the expertise of various parties within it. These efforts are essential to reduce the level of threats that exist in Indonesian cyberspace.[47]

Indonesia Security Incident Response Team on Internet Infrastructure (IDSIRTII), Indonesia Computer Emergency Response Team (IDCERT), and Cyber Crime Sub-Directorate Directorate of Economic Crimes and Special *Bareskrim Polri* oversee cyber security during the course of the country's affairs, in addition to the ITE Law. Despite having ITE Law-mandated policies on cyber security, Indonesia is confronted with the issue of authority division concerning which governing bodies are obligated to combat cyber warfare, cyber crime, cyber terrorism, and cyber hacktivism. Therefore, establishing BSSN as a novel institution is crucial for coordinating activities among multiple institutions, particularly those involved in the cyber incident.[48]

Indonesia subsequently established the National Cyber and Crypto Agency (BSSN) as a model national cyber security institution in response to cyberterrorism incidents of various natures. Furthermore, it is worth noting that Indonesia, classified as a developing nation with the most populous population globally, has emerged as one of the leading users of the largest internet platform worldwide. The challenges associated with managing cyber-security within the sectoral national defense framework, which lacks coordination and integration, ultimately led to the government's establishment of the National Cyber and Crypto Agency (BSSN) on May 19, 2017. This was accomplished via Presidential Regulation (Perpres) Number 53 of 2017, which pertains to the BSSN. Under this BSSN, several additional institutions with interests in national security defense, including the cyber domain, collaborate. Government institutions such as the Ministry of Defense, *TNI, Polri, BIN, Kemenkominfo*, National Crypto Agency, and others are interdependent. They must collaborate to prevent, fend off, and prevent cyber attacks by domestic or foreign state and non-state actors.[49]

Cyber soldiers have evolved into an absolute necessity in the military realm. This is evident from the cyber armies of other nations that have already established such institutions: Bureau 121 of North Korea; Unit 61398 of the

[47] Meity Ardiana and others, 'Corporate Criminal Liability in Procurement of Goods and Services in Hospital', *Yuridika*, 38.2 (2023), 399–414 https://doi.org/10.20473/ydk.v38i2.43674
[48] Ghassan Adhab Atiyah, Nazura Abdul Manap, and Saidatul Nadia Abd Aziz, 'Legal Status of Cryptocurrency Circulation in Iraq: Lessons from the United Arab Emirates and the United States', *Hasanuddin Law Review*, 9.1 (2023), 1 https://doi.org/10.20956/halrev.v9i1.3867
[49] Yudhistira Nugraha and Andrew Martin, 'Towards a Framework for Trustworthy Data Security Level Agreement in Cloud Procurement', *Computers & Security*, 106 (2021), 102266 https://doi.org/10.1016/j.cose.2021.102266

People's Liberation Army (PLA) of China;[50] the Defense Cyber Organization (DCO) of Singapore, which comprises 2,600 special forces; and the Cyber Warfare Unit of Australia. TNI cyber security must ensure the achievement of TNI cyber resilience to facilitate the execution of the organization's primary responsibilities. Indonesian cyber diplomacy is implemented within the framework of multilateral cooperation through the ASEAN Political-Security Community (APSC) in Subchapter B.4.1 of the ASEAN Regional Forum (ARF).

This chapter comprises an accord to enhance collaboration on non-traditional hazards, focusing on transnational and cross-border criminal activities. In addition to the undertakings above, Indonesia, Brunei Darussalam, Myanmar, Cambodia, Laos, the Philippines, Singapore, Malaysia, Vietnam, and Thailand all participate in the ASEAN Cyber Capacity Program (ACCP), which commenced in April 2017. Given that Southeast Asia is one of the regions undergoing substantial digital economic growth, which has rendered it susceptible to cyber attacks, this regime was established based on the ASEAN countries' collective awareness of the various cyber threats they face.[51] Concurrently, ten ASEAN nations and Japan participated in the ASEANJAPAN Cyber Exercise, which Indonesia facilitated via BSSN. This endeavor illustrates the cooperation between Japan and ASEAN member states in addressing various challenges within the cyber domain, including incident management, information sharing, capacity development, and information security awareness among all ASEAN members and Japan.[52]

As a national institution for cyber security, BSSN has yet to achieve a comprehensive enhancement in cyber security as measured by the six technical indicators. Indonesia's capacity for development is limited to sectoral, government, and national CERT indicators. CERT is an organization tasked with coordinating technical aspects of cyber incidents. RFC 2350 facilitated the transformation of CERT into a Computer Security Incident Response Team (CSIRT). The establishment of CERT/CSIRT aimed to serve as a centralized hub for reporting cyber incidents, resolving cyber security concerns, mitigating the recurrence of cyber security incidents, and disseminating diverse information (lessons learned) about cyber matters. BSSN established Gov-CSIRT (Government Computer Security Incident Response Team) by Decree No. 199 of 2019 of the

[50] Barbara Kelemen and Alessandro Fergnani, 'The Futures of Terrorism against China in the Greater Middle East', *Futures*, 124 (2020), 102643 https://doi.org/10.1016/j.futures.2020.102643
[51] Hui Ge and others, 'A Game Theory Based Optimal Allocation Strategy for Defense Resources of Smart Grid under Cyber-Attack', *Information Sciences*, 652 (2024), 119759 https://doi.org/10.1016/j.ins.2023.119759
[52] Changyin Dong and others, 'Evaluating Impact of Remote-Access Cyber-Attack on Lane Changes for Connected Automated Vehicles', *Digital Communications and Networks*, 2023 https://doi.org/10.1016/j.dcan.2023.06.004

Head of the National Cyber and Crypto Agency. The primary objective of Gov-CSIRT is to facilitate the coordination and enhancement of cyber security services within the government sector and strengthen the cyber security capabilities of government resources.[53]

The vast majority of nations have enacted legislation to combat cybercrimes. The regulatory framework governing cyber crimes in India is outlined in Act No. 21 of 2000, which pertains to the Information Technology Act (IT ACT) of 2000. Subsequently, by way of Act No. 10 of 2009, the Information Technology Act of 2008 was amended to include this provision. Criminal jurisdiction is exercised by the requirements outlined in Article 1, paragraph (2), which are grounded in extraterritorial and territorial principles. Singapore subsequently implemented the Computer Misuse Act, which was a 2005 amendment to Act No. 42. By the provisions of Article 11 of the Computer Misuse Act, the application of criminal law in Singapore is governed by the following jurisdictional principles: territorial principles, active national principles, passive national principles, and protection principles.[54] The same applies to Australia. Cybercrimes are governed by Act No. 161 of 2001, which is referred to as the Cybercrime Act of 2001. The intricacies of establishing jurisdiction for cyber offenses are elaborated upon in Article 476.3 (geographical jurisdiction), derived from Section 15.1 of the 1995 Criminal Code's Extended Geographical Jurisdiction - Category A. The process of ascertaining jurisdiction over cyber crimes is elaborated upon in Article 476.3, which pertains to geographical jurisdiction. It specifies that "Criminal acts regulated in Act No. 161 of 2001 are subject to Extended Geographical Jurisdiction – Category A." The jurisdiction over cyber offenses is regulated by the jurisdiction provisions outlined in the Criminal Code of 1995, as stipulated in Article 476.3 of the Cybercrime Act 2001.[55]

Then, in February, the critical cybersecurity infrastructure was established, emphasizing the creation of a framework to mitigate cyber threats. Self-regulation is an elective responsibility regarding government intervention in cybersecurity policy and public-private partnership (PPP) in the United States. It still needs to be stated entirely because specific provisions of cybersecurity legislation overlap with those of other laws. The government of the United States is endeavoring to

[53] Andres Diaz Valdivia, 'Between Decentralization and Reintermediation: Blockchain Platforms and the Governance of "Commons-Led" and "Business-Led" Energy Transitions', *Energy Research & Social Science*, 98 (2023), 103034 https://doi.org/10.1016/j.erss.2023.103034

[54] Jean-Paul Yaacoub and others, 'Security Analysis of Drones Systems: Attacks, Limitations, and Recommendations', *Internet of Things*, 11 (2020), 100218 https://doi.org/10.1016/j.iot.2020.100218

[55] Adam Radomyski and Paweł Bernat, 'Contemporary Determinants of Organising Effective Protection of Civil Aviation Against Terrorism', *Transportation Research Procedia*, 35 (2018), 259–70 https://doi.org/10.1016/j.trpro.2018.12.021

transition from optional to mandatory regulations. Subsequently, cybersecurity innovation-wise, Europe is significantly ahead of the rest of the globe—the EU's organizational structure endeavors to position itself strategically in an interconnected global arena through cooperative action. Recognizing the peril of cybercrime, the EU issued a cybersecurity policy and a proposal for a network and information security (NIS) Directive in 2013.

The European Cyber Crime Center (EC3) contributes to safeguarding European enterprises and citizens through its work on criminal investigations and disseminating information regarding emerging cyber-attack trends. Information security was identified as a critical concern in EU legislation, emphasizing the potential dangers associated with the widespread use of ICT. Information security may be implemented to protect against and prevent hazards and facilitate user compliance with specific legal requirements.[56] At the same time, the Australian government unveiled its cybersecurity strategy in 2009. Furthermore, the Australian federal government has proposed and developed several regulations on the identification, investigation, law, and punishment of illicit and criminal activities in the digital realm. Moreover, Australia's public institutions, governmental bodies, and non-governmental organizations have significantly contributed to mitigating cybercrime and safeguarding cybersecurity. Furthermore, the government of India unveiled the NCSP in July 2013, delineating fourteen objectives, such as enhancing the security of critical infrastructure and educating 500,000 proficient cybersecurity professionals within five years. The NCSP is integral to the country's PPP initiatives to improve the cybersecurity environment.[57]

Numerous collaborations within ASEAN encompass terrorism as a component of their respective domains of operation. Illustrative instances include the ASEAN Convention on Counter-Terrorism (ACCT), the ASEAN Ministerial Meeting on Transnational Crime (AMMTC), the ASEAN-Russia Senior Officials Meeting (ARSOM), and the ASEAN Regional Forum (ARF).[58] The ASEAN Ministerial Meeting on Transnational Crime (AMMTC), which commenced in 1997 and has since been rescheduled every two years, is a ministerial-level forum dedicated to

[56] Ema Mar'ati Sholecha and others, 'Justice Collaborator's Position and Function on Witness Protection's Rights as a Suspect from the Perspective of Criminal Law in Indonesia', *Volksgeist: Jurnal Ilmu Hukum Dan Konstitusi*, 2023, 131–43 https://doi.org/10.24090/volksgeist.v6i1.7246

[57] Alok Mishra and others, 'Attributes Impacting Cybersecurity Policy Development: An Evidence from Seven Nations', *Computers & Security*, 120 (2022), 102820 https://doi.org/10.1016/j.cose.2022.102820

[58] Jamin Ginting and Patrick Talbot, 'Fundraising Aspect of International Terrorism Organization in ASEAN: Legal and Political Aspects', *Lex Scientia Law Review*, 7.1 (2023), 1–30 https://doi.org/10.15294/lesrev.v7i1.60074

examining transnational crime in ASEAN. Periodically distributed every three months, the SOMTC Work Program to Implement the ASEAN Plan of Action to Combat Transnational Crime outlines the strategy for addressing these concerns.[59] In addition, ASEAN is actively engaged in collaborative endeavors with its Dialogue Partners to eradicate transnational crime. This cooperation constitutes a multitude of joint declarations, memorandums of understanding (MoU), plans of action (PoA), and work plans encompassing diverse collaborative projects and initiatives. ASEAN maintains an AMMTC + Dialogue Partner Consultation dialogue mechanism with the Plus Three (People's Republic of China, Japan, and the Republic of Korea (ROK)), respectively, and China. In the context of the SOMTC, ASEAN collaborates with China, Japan, the Republic of Korea, Plus Three, the United States, the European Union, India, Australia, Russia, New Zealand, and Canada through the SOMTC plus Dialogue Partner Consultation dialogue mechanism.[60]

The Indonesian government's establishment of the National Cyber and Crypto Agency (BSSN) on May 19, 2017, as a national cyber security institution serves as an initial indication of a responsible organization. Regarding implementing cyber security in Indonesia, BSSN, as the national CERT/CSIRT, continues to pursue integration, coordination, and harmonization with diverse stakeholders, including the private sector, information infrastructure, and other government agencies. About the second indicator, specifically the presence of a national cyber security strategy, Indonesia currently needs more cybersecurity-related regulations or policies. This indicates that the national cyber security strategy development stage entails further comprehension and standardization.[61]

Public-Private Partnership in Countering Cyber Terrorism to Protection Human Rights

Information operations involving the military, government, state-owned enterprises, corporations, academics, the private sector, individuals, and the international community are intricately linked to national cyber security and resilience. To enhance the technological infrastructure of ASEAN member states, collaboration between countries and the private sector, including SafeNet Inc., Google, and Facebook, is necessary in addition to cooperation between ASEAN

[59] Ridwan Arifin, Sigit Riyanto, and Akbar Kurnia Putra, 'Collaborative Efforts in ASEAN for Global Asset Recovery Frameworks to Combat Corruption in the Digital Era', *Legality : Jurnal Ilmiah Hukum*, 31.2 (2023), 329–43 https://doi.org/10.22219/ljih.v31i2.29381

[60] Thomas Barry, Jonathan Jona, and Naomi Soderstrom, 'The Impact of Country Institutional Factors on Firm Disclosure: Cybersecurity Disclosures in Chinese Cross-Listed Firms', *Journal of Accounting and Public Policy*, 41.6 (2022), 106998 https://doi.org/10.1016/j.jaccpubpol.2022.106998

[61] Dodi Jaya Wardana, Sukardi Sukardi, and Radian Salman, 'Public Participation in the Law-Making Process in Indonesia', *Jurnal Media Hukum*, 30.1 (2023), 66–77 https://doi.org/10.18196/jmh.v30i1.14813

member states. SafeNet Inc., a manufacturer of technology security products, provides information and public security infrastructure and other data protection solutions. Concurrently, social media platforms developed by Google and Facebook, which provide information and communication services, are gaining widespread adoption.[62]

Capacity building in cybersecurity is "assistance and support intended to reduce the risks associated with the use and access of information and communications technologies."[63] From a typological standpoint, optimal cyber security resembles the intersection of every circle. Thus, preserving cyber security necessitates collaboration among all parties involved and every approach; this demonstrates that these diverse strategies are not discretionary but rather critical for preventing and regulating cybercrime. As the policy formulator for national cyber strategy, the government increases the education sector's cyberspace capacity and enacts appropriate laws and policies about cybercrime and cyber security. Following this, the private sector would assist the government and the private sector in collaborating to conduct independent regulation. Conversely, international cooperation and conventions are necessary to support or assist in enhancing cyber security, as the global community views.[64] Coordination and Collaboration of Ministries/Agencies in establishing CSIRT as a solution to the problem of managing cyber threats. Therefore, to address challenges associated with cyber terrorism, Ministries/Institutions and the Private sector must collaborate or engage stakeholder elements by establishing a CSIRT-affiliated organization. This necessitates an adaptive and prompt response, which entails identifying community issues (wicked problems) through stakeholder cooperation so that immediate intervention can occur in managing cyber threats.

A regulation on cybersecurity should govern cross-sectoral coordination and the protection of critical infrastructure against cyber assaults; these aspects must be incorporated into cybersecurity law. Indonesia ought to possess an autonomous organizational framework that can foster collaboration across sectors in addressing cyber incidents, encompassing the public, private, and governmental

[62] Marco Cappai, 'The Role of Private and Public Regulation in the Case Study of Crypto-Assets: The Italian Move towards Participatory Regulation', *Computer Law & Security Review*, 49 (2023), 105831 https://doi.org/10.1016/j.clsr.2023.105831

[63] Zine Homburger, 'The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace', *Global Society*, 33.2 (2019), 224–42 https://doi.org/10.1080/13600826.2019.1569502

[64] Lennon Y.C. Chang and Nicholas Coppel, 'Building Cyber Security Awareness in a Developing Country: Lessons from Myanmar', *Computers & Security*, 97 (2020), 101959 https://doi.org/10.1016/j.cose.2020.101959

domains.[65] Cybercrime should be governed by regulations that regulate specifically the issue of cybercriminal activity and its various forms, in addition to collaborating with law enforcement agencies in other nations on a national and international level. In the new average era, the threat of cyber attacks is becoming more pervasive and complex across multiple sectors.[66] As a result, BSSN and cyber handling elements in various organizations—including Cyber Crime, Police, Ministry of Communication and Information, State Intelligence Agency (BIN), and security elements—need to coordinate and synergize optimally—Cyber in a wide range of industrial sectors. The persistent sectoral ego in Indonesia has resulted in a stagnant approach to cyber management, leading to ongoing incidents of online fraud and personal data compromises in the new average era. Indonesia may draw inspiration from Malaysia's National Cyber Command and Coordination Center (NC4), an institution of specialized divisions that manages Critical National Information Infrastructure (CNII). CNII is responsible for disseminating information, reporting, and safeguarding their critical ICT systems. Government services, energy, water, agriculture, transportation, security and defense, emergency services, information and communications, health services, and transportation are some of the public and private sector sectors that comprise the CNII. Indonesia has the potential to establish an ecosystem for cross-sector collaboration by adopting the approach taken by the United Kingdom and other European nations: utilizing independent non-profit organizations known as ISACs.

Despite most CIs being privately owned, the government is legally obligated to protect citizens and critical infrastructure from disruptive events. The concepts of public-private partnership and government and private critical infrastructure have been the subject of research in various fields. Still, the objectives of PPP in CIR have yet to receive much attention. The concept of public-private partnership and government and private critical infrastructure developed a maturity model to guide local government in including city stakeholders in the city's resilience-building process. They highlighted risk and benefits, mutual coordination, and organizational arrangement as the characteristics that can improve collaboration between government and private CI operators[67]. This Concept is intended to

[65] Indriati Amarini and others, 'Digital Transformation: Creating an Effective and Efficient Court in Indonesia', *Legality : Jurnal Ilmiah Hukum*, 31.2 (2023), 266–84 https://doi.org/10.22219/ljih.v31i2.28013

[66] Patrick Stacey and others, 'Emotional Reactions and Coping Responses of Employees to a Cyber-Attack: A Case Study', *International Journal of Information Management*, 58 (2021), 102298 https://doi.org/10.1016/j.ijinfomgt.2020.102298

[67] Godslove Ampratwum, Robert Osei-Kyei, and Vivian W.Y. Tam, 'Exploring the Concept of Public-Private Partnership in Building Critical Infrastructure Resilience against Unexpected

combat cyber terrorism with cyber threats. The elimination of the geographical dimension of cyber threats. Historically, military threats were region-specific. Consequently, it was manageable, at least from an identification standpoint. Nonetheless, the current scope of cyber threats and vulnerabilities cannot be contained by traditional means alone, such as the use of military and police force, and governments alone are insufficient to combat them; practical and bilateral cooperation between governments and the private sector, which has common interests in addressing them, is necessary[68].

Looking at the partnership of cyberterrorism, we must know how Public-private partnerships (PPPs) in the United States are voluntary self-regulatory obligations. This has yet to be expressed because specific components of CS laws overlap with other laws. The mechanisms for sharing information that develops due to cyber security laws should facilitate communication between all government and private sectors[69]. The NYPD solicits the participation of private sector agencies, businesses, and corporations. To safeguard the network's integrity, prospective members undergo a screening procedure. Once approved, members are urged to utilize the network and the information it provides to bolster their entities' security against and resilience against terrorist acts and to act as a force multiplier in recognizing and reporting suspicious behavior.[70]

Private-public partnerships to combat cyberterrorism are a severe problem. Due to the general lack of a specialized anti-cyberterrorism statute, legal responses to cyberterrorism frequently rely on existing anti-terrorism regulations. This leads to ill-defined responses open to significant interpretation and a lack of oversight, accountability, transparency, etc[71]. The digital transition in the process industry is characterized by a high level of automation and an increasing connection to external networks, which exposes facilities to cyber threats. A summary of cyber-terrorism in the process industry While some notable data and event descriptions can be found in multiple sources addressing cyber-attacks, the information provided needs to be categorized to support security assessment, and sectorial data cannot be extracted. In addition, there needs to be a comprehensive sectoral

Events: A Systematic Review', *International Journal of Critical Infrastructure Protection*, 39 (2022), 100556 https://doi.org/10.1016/j.ijcip.2022.100556

[68] Yuchong Li and Qinghui Liu, 'A Comprehensive Review Study of Cyber-Attacks and Cyber Security; Emerging Trends and Recent Developments', *Energy Reports*, 7 (2021), 8176–86 https://doi.org/10.1016/j.egyr.2021.08.126

[69] Mishra and others.

[70] Christopher Cleary, 'Public-Private Partnerships: Security Organizations', *Encyclopedia of Security and Emergency Management*, 2019, 1–7 https://doi.org/10.1007/978-3-319-69891-5_228-1

[71] Xingxing Wei, 'A Critical Evaluation of China's Legal Responses to Cyberterrorism', *Computer Law & Security Review*, 47 (2022), 105768 https://doi.org/10.1016/j.clsr.2022.105768

statistical analysis available for process industry incidents due to the fragmentation of information[72].

4. Conclusion

The frequency of cyberattacks is concerningly escalating worldwide. Cyberterrorism, a widely acknowledged and publicized menace, is frequently associated with the attacks above. Simultaneously, eliminating terrorism requires reforming societal governance, potentially involving non-governmental and civil society organizations. Subsequently, policies designed to deter radicalization and recruitment for terrorism are rendered ineffective due to the severe restrictions on community participation in regions subject to rigorous government control. The components encompassed within this category are state and non-state organizations, international law (including customary law, court decisions, and international standards), United Nations resolutions and declarations, government and private governance, and international organizations that have a regional or global emphasis. Despite the concerted efforts of regional and international organizations to enhance cybersecurity measures, their advancement seems to halt. Effective cybersecurity culture model formation is significantly influenced by governance and organizational governance. The ITE Law does not presently govern cyber attacks capable of compromising Indonesia's security and defense infrastructure. Because of this, Indonesia necessitates cybercrime-specific regulations. Domestic and foreign state and non-state actors are obligated to collaborate to prevent, thwart, and repel cyber assaults. Hence, to overcome the challenges presented by cyberterrorism, Ministries/Institutions, and the Private Sector must work together or establish affiliate organizations to involve relevant stakeholders. In order to achieve national cyber security, Indonesia currently necessitates the implementation of supplementary regulations and policies on cyber security.

References

Aghajani, Gholamreza, and Noradin Ghadimi, 'Multi-Objective Energy Management in a Micro-Grid,' *Energy Reports*, 4 (2018), 218–25 https://doi.org/10.1016/j.egyr.2017.10.002

Ahmetoglu, Huseyin, and Resul Das, 'A Comprehensive Review on Detection of Cyber-Attacks: Data Sets, Methods, Challenges, and Future Research Directions,' *Internet of Things*, 20 (2022), 100615 https://doi.org/10.1016/j.iot.2022.100615

Akanni, J.O., 'A Non-Linear Optimal Control Model for Illicit Drug Use and

[72] Matteo IAIANI and others, 'Analysis of Cybersecurity-Related Incidents in the Process Industry', *Reliability Engineering & System Safety*, 209 (2021), 107485 https://doi.org/10.1016/j.ress.2021.107485

Terrorism Dynamics in Developing Countries with Time-Dependent Control Variables,' *Decision Analytics Journal*, 8 (2023), 100281 https://doi.org/10.1016/j.dajour.2023.100281

Alhayani, Bilal, Sara Taher Abbas, Dawood Zahi Khutar, and Husam Jasim Mohammed, 'WITHDRAWN: Best Ways Computation Intelligent of Face Cyber Attacks', *Materials Today: Proceedings*, 2021 https://doi.org/10.1016/j.matpr.2021.02.557

Amarini, Indriati, Yusuf Saefudin, Ika Ariani Kartini, Marsitiningsih Marsitiningsih, and Noorfajri Ismail, 'Digital Transformation: Creating an Effective and Efficient Court in Indonesia', *Legality : Jurnal Ilmiah Hukum*, 31.2 (2023), 266–84 https://doi.org/10.22219/ljih.v31i2.28013

Ampratwum, Godslove, Robert Osei-Kyei, and Vivian W.Y. Tam, 'Exploring the Concept of Public-Private Partnership in Building Critical Infrastructure Resilience against Unexpected Events: A Systematic Review,' *International Journal of Critical Infrastructure Protection*, 39 (2022), 100556 https://doi.org/10.1016/j.ijcip.2022.100556

Ardiana, Meity, Adriano Adriano, Kurniadi Doni, and Yulianto Yulianto, 'Corporate Criminal Liability in Procurement of Goods and Services in Hospital,' *Yuridika*, 38.2 (2023), 399–414 https://doi.org/10.20473/ydk.v38i2.43674

Ariefulloh, Ariefulloh, Hibnu Nugroho, Angkasa Angkasa, and Riris Ardhanariswari, 'Restorative Justice-Based Criminal Case Resolution in Salatiga, Indonesia: Islamic Law Perspective and Legal Objectives', *Ijtihad : Jurnal Wacana Hukum Islam Dan Kemanusiaan*, 23.1 (2023), 19–36 https://doi.org/10.18326/ijtihad.v23i1.19-36

Arifin, Ridwan, Sigit Riyanto, and Akbar Kurnia Putra, 'Collaborative Efforts in ASEAN for Global Asset Recovery Frameworks to Combat Corruption in the Digital Era,' *Legality : Jurnal Ilmiah Hukum*, 31.2 (2023), 329–43 https://doi.org/10.22219/ljih.v31i2.29381

Atiyah, Ghassan Adhab, Nazura Abdul Manap, and Saidatul Nadia Abd Aziz, 'Legal Status of Cryptocurrency Circulation in Iraq: Lessons from the United Arab Emirates and the United States,' *Hasanuddin Law Review*, 9.1 (2023), 1 https://doi.org/10.20956/halrev.v9i1.3867

Azhmyakov, Vadim, Erik I. Verriest, Moises Bonilla, and Stefan Pickl, 'Optimal Control Methodology for the Counter-Terrorism Strategies: The Relaxation Based Approach', *Journal of the Franklin Institute*, 359.13 (2022), 6690–6708 https://doi.org/10.1016/j.jfranklin.2022.07.013

Bakry, Muammar, Abdul Syatar, Achmad Abubakar, Chaerul Risal, Ahmad Ahmad, and Muhammad Majdy Amiruddin, 'Strengthening the Cyber

Terrorism Law Enforcement in Indonesia: Assimilation from Islamic Jurisdiction', *International Journal of Criminology and Sociology*, 10 (2021), 1267–76 https://doi.org/10.6000/1929-4409.2021.10.146

Barry, Thomas, Jonathan Jona, and Naomi Soderstrom, 'The Impact of Country Institutional Factors on Firm Disclosure: Cybersecurity Disclosures in Chinese Cross-Listed Firms', *Journal of Accounting and Public Policy*, 41.6 (2022), 106998 https://doi.org/10.1016/j.jaccpubpol.2022.106998

Beechey, Matthew, Konstantinos G. Kyriakopoulos, and Sangarapillai Lambotharan, 'Evidential Classification and Feature Selection for Cyber-Threat Hunting', *Knowledge-Based Systems*, 226 (2021), 107120 https://doi.org/10.1016/j.knosys.2021.107120

Bolbot, Victor, Ketki Kulkarni, Päivi Brunou, Osiris Valdez Banda, and Mashrura Musharraf, 'Developments and Research Directions in Maritime Cybersecurity: A Systematic Literature Review and Bibliometric Analysis', *International Journal of Critical Infrastructure Protection*, 39 (2022), 100571 https://doi.org/10.1016/j.ijcip.2022.100571

Brata, Al Fadilla Yoga, and Rakotoarisoa Maminiaina Heritiana Sedera, 'The Implementing a Carbon Tax as a Means of Increasing Investment Value in Indonesia', *Journal of Sustainable Development and Regulatory Issues (JSDERI)*, 1.2 (2023), 39–50 https://doi.org/10.53955/jsderi.v1i2.6

Bullock, Jane A., George D. Haddow, and Damon P. Coppola, 'Cybersecurity and Critical Infrastructure Protection', in *Introduction to Homeland Security* (Elsevier, 2021), pp. 425–97 https://doi.org/10.1016/B978-0-12-817137-0.00008-0

Burdon, Mark, and Lizzie Coles-Kemp, 'The Significance of Securing as a Critical Component of Information Security: An Australian Narrative', *Computers & Security*, 87 (2019), 101601 https://doi.org/10.1016/j.cose.2019.101601

Cappai, Marco, 'The Role of Private and Public Regulation in the Case Study of Crypto-Assets: The Italian Move towards Participatory Regulation', *Computer Law & Security Review*, 49 (2023), 105831 https://doi.org/10.1016/j.clsr.2023.105831

Chang, Lennon Y.C., and Nicholas Coppel, 'Building Cyber Security Awareness in a Developing Country: Lessons from Myanmar', *Computers & Security*, 97 (2020), 101959 https://doi.org/10.1016/j.cose.2020.101959

Chatzis, Petros, and Eliana Stavrou, 'Cyber-Threat Landscape of Border Control Infrastructures', *International Journal of Critical Infrastructure Protection*, 36 (2022), 100503 https://doi.org/10.1016/j.ijcip.2021.100503

Cheryl, Barr-Kumarakulasinghe, Boon-Kwee Ng, and Chan-Yuan Wong, 'Governing the Progress of Internet-of-Things: Ambivalence in the Quest of

Technology Exploitation and User Rights Protection', *Technology in Society*, 64 (2021), 101463 https://doi.org/10.1016/j.techsoc.2020.101463

Choudhary, Sheraz Ahmad, Muhammad Azhar Khan, Abdullah Zafar Sheikh, Mohd Khata Jabor, Mohd Safarin bin Nordin, Abdelmohsen A. Nassani, and others, 'Role of Information and Communication Technologies on the War against Terrorism and on the Development of Tourism: Evidence from a Panel of 28 Countries', *Technology in Society*, 62 (2020), 101296 https://doi.org/10.1016/j.techsoc.2020.101296

Cleary, Christopher, 'Public-Private Partnerships: Security Organizations', *Encyclopedia of Security and Emergency Management*, 2019, 1–7 https://doi.org/10.1007/978-3-319-69891-5_228-1

Cross, M.K.D., 'Counter-Terrorism & the Intelligence Network in Europe', *International Journal of Law, Crime and Justice*, 72 (2023), 100368 https://doi.org/10.1016/j.ijlcj.2019.100368

Diaz Valdivia, Andres, 'Between Decentralization and Reintermediation: Blockchain Platforms and the Governance of "Commons-Led" and "Business-Led" Energy Transitions', *Energy Research & Social Science*, 98 (2023), 103034 https://doi.org/10.1016/j.erss.2023.103034

Dong, Changyin, Yujia Chen, Hao Wang, Leizhen Wang, Ye Li, Daiheng Ni, and others, 'Evaluating Impact of Remote-Access Cyber-Attack on Lane Changes for Connected Automated Vehicles', *Digital Communications and Networks*, 2023 https://doi.org/10.1016/j.dcan.2023.06.004

Fu, Lipeng, Xueqing Wang, Bingsheng Liu, and Ling Li, 'Investigation into the Role of Human and Organizational Factors in Security Work against Terrorism at Large-Scale Events', *Safety Science*, 128 (2020), 104764 https://doi.org/10.1016/j.ssci.2020.104764

Ge, Hui, Lei Zhao, Dong Yue, Xiangpeng Xie, Linghai Xie, Sergey Gorbachev, and others, 'A Game Theory Based Optimal Allocation Strategy for Defense Resources of Smart Grid under Cyber-Attack', *Information Sciences*, 652 (2024), 119759 https://doi.org/10.1016/j.ins.2023.119759

Ginting, Jamin, and Patrick Talbot, 'Fundraising Aspect of International Terrorism Organization in ASEAN: Legal and Political Aspects', *Lex Scientia Law Review*, 7.1 (2023), 1–30 https://doi.org/10.15294/lesrev.v7i1.60074

Homburger, Zine, 'The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace', *Global Society*, 33.2 (2019), 224–42 https://doi.org/10.1080/13600826.2019.1569502

IAIANI, Matteo, Alessandro TUGNOLI, Sarah BONVICINI, and Valerio COZZANI, 'Analysis of Cybersecurity-Related Incidents in the Process

Industry', *Reliability Engineering & System Safety*, 209 (2021), 107485 https://doi.org/10.1016/j.ress.2021.107485

Jaelani, Abdul Kadir, and Resti Dian Luthviati, 'The Crime Of Damage After the Constitutional Court's Decision Number 76/PUU-XV/2017', *Journal of Human Rights, Culture and Legal System*, 1.1 (2021) https://doi.org/10.53955/jhcls.v1i1.5

Kelemen, Barbara, and Alessandro Fergnani, 'The Futures of Terrorism against China in the Greater Middle East', *Futures*, 124 (2020), 102643 https://doi.org/10.1016/j.futures.2020.102643

Kouloufakos, Triantafyllos, 'Untangling the Cyber Norm to Protect Critical Infrastructures', *Computer Law & Security Review*, 49 (2023), 105809 https://doi.org/10.1016/j.clsr.2023.105809

Kusumaningtyas, Reza Octavia, and James Kalimanzila, 'The Impact of Tax Incentive on Increase Foreign Direct Investment', *Journal of Sustainable Development and Regulatory Issues (JSDERI)*, 1.2 (2023), 51–63 https://doi.org/10.53955/jsderi.v1i2.7

Lattanzio, Gabriele, and Yue Ma, 'Cybersecurity Risk and Corporate Innovation', *Journal of Corporate Finance*, 82 (2023), 102445 https://doi.org/10.1016/j.jcorpfin.2023.102445

Lee, Claire Seungeun, and Ji Hye Kim, 'Latent Groups of Cybersecurity Preparedness in Europe: Sociodemographic Factors and Country-Level Contexts', *Computers & Security*, 97 (2020), 101995 https://doi.org/10.1016/j.cose.2020.101995

Li, Yuchong, and Qinghui Liu, 'A Comprehensive Review Study of Cyber-Attacks and Cyber Security; Emerging Trends and Recent Developments', *Energy Reports*, 7 (2021), 8176–86 https://doi.org/10.1016/j.egyr.2021.08.126

Macas, Mayra, Chunming Wu, and Walter Fuertes, 'Adversarial Examples: A Survey of Attacks and Defenses in Deep Learning-Enabled Cybersecurity Systems', *Expert Systems with Applications*, 238 (2024), 122223 https://doi.org/10.1016/j.eswa.2023.122223

Mahardika, Harryadin, Juliana French, and Agung Sembada, 'Keep Calm and Eat Satay: Indonesia's Consumption-Themed Signals of Defiance against Terrorism', *Australasian Marketing Journal*, 26.3 (2018), 231–38 https://doi.org/10.1016/j.ausmj.2018.06.002

Masyhar, Ali, Muhammad Azil Maskur, Sri Redjeki Prasetyowati, Aldita Evan Prihama, Roy Priyono, and Ahmad Alif, 'Digital Transformation of Youth Movement for Counter Radicalism', 2022, p. 030010 https://doi.org/10.1063/5.0109808

Masyhar, Ali, Ali Murtadho, and Ahmad Zaharuddin Sani Ahmad Sabri, 'The Driving Factors for Recidivism of Former Terrorism Convicts in Socio-Legal Perspective', *Journal of Indonesian Legal Studies*, 8.1 (2023) https://doi.org/10.15294/jils.v8i1.69445

Mishra, Alok, Yehia Ibrahim Alzoubi, Memoona Javeria Anwar, and Asif Qumer Gill, 'Attributes Impacting Cybersecurity Policy Development: An Evidence from Seven Nations', *Computers & Security*, 120 (2022), 102820 https://doi.org/10.1016/j.cose.2022.102820

Mohammadi, Mokhtar, Tarik A. Rashid, Sarkhel H.Taher Karim, Adil Hussain Mohammed Aldalwie, Quan Thanh Tho, Moazam Bidaki, and others, 'A Comprehensive Survey and Taxonomy of the SVM-Based Intrusion Detection Systems', *Journal of Network and Computer Applications*, 178 (2021), 102983 https://doi.org/10.1016/j.jnca.2021.102983

Motsch, William, Alexander David, Keran Sivalingam, Achim Wagner, and Martin Ruskowski, 'Approach for Dynamic Price-Based Demand Side Management in Cyber-Physical Production Systems', *Procedia Manufacturing*, 51 (2020), 1748–54 https://doi.org/10.1016/j.promfg.2020.10.243

Niraja, K.S., and Sabbineni Srinivasa Rao, 'WITHDRAWN: A Hybrid Algorithm Design for near Real Time Detection Cyber Attacks from Compromised Devices to Enhance IoT Security', *Materials Today: Proceedings*, 2021 https://doi.org/10.1016/j.matpr.2021.01.751

Nugraha, Yudhistira, and Andrew Martin, 'Towards a Framework for Trustworthy Data Security Level Agreement in Cloud Procurement', *Computers & Security*, 106 (2021), 102266 https://doi.org/10.1016/j.cose.2021.102266

Okey, Ogobuchi Daniel, Ekikere Umoren Udo, Renata Lopes Rosa, Demostenes Zegarra Rodríguez, and João Henrique Kleinschmidt, 'Investigating ChatGPT and Cybersecurity: A Perspective on Topic Modeling and Sentiment Analysis', *Computers & Security*, 135 (2023), 103476 https://doi.org/10.1016/j.cose.2023.103476

Plotnek, Jordan J., and Jill Slay, 'Cyber Terrorism: A Homogenized Taxonomy and Definition', *Computers & Security*, 102 (2021), 102145 https://doi.org/10.1016/j.cose.2020.102145

QMN-Nguyen, Moon, 'Media Presentations of Vietnam's Cybersecurity Law: A Comparative Approach with Corpus-Based Critical Discourse Analysis', *Computer Law & Security Review*, 50 (2023), 105835 https://doi.org/10.1016/j.clsr.2023.105835

Radomyski, Adam, and Paweł Bernat, 'Contemporary Determinants of Organising Effective Protection of Civil Aviation Against Terrorism', *Transportation Research*

Procedia, 35 (2018), 259–70 https://doi.org/10.1016/j.trpro.2018.12.021

Röell, Christiaan, Ellis Osabutey, Peter Rodgers, Felix Arndt, Zaheer Khan, and Shlomo Tarba, 'Managing Socio-Political Risk at the Subnational Level: Lessons from MNE Subsidiaries in Indonesia', *Journal of World Business*, 57.3 (2022), 101312 https://doi.org/10.1016/j.jwb.2022.101312

Safaei Pour, Morteza, Christelle Nader, Kurt Friday, and Elias Bou-Harb, 'A Comprehensive Survey of Recent Internet Measurement Techniques for Cyber Security', *Computers & Security*, 128 (2023), 103123 https://doi.org/10.1016/j.cose.2023.103123

Saputra, Rian, Tiara Tiolince, Iswantoro Iswantoro, and Sanju Kumar Sigh, 'Artificial Intelligence and Intellectual Property Protection in Indonesia and Japan', *Journal of Human Rights, Culture and Legal System*, 3.2 (2023), 210–35 https://doi.org/10.53955/jhcls.v3i2.69

Seger Guttmann, Tali, Shaked Gilboa, and Judith Partouche-Sebban, '"I Live with Terror inside Me": Exploring Customers' Instinctive Reactions to Terror', *International Journal of Hospitality Management*, 92 (2021), 102734 https://doi.org/10.1016/j.ijhm.2020.102734

Septasari, Dita, 'The Cyber Security and The Challenge of Society 5.0 Era in Indonesia', *Aisyah Journal Of Informatics and Electrical Engineering (A.J.I.E.E)*, 5.2 (2023), 227–33 https://doi.org/10.30604/jti.v5i2.231

Sepúlveda Estay, Daniel A., Rishikesh Sahay, Michael B. Barfod, and Christian D. Jensen, 'A Systematic Review of Cyber-Resilience Assessment Frameworks', *Computers & Security*, 97 (2020), 101996 https://doi.org/10.1016/j.cose.2020.101996

Sholecha, Ema Mar'ati, Ahmat Saiful, Sheilla Yunika, Hariyanto Hariyanto, and Norhaiden Unsil, 'Justice Collaborator's Position and Function on Witness Protection's Rights as a Suspect from the Perspective of Criminal Law in Indonesia', *Volksgeist: Jurnal Ilmu Hukum Dan Konstitusi*, 2023, 131–43 https://doi.org/10.24090/volksgeist.v6i1.7246

Da Silva, Joseph, 'Cyber Security and the Leviathan', *Computers & Security*, 116 (2022), 102674 https://doi.org/10.1016/j.cose.2022.102674

Spalek, Basia, and Salwa El-Awa, 'Governance and Counter-Terrorism: Engaging Moderate and Non-Violent Extremist Movements in Combatting Jihadist-Linked Terrorism', *International Journal of Law, Crime and Justice*, 72 (2023), 100367 https://doi.org/10.1016/j.ijlcj.2019.100367

Stacey, Patrick, Rebecca Taylor, Omotolani Olowosule, and Konstantina Spanaki, 'Emotional Reactions and Coping Responses of Employees to a Cyber-Attack: A Case Study', *International Journal of Information Management*, 58 (2021), 102298 https://doi.org/10.1016/j.ijinfomgt.2020.102298

Suryono, Ryan Randy, Indra Budi, and Betty Purwandari, 'Detection of Fintech P2P Lending Issues in Indonesia', *Heliyon*, 7.4 (2021), e06782 https://doi.org/10.1016/j.heliyon.2021.e06782

Tan, Sen, Peilin Xie, Josep M. Guerrero, Juan C. Vasquez, Yunlu Li, and Xifeng Guo, 'Attack Detection Design for Dc Microgrid Using Eigenvalue Assignment Approach', *Energy Reports*, 7 (2021), 469–76 https://doi.org/10.1016/j.egyr.2021.01.045

Tauda, Gunawan A., Andy Omara, and Gioia Arnone, 'Cryptocurrency: Highlighting the Approach, Regulations, and Protection in Indonesia and European Union', *BESTUUR*, 11.1 (August) (2023), 1 https://doi.org/10.20961/bestuur.v11i1.67125

Tian, Shu, Bo Zhao, and Resi Ong Olivares, 'Cybersecurity Risks and Central Banks' Sentiment on Central Bank Digital Currency: Evidence from Global Cyberattacks', *Finance Research Letters*, 53 (2023), 103609 https://doi.org/10.1016/j.frl.2022.103609

Uchendu, Betsy, Jason R.C. Nurse, Maria Bada, and Steven Furnell, 'Developing a Cyber Security Culture: Current Practices and Future Needs', *Computers & Security*, 109 (2021), 102387 https://doi.org/10.1016/j.cose.2021.102387

Wardana, Dodi Jaya, Sukardi Sukardi, and Radian Salman, 'Public Participation in the Law-Making Process in Indonesia', *Jurnal Media Hukum*, 30.1 (2023), 66–77 https://doi.org/10.18196/jmh.v30i1.14813

Wei, Xingxing, 'A Critical Evaluation of China's Legal Responses to Cyberterrorism', *Computer Law & Security Review*, 47 (2022), 105768 https://doi.org/10.1016/j.clsr.2022.105768

Yaacoub, Jean-Paul, Hassan Noura, Ola Salman, and Ali Chehab, 'Security Analysis of Drones Systems: Attacks, Limitations, and Recommendations', *Internet of Things*, 11 (2020), 100218 https://doi.org/10.1016/j.iot.2020.100218