Jurnal Hukum dan Keadilan

P-ISSN : 0000-0000 Vol. 3 No. 5, August 2026
E-ISSN : 3031-6782
DOI : https://doi.org/10.61942/jhk.v3i5.669
Available : https://jurnalhafasy.com/index.php/jhk

Cybersecurity Law and National Digital Resilience in The Fourth Industrial Revolution

Herlina Damaik
Jambi University, Jambi, Indonesia

Received: July 17, 2026
Revised: August 9, 2026
Accepted: August 23, 2026
Published: August 25, 2026

Corresponding Author:
Author Name*: Herlina Damaik
E-mail*: damaikherlina23@gmail.com

Abstract**:** *The Fourth Industrial Revolution has transformed the landscape of state governance, the economy, and national defense through the convergence of cyber-physical technologies, artificial intelligence, the Internet of Things, and big data interconnected within a single digital ecosystem. This transformation brings significant opportunities for bureaucratic efficiency and digital economic growth, but simultaneously expands the attack surface, threatening vital information infrastructure, citizens' personal data, and the stability of government systems. This article aims to analyze the position of cybersecurity law as a normative instrument in building national digital resilience amidst the disruptions of the Fourth Industrial Revolution, focusing on the Indonesian legal framework in comparison with regulatory practices in the European Union, the United States, and several other developing countries. This research uses a normative juridical method with a statutory approach, a conceptual approach, and a comparative legal approach, supported by a literature review of laws and regulations, recent scientific journals, and official policy documents of state institutions. The research results show that Indonesia's cybersecurity legal framework, consisting of the Electronic Information and Transactions Law, the Personal Data Protection Law, the Presidential Regulation on the Protection of Vital Information Infrastructure, and the Draft Cyber Security and Resilience Law, is still sectoral, responsive, and not fully oriented towards systemic resilience as mandated by the resilience-by-design paradigm in European Union regulations. This article recommends a reorientation of the legal paradigm from a repressive approach based on criminal prosecution to a preventive-adaptive approach that integrates cyber risk management, mandatory incident reporting, standardization of digital product security, and strengthening the institutional capacity of the National Cyber and Crypto Agency, as a legal foundation for sustainable national digital resilience.*

Keywords: Cybersecurity Law; National Digital Resilience; The Fourth Industrial Revolution; Vital Information Infrastructure; Cyber Governance.

INTRODUCTION

The Fourth Industrial Revolution, conceptually introduced by Klaus Schwab at the 2016 World Economic Forum, marks a turning point in civilization where the boundaries between the physical, digital, and biological worlds are increasingly blurred due to the convergence of artificial intelligence, the Internet of Things, cloud computing, big data analytics, and cyber-physical systems. This phenomenon is not simply giving birth to industrial automation as in previous industrial revolutions, but rather creating a new socio-technical ecosystem in which countries, corporations, and individuals are structurally dependent on digital infrastructure to carry out their vital functions, from public services, financial systems, energy networks, transportation, to national defense. This structural dependence then gives rise to new systemic vulnerabilities, because every node in the interconnected digital network has the

Jurnal Hukum dan Keadilan

P-ISSN : 0000-0000 Vol. 3 No. 5, August 2026
E-ISSN : 3031-6782
DOI : https://doi.org/10.61942/jhk.v3i5.669
Available : https://jurnalhafasy.com/index.php/jhk

potential to become an entry point for cyber threats that can spread rapidly and expand throughout the system.[1]

Industrial cyber resilience, as highlighted in a comprehensive study of industrial networks, has become a strategic necessity given that attacks on industrial control systems no longer only threaten data confidentiality, but also the physical safety of people and the continued operation of critical infrastructure such as power plants, water treatment facilities, and telecommunications networks.[2] This paradigm shift demands that the law no longer treat cybersecurity solely as a technical issue left to information technology experts, but rather as a matter of state governance that requires a clear, binding, and enforceable normative framework. It is at this point that cybersecurity law finds its urgency as an instrument for distributing responsibility, establishing minimum security standards, and establishing accountability mechanisms among the government, business actors, and civil society.

The concept of cyber resilience itself has undergone a significant evolution in contemporary legal discourse. While in previous decades, cybersecurity was primarily understood as prevention and protection against attacks, the resilience paradigm emphasizes a system's ability to continue functioning, adapt, and recover quickly despite disruptions or cyberattacks that successfully penetrate defenses.[3] This shift from cybersecurity to cyber resilience has profound legal implications, as the law is no longer sufficient to simply regulate prohibitions and criminal sanctions against hacking, but must also regulate proactive obligations in the form of risk management, system resilience testing, incident reporting, and standardized post-incident recovery mechanisms.

The European Union has positioned itself as a pioneer in translating the cyber resilience paradigm into a concrete legal instrument through the Cyber Resilience Act, which was officially adopted as Regulation (EU) 2024/2847 and entered into full force at the end of 2027.[4] This regulation requires manufacturers of products with digital elements to apply the principles of security-by-design and security-by-default throughout the product lifecycle, including the obligation to report actively exploited vulnerabilities within twenty-four hours to the competent authorities.[5] This horizontal approach represents a regulatory breakthrough because it no longer limits cybersecurity obligations to the critical infrastructure sector, but rather extends them to all digital products circulating in the European single market, thus creating a more comprehensive and consistent regulatory landscape than the sectoral approach currently

[1]Thuraya Alrumaih et al., "Cyber Resilience in Industrial Networks: A State of the Art, Challenges, and Future Directions," Journal of King Saud University – Computer and Information Sciences 35 (2023): 101781, https://doi.org/10.1016/j.jksuci.2023.101781.

[2]Masike Malatji, A. Marnewick, and S. von Solms, "Cybersecurity Capabilities for Critical Infrastructure Resilience," Information & Computer Security 30 (2021): 255–279, https://doi.org/10.1108/ICS-06-2021-0091.

[3]G. Szpor, "The Concept of Cyber Resilience in the European Union Law," Review of European and Comparative Law (2026), https://doi.org/10.31743/recl.19198.

[4]European Union, Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on Horizontal Cybersecurity Requirements for Products with Digital Elements (Cyber Resilience Act), OJ L 2024/2847, 20 November 2024.

[5]P. Chiara, "The Cyber Resilience Act: The EU Commission's Proposal for a Horizontal Regulation on Cybersecurity for Products with Digital Elements," International Cybersecurity Law Review 3 (2022): 255–272, https://doi.org/10.1365/s43439-022-00067-6.

Jurnal Hukum dan Keadilan

P-ISSN : 0000-0000 Vol. 3 No. 5, August 2026
E-ISSN : 3031-6782
DOI : https://doi.org/10.61942/jhk.v3i5.669
Available : https://jurnalhafasy.com/index.php/jhk

adopted by many countries, including Indonesia.

A study of the concept of cyber resilience within the European Union legal framework also shows that resilience cannot be understood partially through a single legal instrument, but rather is the result of a complex interaction between various complementary regulations, ranging from the Network and Information Security Directive, the Cyber Resilience Act, to the Digital Operational Resilience Act for the financial sector.[6] This kind of normative fragmentation, while seemingly complex, actually reflects regulators' awareness that cyber resilience is cross-sectoral and requires a multi-layered governance approach to accommodate the varying risk characteristics of each sector of social life.

Technical standardization also plays a central role in achieving effective cyber resilience. Research on European cybersecurity standardization reveals a structural tension between the technical standardization process developed by independent standards bodies and the need for legally binding public regulation, a situation described as a "two-way wall" that must be bridged for cybersecurity laws to be effectively implemented in practice.[7] This issue is relevant for Indonesia, given that the process of developing national cybersecurity standards often runs separately from the legislative process, creating a gap between general legal norms and operational technical standards.

In the United States, the approach to cybersecurity regulation tends to be sectoral and based on a voluntary risk management framework developed by the National Institute of Standards and Technology, combined with increasingly stringent incident reporting requirements following a series of ransomware attacks on critical infrastructure. This combination of mandatory regulation for certain sectors, such as energy and finance, with voluntary frameworks for others creates a hybrid regulatory model that differs from the European Union's horizontal approach, but still affirms the same principle: that states have a legitimate interest in intervening in markets to ensure digital resilience that impacts the public interest.

Recent developments in the United Kingdom reinforce the global trend toward more comprehensive cybersecurity regulations. The UK Cyber Security and Resilience Bill, introduced to Parliament in November 2025, is designed to update and expand the scope of the Network and Information Systems Regulations of 2018 to enhance national cybersecurity and protect essential services on which people depend, including electricity, clean water, and the national healthcare system. This legislative initiative confirms that developed countries are consistently moving toward a paradigm of mandatory, cross-sectoral, systemic resilience, rather than leaving cybersecurity solely to the voluntary compliance of businesses—a trend that should serve as a guide for Indonesia as it accelerates the reform of its national cybersecurity laws.

A similar phenomenon is also evident in Southeast Asia, where several neighboring countries have or are currently drafting more comprehensive cybersecurity laws. Malaysia, for example, has passed the Cyber Security Act 2024, which establishes a national cybersecurity advisory body with the authority to set security standards for eleven critical

[6]P. Chiara, "Understanding the Regulatory Approach of the Cyber Resilience Act: Protection of Fundamental Rights in Disguise?," European Journal of Risk Regulation 16 (2025): 469–484, https://doi.org/10.1017/err.2025.9.

[7]Irene Kamara, "European Cybersecurity Standardisation: A Tale of Two Solitudes in View of Europe's Cyber Resilience," Innovation: The European Journal of Social Science Research 37 (2024): 1441–1460, https://doi.org/10.1080/13511610.2024.2349626.

Jurnal Hukum dan Keadilan

P-ISSN : 0000-0000 Vol. 3 No. 5, August 2026
E-ISSN : 3031-6782
DOI : https://doi.org/10.61942/jhk.v3i5.669
Available : https://jurnalhafasy.com/index.php/jhk

information infrastructure sectors, while Singapore has already updated its Cybersecurity Act to include cyber-physical systems and cloud computing service providers as specifically regulated entities. This regional dynamic highlights the risk of Indonesia falling behind in the regulatory competition in the region if the Cyber Security and Resilience Bill continues to be delayed, as regional investors and digital service providers tend to consider the certainty and maturity of a country's cybersecurity legal framework as a factor in deciding where to invest in digital infrastructure, including data centers and cloud computing services.

In developing countries, the challenges of implementing cybersecurity laws are distinct. A review of Nigeria's cybersecurity legal framework in the face of the Fourth Industrial Revolution shows that developing countries face a dual challenge: limited institutional and human resource capacity, on the one hand, and pressure to rapidly adopt new technologies to catch up with the digital economy, on the other. Both of these challenges have the potential to widen the gap between regulatory ambition and implementation capacity.[8] A similar situation is also reflected in the study of cybersecurity governance in Pakistan, which highlights the importance of integrating regulatory oversight, organizational risk management, and strengthening institutional resilience as three inseparable pillars in building an effective cybersecurity ecosystem in a country with limited resources.[9]

Brazil offers another interesting precedent through its legislative impact evaluation of the National Program for Digital Security and Resilience, which used a law and economics approach to assess the effectiveness of national cybersecurity policies, and concluded that the success of cybersecurity regulations is largely determined by the economic incentives created for businesses to proactively comply with security standards, rather than solely through the threat of repressive sanctions.[10] This legal and economic perspective provides an important lesson that the effectiveness of cybersecurity laws cannot be measured solely by the strictness of criminal sanctions, but also by the extent to which regulatory design is able to align the economic interests of business actors with public security goals.

In the Indonesian context, the urgency of reforming cybersecurity law is increasingly prominent as the frequency and complexity of cyber incidents affecting government institutions and the private sector increases. A critical review of the urgency of strengthening the implementation of cybersecurity and resilience in Indonesia confirms that the current legal framework, which relies on the Electronic Information and Transactions Law, is inadequate to address the complexity of contemporary cyber threats, particularly due to its focus on post-incident criminal prosecution rather than systemic risk prevention and

[8]Pamela Victor Ibitamuno, "Legal Frameworks for Cybersecurity in Nigeria – Adapting the Fourth Industrial Revolution," Advances in Multidisciplinary and Scientific Research Journal Publication (2023), https://doi.org/10.22624/AIMS/CSEAN-SMART2023P12.

[9]Yasir Majeed, Anas Majeed, and Muhammad Tahir Minhas, "Cybersecurity Governance in the Digital Era and IT: Integrating Regulatory Oversight, Risk Management, and Organisational Resilience in Pakistan," Social Science Review Archives (2026), https://doi.org/10.70670/sra.v4i1.1711.

[10]Marcos Cícero Santos Wanderlei, "Legislative Impact Assessment of the Brazilian National Digital Security and Resilience Program: A Law and Economics Perspective," REMUNOM (2026), https://doi.org/10.66104/re2nmt33.

Jurnal Hukum dan Keadilan

P-ISSN : 0000-0000 Vol. 3 No. 5, August 2026
E-ISSN : 3031-6782
DOI : https://doi.org/10.61942/jhk.v3i5.669
Available : https://jurnalhafasy.com/index.php/jhk

mitigation.[11] This legal vacuum is further exacerbated by the fact that the Cybersecurity and Resilience Bill, first proposed in 2019, has yet to be enacted into law despite repeated inclusion in the annual priority National Legislation Program. This prolonged delay contrasts with the growing urgency, as the National Cyber and Crypto Agency regularly reports an increase in anomalies and suspicious traffic incidents in the national cyberspace, most of which target the government and financial sectors. The gap between the escalating threat on the ground and the slow pace of the legislative process further underscores the academic and practical urgency of this research.

Law enforcement in the realm of digital privacy is also a crucial variable in building national resilience in the digital era. Studies on the role of law enforcement in enforcing privacy regulations to strengthen national resilience show that personal data protection and cybersecurity are intertwined, as massive personal data leaks can be exploited as a vector for further cyberattacks, including social engineering and digital identity-based fraud, which in turn can undermine social stability and public trust in digital government systems.[12] The enactment of Law Number 27 of 2022 concerning Personal Data Protection represents a significant step forward, but its implementation still faces structural challenges, particularly regarding the independence and institutional capacity of the newly established supervisory authority.

The constitutional and philosophical dimensions of cybersecurity law are also beginning to receive more serious academic attention. A comparative study of the constitutionalization of cybersecurity between Indonesia and Malaysia through the maqasid al-sharia framework demonstrates that the harmonization of cybersecurity regulations in Southeast Asia cannot be separated from the constitutional and socio-cultural values of each country. Therefore, cross-border regulatory convergence needs to take into account the diversity of these legal foundations rather than imposing a single, universal regulatory model.[13] This approach is relevant considering that regional cybersecurity cooperation, particularly within the ASEAN framework, is increasingly required to address transnational, cross-border cyber threats.

The development of artificial intelligence adds a new layer of complexity to cybersecurity law. Studies on the urgency of regulating artificial intelligence in relation to cybersecurity and resilience emphasize that artificial intelligence acts as a double-edged sword. On the one hand, it strengthens the detection and response capabilities to cyber threats through automated security analytics. On the other hand, it can also be exploited by cybercriminals to develop more sophisticated, adaptive, and difficult-to-detect attacks. This necessitates a legal framework capable of regulating the use of artificial intelligence both as a defense tool and as a potential threat.[14] Machine learning, in this context, has been

[11]Sarah Safira Aulianisa and Indirwan, "Critical Review of the Urgency of Strengthening the Implementation of Cyber Security and Resilience in Indonesia," Lex Scientia Law Review (2020), https://doi.org/10.15294/lesrev.v4i1.38197.

[12]Irfandi, "The Role of Law Enforcement in Upholding Privacy Regulations to Strengthen National Resilience in the Digital Era," Multidisciplinary Indonesian Center Journal (MICJO) (2026), https://doi.org/10.62567/micjo.v3i1.1790.

[13]Farid Al Hadana et al., "Constitutionalizing Cybersecurity: Indonesia–Malaysia Regulatory Convergence through a Maqasid al-Sharia Framework," Journal of Islamic Law on Digital Economy and Business (2026), https://doi.org/10.20885/jildeb.vol1.iss2.art2.

[14]Ahmad Ramli et al., "The Urgency of Regulating Artificial Intelligence in Relation to

Jurnal Hukum dan Keadilan

P-ISSN : 0000-0000 Vol. 3 No. 5, August 2026
E-ISSN : 3031-6782
DOI : https://doi.org/10.61942/jhk.v3i5.669
Available : https://jurnalhafasy.com/index.php/jhk

widely applied to strengthen cyber resilience in Industry 4.0 environments, particularly in detecting anomalies in cyber-physical systems in real-time, although its application also raises new challenges regarding algorithm transparency and legal accountability for automated decisions taken by artificial intelligence systems.[15]

The urgency of updating the cybersecurity legal framework is also underscored by a study on cybersecurity regulatory opportunities in the European Union and globally, which recommends that cybersecurity regulations be designed horizontally, across products, and across sectors, rather than being left fragmented into various overlapping sectoral regulations that are difficult to enforce consistently.[16] This recommendation was then fully realized through the enactment of the Cyber Resilience Act, demonstrating that academic discourse on the need for horizontal regulation can be translated into concrete legal policy if supported by sufficient political will. This precedent is relevant for Indonesia, given that the Draft Cyber Security and Resilience Law has the potential to adopt a similar horizontal approach, provided the legislative process avoids the prolonged delays that have occurred over the past five years.

This urgency is further heightened by a series of cyber incidents affecting the Indonesian government's digital infrastructure in recent years. One of the most significant incidents occurred on June 20, 2024, when the Temporary National Data Center suffered a ransomware attack, disrupting digital services at over two hundred government agencies, including immigration services, which were paralyzed for several days.[17] The incident served as a significant opportunity to expose the structural vulnerabilities of the Indonesian government's data governance, including the lack of adequate data backup policies and weak network segmentation between agencies, both of which are governance issues that should have been mandatorily regulated through a comprehensive national cybersecurity legal framework. The National Data Center incident serves as a clear illustration that the legal vacuum in cyber risk management is not merely an academic issue, but a real problem that directly impacts public services and public trust in the government's digital transformation.

Based on the above description, this article is proposed to answer two main questions. First, what is the position and characteristics of Indonesian cybersecurity law in supporting national digital resilience in the era of the Fourth Industrial Revolution compared to the regulatory practices of other countries? Second, what legal reform steps are needed to transform Indonesia's cybersecurity legal framework from a repressive-sectoral approach to a preventive-systemic approach oriented towards sustainable national digital resilience. This article is expected to provide an academic contribution in the form of a conceptual map regarding the position of cybersecurity law within the national resilience architecture, while also providing applicable policy recommendations for legislators in formulating a cybersecurity legal framework

Cybersecurity and Cyber Resilience," Cogent Social Sciences (2026), https://doi.org/10.1080/23311886.2026.2632977.

[15]Jia Yu, Alexey Shvetsov, and Saeed Hamood Alsamhi, "Leveraging Machine Learning for Cybersecurity Resilience in Industry 4.0: Challenges and Future Directions," IEEE Access 12 (2024): 159579–159596, https://doi.org/10.1109/ACCESS.2024.3482987.

[16]K. Ludvigsen and Shishir Nagaraja, "The Opportunity to Regulate Cybersecurity in the EU (and the World): Recommendations for the Cybersecurity Resilience Act," arXiv:2205.13196 (2022), https://doi.org/10.48550/arXiv.2205.13196.

[17]Hutama Arif Bramantyo, "Enhancing Cybersecurity in Indonesia's National Data Center Post-Ransomware Attack" (poster, Syracuse University, 2024), https://surface.syr.edu/eli/257.

Jurnal Hukum dan Keadilan

P-ISSN : 0000-0000 Vol. 3 No. 5, August 2026
E-ISSN : 3031-6782
DOI : https://doi.org/10.61942/jhk.v3i5.669
Available : https://jurnalhafasy.com/index.php/jhk

that is responsive to the dynamics of the Fourth Industrial Revolution.

METHODOLOGY

This research uses a normative legal research method, namely research that examines law as a written norm that is conceptualized as a standard rule for human behavior that is considered appropriate.[18] This method was chosen because the focus of the research is to examine the consistency, completeness, and coherence of Indonesian positive legal norms in the field of cybersecurity, as well as to compare them with legal norms in other jurisdictions to formulate recommendations for prescriptive legal reforms. This research uses three complementary approaches. First, the statute approach, which is conducted by reviewing all laws and regulations relevant to cybersecurity in Indonesia, including Law Number 11 of 2008 concerning Electronic Information and Transactions as last amended by Law Number 1 of 2024, Law Number 27 of 2022 concerning Personal Data Protection, Presidential Regulation Number 82 of 2022 concerning the Protection of Vital Information Infrastructure, Presidential Regulation Number 53 of 2017 concerning the National Cyber and Crypto Agency, and the Draft Law on Cyber Security and Resilience, which at the time of this research was compiled was still a draft in the National Legislation Program. Second, the conceptual approach, which is used to trace the development of the concept of cyber resilience in international academic literature, including the paradigm shift from cybersecurity to cyber resilience as the main analytical framework in this article. Third, a comparative legal approach, which is used to compare Indonesia's cybersecurity legal framework with the legal framework in the European Union through the Cyber Resilience Act, the regulatory framework in the United States, and the experiences of other developing countries such as Nigeria, Pakistan, and Brazil, in order to identify best practices that can be adapted to the context of Indonesian national law.

The unit of analysis in this study is the legal norm itself, not the behavior of legal actors. Therefore, the findings consist of descriptions and evaluations of the consistency and completeness of the norm, not statistical generalizations of the compliance behavior of business actors or the public. The selection of secondary legal materials was conducted purposively, prioritizing articles that thematically discuss the concepts of cyber resilience, cybersecurity law, and the implications of the Fourth Industrial Revolution for digital governance, both published by reputable international journal publishers and accredited national law journals, to ensure a balance of global and local perspectives in the resulting analysis.

The legal materials used in this study consist of three types. Primary legal materials include relevant Indonesian laws and regulations as mentioned above, as well as international and regional legal instruments such as Regulation (EU) 2024/2847 on the Cyber Resilience Act and the Budapest Convention on Cybercrime. Secondary legal materials include textbooks, articles from nationally and internationally accredited scientific journals published within the last five years, official reports from state institutions such as the National Cyber and Crypto Agency, and policy documents from international organizations. Tertiary legal materials include legal dictionaries and encyclopedias used to clarify technical and conceptual terms used in this study.

The legal material collection technique was conducted through library research by searching databases of reputable scientific journals, official regulatory databases, and the official websites of relevant state institutions and international organizations. The legal material analysis was conducted qualitatively using descriptive-analytical techniques, namely systematically presenting relevant legal norms and concepts, then analyzing them using the

[18]Soerjono Soekanto, "Penelitian Hukum Normatif," Hukum 1, no. 1 (2019): 4.

Jurnal Hukum dan Keadilan

P-ISSN : 0000-0000 Vol. 3 No. 5, August 2026
E-ISSN : 3031-6782
DOI : https://doi.org/10.61942/jhk.v3i5.669
Available : https://jurnalhafasy.com/index.php/jhk

framework of cyber resilience theory and risk governance theory to produce evaluative and prescriptive conclusions. Comparative legal analysis was conducted using a functional method, namely comparing how each legal system addresses the same functional problem, namely how to build systemic resilience against cyber threats, rather than comparing the formal structure of regulations literally.

This study also applies certain operational limitations to ensure the analysis remains focused and in-depth. First, the legal comparison is not intended to produce a crude legal transplant from one jurisdiction to another, but rather to identify functional principles that can be adapted by taking into account the Indonesian socio-legal context, in line with the principles of comparative legal methodology that emphasize the importance of contextual fit over mere formal similarity. Second, this study limits the review period of secondary legal materials to 2020 to 2026 to ensure that the resulting analysis reflects the most recent legal and technological developments, given that the rapidly changing characteristics of cybersecurity require continually updated studies. Third, this study does not conduct empirical testing of the effectiveness of legal implementation in the field. Given the normative nature of the study, the resulting recommendations are prescriptive in nature and require further empirical research to test their effectiveness in practice after implementation.

The validity of the legal materials used is maintained through source triangulation, namely by comparing findings from one source of legal materials with other sources discussing similar topics, to ensure consistency of argumentation and minimize interpretive bias that may arise from a single source. All secondary legal materials cited in this study are articles that have undergone a peer-review process and published in scientific journals indexed in reputable academic databases, so that the credibility of the arguments constructed can be academically accounted for.

RESULTS AND DISCUSSION

Characteristics and Normative Gaps in Indonesian Cybersecurity Law from the Perspective of National Digital Resilience

Indonesia's current cybersecurity legal framework is built on a foundation historically borne of the need to regulate electronic transactions, rather than a strategic awareness of building comprehensive national cyber resilience. Law No. 11 of 2008 concerning Electronic Information and Transactions, subsequently amended by Law No. 19 of 2016 and most recently by Law No. 1 of 2024, was initially designed to provide legal certainty regarding the validity of electronic transactions and digital signatures, as well as to regulate criminal offenses related to illegal access, electronic data manipulation, and the dissemination of unlawful content. The transaction-oriented and criminal-action-oriented nature of this law has structural consequences, namely a lack of regulations regarding proactive obligations for electronic system operators to build systemic system resilience before cyber incidents occur.

The second amendment to the Electronic Information and Transactions Law, enacted through Law Number 1 of 2024, introduces several important adjustments, including harmonization with the Personal Data Protection Law and reaffirming criminal provisions related to hate speech and disinformation. However, these changes do not address the fundamental issue of how the state requires digital infrastructure providers, both government and private, to implement measurable and auditable cyber risk management standards. A review of the European Union and United States cybersecurity legal frameworks compared to the Indonesian context suggests that Indonesia could adopt a more agile and responsive regulatory model, particularly by learning from the regulatory clarity, cross-sectoral engagement, and proactive law enforcement

Jurnal Hukum dan Keadilan

P-ISSN : 0000-0000 Vol. 3 No. 5, August 2026
E-ISSN : 3031-6782
DOI : https://doi.org/10.61942/jhk.v3i5.669
Available : https://jurnalhafasy.com/index.php/jhk

practiced by the United States through its various sectoral cybersecurity frameworks.[19]

The second normative gap lies in the lack of mandatory, standardized, and clearly defined cyber incident reporting obligations. Unlike the European Union's Cyber Resilience Act, which mandates reporting of actively exploited vulnerabilities within twenty-four hours and reporting incidents within seventy-two hours, Indonesia's current legal framework lacks a generally binding incident reporting mechanism across sectors. Presidential Regulation No. 82 of 2022 concerning the Protection of Vital Information Infrastructure does regulate reporting obligations for certain vital information infrastructure sectors, but its scope is still limited to eight designated sectors: government administration, energy and mineral resources, health, finance, communications and informatics, food security, defense, and transportation. Therefore, it does not yet encompass the digital ecosystem horizontally, as does the European Union's approach, which covers all products with digital elements circulating in the market.

This sectoral coverage gap is a serious issue given the cross-sectoral nature of cyber threats and their ability to propagate through complex digital supply chains. A vulnerability in widely used third-party software can impact hundreds or even thousands of organizations across sectors simultaneously, as demonstrated by numerous global cybersecurity incidents in recent years. Studies on Industry 4.0 data security emphasize that contemporary cybersecurity frameworks must be able to accommodate the complexity of digital supply chains that involve multiple stakeholders, from hardware manufacturers and software developers to cloud computing service providers to end users, each with distinct but interconnected security responsibilities.[20] The absence of a horizontal legal framework governing shared responsibilities along the digital supply chain is one of the most pressing gaps that the Cybersecurity and Resilience Bill needs to address.

The third gap relates to institutional issues. The National Cyber and Crypto Agency, established through Presidential Regulation No. 53 of 2017 and strengthened through Presidential Regulation No. 28 of 2021, has a broad mandate, spanning threat detection and incident response to the development of national cybersecurity human resources. However, the legal basis for establishing this agency remains a presidential regulation, not a law, making its constitutional standing more vulnerable to policy changes and lacking robust law enforcement authority compared to similar agencies in other countries established through separate laws. Studies of cybersecurity governance in Pakistan emphasize the importance of integrating regulatory oversight, risk management, and organizational resilience as an inseparable whole, and emphasize that a cybersecurity oversight agency requires a strong legal foundation and clear authority to effectively carry out its cross-sectoral coordinating function.[21] This principle is relevant for Indonesia, considering that strengthening the legal standing of the National Cyber and Crypto Agency through a separate law will provide stronger legitimacy for the agency to carry out its supervisory functions, enforce compliance, and coordinate across ministries and agencies.

The fourth gap lies in the lack of integration of human rights and civil liberties protection principles into Indonesia's cybersecurity legal framework. A review of the Cyber Resilience Act's regulatory approach

[19]L. Nadriana and H. T. Sukmana, "Cybersecurity Policy and Implementation in Indonesia: Current State and Future Directions," Digital Policy, Regulation and Governance 24, no. 3 (2022): 270–285.

[20]M. Toussaint, Sylvère Krima, and Hervé Panetto, "Industry 4.0 Data Security: A Cybersecurity Frameworks Review," Journal of Industrial Information Integration 39 (2024): 100604, https://doi.org/10.1016/j.jii.2024.100604.

[21]Yasir Majeed, Anas Majeed, and Muhammad Tahir Minhas, "Cybersecurity Governance in the Digital Era and IT," Social Science Review Archives (2026), https://doi.org/10.70670/sra.v4i1.1711.

Jurnal Hukum dan Keadilan

P-ISSN : 0000-0000 Vol. 3 No. 5, August 2026
E-ISSN : 3031-6782
DOI : https://doi.org/10.61942/jhk.v3i5.669
Available : https://jurnalhafasy.com/index.php/jhk

confirms that effective cybersecurity regulation should not be viewed solely as a technical instrument, but rather as an instrument that implicitly protects citizens' fundamental rights, including the right to privacy and personal data protection. Therefore, the design of cybersecurity regulations needs to include oversight and accountability mechanisms that prevent the abuse of cybersecurity authority for the purpose of repressing freedom of expression. [22] Similar concerns are relevant to the Indonesian context, given that the experiences of other countries such as Bangladesh have shown that cybersecurity regulations designed without adequate checks and balances have the potential to be misused to stifle citizens' freedom of expression, as reflected in the criticism directed at Bangladesh's Cybersecurity Act, which is considered to retain repressive provisions from previous laws.

In relation to the constitutional context, the study of the constitutionalization of cybersecurity through a comparison of Indonesia and Malaysia within the framework of maqasid al-syariah offers an alternative perspective that places the protection of life (hifz al-nafs), reason (hifz al-'aql), and property (hifz al-mal) as the philosophical basis for cybersecurity regulations in both countries, and emphasizes that harmonization of regional cybersecurity regulations needs to pay attention to the constitutional and socio-religious values that exist in society, rather than simply adopting the regulatory model of developed countries raw.[23] This perspective provides an important lesson that the process of updating Indonesian cybersecurity law cannot be separated from the constitutional values of Pancasila and the 1945 Constitution of the Republic of Indonesia, especially the principle of protecting human rights as regulated in Article 28G paragraph (1) which guarantees the right to a sense of security and protection from the threat of fear, which in the digital context can be interpreted as a constitutional guarantee of individual and collective digital resilience.

The financial services sector is an interesting exception in Indonesia's cybersecurity regulatory landscape, as it already has a relatively more advanced cybersecurity regulatory framework compared to other sectors, through Financial Services Authority Regulation No. 11 of 2022 concerning the Provision of Information Technology by Commercial Banks and various derivative provisions regarding information technology risk management, including mandatory periodic cybersecurity penetration testing and incident response simulations for commercial banks. Similarly, Bank Indonesia has issued regulations regarding payment system security, requiring payment system service providers to implement minimum cybersecurity standards. This sectoral regulatory advancement in the financial services sector can actually serve as a regulatory blueprint for formulating cybersecurity obligations across other sectors, given that the risk management-based approach implemented by the financial services sector aligns with contemporary cybersecurity principles that emphasize periodic testing and recovery readiness, rather than mere administrative compliance. However, this sectoral regulatory advancement has actually highlighted the gap with other sectors that lack comparable regulations, reaffirming the urgency of a horizontal legal framework that can equalize minimum cybersecurity standards across all sectors of society.

With the health sector as one of the most vulnerable vital information infrastructures, studies on the resilience of health systems in the face of digital transformation show that the health sector faces a dual challenge in the form

[22]P. Chiara, "Understanding the Regulatory Approach of the Cyber Resilience Act," European Journal of Risk Regulation 16 (2025): 469–484, https://doi.org/10.1017/err.2025.9.

[23]Farid Al Hadana et al., "Constitutionalizing Cybersecurity: Indonesia–Malaysia Regulatory Convergence through a Maqasid al-Sharia Framework," Journal of Islamic Law on Digital Economy and Business (2026), https://doi.org/10.20885/jildeb.vol1.iss2.art2.

Jurnal Hukum dan Keadilan

P-ISSN : 0000-0000 Vol. 3 No. 5, August 2026
E-ISSN : 3031-6782
DOI : https://doi.org/10.61942/jhk.v3i5.669
Available : https://jurnalhafasy.com/index.php/jhk

of massive digital transformation through electronic medical records and telemedicine, as well as rapidly increasing cyber threats considering that health data is one of the most sensitive and highly valuable types of personal data on the digital black market.[24] This situation is relevant for Indonesia, considering that a number of large-scale health data breaches have occurred, demonstrating that the national health sector does not yet have a cybersecurity regulatory framework on par with the financial sector, which is more strictly regulated by the Financial Services Authority and Bank Indonesia.

From a cybercrime perspective, the study of ransomware crimes and the evaluation of the 2025 Cybersecurity and Resilience Bill in the context of Indonesian defense confirm that harmonization between the Criminal Code, the Electronic Information and Transactions Law, the National Defense Law, and the cybersecurity bill is an absolute prerequisite for protecting the country's essential infrastructure from increasingly sophisticated ransomware threats, including through the establishment of a national cyber defense agency integrated with the country's overall defense structure.[25] This recommendation aligns with the urgent need to expedite the ratification of the Cybersecurity and Resilience Bill, which remains stalled in the legislative process despite having been repeatedly included as a priority in the National Legislation Program since 2019.

A review of the draft Cybersecurity and Resilience Bill shows that it has adopted several key elements of the contemporary cyber resilience paradigm, including provisions on the role of government, a national cybersecurity strategy, governance of digital products, protection of critical information infrastructure, mechanisms for reporting and responding to cyber incidents, and inter-agency coordination. However, the slow pace of ratification of this bill has created a prolonged legal vacuum, amidst the escalating quantity and complexity of cyber threats. This legal vacuum not only impacts national security but also has the potential to undermine investor confidence in Indonesia's digital ecosystem, given that legal certainty is a key factor in investment decisions in the digital technology sector.

The issue of technical standardization also deserves special attention in the Indonesian context. The absence of a mandatory national cybersecurity standard has led domestic businesses to voluntarily and inconsistently adopt international standards, such as ISO/IEC 27001 on information security management systems or the cybersecurity framework developed by the United States National Institute of Standards and Technology, without clear harmonization regarding which standards are officially recognized by national regulators for the purposes of demonstrating legal compliance. This creates a fragmentation of standards, ultimately making it difficult for supervisory authorities to conduct consistent compliance audits across sectors. A study of European cybersecurity standardization confirms that the successful implementation of cybersecurity regulations depends heavily on the existence of a national standards body with a clear mandate to develop and regularly update technical standards, as well as a mechanism for mutual recognition of credible international standards, so that businesses have certainty regarding which standards are required to meet their legal cybersecurity obligations in a jurisdiction.[26] Indonesia, through the National Standardization Agency and the National Cyber and Crypto Agency, needs to expedite the development of Indonesian National Standards

[24]A. García-Pérez et al., "Resilience in Healthcare Systems: Cyber Security and Digital Transformation," Technovation (2022), https://doi.org/10.1016/j.technovation.2022.102583 .

[25]S. M. Sulubara, "Legal Protection Against Cybercrime from Ransomware Attacks and Evaluation of the 2025 Cyber Security and Resilience Bill in Indonesia's Defense," DE LEGA LATA: Jurnal Ilmu Hukum (2025).

[26]Irene Kamara, "European Cybersecurity Standardisation: A Tale of Two Solitudes in View of Europe's Cyber Resilience," Innovation: The European Journal of Social Science Research 37 (2024): 1441–1460, https://doi.org/10.1080/13511610.2024.2349626.

Jurnal Hukum dan Keadilan

P-ISSN : 0000-0000 Vol. 3 No. 5, August 2026
E-ISSN : 3031-6782
DOI : https://doi.org/10.61942/jhk.v3i5.669
Available : https://jurnalhafasy.com/index.php/jhk

specifically in the field of cybersecurity, which are explicitly referred to in the Draft Law on Cybersecurity and Resilience, to create legal certainty for business actors in fulfilling their compliance obligations.

In terms of the structure of criminal law, the study of cybercrime law enforcement in the Indonesian criminal justice system shows that the repressive and post-incident criminal law approach still dominates the national cyber law enforcement framework, while the preventive and restorative approaches have not been adequately integrated into the criminal justice system, so that a reconstruction of the criminal law paradigm is needed that is more adaptive to the evolving characteristics of cybercrime.[27] The limited capacity of law enforcement officers in digital forensics also contributes to structural obstacles, considering that investigators, prosecutors, and judges are required to have adequate technical competence to be able to convincingly prove cybercrimes in court, a competence that is still not evenly distributed throughout Indonesia.

A concrete case study demonstrating the real-world implications of this legal gap can be seen in the data breach, claimed to have been carried out by a hacker under the pseudonym Bjorka, in late 2022. The breach exposed the personal data of millions of Indonesian citizens from various government databases and sparked widespread public outcry. A review of this case demonstrates that the weak inter-agency coordination in responding to the data breach incident, along with the lack of mandatory early notification to the affected public, is a direct consequence of the lack of a cybersecurity legal framework requiring standardized and transparent incident reporting.[28] The Bjorka case serves as a reminder that legal weaknesses are not merely theoretical issues, but have a real impact on citizens' sense of security regarding their personal data, which in turn can erode public trust in the government's digital transformation programs, including the One Data Indonesia program and the digital population identity currently being intensively developed.

The digital economic dimension also reinforces the urgency of reforming Indonesia's cybersecurity law. A study of the paradox of Indonesia's digital economic development shows that the rapid growth of the digital economy sector, which includes e-commerce, digital financial services, and other digital platforms, has not been proportionately matched by an adequate strengthening of the cybersecurity legal foundation, creating a paradox whereby rapid digital economic growth actually increases the aggregate national cyber risk exposure.[29] This paradox emphasizes that cybersecurity law cannot be viewed solely as a national security instrument, but also as a prerequisite for the sustainable growth of the digital economy itself, because investor and consumer confidence in the national digital ecosystem is greatly influenced by perceptions of the level of security and legal certainty in force.

Overall, this sub-chapter demonstrates that Indonesia's cybersecurity legal framework suffers from four major structural gaps: a normative orientation that remains repressive-post-incident rather than preventive-systemic; limited sectoral coverage compared to a horizontal, cross-sectoral approach; the institutional standing of the National Cyber and Crypto Agency that has not been strengthened through a separate law; and the lack of explicit integration of human rights protection

[27]R. F. Rahmat et al., "Classifying Indonesian Cyber Crime Cases under ITE Law Using a Hybrid of Mutual Information and Support Vector Machine," International Journal of Safety and Security Engineering 13, no. 5 (2023), https://doi.org/10.18280/ijsse.130507.

[28]M. Zaki Rizaldi, Rizki Dwi Putra, and Asmak Ul Hosnah, "Analisis Kasus Cybercrime Dengan Studi Kasus Hacker Bjorka Terhadap Pembocoran Data," JUSTITIA Jurnal Ilmu Hukum dan Humaniora 6, no. 2 (2023): 619–627.

[29]Vience Mutiara Rumata and Ashwin Sasongko Sastrosubroto, "The Paradox of Indonesian Digital Economy Development," in E-Business – Higher Education and Intelligence Applications (London: IntechOpen, 2021), https://doi.org/10.5772/intechopen.92140.

Jurnal Hukum dan Keadilan

P-ISSN : 0000-0000 Vol. 3 No. 5, August 2026
E-ISSN : 3031-6782
DOI : https://doi.org/10.61942/jhk.v3i5.669
Available : https://jurnalhafasy.com/index.php/jhk

principles into the design of cybersecurity regulations. These four gaps serve as the starting point for formulating recommendations for legal reform, which will be discussed in the following sub-chapter.

Reorienting the Legal Paradigm Towards Sustainable National Digital Resilience

Based on the identification of normative gaps in the previous subchapter, this article proposes four main recommendations for reorienting Indonesia's cybersecurity legal paradigm to support sustainable national digital resilience in the Fourth Industrial Revolution era.

The first recommendation is to accelerate the ratification of the Cybersecurity and Resilience Bill by strengthening three substantive aspects: the regulation of mandatory cyber risk management obligations for electronic system providers across sectors, the obligation to report cyber incidents with clear and standardized deadlines, and a cybersecurity certification mechanism for digital products and services circulating in the domestic market. A study on strategic planning for cybersecurity governance to support the resilience of national digital infrastructure confirms that the effectiveness of the cybersecurity legal framework is largely determined by the extent to which the regulation can be translated into measurable strategic planning, has clear performance indicators, and involves all stakeholders in a participatory manner in the formulation and implementation process.[30] This strategic planning principle needs to be adopted in the preparation of implementing regulations for the Draft Law on Cyber Security and Resilience, particularly in formulating national cyber resilience indicators that can be measured periodically.

A regulatory model for cyber risk management obligations could adapt the lifecycle-based approach adopted in the European Union's Cyber Resilience Act, which requires manufacturers to implement cybersecurity risk assessments from the product design stage, rather than only after the product is on the market. A review of the Cyber Resilience Act's regulatory approach shows that this obligation substantially serves a dual function: as a cybersecurity instrument and as an instrument for protecting citizens' fundamental rights, as unsafe digital products have the potential to become a means of violating users' privacy and personal security.[31] This product lifecycle-based regulatory model is relevant for Indonesia considering the rapid growth of the Internet of Things in the household, healthcare, and industrial sectors, most of whose products are still imported and not yet subject to adequate domestic cybersecurity standards.

The second recommendation is to strengthen the legal standing and authority of the National Cyber and Crypto Agency through a separate law that explicitly grants compliance oversight authority, technical investigation authority for cyber incidents, and binding coordination authority across ministries and agencies. Studies on cyber resilience in industrial networks confirm that the effectiveness of responses to cyber incidents affecting critical infrastructure depends heavily on the speed of interagency coordination and the availability of a clear governance framework regarding the division of authority between central authorities and infrastructure operators on the ground.[32] Without legally

[30]Ghina Fauziyyah, "Strategic Planning of Cybersecurity Governance in Supporting National Digital Infrastructure Resilience," International Journal of Social Research (2025), https://doi.org/10.59888/insight.v3i5.104.

[31]P. Chiara, "The Cyber Resilience Act: The EU Commission's Proposal for a Horizontal Regulation on Cybersecurity for Products with Digital Elements," International Cybersecurity Law Review 3 (2022): 255–272, https://doi.org/10.1365/s43439-022-00067-6.

[32]Thuraya Alrumaih et al., "Cyber Resilience in Industrial Networks: A State of the Art, Challenges, and Future Directions," Journal of King Saud University – Computer and Information Sciences 35 (2023): 101781, https://doi.org/10.1016/j.jksuci.2023.101781.

Jurnal Hukum dan Keadilan

P-ISSN : 0000-0000 Vol. 3 No. 5, August 2026
E-ISSN : 3031-6782
DOI : https://doi.org/10.61942/jhk.v3i5.669
Available : https://jurnalhafasy.com/index.php/jhk

binding coordination authority, the National Cyber and Crypto Agency will continue to face structural obstacles in carrying out its coordinating function, particularly when dealing with ministries and sectoral institutions that have their own sectoral egos.

Institutional strengthening is relevant not only for the National Cyber and Crypto Agency, but also for the Personal Data Protection Agency, established under the mandate of Law Number 27 of 2022 concerning Personal Data Protection. This agency carries out dual functions interrelated with national cyber resilience: monitoring compliance with personal data protection and handling public complaints regarding alleged personal data breaches, including those arising from cybersecurity incidents. The effectiveness of this agency depends heavily on institutional independence and sufficient resources to carry out its oversight function proactively, rather than merely reacting to incoming complaints. Experience from other countries shows that an effective data protection authority requires strong investigative powers, including the authority to conduct independent compliance audits of large-scale electronic system operators, as well as the authority to impose significant administrative sanctions to create a deterrent effect. Therefore, close coordination between the Personal Data Protection Agency and the National Cyber and Crypto Agency is crucial, given that both agencies essentially address two sides of the same issue: protecting the national digital ecosystem from data threats and misuse.

This institutional strengthening also needs to be accompanied by a systematic increase in the capacity of national cybersecurity human resources. A systematic literature review of cyber resilience measurement in the industrial Internet of Things demonstrates that effective cyber resilience measurement requires a combination of technical indicators, such as post-incident system recovery time, and non-technical indicators, such as human resource capacity and organizational governance maturity, both of which determine an entity's level of cyber resilience.[33] Indonesia needs to develop a national cyber resilience index that integrates both types of indicators, as an instrument for periodically evaluating the effectiveness of national cybersecurity policy implementation, as well as a database for formulating evidence-based policies.

Before moving on to the third recommendation, it is important to emphasize that strengthening the legal and institutional substance as outlined above will only be effective if accompanied by strengthening the periodic monitoring and evaluation mechanisms for the implementation of national cybersecurity policies. Experience in various jurisdictions shows that cybersecurity regulations that are sound on paper often fail to deliver tangible impact due to weak post-implementation evaluation mechanisms, leaving authorities without an adequate database to identify regulatory weaknesses early and make responsive policy adjustments. Therefore, Indonesia's future cybersecurity legal framework should ideally also include the obligation to prepare periodic national cyber resilience evaluation reports, which are submitted to the House of Representatives as a form of public accountability for the effectiveness of implemented cybersecurity policies. This is in line with the principles of good governance, which emphasize transparency and accountability in all public policies, including those in the field of cybersecurity, which has often been viewed as a technical area closed to broad public scrutiny.

The third recommendation is the integration of the cybersecurity legal framework with the artificial intelligence legal framework, given that these two fields are increasingly inseparable in the context of the Fourth Industrial Revolution. A study on the urgency of artificial intelligence regulation in relation to cybersecurity and resilience

[33]M. Lezzi et al., "Measuring Cyber Resilience in Industrial IoT: A Systematic Literature Review," Management Review Quarterly 76 (2025): 1107–1161, https://doi.org/10.1007/s11301-025-00495-8.

Jurnal Hukum dan Keadilan

P-ISSN : 0000-0000 Vol. 3 No. 5, August 2026
E-ISSN : 3031-6782
DOI : https://doi.org/10.61942/jhk.v3i5.669
Available : https://jurnalhafasy.com/index.php/jhk

recommends that artificial intelligence regulations include specific provisions regarding the cybersecurity of artificial intelligence systems, including mandatory algorithm audits, model transparency, and legal accountability mechanisms for automated decisions that impact cybersecurity, as an integral part of a comprehensive artificial intelligence regulatory framework.[34] Indonesia, through the National Strategy for Artificial Intelligence 2020–2045 and the circular on artificial intelligence ethics issued by the Ministry of Communication and Digital, has an initial foundation for integrating the cybersecurity dimension into national artificial intelligence policy, but this foundation is still in the form of ethical guidelines that are not legally binding, so it needs to be upgraded to a more binding legal norm.

The application of machine learning to strengthen cyber resilience in Industry 4.0 systems also opens up new opportunities and legal challenges. Studies on the use of machine learning for cybersecurity resilience in Industry 4.0 emphasize that while this technology offers significantly faster and more accurate threat detection capabilities than conventional methods, its implementation faces significant challenges related to the availability of quality training data, the risk of algorithmic bias, and the need for a clear legal framework regarding legal liability when AI-based systems fail to detect or even misclassify a cyber threat.[35] Indonesia's future cybersecurity legal framework needs to address the issue of legal accountability for the failure of these automated systems, given that more and more of the nation's vital information infrastructure is starting to rely on artificial intelligence-based threat detection systems.

A comprehensive survey of Industry 4.0 security and privacy and beyond shows that the technical challenges of cybersecurity in the Fourth Industrial Revolution era are multidimensional, encompassing security at the device layer, network layer, data layer, and application layer, each of which requires a different risk mitigation approach but must be integrated within a coherent cybersecurity governance framework.[36] This multidimensional complexity emphasizes that cybersecurity law cannot be formulated generically, but rather needs to contain sufficiently detailed technical provisions, both in the form of laws and implementing regulations, to provide clear compliance guidelines for business actors across various layers of the digital ecosystem.

The fourth recommendation is to strengthen international and regional cooperation within the cybersecurity legal framework, particularly through harmonization of standards with the Budapest Convention on Cybercrime, the most widely ratified international legal instrument in the field of cybercrime. Studies on the diffusion of the Budapest Convention indicate that countries that adopt the Budapest Convention's standards, either through formal ratification or substantive harmonization into national law, tend to have more effective cross-border law enforcement cooperation capacity in addressing transnational cybercrime than countries that do not.[37] Although Indonesia has not ratified the Budapest Convention, substantive harmonization of its main principles, particularly regarding the criminalization of

[34]Ahmad Ramli et al., "The Urgency of Regulating Artificial Intelligence in Relation to Cybersecurity and Cyber Resilience," Cogent Social Sciences (2026), https://doi.org/10.1080/23311886.2026.2632977.

[35]Jia Yu, Alexey Shvetsov, and Saeed Hamood Alsamhi, "Leveraging Machine Learning for Cybersecurity Resilience in Industry 4.0," IEEE Access 12 (2024): 159579–159596, https://doi.org/10.1109/ACCESS.2024.3482987.

[36]Gurjot Singh Gaba et al., "A Survey on Security and Privacy of Industry 4.0 and Beyond: Technical Aspects, Use Cases, Challenges, and Research Directions," IEEE Open Journal of the Communications Society 6 (2025): 8865–8929, https://doi.org/10.1109/OJCOMS.2025.3616289.

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

Jurnal Hukum dan Keadilan

P-ISSN : 0000-0000 Vol. 3 No. 5, August 2026
E-ISSN : 3031-6782
DOI : https://doi.org/10.61942/jhk.v3i5.669
Available : https://jurnalhafasy.com/index.php/jhk

illegal access, system disruption, and misuse of devices, has been partially reflected in the Electronic Information and Transactions Law, so that the next step that can be taken is to strengthen the mutual legal assistance mechanism to handle cross-border cybercrime more systematically.

Strengthening ASEAN regional cooperation is also crucial, given the borderless nature of cyber threats. A study of Indonesia's role in shaping cybersecurity and resilience confirms that Indonesia, as the country with the largest internet user population in Southeast Asia, has both a strategic interest and a regional leadership responsibility to promote harmonization of ASEAN's cybersecurity legal framework, including through strengthening threat intelligence sharing mechanisms among member states.[38] This regional leadership aligns with Indonesia's position as the largest digital economic power in the region, which makes Indonesia's national cyber resilience have direct implications for the stability of the regional digital ecosystem as a whole.

From a regulatory economics perspective, an evaluation of the legislative impact of Brazil's national digital security program provides valuable lessons that the design of economic incentives is no less important than the threat of criminal sanctions in encouraging business compliance with cybersecurity standards.[39] Indonesia could consider developing a fiscal incentive scheme or streamlining licensing for businesses that proactively implement nationally recognized cybersecurity certifications, complementing the command-and-control approach that currently dominates the national cybersecurity legal framework. Such an incentive-based approach could also foster a more organic culture of cybersecurity compliance among businesses, rather than compliance driven solely by fear of sanctions.

The reorientation of Indonesia's cybersecurity legal paradigm also requires consideration of the dimensions of social resilience and public digital literacy as a layer of defense that is no less important than formal regulations. National digital resilience is not solely a product of formal legal compliance, but also the result of society's collective awareness of maintaining their own digital security, from vigilance against social engineering to maintaining the confidentiality of digital credentials. Therefore, a comprehensive cybersecurity legal framework needs to include provisions regarding mandatory public education and improving digital literacy as part of a shared responsibility between the government, electronic system providers, and civil society, in line with the principles of participatory and multi-layered cyber governance as demonstrated by the experiences of the various jurisdictions discussed above.

This dimension of digital literacy is becoming increasingly crucial given that the majority of cybersecurity incidents, both in Indonesia and globally, stem from the exploitation of human factors through social engineering techniques, such as phishing and pretexting, rather than purely technical vulnerabilities in systems. This situation demands that the cybersecurity legal framework not only regulates the technical obligations of electronic system operators but also stipulates minimum obligations for educational institutions and government agencies to conduct regular cybersecurity awareness programs for civil servants and the general public. The Ministry of Communication and Digital, through its periodically released national digital literacy index, has recorded a gradual increase in the level of digital literacy among Indonesians. However, this increase needs to be balanced with more concrete legal obligations so that

[38]I Nyoman Aji Suadhana Rai, Dudy Heryadi, and Asep Kamaluddin, "The Role of Indonesia to Create Security and Resilience in Cyber Spaces," Jurnal Politica: Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional 13, no. 1 (2022): 43–66.

[39]Marcos Cícero Santos Wanderlei, "Legislative Impact Assessment of the Brazilian National Digital Security and Resilience Program: A Law and Economics Perspective," REMUNOM (2026), https://doi.org/10.66104/re2nmt33.

Jurnal Hukum dan Keadilan

P-ISSN : 0000-0000 Vol. 3 No. 5, August 2026
E-ISSN : 3031-6782
DOI : https://doi.org/10.61942/jhk.v3i5.669
Available : https://jurnalhafasy.com/index.php/jhk

digital literacy programs are not merely recommendations without clear normative binding force.

In addition to strengthening the demand side through public digital literacy, strengthening the supply side through the development of a domestic cybersecurity industry also needs to be part of a comprehensive legal policy. Indonesia's dependence on foreign cybersecurity products and services creates its own vulnerabilities from a digital sovereignty perspective, given that network traffic data and attack patterns detected by foreign cybersecurity systems are not always fully accessible and analyzeable by national cybersecurity authorities. Therefore, the future cybersecurity legal framework should ideally include incentives for developing domestic cybersecurity research and industry capacity, including through strategic partnerships between the National Cyber and Crypto Agency (BKSDA), universities, and the domestic private sector, as part of a long-term strategy to reduce dependence on foreign cybersecurity technology while building a stronger foundation for national digital resilience.

The fifth, equally important element is strengthening mutual legal assistance mechanisms and cross-border law enforcement cooperation to address transnational cybercrime. A study of strategies to combat cross-border cybercrime through the implementation of mutual legal assistance mechanisms under Minister of Law and Human Rights Regulation No. 12 of 2022 shows that existing mutual legal assistance mechanisms still face bureaucratic obstacles that slow the exchange of electronic evidence across borders, while cybercriminals can move their attack infrastructure instantly across jurisdictions in a matter of minutes.[40] The speed gap between the formal legal process, which tends to be slow, and the very fast digital mobility of cybercriminals requires Indonesia to accelerate the digitalization of the mutual legal assistance process, including through the establishment of a special cross-border emergency communication channel for handling urgent cyber incidents, in line with the practice of a 24/7 network that has been developed within the framework of the Budapest Convention.

The sixth element that needs to be considered is the lessons learned from the multi-layered regulatory approach implemented by the European Union, where the Cyber Resilience Act does not stand alone but operates alongside the second Network and Information Security Directive and the Digital Operational Resilience Act for the financial sector. Studies on European cybersecurity standardization show that the success of this layered approach depends heavily on consistent definitions and taxonomies of cyber risk across applicable legal instruments, thereby avoiding duplication of reporting obligations or compliance confusion for businesses operating across sectors.[41] Indonesia needs to anticipate the risk of similar duplication by ensuring that the Cybersecurity and Resilience Bill, if passed, is designed in harmony with existing sectoral regulations, such as the banking sector cybersecurity provisions issued by the Financial Services Authority and the payment system security provisions issued by Bank Indonesia, so as not to create overlapping compliance obligations that would burden businesses without adding significant cyber resilience value.

In summary, this sub-chapter demonstrates that reorienting Indonesia's cybersecurity legal paradigm toward sustainable national digital resilience requires synergy between four elements: strengthening legal substance through accelerated ratification of the Cyber Security and Resilience Bill with a preventive-systemic orientation;

[40]Nadira Karisma Ramadanti, "Strategi Pemberantasan Cybercrime Lintas Batas: Implementasi Mekanisme Mutual Legal Assistance Berdasarkan Permenkumham Nomor 12 Tahun 2022," Padjadjaran Law Review 12, no. 2 (2024): 184–195.

[41]Irene Kamara, "European Cybersecurity Standardisation: A Tale of Two Solitudes in View of Europe's Cyber Resilience," Innovation: The European Journal of Social Science Research 37 (2024): 1441–1460, https://doi.org/10.1080/13511610.2024.2349626.

Jurnal Hukum dan Keadilan

P-ISSN : 0000-0000 Vol. 3 No. 5, August 2026
E-ISSN : 3031-6782
DOI : https://doi.org/10.61942/jhk.v3i5.669
Available : https://jurnalhafasy.com/index.php/jhk

strengthening the National Cyber and Crypto Agency through a stronger legal foundation; integrating the cybersecurity legal framework with artificial intelligence regulations; and strengthening international and regional cooperation complemented by an economic incentive approach and strengthening public digital literacy. The combination of these four elements is believed to be able to transform Indonesia's cybersecurity legal framework from a reactive and sectoral approach to one that truly supports national digital resilience in a systemic and sustainable manner amidst the acceleration of the Fourth Industrial Revolution.

CONCLUSION

This article concludes that cybersecurity law occupies a central position as a normative foundation for national digital resilience in the era of the Fourth Industrial Revolution, an era marked by the convergence of cyber-physical technologies that expands the structural dependence of the state and society on digital infrastructure, while simultaneously expanding the surface of vulnerability to systemic cyber threats. The current Indonesian cybersecurity legal framework, which is based on the Electronic Information and Transactions Law, the Personal Data Protection Law, and the Presidential Regulation on the Protection of Vital Information Infrastructure, still leaves four main structural gaps, namely a normative orientation that is more repressive-post-incident than preventive-systemic, limited sectoral coverage compared to the horizontal cross-sectoral approach as practiced by the European Union through the Cyber Resilience Act, the institutional position of the National Cyber and Crypto Agency that has not been strengthened through a separate law, and the lack of explicit integration of human rights protection principles into the design of national cybersecurity regulations. To address these gaps, this article recommends a reorientation of the legal paradigm through four integrated strategic steps: accelerating the ratification of the Cybersecurity and Resilience Bill by strengthening cyber risk management obligations, mandatory and standardized incident reporting, and digital product security certification; strengthening the legal standing and authority of the National Cyber and Crypto Agency through a separate law that provides binding oversight and coordination authority; integrating the cybersecurity legal framework with artificial intelligence regulations, given the increasingly inseparable nature of the two fields; and strengthening international and regional cooperation, complemented by an economic incentive approach for voluntary compliance and strengthening public digital literacy as a layer of social defense. These four steps, if implemented in an integrated manner, are believed to be able to transform Indonesia's cybersecurity legal framework from a historically reactive and sectoral approach to a legal framework that systemically supports adaptive, resilient, and sustainable national digital resilience in the face of the ever-evolving dynamics of the Fourth Industrial Revolution.

REFERENCE

Alrumaih, Thuraya, Mohammed Alenazi, Nouf Alsowaygh, Abdulmalik Humayed, and I. Alablani. "Cyber Resilience in Industrial Networks: A State of the Art, Challenges, and Future Directions." Journal of King Saud University – Computer and Information Sciences 35 (2023): 101781. https://doi.org/10.1016/j.jksuci.2023.101781.

Aulianisa, Sarah Safira, and Indirwan. "Critical Review of the Urgency of Strengthening the Implementation of Cyber Security and Resilience in Indonesia." Lex Scientia Law Review (2020). https://doi.org/10.15294/lesrev.v4i1.38197.

Badan Siber dan Sandi Negara. Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara, sebagaimana diubah dengan Peraturan Presiden Nomor 28 Tahun 2021.

Bramantyo, Hutama Arif. "Enhancing Cybersecurity in Indonesia's National Data Center Post-Ransomware Attack."

Jurnal Hukum dan Keadilan

P-ISSN : 0000-0000 Vol. 3 No. 5, August 2026
E-ISSN : 3031-6782
DOI : https://doi.org/10.61942/jhk.v3i5.669
Available : https://jurnalhafasy.com/index.php/jhk

Poster, Syracuse University, 2024. https://surface.syr.edu/eli/257.

Chiara, P. "The Cyber Resilience Act: The EU Commission's Proposal for a Horizontal Regulation on Cybersecurity for Products with Digital Elements." International Cybersecurity Law Review 3 (2022): 255–272. https://doi.org/10.1365/s43439-022-00067-6.

Chiara, P. "Understanding the Regulatory Approach of the Cyber Resilience Act: Protection of Fundamental Rights in Disguise?" European Journal of Risk Regulation 16 (2025): 469–484. https://doi.org/10.1017/err.2025.9.

European Union. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on Horizontal Cybersecurity Requirements for Products with Digital Elements (Cyber Resilience Act). Official Journal of the European Union L 2024/2847, 20 November 2024.

Fauziyyah, Ghina. "Strategic Planning of Cybersecurity Governance in Supporting National Digital Infrastructure Resilience." International Journal of Social Research (2025). https://doi.org/10.59888/insight.v3i5.104.

Gaba, Gurjot Singh, Alparslan Sari, Ismail Butun, Parminder Singh, Andrei Gurtov, and Madhusanka Liyanage. "A Survey on Security and Privacy of Industry 4.0 and Beyond: Technical Aspects, Use Cases, Challenges, and Research Directions." IEEE Open Journal of the Communications Society 6 (2025): 8865–8929. https://doi.org/10.1109/OJCOMS.2025.3616289.

García-Pérez, A., J. Cegarra-Navarro, M. Sallos, Eva Martínez-Caro, and A. Chinnaswamy. "Resilience in Healthcare Systems: Cyber Security and Digital Transformation." Technovation (2022). https://doi.org/10.1016/j.technovation.2022.102583.

Hadana, Farid Al, Tashekal, S. Sukarman, and Farhan Margono. "Constitutionalizing Cybersecurity: Indonesia–Malaysia Regulatory Convergence through a Maqasid al-Sharia Framework." Journal of Islamic Law on Digital Economy and Business (2026). https://doi.org/10.20885/jildeb.vol1.iss2.art2.

Ibitamuno, Pamela Victor. "Legal Frameworks for Cybersecurity in Nigeria – Adapting the Fourth Industrial Revolution." Advances in Multidisciplinary and Scientific Research Journal Publication (2023). https://doi.org/10.22624/AIMS/CSEAN-SMART2023P12.

Irfandi. "The Role of Law Enforcement in Upholding Privacy Regulations to Strengthen National Resilience in the Digital Era." Multidisciplinary Indonesian Center Journal (MICJO) (2026). https://doi.org/10.62567/micjo.v3i1.1790.

Kamara, Irene. "European Cybersecurity Standardisation: A Tale of Two Solitudes in View of Europe's Cyber Resilience." Innovation: The European Journal of Social Science Research 37 (2024): 1441–1460. https://doi.org/10.1080/13511610.2024.2349626.

Le Nguyen, C., and W. Golman. "Diffusion of the Budapest Convention on Cybercrime." Computer Law & Security Review 40 (2021): 105521. https://doi.org/10.1016/j.clsr.2020.105521.

Lezzi, M., A. Corallo, M. Lazoi, and Aldo Nimis. "Measuring Cyber Resilience in Industrial IoT: A Systematic Literature Review." Management Review Quarterly 76 (2025): 1107–1161. https://doi.org/10.1007/s11301-025-00495-8.

Ludvigsen, K., and Shishir Nagaraja. "The Opportunity to Regulate Cybersecurity in the EU (and the World): Recommendations for the Cybersecurity

P-ISSN : 0000-0000 Vol. 3 No. 5, August 2026
E-ISSN : 3031-6782
DOI : https://doi.org/10.61942/jhk.v3i5.669
Available : https://jurnalhafasy.com/index.php/jhk

Resilience Act." arXiv:2205.13196 (2022). https://doi.org/10.48550/arXiv.2205.13196.

Majeed, Yasir, Anas Majeed, and Muhammad Tahir Minhas. "Cybersecurity Governance in the Digital Era and IT: Integrating Regulatory Oversight, Risk Management, and Organisational Resilience in Pakistan." Social Science Review Archives (2026). https://doi.org/10.70670/sra.v4i1.1711.

Malatji, Masike, A. Marnewick, and S. von Solms. "Cybersecurity Capabilities for Critical Infrastructure Resilience." Information & Computer Security 30 (2021): 255–279. https://doi.org/10.1108/ICS-06-2021-0091.

Nadriana, L., and H. T. Sukmana. "Cybersecurity Policy and Implementation in Indonesia: Current State and Future Directions." Digital Policy, Regulation and Governance 24, no. 3 (2022): 270–285.

Peraturan Presiden Republik Indonesia Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital.

Rahmat, R. F., A. H. Aziira, S. Purnamawati, Y. M. Pane, S. Faza, Al-Khowarizmi, and F. Nadi. "Classifying Indonesian Cyber Crime Cases under ITE Law Using a Hybrid of Mutual Information and Support Vector Machine." International Journal of Safety and Security Engineering 13, no. 5 (2023). https://doi.org/10.18280/ijsse.130507.

Rai, I Nyoman Aji Suadhana, Dudy Heryadi, and Asep Kamaluddin. "The Role of Indonesia to Create Security and Resilience in Cyber Spaces." Jurnal Politica: Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional 13, no. 1 (2022): 43–66.

Ramadanti, Nadira Karisma. "Strategi Pemberantasan Cybercrime Lintas Batas: Implementasi Mekanisme Mutual Legal Assistance Berdasarkan Permenkumham Nomor 12 Tahun 2022." Padjadjaran Law Review 12, no. 2 (2024): 184–195.

Ramli, Ahmad, Sigid Suseno, R. Mayana, Ramalinggam Rajamanickam, and Rubben Denova Rohmana. "The Urgency of Regulating Artificial Intelligence in Relation to Cybersecurity and Cyber Resilience." Cogent Social Sciences (2026). https://doi.org/10.1080/23311886.2026.2632977.

Rizaldi, M. Zaki, Rizki Dwi Putra, and Asmak Ul Hosnah. "Analisis Kasus Cybercrime Dengan Studi Kasus Hacker Bjorka Terhadap Pembocoran Data." JUSTITIA Jurnal Ilmu Hukum dan Humaniora 6, no. 2 (2023): 619–627.

Rumata, Vience Mutiara, and Ashwin Sasongko Sastrosubroto. "The Paradox of Indonesian Digital Economy Development." In E-Business – Higher Education and Intelligence Applications. London: IntechOpen, 2021. https://doi.org/10.5772/intechopen.92140.

Santos Wanderlei, Marcos Cícero. "Legislative Impact Assessment of the Brazilian National Digital Security and Resilience Program: A Law and Economics Perspective." REMUNOM (2026). https://doi.org/10.66104/re2nmt33.

Soekanto, Soerjono. "Penelitian Hukum Normatif." Hukum 1, no. 1 (2019): 4.

Sulubara, S. M. "Legal Protection Against Cybercrime from Ransomware Attacks and Evaluation of the 2025 Cyber Security and Resilience Bill in Indonesia's Defense." DE LEGA LATA: Jurnal Ilmu Hukum (2025).

Szpor, G. "The Concept of Cyber Resilience in the European Union Law." Review of European and Comparative Law (2026). https://doi.org/10.31743/recl.19198.

Toussaint, M., Sylvère Krima, and Hervé Panetto. "Industry 4.0 Data Security: A Cybersecurity Frameworks Review." Journal of Industrial Information Integration 39 (2024): 100604. https://doi.org/10.1016/j.jii.2024.100604.

Jurnal Hukum dan Keadilan

P-ISSN : 0000-0000 Vol. 3 No. 5, August 2026
E-ISSN : 3031-6782
DOI : https://doi.org/10.61942/jhk.v3i5.669
Available : https://jurnalhafasy.com/index.php/jhk

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Yu, Jia, Alexey Shvetsov, and Saeed Hamood Alsamhi. "Leveraging Machine Learning for Cybersecurity Resilience in Industry 4.0: Challenges and Future Directions." IEEE Access 12 (2024): 159579–159596. https://doi.org/10.1109/ACCESS.2024.3482987.