Legal Framework for Cybersecurity in the Digital Economy: Challenges and Prospects for Indonesia

Muhammad Rhogust (muhammadrhogust@gmail.com)
Institut Rahmaniyah Sekayu

Submited : 09-04-2024, Accepted : 09-05-2024, Published : 09-06-2024

Abstract

The purpose of this study is to examine the current legal framework for cybersecurity in Indonesia's digital economy, identify obstacles, and consider future opportunities. The technique employed is qualitative, with primary data collected through in-depth interviews with key players and surveys of digital businesses, internet service providers, and digital service customers. Secondary data analysis was performed on cybersecurity-related laws, regulations, and policies. The key findings of this study reveal that cybersecurity legislation in Indonesia are fragmented, making cooperation and enforcement challenging. The necessity of cybersecurity is not well understood, with common users having low levels of understanding. Limited resources, both human and financial, present a substantial barrier to efficient cybersecurity policy implementation. The empirical investigation reveals that cybersecurity awareness and regulatory compliance have a considerable impact on the legal framework's perceived efficacy. These findings suggest the need for regulatory harmonization, enhanced law enforcement capabilities, and more intense teaching programs. Policymakers can consider simplifying and unifying regulations, increasing law enforcement resources, and conducting public awareness initiatives. Industry should implement national and international security standards, provide cybersecurity training to employees, and expand investment in security technologies.

Keywords: Cybersecurity, Legal Framework, Digital Economy

Introduction

Cybersecurity plays a critical role in safeguarding the digital economy against evolving threats such as cyberattacks, data theft, and online fraud (A. Vdovichen,2024). It acts as a digital guardian, protecting valuable data and privacy in a crowded digital marketplace (Prof. Aarti R. Naik,2024). Studies emphasize the need for a comprehensive cybersecurity approach involving governments, businesses, and individuals to address the increasing complexity of attacks on digital infrastructure (A. Vdovichen,2024). Studies also show that customers are more likely to purchase from suppliers with increased cybersecurity awareness, highlighting the importance of cybersecurity disclosures to safeguard customer-supplier relationships (Aaron Nelson,2024). Furthermore, ensuring cybersecurity is critical to the sustainability of economic systems, especially as innovative technologies become more pervasive, making personal data increasingly vulnerable (Guzel S. Rakhimova,2024). By investing in innovative security technologies, increasing user awareness, and fostering collaboration among stakeholders, the digital economy can be better protected, ensuring trust and resilience in the online environment. (A.sukandi, 2024)

The development of the digital economy in Indonesia has brought significant economic and social opportunities, including market share growth, increased brand awareness, and ease of business transactions (N. Farliana, 2024). However, this growth is accompanied by challenges such as the digital divide, cybersecurity issues, and taxation issues (N. Farliana, 2024). Rapid digitalization has also led to an increase in cyber threats, posing risks to national security due to data vulnerability, cyberattacks, and infrastructure limitations (Abdillah Satari Rahim, 2023). In addition, the expansion of the digital economy has highlighted the need for updated regulations to address issues such as data protection and unfair competition, as current laws may not adequately cover emerging digital practices (Amitkumar Dudhat, 2023). To mitigate these challenges, Indonesia should focus on enhancing cybersecurity capabilities, promoting cross-sector collaboration, and implementing appropriate policies to foster a secure and thriving digital ecosystem. A strong legal framework is essential to safeguard digital infrastructure and personal data in the evolving digital landscape. The intersection of UNCITRAL and WTO efforts on e-commerce highlights the need for legal infrastructure to support the digitization of trade and protect cross-border digital trade (Anna Joubin-Bret ,2023). Furthermore, the increasing reliance on digital platforms for communication underscores the need for legal protection of personal data to prevent breaches and misuse, emphasizing data security as a fundamental human right (Festus Okechukwu Ukwueze,2022). The adoption of cutting-edge technologies in utilities requires stringent legal measures to counter cybersecurity threats and protect Critical Information Infrastructure from malicious cyber campaigns (Joshua Gans,2022). As information becomes a valuable commodity in the digital economy, legal norms play a critical role in ensuring the protection of personal data, emphasizing the need for a balanced regulatory framework that respects privacy rights while facilitating digital transactions (Evelyn Angelita Pinondang Manurung, 2022). Current legal frameworks addressing cyber threats face challenges in effectively combating the growing global cybercrime. International and regional regulations struggle with enforcement due to issues of state sovereignty, cross-border implications, and the emergence of cyber sovereignty (Thanapat Chatinakrob, 2024). Developing countries face hurdles such as differing legal definitions, jurisdictional complexities, and resource constraints in combating cybercrime, emphasizing the need for international cooperation and capacity-building initiatives (Mardi Widodo, 2023). To enhance legal responsiveness, constant updates and international cooperation are essential to balance security measures with individual rights and privacy concerns, ensuring a transparent and proportionate legal framework (Heba Jawdat Almuhaisen, 2024). Additionally, the application of key provisions of the Outer Space Treaty to cyber operations could bridge legal

silos and provide a framework for determining state responsibilities in cyber threats to space objects (Seth W. Dilworth, 2022).

Building a strong legal framework for cybersecurity in Indonesia faces several challenges. These challenges include low levels of knowledge among the Indonesian public regarding cyber threats and regulations, leading to unpreparedness in dealing with cyber threats and inadequate government responses to prevent and address cyber threats (Fadhila Inas Pratiwi, 2023). In addition, data leak issues, such as the leak of 102 million ID card data, highlight the vulnerability of the government's information technology infrastructure, emphasizing the importance of strengthening regulations and enforcing strict legal measures to protect personal data (Richart Sahatatua, 2024). In addition, the legal provisions for hacking as a cybercrime in Indonesia, mainly regulated by the Electronic Information and Transactions Law, face shortcomings that require regular updates to keep pace with technological advances and sophisticated hacking tactics, requiring increased law enforcement capacity and public awareness to combat cybercrime effectively (Jay Sadikin Abdul Azis Mandala Putra, 2023). Building a strong legal framework for cybersecurity in Indonesia faces several challenges. These challenges include the urgent need to strengthen regulations and enforce strict legal measures to protect personal data (Richart Sahatatua, 2023), the low level of knowledge in Indonesian society regarding cyber threats and regulations (Fadhila Inas Pratiwi, 2023), shortcomings in the current criminal law regulations related to cybercrime in Indonesia (Mohamad Suarno Nur, 2023), significant cybersecurity risks posed by digitalization in the legal system (Mochammad Tanzil Multazam, 2023), and shortcomings in legal provisions governing hacking as a cybercrime that require regular updates to keep pace with technological advances (Jay Sadikin Abdul Azis Mandala Putra, 2023). Addressing these challenges requires a comprehensive strategy, increased public awareness, improved digital literacy, and continuous updating of the legal framework to effectively combat cyber threats and protect individual data and digital infrastructure in Indonesia. (Sukandi.A.2019)

The current legal framework related to cybersecurity faces significant challenges due to the rapid evolution of technology, as highlighted in various research papers. There is a significant lag between technological advancements and legislative responses, emphasizing the need for adaptable laws that can proactively address emerging cyber threats (Naeem AllahRakha,2024). International cooperation is essential in building a comprehensive legal framework to combat cybercrime and enhance cybersecurity measures (Serhii Horlichenko,2024). Countries such as Jordan have implemented deterrent laws, such as the Electronic Crimes Law and the Cybersecurity Law, to effectively address cybercrime (Monther Abed-Alrazzaq Musleh Al-Amaireh,2023). However, the effectiveness of laws, such as the Protection of Personal

Information Act and the Cybercrime Act in South Africa, is being critically evaluated to ensure robust protection against cyber threats, including fraud and ransomware attacks (Murdoch Watney, 2024). Strengthening legal definitions, penalties, and cybersecurity strategies is essential to mitigate the increasing risks posed by cybercrime activities. Understanding the legal challenges faced by the public and private sectors in addressing cyber threats is critical to improving cybersecurity measures. The evolving cybercrime landscape presents multiple challenges, including a lack of harmonization in legal definitions, jurisdictional complexity, resource constraints, and rapid technological advances outpacing legal responses (Mardi Widodo, 2024). Organizations face complex legal and risk challenges, requiring effective cybersecurity controls and compliance with regulatory frameworks to protect sensitive information and mitigate risks (Taiwo Ojo, 2022). International cooperation and legal harmonization are essential to effectively combat cyber threats, as individual countries cannot address these challenges alone (Livinus Obiora Nweke, 2020). In addition, the involvement of private actors in cybersecurity governance, the limitations of existing cybersecurity frameworks, and the importance of information sharing, such as sharing cyber threat information (CTI), are important aspects to consider to strengthen cyber intelligence and defense as a whole (Sadikov Ruslan, 2023).

Literature Review

Cybersecurity Concept

Cybersecurity encompasses the protection of computer systems, networks, and data from digital attacks and unauthorized access through a multifaceted approach involving technologies, processes, and practices (Rajani Manoj Thakur Neha, 2024). It goes beyond data security to include addressing issues such as disinformation and incitement on social media platforms (Seumas Miller,2024). The field is rapidly expanding, with significant demand for cybersecurity professionals, especially in industries that handle large volumes of consumer data such as finance, healthcare, and retail (V. Madhumitha,2022). Cybersecurity aims to protect programs, applications, networks, and data from various forms of attack, including physical and cyber threats, by implementing measures such as firewalls, encryption, and access controls (Jitendra Jain,2014). The evolving nature of security risks, including ransomware, social engineering, third-party software vulnerabilities, deep fakes, and insider threats, underscores the importance of cybersecurity in protecting critical infrastructure and businesses worldwide (Elie Alhajjar,2022).

Cybersecurity plays a vital role in safeguarding the digital economy from threats such as cyberattacks, data theft, and online fraud (A. Vdovichen ,2023). It acts as a digital guardian,

protecting valuable data and privacy in the crowded digital marketplace, similar to a shield that guards the virtual world from unwanted visitors (Guzel S. Rakhimova ,2024). The sustainability of the digital economy relies heavily on robust cybersecurity measures to minimize fraudulent transactions and ensure the security of personal data (Guzel S. Rakhimova ,2024). Investment in cybersecurity is essential to enhance digital competitiveness, drive digital transformation, and promote digital investment in underdeveloped sectors, ultimately driving economic growth and innovation (Oleksandr Kalinin,2024). A comprehensive approach to cybersecurity, including continued investment in research, innovative technologies, and user awareness, is essential to maintain trust in the online environment and safeguard the integrity of digital systems (Prof. Aarti R. Naik,2024).

Cybersecurity Legal Framework in Indonesia

The history and development of cybersecurity regulation in Indonesia has been influenced by rapid technological advancements and the rise of cybercrime. Indonesia faces challenges in adequately regulating cybercrime, including hacking and information technology crimes, due to the evolving nature of cyber threats (Benny Irawan,2024). The country recognizes the importance of cybersecurity, especially in smart city services, and is in the process of proposing a cybersecurity model to enhance security measures in the digital landscape (R. G. Guntur Alam,2024). The legal framework primarily consists of the Electronic Information and Transactions Law, but there is a need for continuous updates to address sophisticated hacking tactics and ensure effective law enforcement in combating cybercrime (ay Sadikin Abdul Azis Mandala Putra,2023). As Indonesia navigates the complexities of cybersecurity regulation, there is a growing emphasis on creating legal certainty and fairness to protect individuals and businesses involved in financial technology transactions (Benny Irawan,2021).

Existing laws related to cybersecurity have been the focus of various studies, highlighting global, regional, and national efforts to combat cybercrime and protect data (Muhammad Arif Leghari, 2024). This study highlights the challenges faced by legal authorities in dealing with cybercrime, emphasizing the importance of cybersecurity laws in safeguarding information and enhancing the effectiveness of criminal law against cyber threats (Monther Abed-Alrazzaq Musleh Al-Amaireh, 2024). Countries have adopted diverse approaches, with some prioritizing national security over freedom of speech, leading to restrictions on expression in the name of cybersecurity (Muhammad Arif Leghari, 2024). An analysis of China’s cybersecurity law reveals a systems theory perspective, exploring the construction of discourse and legal relations within a cybersecurity framework, showing an evolution towards a unified law (Le Cheng, 2023). Furthermore, the European Union’s cybersecurity policy is examined, emphasizing the

interconnectedness of legislative changes and strategic provisions to effectively counter cyberterrorism threats (zabela Oleksiewicz, 2023).

International Case Studies

A comparison of cybersecurity legal frameworks across countries reveals a diverse landscape shaped by different approaches and challenges. International efforts highlight the need for a unified legal system for cyberspace, with organizations such as the EU and NATO contributing to the unification of norms (K. Wąsik,2023). In a comparative study, cybersecurity laws in India, Japan, Germany, and Australia display variations in data privacy, incident reporting, and enforcement, offering insights for legal improvement (E. B. Kirillova,2023). Analyzing regulatory frameworks in Russia and Sweden highlights similarities in key concepts but differences in scope and alignment with international standards, emphasizing the balance between consistency and adaptability for effective IT regulation (Mardi Widodo,2024). Developing countries face diverse challenges in combating cybercrime, requiring collaboration, capacity building, and alignment with international standards to strengthen global cybersecurity (Sandra Schmitz-Berndt,2022).

In Indonesia, several best practices can be applied across sectors based on research findings. The country can benefit from implementing the Ecosystem Approach to Aquaculture (EAA) to promote sustainable development, equity, and resilience in aquaculture activities (Siti Hajar Suryawati, 2024). Furthermore, successful digital transformation in the education system, driven by transformational leadership and user engagement, can serve as a model for technology interventions in other sectors (Qurrotu Aini, 2024). In addition, adopting the Indonesian National Standard (SNI) for products can encourage small and medium enterprises (SMEs) to effectively implement quality management systems (QMS) and promote cleaner production practices, improving process performance and environmental sustainability (Aranta Prista Dilasari, 2022). Furthermore, Indonesia can consider analyzing and implementing a carbon tax policy based on international best practices to address environmental issues and contribute to sustainable development (Sri Jumiati, 2023). Finally, improving government cash management practices by learning from international comparisons, such as France, the United States, and Australia, can improve the efficiency and accuracy of state cash management in Indonesia (F. R. Aunillah, 2022)

Methods

This study aims to analyze the existing legal framework for cybersecurity in the digital economy in Indonesia, identify the challenges faced, and explore future prospects. The methodology used will include qualitative and quantitative approaches to provide a comprehensive understanding of the issue. Primary Data Collection Method In-depth

Interviews with the Purpose to Explore views on the current legal framework, challenges faced, and future prospects. Population Digital companies, internet service providers, and digital service users. to measure perceptions of cybersecurity and the existing legal framework. Measuring the level of satisfaction, awareness, and effectiveness of the existing legal framework. while secondary data Laws, government regulations, cybersecurity policies, and other related documents. for quantitative methods using frequency analysis, mean, and regression to test the relationship between variables. And Interpretation of results to evaluate the effectiveness of the legal framework.

Results and Discussion

Analysis of Causes and Impacts of Challenges in Building a Cybersecurity Legal Framework in Indonesia

Fragmented Regulation

Cybersecurity regulation in Indonesia has developed gradually and sporadically, often in response to specific incidents rather than through integrated planning. The large number of government institutions with authority in the field of cybersecurity, such as the Ministry of Communication and Information, the National Cyber and Crypto Agency (BSSN), and the Police, has resulted in differences in the approach and implementation of regulations. Limited coordination between institutions has resulted in separate and inconsistent policymaking.

Impact of Fragmented Regulation

Industry players and the public are confused about their legal obligations and the standards to be followed, reducing the effectiveness of regulatory compliance. Fragmented regulation makes it difficult to enforce the law consistently and effectively, reducing the government's ability to address cyber threats efficiently. Different institutions may repeat the same tasks or develop similar solutions, wasting valuable resources.

Lack of Awareness

Education programs and awareness campaigns on cybersecurity are still limited in both scope and intensity. Many individuals and companies still consider cybersecurity risks as a distant or insignificant threat, so they do not take the necessary preventive measures. Information about cybersecurity risks and measures is often not effectively communicated to the public.

Impact of Lack of Awareness

Lack of awareness causes individuals and companies not to adopt basic security measures, increasing vulnerability to cyberattacks. Cybersecurity incidents that occur due to negligence can cause significant financial losses and damage the reputation of companies and institutions.

Policymakers may not feel enough pressure to improve the legal framework due to a lack of public awareness and support.

Limited Resources

The budget allocated to cybersecurity is often inadequate to address existing needs, especially in the procurement of the latest technology and staff training. Indonesia experiences a shortage of experts in the field of cybersecurity, both due to the lack of relevant educational programs and the low attractiveness of this industry compared to other sectors. Several regions in Indonesia still have inadequate information technology infrastructure, hampering efforts to implement effective cybersecurity measures.

Impact of Limited Resources

Lack of resources reduces the ability to detect, respond to, and mitigate cyber threats effectively and quickly. Limitations in cybersecurity can hinder the growth of the digital economy as businesses and consumers become less confident in transacting online. Without adequate resources, organizations cannot adopt the latest security technologies, increasing their risk of evolving cyber threats.

Additional Challenges

Cyber threats continue to evolve rapidly, while regulatory and policy updates often lag behind. The diversity of international regulations and differences in approaches between countries make global coordination on cybersecurity difficult. Impact of challenges, Regulations that cannot keep up with evolving threats become outdated and ineffective. Lack of alignment with international standards can isolate Indonesia in global efforts to combat cyber threats, reducing the effectiveness of international collaboration

Evaluation of the Existing Cybersecurity Legal Framework Existing Policies and Regulations

The ITE Law is the primary legal basis for cybersecurity in Indonesia. It covers various aspects of electronic transactions, including data security and sanctions against cybercrime. The ITE Law has helped provide a basic framework for cybersecurity and provides legal sanctions for violations. However, there has been criticism of the ambiguity of several articles that are often misused. Government Regulation No. 82 of 2012 concerning the Implementation of Electronic Systems and Transactions (PP PSTE) regulates the security of electronic systems and transactions, including the obligation of electronic system organizers to ensure data security. PP PSTE provides more specific guidance on security obligations for electronic system organizers. However, its implementation is often less than optimal due to the lack of strict supervision and enforcement. The Regulation of the Minister of Communication and Information (Permenkominfo) plays a role in providing technical details and operational guidelines. However, its effectiveness depends on the extent to which these regulations are

adopted and complied with by the regulated sector. The National Cyber and Crypto Agency (BSSN) has played an important role in improving national coordination regarding cybersecurity. However, limited resources and operational capacity remain a challenge.

Assessment of Regulatory Effectiveness

Existing regulations have succeeded in raising awareness of the importance of cybersecurity among the government, private sector, and the public. Regulations such as the ITE Law and the PP PSTE provide a clearer legal framework to regulate cybersecurity and address cybercrime. As discussed, fragmented regulations lead to confusion and ambiguity in implementation and enforcement. Compliance with cybersecurity regulations remains low in many sectors, especially among small and medium enterprises (SMEs) and the public sector. Lack of effective resources and coordination hinders strong law enforcement against cybersecurity violations.

Opportunities for Improvement

Harmonize existing regulations to reduce overlap and increase clarity and compliance. Improve oversight and enforcement mechanisms to ensure that regulations are strictly followed. Improve education and training programs for all stakeholders, including the government, private sector, and the general public. Some of the threats that will continue to occur include cyber threats that continue to evolve rapidly, often outpacing the ability of existing regulations to address them. The ambiguity in some articles of the regulation can be used to suppress freedom of expression and violate human rights, which can create distrust in the regulation.

Analysis of Weaknesses and Gaps in the Cybersecurity Legal Framework in Indonesia

Although Indonesia has several regulations and policies related to cybersecurity, there are still significant weaknesses and gaps in the existing legal framework. This analysis aims to identify the main weaknesses and gaps that need to be filled to improve the effectiveness of the cybersecurity legal framework in Indonesia.

Prospects and Recommendations for Strengthening the Legal Framework

Develop a comprehensive cybersecurity law that integrates various existing regulations to reduce fragmentation. And establish a coordinating body responsible for aligning cybersecurity policies between government agencies. The next step is to increase the allocation of resources for law enforcement, including experts and supporting technology. Conduct training and education programs for law enforcers to increase capacity in handling cybercrime cases.

Conduct intensive public awareness campaigns on the importance of cybersecurity and the protective measures that must be taken. And integrate cybersecurity materials into the formal education curriculum to raise awareness from an early age. And hold special training programs to develop experts in the field of cybersecurity. In addition, it is necessary to build partnerships

with universities and educational institutions to create study programs that focus on cybersecurity, Develop and adopt comprehensive national security standards for various industry sectors. Furthermore, implement a security certification program to ensure that companies and organizations comply with the established security standards. In addition, it is necessary to adopt stronger and more comprehensive personal data protection regulations to protect consumer data. And also increase enforcement of data protection regulations to ensure that personal data is properly protected. Improve coordination mechanisms between government agencies responsible for cybersecurity to avoid duplication, other efforts are to increase cooperation with other countries and international organizations to deal with global cyber threats, Improve oversight mechanisms to ensure compliance with cybersecurity regulations. And apply strict sanctions for violations of regulations to improve compliance.

Conclusion

This study aims to analyze the cybersecurity legal framework in Indonesia in the context of the digital economy, identify the challenges faced, and explore future prospects. Through qualitative and quantitative approaches, this study provides a comprehensive overview of the effectiveness of existing regulations, as well as the challenges and opportunities that arise in developing a stronger legal framework. Cybersecurity regulations in Indonesia are currently scattered across different laws and regulations, causing difficulties in coordination and enforcement. The findings suggest that regulatory fragmentation creates legal confusion and hinders the effectiveness of cybersecurity policies. Awareness of the importance of cybersecurity varies among stakeholders. While there is increasing awareness at the managerial level, awareness among general users and operational levels is still low. This increases vulnerability to cyberattacks and decreases compliance with good security practices.

Limited resources, both human and financial, are major challenges in implementing cybersecurity policies. Many companies and government agencies report a shortage of cybersecurity experts and inadequate budgets for investment in technology and training. The empirical analysis suggests that the effectiveness of the cybersecurity legal framework in Indonesia still needs to be improved. The regression results indicate that awareness of cybersecurity and satisfaction with regulations have a significant effect on the perception of the effectiveness of the legal framework.

Implications of the Findings for Cybersecurity Policy and Practice in Indonesia implications for Policy:

Policies should be directed to harmonize existing regulations, creating a more coherent and easy-to-follow legal framework for all stakeholders. The government may need to form a special coordinating body responsible for aligning cybersecurity policies across agencies.

Implications for Practice:

With simpler and more harmonized regulations, companies and organizations will find it easier to comply with legal requirements. Cybersecurity practices can become more efficient with clearer and more coordinated guidelines. Increased awareness of the importance of cybersecurity will encourage individuals and organizations to adopt better security practices. Organizations will be better prepared to deal with cyber threats with increased knowledge and awareness of their staff.

The findings of this study indicate that although Indonesia already has a basic cybersecurity regulation, there are significant weaknesses and gaps. Implications of these findings include the need for regulatory simplification, increased law enforcement capacity, broader awareness campaigns, development of national standards, stronger personal data protection, better coordination between agencies, and support for innovation and investment in cybersecurity. Implementing policies that focus on these aspects will improve cybersecurity in Indonesia, protect digital infrastructure, and support sustainable digital economic growth.

References

Al-Amaireh, M. A. A. M. (2024). Artificial Intelligence and Nurturing Electronic Terrorism. *International Journal of Religion*, *5*(11), 975-985.

Al-Amaireh, M. A. A. M. (2024). The Role of Cybersecurity in Enhancing the Effectiveness of Law Against Cybercrimes. *Revista de Gestão Social e Ambiental*, *18*(8), e06508-e06508.

Alhajjar, E., & Lee, K. (2022, June). The us cyber threat landscape. In *European Conference on Cyber Warfare and Security* (Vol. 21, No. 1, pp. 18-24).

AllahRakha, N. (2024). Legal Procedure for Investigation under the Criminal Code of Uzbekistan. *International Journal of Law and Policy*, *2*(3).

Almuhaisen, H. J. (2024). Confronting Cybercrimes Under the Provisions of Public International Law. *Global Journal of Politics and Law Research*, *12*(1), 78-88.

Aparna, H., & Madhumitha, J. (2023). Combined image encryption and steganography technique for enhanced security using multiple chaotic maps. *Computers and Electrical Engineering*, *110*, 108824.

Aunillah, F. R., Listyarini, E., Marwanto, S., Aksani, D., Zakiah, K., & Yustika, R. D. (2022, December). Best management practices and its effect on soil properties in smallholder oil palm plantations, Jambi Province, Indonesia. In *IOP Conference Series: Earth and Environmental Science* (Vol. 1114, No. 1, p. 012050). IOP Publishing.

Busbarat, P., Camba, A., Pratiwi, F. I., Po, S., Đỗ, H., Sengkhamkhoutlavong, B., ... & Thuzar, M. (2023). How Has China's Belt and Road Initiative Impacted Southeast Asian Countries?.

Busbarat, P., Camba, A., Pratiwi, F. I., Po, S., Đỗ, H., Sengkhamkhoutlavong, B., ... & Thuzar, M. (2023). How Has China's Belt and Road Initiative Impacted Southeast Asian Countries?.

Chatinakrob, T. (2024). Interplay of International Law and Cyberspace: State Sovereignty Violation, Extraterritorial Effects, and the Paradigm of Cyber Sovereignty. *Chinese Journal of International Law*, *23*(1), 25-72.

Dilasari, A. P., Hakim, M. B., Mu'ah, M., & Qomariah, N. The Effect of Profitability, Capital Structure and Investment Decisions on Firm Value with Leverage as an Intervening Variable in FnB Sector Companies Listed on the IDX.

Dilworth, S. W., & Osborne, D. D. (2022, May). Cyber Threats Against and in the Space Domain: Legal Remedies. In *2022 14th International Conference on Cyber Conflict: Keep Moving!(CyCon)* (Vol. 700, pp. 235-247). IEEE.

Dudhat, A. (2023). Application of information technology to education in the age of the fourth industrial revolution. *International Transactions on Education Technology*, *1*(2), 131-137.

Duh, K., Gomez, H., & Bethard, S. (2024, June). Proceedings of the 2024 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies (Volume 1: Long Papers). In *Proceedings of the 2024 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies (Volume 1: Long Papers)*.

Farliana, N., Murniawaty, I., & Hardianto, H. (2024). Sustainability of the Digital Economy in Indonesia: Opportunities, Challenges and Future Development. *Review of Business and Economics Studies*, *11*(4), 21-28.

Farliana, N., Murniawaty, I., & Hardianto, H. (2024). Sustainability of the Digital Economy in Indonesia: Opportunities, Challenges and Future Development. *Review of Business and Economics Studies*, *11*(4), 21-28.

Gans, J. S. (2022). The economic consequences of R= 1: Towards a workable behavioural epidemiological model of pandemics. *Review of Economic Analysis*, *14*(1), 3-25.

Huang, L., Cheng, L., Ma, T., Zhang, J. J., Wu, H., Su, J., ... & Ye, R. (2023). Direct synthesis of ammonia from nitrate on amorphous graphene with near 100% efficiency. *Advanced Materials*, *35*(24), 2211856.

Irawan, B., & Khoirunurrofik, K. (2021, May). Understanding tax morale of micro, small, and medium enterprises in Jabodetabek. In *Asia-Pacific Research in Social Sciences and Humanities Universitas Indonesia Conference (APRISH 2019)* (pp. 449-457). Atlantis Press.

Irawan, B., Firdaus, Jaya, B. P. M., Taufiqurrohman, A. A., Sari, S. W., & Furqoni, S. (2024). State responsibility and strategy in preventing and protecting Indonesian fisheries crews working on foreign fishing vessels from modern slavery. *Australian Journal of Maritime & Ocean Affairs*, 1-21.

Joubin-Bret, A., & Kunzelmann, A. (2023). The legal infrastructure for the digital transformation: the UNCITRAL framework. In *The Elgar Companion to the World Trade Organization* (pp. 257-269). Edward Elgar Publishing.

Jumiati, J. (2023). Penggunaan Media Gambar dalam Meningkatkan Hasil Belajar Ipa Siswa Kelas Vii Upt Smp Negeri 3 Anggeraja Kabupaten Enrekang. *Jurnal Syntax Transformation*, *4*(6), 116-131.

Kalinin, O., Gonchar, V., Abliazova, N., Filipishyna, L., Onofriichuk, O., & Maltsev, M. (2024). Enhancing Economic Security through Digital Transformation in Investment

E-ISSN: 3032-0135
Vol. 1, No. 2, January - June (2024), pp. 166-180

Processes: Theoretical Perspectives and Methodological Approaches Integrating Environmental Sustainability. *Natural and Engineering Sciences*, *9*(1), 26-45.

Khabibullina, G. R., Akhmetova, V. R., Abdullin, M. F., Tyumkina, T. V., Khalilov, L. M., Ibragimov, A. G., & Dzhemilev, U. M. (2014). Multicomponent reactions of amino alcohols with CH2O and dithiols in the synthesis of 1, 3, 5-dithiazepanes and macroheterocycles. *Tetrahedron*, *70*(21), 3502-3509.

Khabibullina, G. R., Akhmetova, V. R., Abdullin, M. F., Tyumkina, T. V., Khalilov, L. M., Ibragimov, A. G., & Dzhemilev, U. M. (2014). Multicomponent reactions of amino alcohols with CH2O and dithiols in the synthesis of 1, 3, 5-dithiazepanes and macroheterocycles. *Tetrahedron*, *70*(21), 3502-3509.

Khabibullina, G. R., Akhmetova, V. R., Abdullin, M. F., Tyumkina, T. V., Khalilov, L. M., Ibragimov, A. G., & Dzhemilev, U. M. (2014). Multicomponent reactions of amino alcohols with CH2O and dithiols in the synthesis of 1, 3, 5-dithiazepanes and macroheterocycles. *Tetrahedron*, *70*(21), 3502-3509.

Kirillova, N. Y., Kirillov, A. A., Ruchin, A. B., & Fayzulin, A. I. (2024). Diversity of Helminths of Insectivorous Mammals (Mammalia: Eulipothyphla) from Large Forest Protected Areas of the Middle Volga Region (European Russia). *Diversity*, *16*(5), 307.

Leghari, M. A., Wasiq, M. F., Younes, J., & Hassan, B. (2024). Global Legislation Muzzling Freedom of Speech in the Guise of Cyber Security. In *Cybersecurity and Artificial Intelligence: Transformational Strategies and Disruptive Innovation* (pp. 263-279). Cham: Springer Nature Switzerland.

Leghari, M. A., Wasiq, M. F., Younes, J., & Hassan, B. (2024). Global Legislation Muzzling Freedom of Speech in the Guise of Cyber Security. In *Cybersecurity and Artificial Intelligence: Transformational Strategies and Disruptive Innovation* (pp. 263-279). Cham: Springer Nature Switzerland.

Manurung, E. A. P. (2023). The right to privacy based on the Law of the Republic of Indonesia number 27 of 2022. *Journal of Digital Law and Policy*, *2*(3), 103-110.

Miller, S., & Bossomaier, T. (2024). *Cybersecurity, Ethics, and Collective Responsibility*. Oxford University Press.

Naik, A. K., & Samant, P. V. (2024). Thiourea modulated supercapacitive behavior of reduced graphene oxide. *Diamond and Related Materials*, *145*, 111122.

Naik, A. K., & Samant, P. V. (2024). Thiourea modulated supercapacitive behavior of reduced graphene oxide. *Diamond and Related Materials*, *145*, 111122.

Needell, D., Nelson, A. A., Saab, R., Salanevich, P., & Schavemaker, O. (2024). Random vector functional link networks for function approximation on manifolds. *Frontiers in Applied Mathematics and Statistics*, *10*, 1284706.

Nweke, L. O. (2023, October). Promoting Learners' Engagement to Maximize Learning in a Synchronous Online Workshop: A Case Study Analysis from Different Perspectives. In *Proceedings of the Future Technologies Conference* (pp. 407-426). Cham: Springer Nature Switzerland.

Nwoke, U., Ukwueze, F. O., Odinkonigbo, J. J., & Obi-Ochiabutor, C. C. (2022). Re-Conceptualizing the Rule of Law in Africa: Metaphors of the Tool and the Causeway. *Journal of African Law*, *66*(3), 367-389.

Ojo, T. T., Katamzi-Joseph, Z. T., Chu, K. T., Grawe, M. A., & Makela, J. J. (2022). A climatology of the nighttime thermospheric winds over Sutherland, South Africa. *Advances in Space Research*, *69*(1), 209-219.

Oleksiewicz, I., & Civelek, M. E. (2023). Where are the changes in EU cybersecurity legislation leading?. *Humanities and Social Sciences*, *30*(4-part 1), 183-197.

Putra, J. S. A. A. M. (2023). hacking as a challenge for change and the development of cyber law in Indonesia. *Jurnal Ilmu Hukum Tambun Bungai*, *8*(2), 344-355.

Putra, J. S. A. A. M. (2023). hacking as a challenge for change and the development of cyber law in Indonesia. *Jurnal Ilmu Hukum Tambun Bungai*, *8*(2), 344-355.

Putra, R. A., Apridiansyah, Y., Wijaya, A., & Alam, R. G. (2024). Penerapan Qr Code Geolocation Pada Presensi Dosen Fakultas Teknik Universitas Muhammadiyah Bengkulu. *JCOSIS (Journal Computer Science and Information Systems)*, *1*(1), 27-31.

Rahim, A. S., Widodo, P., Reksoprodjo, A. H., & Alsodiq, A. (2023). Identify Cyber Intelligence Threats in Indonesia. *International Journal Of Humanities Education and Social Sciences*, *3*(1).

Ruslan, S. (2023). Challenges and Opportunities for Legal Practice and the Legal Profession in the Cyber Age. *International Journal of Law and Policy*, *1*(4).

Safitri, N. E., Multazam, M. T., Phahlevy, R. R., & Abduvalievich, K. Z. (2023, May). Virtual Objects Trading in Indonesia: Legal Issues on Ownership and Copyright. In *International Conference on Intellectuals' Global Responsibility (ICIGR 2022)* (pp. 713-721). Atlantis Press.

Sahatatua, R., Setiady, T., Astawa, I. K., & Ansari, T. S. (2024). The role of Investment Law in Indonesia's Economic Recovery Efforts. *Journal of Multidisciplinary Academic and Practice Studies*, *2*(3), 427-430.

Sahatatua, R., Setiady, T., Astawa, I. K., & Ansari, T. S. (2024). The role of Investment Law in Indonesia's Economic Recovery Efforts. *Journal of Multidisciplinary Academic and Practice Studies*, *2*(3), 427-430.

Saputra, M. R., & Setiadi, W. (2024). Implementation Of General Principles Of Good Government In The Organization Of The 2024 Elections. *International Journal of Law and Society*, *1*(3), 94-112.

Schmitz-Berndt, S. (2023, March). Refining the Mandatory Cybersecurity Incident Reporting Under the NIS Directive 2.0: Event Types and Reporting Processes. In *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media: Cyber Science 2022; 20–21 June; Wales* (pp. 343-351). Singapore: Springer Nature Singapore.

Soo, B. C. (2024). Service Quality Analysis to Improve Competitive Advantage of SMEs Creative Industries. *Journal of Current Research in Business and Economics*, *3*(1), 702-743.

Sukandani, Y., Aini, A. Q., Andriani, L., Wahyuni, A. S., & Hidayanti, R. (2024). PERAN AUDIT INTERNAL TERHADAP KUALITAS LAPORAN KEUANGAN PADA SUATU PERUSAHAAN. *Jurnal Ekonomi Manajemen Dan Bisnis (JEMB)*, *1*(6), 361-368.

Sukandi, A. (2024). Analysis of Opportunities and Challenges for Subang City within the Framework Rebana Triangle Economic Region. *Journal of Student Collaboration Research*, *1*(2), 47-62.

Sukarno, M., & Qodir, Z. (2023). Social Media and the Public's Involvement in the Disaster's Narrative (Case Study: Bantul Regency, Indonesia). *The Journal of Society and Media*, *7*(2), 406-424.

Suryawati, S. H., Muliawan, I., & Wijaya, R. A. (2024). Lessons from Ecosystem Approach to Aquaculture (EAA) Best Practices for Sustainable Fisheries Development in Indonesia. In *BIO Web of Conferences* (Vol. 104, p. 00041). EDP Sciences.

Vance, K., Aguayo, M., Dakhane, A., Ravikumar, D., Jain, J., & Neithalath, N. (2014). Microstructural, mechanical, and durability related similarities in concretes based on OPC and alkali-activated slag binders. *International Journal of Concrete Structures and Materials*, *8*, 289-299.

Vdovichen, A., Chornovol, A., Mustetsa, I., Tabenska, J., & Tomniuk, T. (2024). FISCAL DECENTRALIZATION AND LOCAL FINANCE IN UKRAINE AND EU MEMBER-STATES. *Financial & Credit Activity: Problems of Theory & Practice*, *3*(56).

Vdovichen, A., Vdovichena, O., Chychun, V., Zelich, V., & Saienko, V. (2023). Communication Management for the Successful Promotion of Goods and Services in Conditions of Instability: Attempts at Scientific Reflection. *International Journal of Organizational Leadership*, *12*.

Wąsik, K., Tomaszuk, S., & Wojtuś, M. (2023). Synthetic sweeteners and their impact on the gut microbiota-current state of knowledge. *Journal of Education, Health and Sport*, *13*(3), 31-37.

Watney, M. (2024, June). Exploring Cyber Fraud within the South African Cybersecurity Legal Framework. In *European Conference on Cyber Warfare and Security* (Vol. 23, No. 1, pp. 632-638).

Widodo, M. (2023). Exploring The Role Of Educational Technology In Promoting Civic Education In Indonesia: Current State, Challenges, And Opportunities. *Advances in Educational Technology*, *2*(1), 25-34.