The 7th Open Society Conference (OSC) 2025
Faculty of Law, Social and Political Science
Universitas Terbuka
DOI: 10.33830/osc.v3i1.7023 / ISSN: 3032-2227

Legal and Technological Approaches to Cybercrime Risk Mitigation: A Case Study of Cyber Law and Cybersecurity Implementation in Southeast Asia

Seri Mughni Sulubara[1], Virdyra Tasril[2], Nurkhalisah[1]
[1] Lecturer Law Program, Department of Law, Muhammadiyah Mahakarya Aceh University, Bireun, Indonesia
[2] Lecturer Software Engineering Technology Program, Medan State Polytechnic, Medan, Indonesia
e-mail: serimughni@ummah.ac.id

Abstract

This study examines the integration of legal and technological approaches in mitigating the risks of cybercrime, with a focus on the implementation of cyber law regulations and cybersecurity technology in the Southeast Asian region. The study uses normative research methods and case studies, examining various legal policies, regulations, and technological security practices in ASEAN countries. The research findings indicate that the increasing threat of cybercrime necessitates the harmonization of cross-border legal regulations and the implementation of adaptive and collaborative cybersecurity technologies. However, there are significant challenges related to the imbalance in technological capacity and law enforcement among countries, as well as limitations in regional coordination. The study emphasizes the importance of synergy between a strong legal framework, enhanced technical capacity, and inter-state cooperation to create a secure and resilient digital ecosystem against cybercrime threats. Strategic recommendations are provided to strengthen policy harmonization, develop cybersecurity infrastructure, and enhance awareness and capacity among law enforcement agencies in Southeast Asia.

Keywords: *Legal and Technological Approaches, Cybercrime Risk Mitigation, Cyber Law, Cybersecurity, Southeast Asia.*

INTRODUCTION

The rapid development of information and communication technology in the digital age has provided various benefits for individuals, companies, and governments around the world. However, this progress has also brought new challenges in the form of increasingly complex and cross-border cybercrime [1]. Cybercrime, such as data theft, online fraud, malware attacks, and system hacking, can threaten national security, harm the economy, and reduce public trust in the use of digital technology [2]. Countries in the Southeast Asian region are known for their highly dynamic digital growth. However, the high penetration of technology is accompanied by an increase in cybercrime risks. To address these challenges, a comprehensive approach is needed, namely the integration of legal regulations (cyber law) and the implementation of cybersecurity technology [3]. Cyber law serves as the legal foundation for preventing and enforcing laws against cybercrime, while technological solutions are essential tools for protecting data and information systems from various threats [4].

DOI: 10.33830/osc.v3i1.7023 / ISSN: 3032-2227

The implementation of cyber law and cybersecurity technology in Southeast Asia faces several challenges, such as differences in regulations between countries, human resource capacity, and international collaboration in dealing with cross-border cyber attacks [5]. Case studies in this region are important to assess the effectiveness of the implementation of these two approaches and to find the best solutions for mitigating cybercrime risks in an increasingly borderless digital era. The digital revolution that has swept the world has brought significant transformations to various sectors of life, from the economy and government to social interactions. Southeast Asia is among the region most actively leveraging digital technology advances, with rapid growth in internet users and the adoption of digital systems in both the public and private sectors [6], [7], [8]. While this brings great opportunities, it also increases exposure to increasingly complex and damaging cybercrime threats [9], [10], [11].

Cybercrime practices in this region are not only growing in terms of quantity such as phishing, financial fraud, and ransomware cases but also in the quality of attacks targeting strategic objectives, including critical infrastructure and public data [12]. This phenomenon has triggered an urgent need for comprehensive protection. For this reason, a comprehensive approach based on cyber law and cybersecurity technology has become crucial in mitigating the risks of cybercrime [2]. On the one hand, cyber law must be able to provide a clear legal framework, strengthen law enforcement, and deter perpetrators. On the other hand, strengthening cybersecurity plays a vital role in technically blocking and countering various cyber threats, ranging from early detection systems, vulnerability management, to incident response [13].

However, Southeast Asia faces a number of challenges in implementing these two approaches. There are disparities in the formulation of regulations, imbalances in institutional capacity and human resources, and weak cross border coordination in dealing with cross-border cybercrime [1]. Cooperation and harmonization of security standards and cyber law regulations at the regional level have become an important agenda amid increasing vulnerability. Therefore, this study examines case studies on the implementation of cyber law and cybersecurity in Southeast Asia to explore the effectiveness of legal and technological approaches in reducing cybercrime risks, while identifying challenges and opportunities for strengthening inter-country collaboration. As such, this study is expected to provide a strategic foundation for formulating adaptive policies to address the dynamics of cybercrime in the digital age [14].

METHOD

Legal and Technological Approaches to Cybercrime Risk Mitigation: A Case Study of Cyber Law and Cybersecurity Implementation in Southeast Asia, which refers to normative and qualitative research practices in the study of cyber security law and technology in the Southeast Asian region using qualitative research methods with a normative legal approach and case studies. This method was chosen to explore the legal and technological aspects of cybercrime risk mitigation in Southeast Asia in a comprehensive and detailed manner [15]. This approach focuses on the study of applicable legislation (cyber law) in Southeast Asian countries, as well as relevant international policies and legal instruments. The main data was obtained from literature studies in the form of primary legal documents such as national laws, government regulations, international agreements, as well as secondary materials in the form of scientific literature, policy reports, and official documents related to cybersecurity. The analysis was conducted using a deductive method to assess the suitability, strengths, and weaknesses of regulations and their

DOI: 10.33830/osc.v3i1.7023 / ISSN: 3032-2227

implementation at the regional level. In Southeast Asia, some of the main laws that were the focus of the analysis include:

1. Indonesia: Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law), which was later updated by Law No. 19 of 2016. This law serves as the legal basis for handling cybercrime in Indonesia, although there are still challenges in law enforcement and personal data protection.
2. Singapore: The Computer Misuse Act, considered one of the most comprehensive cyber regulations in the region, regulates illegal acts involving computers and networks.
3. Malaysia: The Computer Crimes Act 1997 and the Personal Data Protection Act 2010 specifically regulate computer crimes and personal data protection.
4. Thailand: The Computer Crime Act, last revised in 2017, and the Personal Data Protection Act 2019, which focus on national cybersecurity and digital data protection.

Data collection was conducted using library research and documentary research techniques to obtain relevant, valid, and up-to-date information. The use of official sources from government and regional ASEAN institutions, such as the Indonesian National Cyber and Crypto Agency (BSSN) and the ASEAN Cybersecurity Cooperation Strategy (ACCS), served as important references in this study. Data analysis was conducted using qualitative methods, including content analysis and comparative analysis across countries. The analysis focuses on the effectiveness of legal policies, the alignment of regulations with cybersecurity technology practices, as well as the barriers and opportunities for regional collaboration. The results of the analysis are directed toward formulating policy recommendations and adaptive legal-technology integration strategies in Southeast Asia. This method follows the practices of normative legal research in the field of cybersecurity and information security technology studies, as used in related research on ASEAN and cybersecurity [16].

RESULTS AND DISCUSSION

The integration of cyber law and cybersecurity technology has become an appropriate approach to mitigating the risks of cybercrime [17]. Cyber law provides a legal framework that enables law enforcement, the establishment of norms, and sanctions for perpetrators of cybercrime, while technology enables rapid detection and response to technical threats [18]. The example of Singapore shows that comprehensive legislative policies and good technology implementation can create a robust cybersecurity system. On the other hand, Indonesia and several other countries still face significant obstacles, such as weak law enforcement, lack of cross-border regulatory harmonization, and disparities in human resource capacity and technological infrastructure. This shows that legal and technological approaches must be supported by institutional capacity building and closer cooperation between countries to achieve effective risk mitigation.

Cybercrime is cross-border in nature, so national measures are not sufficient. Regional cooperation is crucial for exchanging threat information, coordinating incident responses, and establishing uniform regulatory standards [19]. ASEAN mechanisms are showing progress, but

DOI: 10.33830/osc.v3i1.7023 / ISSN: 3032-2227

further strengthening is needed to make policy execution more tangible and impactful. This study recommends updating legislation to adapt to technological dynamics, increasing training and providing human resources with expertise in cybersecurity, accelerating regulatory harmonization at the regional level, and investing more in resilient technology infrastructure [20]. Cyber law enforcement also needs to be strengthened with digital forensic technology and more intensive international cooperation [21]. In Southeast Asia, some of the main laws that are the focus of analysis include [22]:

1. Indonesia: Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law), which was later updated by Law No. 19 of 2016. This law serves as the legal basis for handling cybercrime in Indonesia, although there are still challenges in law enforcement and personal data protection [23].
2. Singapore: The Computer Misuse Act, considered one of the most comprehensive cyber regulations in the region, regulates illegal acts involving computers and networks.
3. Malaysia: The Computer Crimes Act 1997 and the Personal Data Protection Act 2010 specifically regulate computer crimes and personal data protection.
4. Thailand: The Computer Crime Act, last revised in 2017, and the Personal Data Protection Act 2019, which focus on national cybersecurity and digital data protection.

Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law), which was amended by Law No. 19 of 2016, is the main legal basis for handling cybercrime in Indonesia [24]. However, the implementation of this law faces a number of significant challenges in law enforcement and personal data protection [25]. Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE Law), which has been updated with Law No. 19 of 2016, is the main legal basis for handling cybercrime in Indonesia [26]. This law regulates various aspects of electronic information, electronic transactions, and legal protection for electronic documents and signatures. The purpose of this law is to provide legal certainty, benefits, caution, and encourage the optimal and responsible use of information technology [27].

Singapore's Computer Misuse Act (CMA) is one of the most comprehensive cyber regulations in Southeast Asia, regulating various illegal acts related to the use of computers and networks. The CMA was created to protect computer materials from unauthorized access and modification that could cause harm, as well as to prevent the misuse of national digital identities [28]. The main laws in Malaysia governing computer crimes are the Computer Crimes Act 1997 (CCA 1997) and, for the protection of personal data, the Personal Data Protection Act 2010 (PDPA 2010). The CCA 1997 regulates various crimes related to the misuse of computers and networks, including:

1. Unauthorized access to computer material or data with intent (e.g., hacking).
2. Unauthorized modification of computer content (changing data or programs without permission).
3. Misuse of data access (e.g., sharing passwords with unauthorized parties).
4. Attempts and conspiracies to commit computer crimes are also regulated and punishable.

Personal Data Protection Act 2010 (PDPA 2010):

1. PDPA 2010 regulates the collection, storage, use, and disclosure of personal data by

DOI: 10.33830/osc.v3i1.7023 / ISSN: 3032-2227

private sector entities.
2. It aims to protect individuals' privacy from misuse of personal data and strengthen the security and accountability of data management.
3. The PDPA establishes data protection principles, such as data subject consent, data use restrictions, and data confidentiality obligations.
4. Although applicable to the private sector, the PDPA is an important component of Malaysia's legal framework to support cybersecurity and the protection of personal information from cybercrime.

The Thai Computer Crime Act (CCA), which was last revised in 2017 (Computer Crimes Act No. 2 B.E. 2560 / A.D. 2017), brought a number of important changes to the regulation of computer crime in Thailand. Thailand's Personal Data Protection Act (PDPA), which came into effect in 2019, is a regulation focused on the protection of personal data and digital data security in the country [29]. The PDPA regulates the collection, processing, storage, and use of personal data based on the principles of transparency, fairness, and data security to protect individual privacy rights. The PDPA also imposes obligations on data controllers to obtain the consent of data owners, maintain data confidentiality, and report data breaches to authorities and relevant parties [30].

Southeast Asian countries have relatively comprehensive legal frameworks related to cyber law, but there are differences in the level of development and implementation. Indonesia relies on the updated Electronic Information and Transaction Law (ITE Law) as the main legal basis for dealing with cybercrime; however, law enforcement still faces weaknesses such as limited legal coverage and suboptimal enforcement capacity [31]. Singapore has comprehensive regulations, including the Computer Misuse Act and Cybersecurity Act, which provide strong protection for critical infrastructure and emphasize cross-sector collaboration in addressing cyber threats [32]. Malaysia and Thailand have also developed specific regulations, such as the Personal Data Protection Act and Cybersecurity Act, which emphasize aspects of personal data protection and national security [33]. Despite harmonization efforts at the regional level, regulatory disparities and legal capacities between countries pose a major challenge to effective collaboration in the region.

Cybersecurity technology is implemented in the form of establishing various related institutions, such as Computer Emergency Response Teams (CERT) in each country, which play an active role in early detection and mitigation of cyber incidents [34]. The use of technologies such as firewalls, intrusion detection systems, data encryption, and vulnerability management systems has become part of the technical strategy of Southeast Asian countries. Indonesia, for example, through the National Cyber and Cryptography Agency (BSSN), conducts monitoring and releases annual cybersecurity reports, as well as supports technical capacity building through regional and international cooperation [35]. Despite the implementation of technology, challenges remain in the form of shortages of highly skilled human resources and cybersecurity infrastructure that still needs to be strengthened in some member countries [36]. The results of the study confirm that an integrative approach between law (cyber law) and technology (cybersecurity) is an important strategy in mitigating the risk of cybercrime in Southeast Asia, but its effectiveness is highly dependent on national implementation capabilities and solid regional coordination [37]. Case studies in several ASEAN countries reveal that despite significant progress, there are still many challenges that must be addressed to counter increasingly sophisticated and transnational

DOI: 10.33830/osc.v3i1.7023 / ISSN: 3032-2227

cyber threats [38], [39], [40], [41].

CONCLUSION

An integrative approach between legal aspects (cyber law) and cybersecurity technology is a crucial and effective strategy in mitigating the risk of cybercrime in the Southeast Asian region. Countries in this region, including Indonesia, Singapore, Malaysia, and Thailand, have developed different regulations and technological practices, but have generally established legal frameworks and technical mechanisms to address increasingly complex cyber threats. Cyber law provides a clear legal foundation for law enforcement and the imposition of sanctions, as well as establishing the necessary norms and rules, while cybersecurity technology serves as the primary tool for prevention, detection, and response to cyber incidents.

However, the effectiveness of implementing this approach still faces various challenges, such as cross-border regulatory disparities, uneven human resource and technological capacity, barriers to inter-agency coordination, and a lack of regulatory harmonization at the regional level. For example, Indonesia still faces obstacles in enforcing the ITE Law related to the technical expertise of law enforcement and digital evidence, while Singapore implements a risk-based approach with more comprehensive regulations and centralized coordination. Malaysia and Thailand also continue to update their regulations to adapt to technological dynamics and cyber threats.

Regional cooperation through ASEAN is a key factor in strengthening cybercrime risk mitigation, with initiatives such as the ASEAN Cybersecurity Cooperation Strategy promoting regulatory harmonization and operational collaboration. To enhance cyber resilience, key recommendations include updating and harmonizing regulations that are adaptive to technological developments, enhancing the capacity of human resources and law enforcement institutions, strengthening cross-border coordination, and investing in reliable cybersecurity infrastructure. The success of cybercrime risk mitigation in Southeast Asia depends on the synergy between strengthening legal and technological aspects, as well as close collaboration among countries in addressing the rapidly evolving cross-border cybercrime challenges in the digital age.

REFERENCES

[1] G. Sarkar and S. K. Shukla, “Behavioral analysis of cybercrime: Paving the way for effective policing strategies,” *J. Econ. Criminol.*, vol. 2, no. September, p. 100034, 2023, doi: 10.1016/j.jeconc.2023.100034.

[2] S. M. Sulubara, H. Fauzi, B. Muslim, M. F. Ferdiansyah, and M. Musmulyadi, “Judi Online Sebagai Cybercrime Serta Tantangan Penegakan Hukum Pidana di Era Digital : Antara Regulasi , Pembuktian , dan Ancaman Cybercrime,” *J. Ris. Rumpun Ilmu Sos. Polit. dan Hum.*, vol. 4, no. 2, pp. 539–552, 2025, doi: https://doi.org/10.55606/jurrish.v4i2.4990.

[3] S. M. Sulubara, V. Tasril, and Nurkhalisah, *Perlindungan Hukum Tindak Pidana Cybercrime Dalam Cyberlaw Di Indonesia: Perkembangan Tekhnologi Dan Tantangan Hukum Dalam Mewujudkan Cybersecurity*, Edisi Pert. Kartasura, Sukoharjo: Tahta Media, 2025.

[4] S. M. Sulubara and V. Tasril, “Legal Protection Of Cybercrime Crimes From Ransomware Attacks And Evaluation Of The Cyber Security And Resilience Bill 2025 In Indonesia ’ S Defense,” *LEGA LATA J. Ilmu Huk.*, vol. 10, no. December, pp. 287–297, 2025, doi: 10.30596/dll.v10i2.25786.

[5] F. R. Seri Mughni Sulubara, Hidayati Purnama Lubis, Nanci Yosepin Simbolon, *Teori Hukum Perdata (Studi Kasus: Transaksi E-Commerce Shopee Paylater*, Edisi Pert. CV. Tahta Media Group, 2024.

[6] A. A. Seri Mughni Sulubara, “Legalitas Fintech Peer To Peer Lending Pinjaman Online dalam Aspek Hukum Konvensional,” *MANDUB J. Polit. Sos. Huk. dan Hum.*, vol. 2, no. 2, pp. 177–187, 2024, doi: https://doi.org/10.59059/mandub.v2i2.1184.

DOI: 10.33830/osc.v3i1.7023 / ISSN: 3032-2227

[7] Seri Mughni Sulubara, Yury Ulandary, Riska Riska, and Desi Purnama Sari, "Gen Z Wajib Tau! Edukasi dan Penguatan Pasal-Pasal UUD 1945 bagi Generasi Z (Pasca Milenal) bagi Siswa-Siswi SMA Negeri 4 Takengon," *Karunia Jurnal Has. Pengabdi. Masy. Indones.*, vol. 2, no. 4, pp. 96–109, 2023, doi: 10.58192/karunia.v2i4.1552.
[8] I. Seri Mughni Sulubara, "Regulasi dan Lisensi Mengenai Perlindungan Hukum Investor di Platform Fintech Peer-To-Peer Lending dalam Hukum Konvensional," *J. Hukum, Polit. dan Ilmu Sos.*, vol. 3, no. 4, pp. 431–442, 2024, doi: https://doi.org/10.55606/jhpis.v3i4.4499.
[9] H. Azrica and S. M. Sulubara, "Legalitas Transaksi E Commerce Dalam Platfortm Shopee Ditinjau Dalam Kitab Undang-Undang Hukum Perdata (Burgerlijk Wetboek), Undang-Undang Nomor: 8 Tahun 1999 Tentang Perlindungan Konsumen Dan Persfektif Fiqih Muamalah," *Hakim J. Ilmu Huk. dan Sos.*, vol. 1, no. 3, pp. 1–23, 2023, doi: https://doi.org/10.51903/hakim.v1i3.1305.
[10] S. M. Sulubara, H. P. Lubis, and N. Y. Simbolon, "Legal Review of Electronic Commerce-Based Buying and Selling on the Shopee Platform Against Consumers Using Shopee PayLater," *Proceeding IROFONIC 2024*, vol. Proceeding, no. 02, pp. 392–402, 2024.
[11] S. M. Sulubara, H. P. Lubis, and N. Y. Simbolon, "Legality Of Shopee Paylater Payments For Shopee Platform E-Commerce Transactions In Conventional Law," *Deleg. J. Ilmu Huk.*, vol. 9, no. 2, pp. 247–256, 2024, doi: 10.30596/dll.v9i2.20414.
[12] S. M. Sulubara, "Menyajikan Berbagai Insiden Cybercrime yang Terjadi di Indonesia , Termasuk Pencurian Data dan Peretasan Situs Web Pemerintah," *Konsensus J. Ilmu Polit. dan Komun.*, vol. 1, no. 6, pp. 199–206, 2024, doi: https://doi.org/10.62383/konsensus.v1i6.692.
[13] Seri Mughni Sulubara, "Perlindungan Data Pribadi dalam Kasus Ransomware : Apa Kata Hukum ?," *Eksekusi J. Ilmu Huk. dan Adm. Negara*, vol. 2, no. November, pp. 426–434, 2024, doi: https://doi.org/10.55606/eksekusi.v2i4.1823.
[14] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," *Energy Reports*, vol. 7, pp. 8176–8186, 2021, doi: 10.1016/j.egyr.2021.08.126.
[15] M. Zainuddin and A. D. Karina, "Penggunaan Metode Yuridis Normatif dalam Membuktikan Kebenaran pada Penelitian Hukum," *Smart Law J.*, vol. 2, no. 2, pp. 114–123, 2023, [Online]. Available: https://journal.unkaha.com/index.php/slj/article/view/26
[16] K. Chimmanee and S. Jantavongso, "Digital forensic of Maze ransomware: A case of electricity distributor enterprise in ASEAN," *Expert Syst. Appl.*, vol. 249, no. PB, p. 123652, 2024, doi: 10.1016/j.eswa.2024.123652.
[17] B. Kaulu, G. Kaulu, and P. Chilongo, "Factors influencing customers' intention to adopt e-banking: a TAM and cybercrime perspective using structural equation modelling," *J. Money Bus.*, vol. 4, no. 1, pp. 38–53, 2024, doi: 10.1108/jmb-01-2024-0007.
[18] G. Onwuadiamu, "Cybercrime in criminology; A systematic review of criminological theories, methods, and concepts," *J. Econ. Criminol.*, vol. 8, no. February, p. 100136, 2025, doi: 10.1016/j.jeconc.2025.100136.
[19] N. Khadam *et al.*, "How to punish cyber criminals: A study to investigate the target and consequence based punishments for malware attacks in UK, USA, China, Ethiopia & Pakistan," *Heliyon*, vol. 9, no. 12, 2023, doi: 10.1016/j.heliyon.2023.e22823.
[20] D. Wright and R. Kumar, "Assessing the socio-economic impacts of cybercrime," *Soc. Impacts*, vol. 1, no. 1–2, p. 100013, 2023, doi: 10.1016/j.socimp.2023.100013.
[21] N. Khadam *et al.*, "How to punish cyber criminals: A study to investigate the target and consequence based punishments for malware attacks in UK, USA, China, Ethiopia & Pakistan," *Heliyon*, vol. 9, no. 12, p. e22823, 2023, doi: 10.1016/j.heliyon.2023.e22823.
[22] R. Nugraha, "Perspektif Hukum Indonesia (Cyberlaw) Penanganan Kasus Cyber di Indonesia," *J. Ilm. Huk. Dirgant.*, vol. 11, no. 2, pp. 44–56, 2021.
[23] S. N. Fitri, "Politik Hukum Pembentukan Cyber Law Undang-Undang Informasi dan Transaksi Elektronik di Indonesia," *J. Justisia J. Ilmu Hukum, Perundang-undangan dan Pranata Sos.*, vol. 7, no. 1, p. 104, 2022, doi: 10.22373/justisia.v7i1.12719.
[24] Murthada Murthada and Seri Mughni Sulubara, "Implementasi Hak Asasi Manusia di Indonesia berdasarkan Undang-Undang Dasar 1945," *Dewantara J. Pendidik. Sos. Hum.*, vol. 1, no. 4, pp. 111–121, 2022, doi: 10.30640/dewantara.v1i4.426.
[25] B. Handoyo, H. MZ, I. Rahma, and Asy'ari, "Tinjaun Yuridis Penegakkan Hukum Kejahatan Cyber Crime Studi Implementasi Undang-Undang Nomor 11 Tahun 2008," *MAQASIDI J. Syariah dan Huk.*,

DOI: 10.33830/osc.v3i1.7023 / ISSN: 3032-2227

vol. 4, no. 1, pp. 40–55, 2024, doi: 10.47498/maqasidi.v4i1.2966.
[26] M. S. Akub, "Pengaturan Tindak Pidana Mayantara (Cyber Crime) Dalam Sistem Hukum Indonesia," *Al-Ishlah J. Ilm. Huk.*, vol. 21, no. 2, pp. 85–93, 2020, doi: 10.33096/aijih.v21i2.19.
[27] R. S. B. Pansariadi and N. Soekorini, "Tindak Pidana Cyber Crime dan Penegakan Hukumnya," *Binamulia Huk.*, vol. 12, no. 2, pp. 287–298, 2023, doi: 10.37893/jbh.v12i2.605.
[28] C. Wei-Jung, "Cyberstalking and law enforcement," *Procedia Comput. Sci.*, vol. 176, pp. 1188–1194, 2020, doi: 10.1016/j.procs.2020.09.115.
[29] Z. Wang, H. Zhu, P. Liu, and L. Sun, "Social engineering in cybersecurity: a domain ontology and knowledge graph application examples," *Cybersecurity*, vol. 4, no. 1, 2021, doi: 10.1186/s42400-021-00094-6.
[30] M. A. Ferrag *et al.*, "Generative AI in cybersecurity: A comprehensive review of LLM applications and vulnerabilities," *Internet Things Cyber-Physical Syst.*, vol. 5, no. October 2024, pp. 1–46, 2025, doi: 10.1016/j.iotcps.2025.01.001.
[31] K. Achuthan, S. Khobragade, and R. Kowalski, "Cybercrime through the public lens: a longitudinal analysis," *Humanit. Soc. Sci. Commun.*, pp. 1–16, 2025, doi: 10.1057/s41599-025-04459-x.
[32] D. H. Elsayed, T. H. Ismail, and E. A. Ahmed, "The impact of cybersecurity disclosure on banks ' performance : the moderating role of corporate governance in the MENA region," *Futur. Bus. J.*, vol. 10, no. 1, pp. 1–15, 2024, doi: 10.1186/s43093-024-00402-9.
[33] K. Pipyros and S. Liasidou, "A new cybersecurity risk assessment framework for the hospitality industry: techniques and methods for enhanced data protection and threat mitigation," *Worldw. Hosp. Tour. Themes*, 2025, doi: 10.1108/WHATT-12-2024-0296.
[34] C. Hu, T. Wu, C. Liu, and C. Chang, "Joint contrastive learning and belief rule base for named entity recognition in cybersecurity," *Cybersecurity*, vol. 7, no. 1, 2024, doi: 10.1186/s42400-024-00206-y.
[35] M. A. Hossain and M. S. Islam, "Enhanced detection of obfuscated malware in memory dumps: a machine learning approach for advanced cybersecurity," *Cybersecurity*, vol. 7, no. 1, 2024, doi: 10.1186/s42400-024-00205-z.
[36] A. Tomas, D. Vicente, L. D. Marcos, and O. A. Tevar, "Factors influencing employee compliance with information security policies : a systematic literature review of behavioral and technological aspects in cybersecurity," *Futur. Bus. J.*, 2025, doi: 10.1186/s43093-025-00452-7.
[37] M. H. Shah, P. Jones, and J. Choudrie, "Cybercrimes prevention: promising organisational practices," *Inf. Technol. People*, vol. 32, no. 5, pp. 1125–1129, 2019, doi: 10.1108/ITP-10-2019-564.
[38] A. Alyami, D. Sammon, K. Neville, and C. Mahony, "Critical success factors for Security Education, Training and Awareness (SETA) programme effectiveness: an empirical comparison of practitioner perspectives," *Inf. Comput. Secur.*, vol. 32, no. 1, pp. 53–73, 2024, doi: 10.1108/ICS-08-2022-0133.
[39] N. N. Cele and S. Kwenda, "Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review," *J. Financ. Crime*, vol. 32, no. 1, pp. 31–48, 2024, doi: 10.1108/JFC-10-2023-0263.
[40] B. S. von Skarczinski, A. Dreißigacker, and F. Teuteberg, "Toward enhancing the information base on costs of cyber incidents: implications from literature and a large-scale survey conducted in Germany," *Organ. Cybersecurity J. Pract. Process People*, vol. 2, no. 2, pp. 79–112, 2022, doi: 10.1108/ocj-08-2021-0020.
[41] R. van Wegberg, J. J. Oerlemans, and O. van Deventer, "Bitcoin money laundering: mixed results?: An explorative study on money laundering of cybercrime proceeds using bitcoin," *J. Financ. Crime*, vol. 25, no. 2, pp. 419–435, 2018, doi: 10.1108/JFC-11-2016-0067.