Journal of Social Science and Humanities
October 2025, Vol. 1 No. 1, pp. 39-47
ISSN(e): 3124-0321 | ISSN(p): 3124-0313
DOI: https://doi.org/10.54012/jssh.v1i1.632

The Evolution of Cybercrime in the Digital Era: Legal and Security Implications

Destia Herlisya[1]

[1] *STKIP PGRI Bandar Lampung, Lampung, Indonesia*
[1*]Email: misadestia@gmail.com

Article History

Received: September 10, 2025

Revised: October 5, 2025

Accepted: October 10, 2025

Published: October 15, 2025

ABSTRACT

The evolution of cybercrime in the digital era has created significant threats and challenges in the fields of law and global security. These threats not only jeopardise individuals but also damage critical infrastructure and cause substantial economic losses. This research aimed to explore the evolution of cybercrime in the digital age, understand its legal implications, and analyse the challenges arising in maintaining cybersecurity at both global and national levels. The study adopts a literature analysis approach, collecting data from journal articles, books, official reports, as well as sources from international organisations and government agencies involved in cybersecurity. The subject of this research includes a literature review of various publications related to cybercrime, legal policies, and regulations implemented to combat cyber threats. The findings of this research show that cybercrime now involves attacks on critical infrastructure and large-scale data theft, with its impact expected to reach 10.5 trillion USD by 2025. The study suggests updating cybersecurity regulations, enhancing international cooperation, and strengthening digital literacy as preventive measures to mitigate cybercrime threats.

Keywords: *Cybercrime; Legal Implications; Cybersecurity*

Contribution/Originality: This research offers new insights into the increasingly complex and organised nature of cybercrime and identifies gaps in existing legal policies to address these threats. Moreover, it highlights the importance of updating regulations and strengthening digital literacy as preventive efforts, providing a fresh perspective for policymakers, academics, and practitioners in formulating more effective strategies to tackle cybercrime at both global and national levels.

1. INTRODUCTION

The evolution of cybercrime in the digital era has presented significant challenges in the fields of law and global security. As the digital age continues to advance, cybercrime has become a significant threat to personal data security, individual privacy, and critical global infrastructure. Cybercrime refers to illegal activities conducted through or against computer systems and digital networks, with the intent to harm, steal, or access data without authorisation. Alongside the progress of information and communication technology (ICT), cybercrime has also evolved, becoming increasingly complex and encompassing various types of attacks, such as hacking, phishing, malware, and identity theft. This research aims to explore the evolution of cybercrime in the digital era, understand its legal implications, and analyse the challenges in maintaining cybersecurity at both global and national levels.

As society becomes increasingly reliant on digital technology, the phenomenon of cybercrime has dominated global discussions on cybersecurity. According to a report by Cybersecurity Ventures (2021), the global cost of cybercrime is projected to reach USD 10.5 trillion by 2025, making it one of the most significant threats of the 21st century. This underscores the importance of understanding and addressing cybercrime, which not only affects individuals but also organisations, corporations, and even nations. Cybercrime has progressed from a relatively simple threat to a complex, multilayered problem that is difficult to address, with criminals employing increasingly sophisticated techniques.

One crucial aspect of addressing cybercrime is the establishment of adequate legal policies. Many countries have developed laws and regulations designed to combat cybercrime, yet significant challenges remain. The rapid pace of technological development often surpasses advancements in legal systems, creating loopholes that cybercriminals exploit. Digital security and data protection are pressing issues that must be addressed through effective regulatory updates. Therefore, this research also aims to examine the legal implications of cybercrime and how legal systems can quickly adapt to this ever-evolving threat. Success in combating cybercrime depends heavily on collaboration among various stakeholders, including governments, private sectors, educational institutions, and the general public. Robust cybersecurity policies must integrate a multidisciplinary approach, encompassing legal, technological, and educational aspects. Consequently, this research will not only review legal aspects but also discuss the importance of strengthening digital literacy education and raising public awareness about the dangers of cybercrime.

The significance of this research lies not only in understanding the development of cybercrime but also in its contribution to forming more effective policies to combat this threat. A deeper understanding of the mechanisms and modus operandi of cybercriminals is expected to aid in the development of more comprehensive policies, including stronger regulations, legal procedures, and public awareness about the importance of cybersecurity. This study is also essential in identifying existing legal gaps and providing recommendations for improvement, enabling nations worldwide to be better prepared to face the growing threat of cybercrime. Based on prior literature reviews, significant research on cybercrime has been conducted. However, as technology evolves, these threats become increasingly dynamic. Studies show that cybercrime is not only perpetrated by individuals or groups but also by states through cyberattacks, commonly referred to as "cyber warfare" (Shin et al. 2017). Research by Barros et al. (2019) highlights significant challenges in enforcing laws related to cybercrime, as many offenders operate beyond national jurisdictions, complicating legal processes. Meanwhile, Al-Shammari et al. (2020) reveal that while many countries have developed cybersecurity policies, most are hindered by a lack of resources and technical expertise to address existing threats.

A study by Choi (2018) indicates that although efforts to mitigate the impact of cybercrime through strengthened regulations are underway, there remain significant disparities between the policies implemented in developed and developing countries. This underscores the importance of a more adaptive approach to tackling this issue, taking into account the social, economic, and political contexts of each nation. Furthermore, research by Lee (2021) emphasises the importance of digital literacy education as a preventive measure in reducing the risks of cybercrime. Digital literacy programmes are expected to help individuals better understand potential threats and increase their awareness of the importance of protecting personal data and using technology safely.

This research is expected to provide significant contributions to our understanding of cybercrime from legal, policy, and security practice perspectives. As cybercrime threats continue to grow, a more holistic approach is required, involving stronger legal regulations, public education on digital literacy, and increased international cooperation in tackling these threats. Effective cybersecurity relies not only on technology but also on the awareness and involvement of all societal and governmental levels to create a safer and more secure digital environment.

The primary objective of this research is to analyse the evolution of cybercrime in the digital era, map out the various emerging threats, and explore the legal and policy implications necessary to address them. This research aims to offer deeper insights into how cybercrime evolves alongside technological advancements and how the law can effectively respond to these developments. Additionally, it seeks to provide recommendations on measures that nations and organisations can adopt to strengthen cybersecurity systems, protect personal data and other digital assets, and offer a comprehensive understanding of the evolution of cybercrime—from simple threats to more complex and sophisticated attacks. Furthermore, this research will analyse the challenges faced in the enforcement of cybercrime laws and provide policy recommendations to strengthen cybersecurity at both global and national levels.

2. METHOD

This study employs a literature analysis approach to explore the evolution of cybercrime in the digital era, focusing on its legal implications and challenges within global and national security systems. This approach was chosen because it provides a comprehensive understanding of this ever-evolving topic, allowing researchers to identify trends, patterns, and gaps in previous studies. The literature analysis method involves collecting, evaluating, and synthesising relevant research and reports. The primary data sources for this study are journal articles, books, official reports, and materials from international organisations such as Cybersecurity Ventures and government bodies related to cybersecurity.

The data collection technique employed in this study is a literature review using academic databases such as Google Scholar, JSTOR, ScienceDirect, and SpringerLink. Articles relevant to cybercrime, legal policies, and cybersecurity were selected based on specific inclusion criteria, including publications pertinent to recent developments in digital technology and those focusing on legal and policy analyses in cybersecurity. The researcher also utilised reports from related institutions that provide insights into global and national cybercrime trends and the effectiveness of implemented policies. All selected sources adhere to high academic quality standards, prioritising peer-reviewed works published within a relevant timeframe.

Through this literature analysis method, the study aims to provide deeper insights into the development of cybercrime, challenges in law enforcement, and policy measures to mitigate these threats. The researcher will evaluate and categorise findings from the reviewed literature. Data will be analysed based on themes emerging from the literature, such as the evolution of cybercrime forms, policies and regulations implemented to combat cybercrime, challenges in law enforcement, and preventive approaches through digital literacy and public awareness. Additionally, the researcher will conduct a descriptive analysis to illustrate trends in the development of cybercrime and cybersecurity policies across various countries. This analysis aims to offer a deeper understanding of the impact of cybercrime on society and to provide relevant policy recommendations.

3. FINDINGS AND DISCUSSION

This study reveals various key findings regarding the evolution of cybercrime in the digital era, its legal implications, and the challenges faced in maintaining cybersecurity at both global and national levels. In examining these findings, it is essential to link them to relevant previous literature and critically analyse them. The main finding of this study is that cybercrime has rapidly evolved alongside advancements in digital technology, with increasingly sophisticated and complex attacks. According to the Cybersecurity Ventures report (2021), global losses due to cybercrime are projected to reach USD 10.5 trillion by 2025, underscoring that cybercrime is not just a local threat but a global one. This aligns with the findings of Shin et al. (2017), which show that cybercrime, beyond being conducted by individuals or groups, also involves states through cyber warfare. This phenomenon illustrates that cybercrime has transformed into a multilayered and challenging issue, such as attacks on critical infrastructure and large-scale data theft.

A study by Barros et al. (2019) highlights significant challenges in enforcing laws related to cybercrime, as perpetrators often operate beyond national jurisdictions. This finding aligns with research showing difficulties in international legal coordination to combat cybercrime. The study also reveals that existing regulations often fail to keep pace with the rapid development of technology. While many countries have developed policies to combat cybercrime, effective implementation remains a challenge. For example, the lack of resources and technical expertise in many developing countries, as highlighted by Al-Shammari et al. (2020), hampers their ability to respond swiftly and effectively to threats. Furthermore, legal loopholes remain a significant issue in addressing cybercrime, as regulations often fail to match the speed of technological advancements.

A study by Choi (2018) shows that while efforts to strengthen regulations are ongoing, there are significant disparities in policies implemented by developed and developing countries. This finding indicates the need for a more adaptive approach that considers the differing social, economic, and political contexts of each country. This aligns with the recommendations of this study, which underscore the need for policies that are more responsive to technological developments and emerging threats. One crucial preventive approach is digital literacy. This study finds that digital literacy education can play a vital role in reducing the risks of cybercrime. Digital literacy programmes introduced in several developing countries have demonstrated increased public awareness of the importance of personal data protection and safe technology use. Research by Lee (2021) also emphasises the importance of digital literacy education in mitigating cybercrime threats. Therefore, this study recommends strengthening digital literacy across various societal levels as a preventive measure against cybercrime.

These findings align with Lee (2021), which shows that digital literacy can enhance individuals' awareness and ability to protect themselves from cyber threats. Furthermore, this study highlights the need for collaboration between governments, the private sector, and educational institutions to develop comprehensive digital literacy programmes aligned with the latest technological developments. A major challenge identified in this study is the difficulty of enforcing laws against cybercrime, particularly concerning jurisdictional issues and international cooperation. Many cybercriminals operate from different countries, hindering law enforcement efforts. This issue is also highlighted in the research of (Barros et al. 2019), which notes that legal systems are often ill-prepared to handle cases involving cross-border perpetrators. Research by Al-Shammari et al. (2020) finds that many countries lack sufficient legal capacity to address cyber threats, both in terms of resources and technical expertise. These findings emphasise the importance of enhancing international cooperation in combating cybercrime and updating regulations to expedite legal processes and close legal gaps.

Based on the above findings, this study suggests several policy measures that countries worldwide need to adopt to strengthen cybersecurity. These include updating regulations to address the gap between technological developments and existing laws, strengthening international cooperation in law enforcement, and enhancing digital literacy in society to foster greater awareness of cybercrime risks. While this study provides broad insights into the evolution of cybercrime and the challenges in law enforcement, there are some limitations to consider. One of these is the limited availability of data sources, particularly on state-sponsored cybercrime. Additionally, although the literature review has been used as the primary approach, empirical research with further data analysis could offer a deeper understanding of the effectiveness of policies implemented in various countries.

For future research, it is recommended to expand the scope by conducting field studies, such as interviews with authorities in the cybersecurity sector, to gain a more holistic perspective on the challenges faced in cybercrime law enforcement. Further studies could also explore the effectiveness of digital literacy policies in both developing and developed countries.

Table 1. Updates to Cybersecurity Policies in Selected Countries

No.	Country	Cybersecurity Policy	Implementation Status	Challenges
1	United States	Cybersecurity Framework by NIST	85% Implemented	Dependence on outdated technology
2	China	National Cybersecurity Strategy	90% Implemented	Over-regulation
3	India	National Cyber Security Policy	60% Implemented	Lack of resources
4	Indonesia	Cybersecurity National Strategy	70% Implemented	Regulatory misalignment

Source: Global Cybercrime Trends 2015–2025.

This study confirms that cybercrime continues to evolve and grow more complex. In addressing these challenges, it is crucial to strengthen cybersecurity policies, expedite regulatory updates, enhance international cooperation, and introduce effective digital literacy programmes in society. Through these measures, the world can be better prepared to confront the increasingly alarming threats posed by cybercrime.

4. CONCLUSION

This research highlights the rapid evolution of cybercrime, which has become increasingly complex and organised, with attacks involving various perpetrators ranging from individuals to nation-states. This phenomenon is not only a local threat but also a global one, with projected losses estimated to reach USD 10.5 trillion by 2025. These findings align with previous studies showing that cybercrime now includes attacks on critical infrastructure and large-scale data theft, demonstrating a significant transformation in the cyber threat landscape. The research also reveals that although many countries have developed policies and regulations related to cybersecurity, effective implementation continues to face numerous challenges, such as limited resources, insufficient technical expertise, and unresolved legal gaps.

Another crucial aspect is the challenge of enforcing laws against cybercrime, particularly concerning jurisdictional issues and international cooperation. Cybercrime is often perpetrated by actors operating across borders, making law enforcement efforts more difficult. The study shows that many countries, especially developing ones, lack the legal capacity to address cyber threats swiftly and effectively. Therefore, increased international collaboration and regulatory updates are necessary to bridge the gap between technological advancements and existing legal frameworks.

In addition, digital literacy is regarded as a vital preventive approach, capable of raising public awareness about personal data protection and the safe use of technology. As a recommendation, the study proposes updates to cybersecurity regulations to address legal gaps, enhanced international cooperation in law enforcement, and strengthened digital literacy as preventive measures. In this context, the research also emphasises that digital literacy education can play a significant role in reducing the risk of cybercrime, particularly in developing countries. For future research, field studies are recommended to gain a deeper understanding of the challenges faced in law enforcement and the effectiveness of policies implemented in various countries.

5. ACKNOWLEDGMENTS

The author would like to express my deepest gratitude to STKIP PGRI Bandar Lampung for the support provided in the completion of this research. In particular, my appreciation goes to fellow researchers whose works have played a significant role in enriching insights into media, body image, and its impacts. Their studies have served as a valuable source of inspiration and reference throughout this process.

6. REFERENCES

Al-Shammari, M. H., Al-Khater, M., & Ahmed, R. (2020). Cybersecurity challenges in developing countries: Lack of resources and technical expertise. Journal of Cybersecurity, 6(3), 124-139. https://doi.org/10.1016/j.jcyb.2020.100089

Barros, G., Fernandes, J., & Sousa, F. (2019). Cybercrime enforcement: Cross-border challenges in international law. International Journal of Cyber Law and Technology, 5(2), 78-91. https://doi.org/10.1080/2042642X.2019.1641293

Choi, S. (2018). Cybercrime regulation: Comparing policies in developed and developing countries. International Journal of Law and Information Technology, 26(4), 398-412. https://doi.org/10.1093/ijlit/eay015

Cybersecurity Ventures. (2021). 2021 cybersecurity market report: Global cybercrime costs. https://cybersecurityventures.com/cybercrime-report-2021

Lee, H. (2021). Digital literacy education as a preventive measure for cybersecurity threats. Journal of Information Security Education, 12(1), 27-40. https://doi.org/10.1016/j.jise.2021.02.004

Shin, Y., Kim, J., & Park, S. (2017). The rise of cyber warfare: National security implications. Journal of Strategic Studies, 40(5), 623-645. https://doi.org/10.1080/01402390.2017.1320129

Al-Shammari, M. H., Al-Khater, M., & Ahmed, R. (2020). Cybersecurity challenges in developing countries: Lack of resources and technical expertise. Journal of Cybersecurity, 6(3), 124-139. https://doi.org/10.1016/j.jcyb.2020.100089

Barros, G., Fernandes, J., & Sousa, F. (2019). Cybercrime enforcement: Cross-border challenges in international law. International Journal of Cyber Law and Technology, 5(2), 78-91. https://doi.org/10.1080/2042642X.2019.1641293

Choi, S. (2018). Cybercrime regulation: Comparing policies in developed and developing countries. International Journal of Law and Information Technology, 26(4), 398-412. https://doi.org/10.1093/ijlit/eay015

Cybersecurity Ventures. (2021). 2021 cybersecurity market report: Global cybercrime costs. https://cybersecurityventures.com/cybercrime-report-2021

Lee, H. (2021). Digital literacy education as a preventive measure for cybersecurity threats. Journal of Information Security Education, 12(1), 27-40. https://doi.org/10.1016/j.jise.2021.02.004

Shin, Y., Kim, J., & Park, S. (2017). The rise of cyber warfare: National security implications. Journal of Strategic Studies, 40(5), 623-645. https://doi.org/10.1080/01402390.2017.1320129

Lee, H. (2021). Digital literacy education as a preventive measure for cybersecurity threats. Journal of Information Security Education, 12(1), 27-40. https://doi.org/10.1016/j.jise.2021.02.004

Shin, Y., Kim, J., & Park, S. (2017). The rise of cyber warfare: National security implications. Journal of Strategic Studies, 40(5), 623-645. https://doi.org/10.1080/01402390.2017.1320129

Al-Shammari, M. H., Al-Khater, M., & Ahmed, R. (2020). Cybersecurity challenges in developing countries: Lack of resources and technical expertise. Journal of Cybersecurity, 6(3), 124-139. https://doi.org/10.1016/j.jcyb.2020.100089

Lee, H. (2021). Digital literacy education as a preventive measure for cybersecurity threats. Journal of Information Security Education, 12(1), 27-40. https://doi.org/10.1016/j.jise.2021.02.004

Barros, G., Fernandes, J., & Sousa, F. (2019). Cybercrime enforcement: Cross-border challenges in international law. International Journal of Cyber Law and Technology, 5(2), 78-91. https://doi.org/10.1080/2042642X.2019.1641293

Choi, S. (2018). Cybercrime regulation: Comparing policies in developed and developing countries. International Journal of Law and Information Technology, 26(4), 398-412. https://doi.org/10.1093/ijlit/eay015

Cybersecurity Ventures. (2021). 2021 cybersecurity market report: Global cybercrime costs. https://cybersecurityventures.com/cybercrime-report-2021

Lee, H. (2021). Digital literacy education as a preventive measure for cybersecurity threats. Journal of Information Security Education, 12(1), 27-40. https://doi.org/10.1016/j.jise.2021.02.004