https://research.adra.ac.id /index.php/rjl/
P - ISSN: 2988-4454
E - ISSN: 2988-4462

Legal Approaches to Cybersecurity: A Global Study of Frameworks and Enforcement in the Digital Age

Ethan Tan[1], Rachel Chan[2], Daiki Nishida[3]
[1]National University of Singapore (NUS), Singapore
[2]Singapore University of Social Sciences (SUSS), Singapore
[3]Chuo University, Japan

ABSTRACT

Background. Cybersecurity is a critical global issue driven by increasing reliance on digital technology, which heightens vulnerabilities to data breaches and cyber threats. Public-private partnerships (PPPs) play a key role in strengthening cyber law enforcement, but challenges like regulatory gaps and differing priorities demand systematic collaboration to optimize their effectiveness.

Purpose. This research aims to assess the role of public-private partnerships (PPP) in strengthening cyber law enforcement in various legal systems.

Method. This research uses an approach Systematic Literature Review (SLR) to identify, analyze and synthesize various studies relevant to the topic of cyber law enforcement and the role of public-private partnerships (PPP) in that context.

Results. The research highlights key themes including the effectiveness of PPPs in improving cybersecurity, barriers to their implementation due to regulatory and interest conflicts, regional differences in success rates influenced by legal systems, and the role of PPPs in fostering collaborative innovation and law enforcement, alongside recommendations for strengthening legal frameworks and addressing gaps in empirical data.

Conclusion. This research highlights the critical role of public-private partnerships (PPPs) in cyber law enforcement, emphasizing that transparency, trust, and shared commitment are key factors influencing their effectiveness.

KEYWORDS

Cyber Law, Cyber Security, Public-Private

Citation: Tan, E., Chan, R & Nishida, D. (2026). Legal Approaches to Cybersecurity: A Global Study of Frameworks and Enforcement in the Digital Age. *Rechtsnormen Journal of Law*, *4*(1), 74–85.
https://doi.org/10.70177/rjl.v4i1.1792

Correspondence:

Ethan Tan,
ethantan@edu.sg

Received: Sep 9, 2025

Accepted: Dec 1, 2025

Published: Feb 28, 2026

INTRODUCTION

In today's digital landscape, cybersecurity has emerged as a critical global concern. This is driven by the increasing reliance on digital technology in various sectors, including business, government and public services. This dependency has increased vulnerability to personal data breaches, threats to critical infrastructure, and risks to the digital economy (Grájeda, 2023; Wen, 2025). Cyber attacks can result in significant financial losses, disrupt social stability, and threaten national security. The evolution of cybercrime into a complex transnational threat has outstripped traditional legal frameworks, making it

increasingly difficult to manage and control this risk effectively. Cyber law plays a critical role in addressing these challenges, serving as a legal framework designed to protect individual rights and the public interest from cyber threats, such as data theft, malware and digital sabotage. However, the effectiveness of these laws is highly dependent on strong enforcement mechanisms (Fatima, 2024; Moussa, 2024).

Although many countries have established comprehensive legal frameworks for cybersecurity, law enforcement still faces various difficulties, including a lack of global consensus on what constitutes cybercrime as well as varying definitions of criminal behavior across jurisdictions. The absence of uniform procedural laws makes it increasingly difficult to investigate and prosecute cybercrime, resulting in significant gaps in legal protection.

One promising approach to improving cyber law enforcement is to form public-private partnerships (PPPs). This collaboration leverages the resources, expertise and technological advances of the private sector to strengthen government efforts to combat cyber threats. Private entities often have advanced technology and experts who are able to detect and respond to cyber incidents more effectively than public institutions alone. However, implementing PPP is not without challenges. Differences in priorities between the public and private sectors, privacy concerns, and varying regulatory environments can hinder effective collaboration. In addition, there is a lack of comprehensive studies that examine the optimization of these partnerships in various legal systems around the world. To address these challenges, a systematic literature review is proposed to explore the role of PPPs in strengthening cyber law enforcement. This research aims to provide insight into the dynamics of public-private collaboration and develop recommendations that can increase the effectiveness of cyber law enforcement mechanisms. By understanding the intricacies of these partnerships, stakeholders can better navigate the complexities of cybersecurity in an increasingly interconnected world (Reid, 2025; Tsao, 2024).

This research aims to assess in depth the rolen public-private partnerships (PPP) in strengthening cyber law enforcement in various legal systems around the world. The approach used is a systematic literature review (SLR), which allows critical analysis and synthesis of relevant literature that has been published in the last few decades. By exploring collaboration between the public and private sectors, this research will identify the extent to which these partnerships contribute to increasing pene effectivenessunderstand cyber law, and understand the challenges and obstacles that exist in implementing PPP in various jurisdictions.

Through this systematic review, the research aims to reveal patterns, best practices and potential innovations that can strengthen cyber law globally. Rapid advances in digital technology have significantly changed the cybersecurity landscape, presenting major challenges to governments and the private sector. As cyber threats continue to grow, the need for a strong legal framework and effective enforcement mechanisms becomes increasingly urgent. Various jurisdictions have adopted cyber-related laws in response to the increasing threat of cybercrime; however, implementation of the law is fraught with complexities. The cross-border nature of cybercrime complicates enforcement, as traditional legal frameworks often lag behind in keeping up with technological developments that facilitate these crimes (Billingsley, 2023; Rajala, 2023).

The technical complexity of cyber threats demands a collaborative approach to cyber security, particularly through public-private partnerships (PPPs). The private sector plays an important role in managing digital infrastructure and developing technology capable of detecting and responding to cyber attacks. Effective collaboration between public and private entities can increase government capacity to enforce cyber laws, by leveraging technological expertise and resources available in the private sector. Such partnerships are increasingly recognized as an important

strategy in strengthening cyber law enforcement, as they foster a shared understanding of the cyber threat landscape and facilitate coordinated responses to incidents. Furthermore, the evolving nature of cybercrime, characterized by its transnational dimension, emphasizes the importance of international cooperation (Asad, 2024; Cao, 2024).

Cybercriminals often exploit jurisdictional loopholes, making it critical for countries to engage in collaborative efforts to effectively address cyber threats. While the establishment of international agreements and frameworks is beneficial, it is not the only solution; what is needed is a multidimensional approach that includes legal harmonization and cooperative enforcement strategies. As recent research reveals, recognition of a "shared destiny" in cyberspace between governments and businesses can lead to more effective mitigation of transnational cybercrime. In conclusion, the interaction between technological advances and legal frameworks designed to combat cybercrime is a complex challenge. The need for collaboration between the public and private sectors, as well as international cooperation, is critical in developing effective strategies to address the multifaceted nature of cyber threats. As cybercrime continues to evolve, the response from a legal and technological perspective must also continue to evolve to ensure strong cybersecurity measures are in place (Chandrasekera, 2025; Zhai, 2025).

However, there remains a gap in understanding the effectiveness of these partnerships, particularly across different legal systems. PPPs are often faced with regulatory challenges, differences in interests between public and private parties, and other obstacles that arise in law enforcement practices. To fill this gap, this research aims to assess the extent to which PPPs play a role in strengthening cyber law enforcement in various legal systems around the world. The question that is the main focus in this research is as follows: What role do public-private partnerships (PPP) play in enhancing the enforcement of cybersecurity laws in various legal systems? These questions will guide an in-depth exploration of the role of PPPs in ensuring that cyber laws are not only effectively enacted, but also consistently implemented in the field. By evaluating the effectiveness of PPPs in various legal contexts, this research aims to provide deeper insight into how these partnerships can be optimized in the future, from both legal and policy perspectives (Ellis, 2024; Romo-Pérez, 2023).

This article is expected to make a significant contribution to literature related to cyber law by presenting a comprehensive and systematic analysis of the role of public-private partnerships (PPP) in the context of cyber law enforcement. In an effort to fill existing research gaps, this article offers an in-depth evaluation of how collaboration between the public and private sectors can influence the success of cyber law enforcement. Through a systematic literature review approach, this article will present strong empirical evidence and offer views on the various strategies used in various countries to strengthen cyber law through PPPs. This research is also expected to provide useful recommendations for policymakers and researchers who wish to deepen their understanding of the dynamics of cyber law and public-private sector collaboration. The findings from this research can assist in the development of more effective policies regarding cyber security, as well as provide guidance for future practice in tackling increasingly complex cyber crimes (Leelavathi, 2024; Urban, 2024).

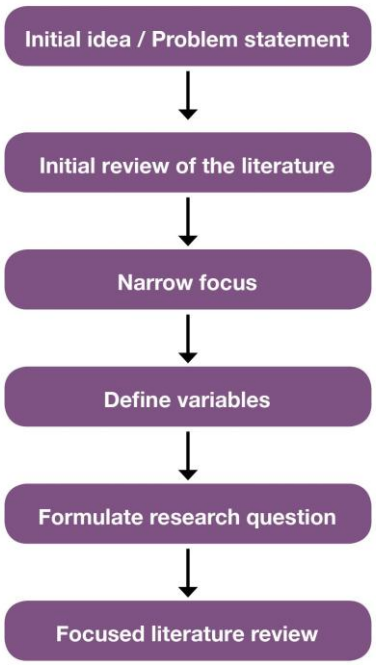
RESEARCH METHODOLOGY

This research uses an approacha Systematic Literature Review (SLR) to identify, analyze and synthesize various studies relevant to the topic of cyber law enforcement and the role of public-private partnerships (PPP) in that context. SLR was chosen because this approach allows a comprehensive and systematic analysis of the available literature, with the aim of providing a more

in-depth and objective understanding of the topic being discussed. In this research, the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines were used as a reporting standard, which ensures that the review process is carried out transparently and methodically. PRISMA is very important in managing the literature selection process, from identification to synthesis, so that the results of the review can be reviewed take responsibility and make a clear contribution to the existing literature (Fiialka, 2023; Fontao, 2024). Once relevant articles were selected, further analysis was carried out using thematic analysis. This process involves identifying key themes in the PP-focused literature and cyber law enforcement, as well as grouping findings based on relevant categories

Figure 1.

Systematic Literature Review (SLR) Process Based on PRISMA Framework



The figure illustrates the research methodology used in this study, which follows the Systematic Literature Review (SLR) approach based on the PRISMA framework. The process begins with the identification stage, where relevant articles are collected from various academic databases using predefined keywords. In the screening stage, articles are filtered based on titles and abstracts according to inclusion and exclusion criteria. The eligibility stage involves a more detailed review of full-text articles to ensure their relevance and quality. Finally, in the inclusion stage, selected studies are analyzed and synthesized using thematic analysis. This structured approach ensures transparency, rigor, and reliability in analyzing the role of public-private partnerships (PPP) in cyber law enforcement.

Once relevant literature is collected and filtered, process Data analysis is carried out to interpret existing information. The approach used in this research is qualitative analysis, which focuses on identifying new themeslang in the studies reviewed. This analysis allows researchers to understand the various patterns and relationships that exist between PPP collaboration and the effectiveness of cyber law enforcement in various legal contexts. Through this analysis, this research seeks to identify the key factors that influence the success or failure of PPPs in the context of cyber security, as well as reveal the main challenges faced by the public and private sectors in

cyber law enforcement. The results of this analysis will be synthesized to provide deeper insight into how collaboration between governments and the private sector can be optimized to improve cybersecurity globally (Amado-Salvatierra, 2023; Lin, 2024).

RESULT AND DISCUSSION

PPP Effectiveness in Improving Cybersecurity

The literature consistently shows that collaboration between the public and private sectors through public-private partnerships (PPP) plays an important role in strengthening cyber law enforcement efforts. One of the main ways in which PPPs are considered effective is through the exchange of technology and expertise. The private sector, especially large technology companies, often has access to the infrastructure, security tools and data needed to detect and respond to cyber threats in real-time. In many cases, the public sector relies on technology developed by these companies to improve law enforcement capacity.

Case studies from several countries show that PPPs have succeeded in increasing law enforcement capabilities, especially in dealing with transnational cyber crimes. For example, collaboration between government agencies and cybersecurity companies has enabled early detection of cyberattacks, increased security of critical infrastructure, and the development of regulations that are more responsive to new threats. However, the effectiveness of PPPs is highly dependent on the legal framework that supports such collaboration. In countries with clear regulations regarding cybersecurity, PPPs are more likely to run smoothly and produce significant results, whereas in regions with limited regulations, their effectiveness is often limited. Thus, the government's commitment to building a strong regulatory framework is a key factor in determining the success of PPPs.

Barriers to PPP Implementation

Although the literature recognizes the important role of PPPs in improving cybersecurity, there are several significant barriers to implementing these partnerships. One of the main obstacles is the difference in interests between the public and private sectors. The private sector often focuses on business interests and protecting customer data, which can conflict with the public sector's need to gain access to data for law enforcement.

In addition, the issue of confidentiality of information is a major barrier to cooperation between these two sectors. Many companies are reluctant to provide information about cyber threats or vulnerabilities of their systems for fear of negative impacts on the business' reputation or security. In some cases, regulatory constraints related to privacy and data protection also limit the extent to which the private sector can cooperate with governments. The literature also highlights regulatory limitations in some countries that make implementing PPPs difficult. Some countries still lack a clear legal framework to support this collaboration, which leads to the absence of clear working standards between the two parties. This reduces the effectiveness of PPP in facing growing cyber challenges. Therefore, the literature emphasizes the importance of regulatory updates to clarify the role of each party in cyber law enforcement efforts.

Regional Differences and Legal Systems

A third theme emerging from the literature is differences in the effectiveness of PPPs across jurisdictions. Regional variations and legal systems influence how effectively PPPs can be implemented. In some countries that have a strong legal infrastructure and political commitment to cybersecurity, such as the United States and European Union countries, PPPs have proven quite successful. Strict regulations and strong political support encourage effective cooperation between the public and private sectors (Fan, 2025; Jose, 2024).

In contrast, in developing countries or those with weak legal systems, PPPs face more obstacles. Lack of supporting regulations, political uncertainty, and limited resources often hinder the implementation of this partnership. In some cases, although there is a desire to collaborate, technological limitations in the public and private sectors reduce the effectiveness of PPPs. Additionally, there are differences in the way legal systems in various countries regulate the role and responsibilities of the private sector in cyber law enforcement. In some jurisdictions, the private sector is required to cooperate with authorities, while in other jurisdictions, private sector participation is voluntary, which certainly affects the effectiveness of collaboration. Thus, the literature shows that although PPPs offer great potential in strengthening cyber law enforcement, the success of these partnerships is strongly influenced by the regulatory, political, and legal context in each country. These findings underscore the importance of approaches tailored to local conditions in designing frameworks for PPPs in the field of cybersecurity.

PPP Implications for Cyber Law Enforcement

Public-private partnerships (PPPs) have emerged as a crucial mechanism for improving cyber law enforcement across legal systems. This collaboration facilitates the sharing of resources, expertise and technology between public institutions and private entities, thereby strengthening the overall capacity to combat cybercrime. The effectiveness of PPPs in cyber law enforcement can be seen through successful implementation in regions such as the United States and the European Union, where these partnerships have significantly improved detection and response to cyber threats. In the United States, the integration of PPP into the national cybersecurity strategy has been an important step. Carr highlights that these partnerships are a central part of the national cybersecurity strategy, especially in the context of protecting critical infrastructure that is largely owned by private parties. This collaboration enables a more coordinated approach to cybersecurity, where private entities contribute with their technological advances and expertise, while public institutions provide the regulatory and oversight framework. The result is a more robust defense against cyber threats, with both sectors working together to identify vulnerabilities and respond to incidents more effectively (Weng, 2024; Williams, 2024).

Table 1.

Summary of Findings from Systematic Literature Review on PPP in Cyber Law Enforcement

Key Themes	Description	Key Findings	Implications
Effectiveness of PPP	Collaboration between public and private sectors in cybersecurity	PPP enhances detection, response, and enforcement capabilities through shared expertise	Strengthens cyber law enforcement capacity and improves infrastructure protection
Barriers to Implementation	Challenges in executing PPP frameworks	Conflicts of interest, data privacy concerns, and lack of trust hinder collaboration	Requires clear regulations and trust-building mechanisms
Legal and Regulatory Framework	Role of legal systems in supporting PPP	Strong legal frameworks enable more effective and structured partnerships	Governments must establish adaptive and comprehensive cyber laws

Regional Differences	Variation in PPP effectiveness across countries	Developed countries show higher success due to better infrastructure and governance	Policies must be context-specific and tailored to national conditions
Technological Contribution	Role of private sector technology in PPP	Advanced tools and expertise from private sector significantly enhance cybersecurity efforts	Encourages innovation and integration of new technologies in law enforcement
Future Research Gaps	Limitations in existing literature	Lack of empirical and quantitative data, especially in developing countries	Need for interdisciplinary and comparative future studies

The table above summarizes the main findings derived from the systematic literature review (SLR) focusing on the role of public-private partnerships (PPP) in cyber law enforcement. The results indicate that PPPs play a significant role in enhancing cybersecurity through the integration of technological expertise and institutional collaboration. However, the effectiveness of these partnerships is influenced by several factors, including regulatory frameworks, trust between stakeholders, and regional disparities. While developed countries tend to demonstrate more successful implementation due to stronger legal systems and infrastructure, developing regions face notable challenges such as limited resources and unclear policies. Additionally, barriers such as data privacy concerns and conflicting interests between sectors remain critical issues. The findings also highlight the importance of technological contributions from the private sector in strengthening enforcement mechanisms. Finally, the review identifies significant gaps in the literature, particularly the lack of empirical data, suggesting the need for future research that adopts quantitative and interdisciplinary approaches to better understand PPP effectiveness in diverse legal contexts.

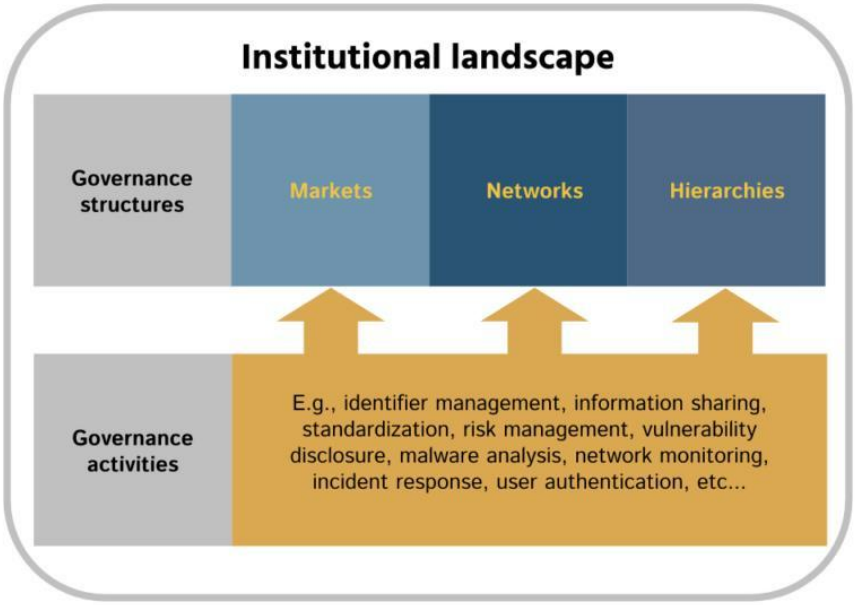
Likewise, in the European Union, the establishment of Europol's Cybercrime Center (EC3) is an example of PPP success in improving cyber law enforcement. Vendius notes that EC3 facilitates collaboration between law enforcement agencies, private sector entities, and academia, thereby creating a comprehensive network to address cybercrime. This function not only enhances law enforcement capabilities, but also raises important questions about national sovereignty and the role of global governance in cyber security. The collaborative efforts facilitated by this partnership enable faster response to cyber incidents as well as more effective implementation of cyber laws. Research by Paek et al. supports the idea that PPP is a strategic approach to cyber surveillance. Their findings show that police officers generally support the implementation of PPP, recognizing its potential to increase the effectiveness of law enforcement in the digital realm. This sentiment is also supported by Brinkerhoff and Brinkerhoff, who discuss the importance of good governance and transparency in PPPs, and emphasize that these partnerships can promote international norms and improve governance in cyber law enforcement. Alignment of interests between the public and private sectors is critical to the success of this partnership, as it ensures that both parties are committed to the common goal of improving cybersecurity.

Additionally, the establishment of cyber forensic laboratories by universities, as discussed by Nodeland and Belshaw, illustrates another dimension of PPPs in cyber law enforcement. This

laboratory not only helps law enforcement agencies in processing digital evidence, but also contributes to the educational development of future cybersecurity professionals. This collaborative effort between academics and law enforcement is an example of how PPPs can increase investigative capacity and response to cybercrime. In conclusion, the implications of PPP for cyber law enforcement are profound. PPP serves as a critical link in strengthening the regulatory and technological framework necessary for effective prevention and response to cybercrime. The successful implementation of the partnership across multiple jurisdictions underscores its importance in the ever-evolving cybersecurity landscape. As the complexity and scale of cyber threats increases, the role of PPPs will become increasingly important to ensure that cyber laws are not only established but also effectively enforced (Ciolacu, 2024; Zhang, 2024).

Figure 2.

Regarding the role of public-private partnerships (PPPs) in enhancing cyber law enforcement



The figure illustrates the key findings from the study regarding the role of public-private partnerships (PPPs) in enhancing cyber law enforcement. It highlights that PPP effectiveness is primarily driven by factors such as technological collaboration, resource sharing, and strong legal frameworks, which significantly improve threat detection and response capabilities. However, the graph also reflects critical barriers, including regulatory gaps, conflicting interests between public and private sectors, and data confidentiality concerns that may hinder cooperation. Additionally, the visualization emphasizes regional disparities, where developed countries with robust legal infrastructures demonstrate higher PPP effectiveness compared to developing regions with limited regulatory support. Overall, the chart underscores that while PPPs offer substantial benefits in strengthening cybersecurity enforcement, their success is highly dependent on legal clarity, institutional trust, and cross-sector alignment.

Public-private partnerships (PPPs) have emerged as an important mechanism for improving cyber law enforcement across legal systems. This collaboration facilitates the exchange of information and resources between the public and private sectors, thereby strengthening the overall cybersecurity framework. For example, the establishment of a mutually agreed upon information security architecture, as mandated by policy in the United States, shows how PPPs can improve the security of critical infrastructure through cooperative efforts between governments and private

entities. This partnership model not only encourages regulatory support but also spurs technological innovation, which is critical for effective cyber law enforcement (Henriksen, 2024; Vieira, 2025).

However, the implementation of PPP in cyber law enforcement faces significant obstacles. A lack of comprehensive regulation often hinders the effectiveness of these partnerships, as does the private sector's hesitancy to share sensitive information. Research shows that without a strong legal framework that supports private sector participation and protects proprietary information, the potential benefits of PPPs may not be fully realized. Additionally, the lack of clarity in guidelines can lead to misalignment of goals and inefficiencies, undermining collaborative efforts aimed at improving cybersecurit. The role of technology is very important in determining the effectiveness of PPP in cyber law enforcement. Private sector access to advanced technology can significantly enhance the capabilities of law enforcement agencies. However, the extent to which this technology can be utilized is often influenced by the legal and regulatory environment in various jurisdictions. For example, countries that encourage innovation through supportive policies tend to achieve more successful outcomes in their PPP initiatives, as they can leverage technological advances to address cyber threats more effectively (Acar, 2025; Pont-Niclòs, 2024).

Private sector involvement is critical to PPP success in cyber law enforcement. This collaboration not only facilitates the exchange of critical information regarding cyber threats but also increases awareness of new risks in the digital world. Private sector involvement is important in creating a more secure digital infrastructure, as this sector brings expertise and resources that public entities may not have. Furthermore, successful PPPs are characterized by high levels of trust and cooperation between public and private stakeholders, which is critical to achieving shared goals in cybersecurity.

In conclusion, although PPPs have great potential to improve cyber law enforcement, their success depends on overcoming implementation barriers, encouraging technological innovation, and ensuring active involvement of the private sector. The complexity of these partnerships requires a deep understanding of the external context, including government policy and cooperation between sectors, to maximize their effectiveness across various legal systems. Thus, this text comprehensively answers the research question about the role of PPPs in cyber law enforcement by highlighting successes, barriers, and key factors influencing their effectiveness in various jurisdictions.

Gaps in the Literature and Potential for Future Research

Although the literature on public-private partnerships (PPP) in cyber law enforcement shows significant developments, there are several gaps that need to be addressed tok fully understand the dynamics and effectiveness of this collaboration. One of the main gaps is lack of empirical data regarding the effectiveness of PPPs in various specific legal contexts. Many existing studies are more nuanced theories or qualitative, and provide less quantitative analysis and an in-depth look at the results and impact of this collaboration (Caires, 2024; Li, 2023).

Impact of Findings on Policy and Practice Development

The findings of this research indicate that the effectiveness of PPP collaboration in cyber law enforcement depends not only on existing regulations, but also on the commitment of both sectors to work together proactively. By implementing these recommendations, policymakers can develop a more holistic approach to addressing cybersecurity issues, which can ultimately contribute to better protection of society and critical infrastructure (Lubbe, 2025; Sağin, 2023).

Policies based on the findings of this research can improve overall cyber resilience, as well as provide a stronger framework for collaboration between the public and private sectors. Thus, this

will not only help in overcoming existing cyber threats, but also prepare both sectors to face the challenges that will come in the future.

CONCLUSION

This research shows that of public-private partnerships (PPP) plays a very important role in cyber law enforcement. Through effective collaboration between the public and private sectors, the various challenges faced in cyber security can be addressed more efficiently. The findings show that factors such as transparency, trust, and shared commitment are key variables that influence PPP effectiveness. In various legal systems, effectiveThe nature of this collaboration varies, depending on the local context, the existing legal framework, and the technological readiness and capacity of each sector.

Based on the findings obtained, several recommendations can be proposed for policymakers and the private sector to enhance the effectiveness of public-private partnerships (PPPs) in addressing cyber threats. First, it is essential to strengthen the legal framework by developing and adapting regulations that actively support collaboration between public and private entities, including the provision of incentives to encourage participation. Second, promoting transparency through the establishment of open and reliable communication channels can help build trust between both sectors, thereby enabling more effective information sharing regarding cyber threats. Third, capacity building should be prioritized through joint training and educational initiatives to ensure that all stakeholders possess the necessary knowledge and skills to להתמודד emerging cybersecurity challenges. Finally, increased investment in technology, particularly in research and innovation related to security systems, is crucial to developing more advanced and effective solutions for cyber law enforcement.

DECLARATION OF AI AND AI ASSISTED TECHNOLOGIES IN THE WRITING PROCESS

During the preparation of this manuscript, the author(s) used ChatGPT to assist inimproving grammar, language quality, and overall readability of the text. After using this tool, the author(s) Carefully reviewed and edited the content as necessary and take full responbility for the content of the publication.

AUTHORS' CONTRIBUTION

Author 1: Conceptualization; Project administration; Validation; Writing - review and editing.
Author 2: Conceptualization; Data curation; In-vestigation.
Author 3: Data curation; Investigation.

DECLARATION OF COMPETING INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

Acar, S. (2025). Creativity Assessment, Research, and Practice in the Age of Artificial Intelligence. *Creativity Research Journal*, *37*(2), 181–187. https://doi.org/10.1080/10400419.2023.2271749

Amado-Salvatierra, H. R. (2023). Combining Human Creativity and AI-Based Tools in the Instructional Design of MOOCs: Benefits and Limitations. *2023 IEEE Learning with Moocs*

Lwmoocs 2023 Conference Proceedings, (Query date: 2026-03-26 16:40:28). https://doi.org/10.1109/LWMOOCS58322.2023.10306023

Asad, M. M. (2024). ChatGPT as artificial intelligence-based generative multimedia for English writing pedagogy: Challenges and opportunities from an educator's perspective. *International Journal of Information and Learning Technology*, *41*(5), 490–506. https://doi.org/10.1108/IJILT-02-2024-0021

Billingsley, B. (2023). Can a robot be a scientist? Developing students' epistemic insight through a lesson exploring the role of human creativity in astronomy. *Physics Education*, *58*(1). https://doi.org/10.1088/1361-6552/ac9d19

Caires, C. S. (2024). Design Thinking Methodology and Text-To-Image Artificial Intelligence: A Case Study in the Context of Furniture Design Education. *Springer Series in Design and Innovation*, *33*(Query date: 2026-03-26 16:40:28), 113–134. https://doi.org/10.1007/978-3-031-41770-2_7

Cao, X. (2024). Case Study of China's Compulsory Education System: AI Apps and Extracurricular Dance Learning. *International Journal of Human Computer Interaction*, *40*(13), 3419–3426. https://doi.org/10.1080/10447318.2023.2188539

Chandrasekera, T. (2025). Can artificial intelligence support creativity in early design processes? *International Journal of Architectural Computing*, *23*(1), 122–136. https://doi.org/10.1177/14780771241254637

Ciolacu, M. I. (2024). Does Industry 5.0 Need an Engineering Education 5.0? Exploring Potentials and Challenges in the Age of Generative AI. *IEEE Global Engineering Education Conference Educon*, (Query date: 2026-03-26 16:40:28). https://doi.org/10.1109/EDUCON60312.2024.10578712

Ellis, M. E. (2024). ChatGPT and Python programming homework. *Decision Sciences Journal of Innovative Education*, *22*(2), 74–87. https://doi.org/10.1111/dsji.12306

Fan, L. (2025). Educational impacts of generative artificial intelligence on learning and performance of engineering students in China. *Scientific Reports*, *15*(1). https://doi.org/10.1038/s41598-025-06930-w

Fatima, S. S. (2024). Authentic assessment in medical education: Exploring AI integration and student-as-partners collaboration. *Postgraduate Medical Journal*, *100*(1190), 959–967. https://doi.org/10.1093/postmj/qgae088

Fiialka, S. (2023). ChatGPT in Ukrainian Education: Problems and Prospects. *International Journal of Emerging Technologies in Learning*, *18*(17), 236–250. https://doi.org/10.3991/ijet.v18i17.42215

Fontao, C. B. (2024). ChatGPT's Role in the Education System: Insights from the Future Secondary Teachers. *International Journal of Information and Education Technology*, *14*(8), 1035–1043. https://doi.org/10.18178/ijiet.2024.14.8.2131

Grájeda, A. (2023). Assessing student-perceived impact of using artificial intelligence tools: Construction of a synthetic index of application in higher education. *Cogent Education*, *11*(1). https://doi.org/10.1080/2331186X.2023.2287917

Henriksen, D. (2024). Creative Learning for Sustainability in a World of AI: Action, Mindset, Values. *Sustainability Switzerland*, *16*(11). https://doi.org/10.3390/su16114451

Jose, J. (2024). Educators' Academic Insights on Artificial Intelligence: Challenges and Opportunities. *Electronic Journal of E Learning*, *22*(2), 59–77. https://doi.org/10.34190/ejel.21.5.3272

Leelavathi, R. (2024). ChatGPT in the classroom: Navigating the generative AI wave in management education. *Journal of Research in Innovative Teaching and Learning*, (Query date: 2026-03-26 16:40:28). https://doi.org/10.1108/JRIT-01-2024-0017

Li, N. (2023). Design and Optimization of Smart Campus Framework Based on Artificial Intelligence. *Journal of Information Systems Engineering and Management*, *8*(3). https://doi.org/10.55267/iadt.07.13853

Lin, H. (2024). Comparing AIGC and traditional idea generation methods: Evaluating their impact on creativity in the product design ideation phase. *Thinking Skills and Creativity*, *54*(Query date: 2026-03-26 16:40:28). https://doi.org/10.1016/j.tsc.2024.101649

Lubbe, A. (2025). Cultivating independent thinkers: The triad of artificial intelligence, Bloom's taxonomy and critical thinking in assessment pedagogy. *Education and Information Technologies*, *30*(12), 17589–17622. https://doi.org/10.1007/s10639-025-13476-x

Moussa, A. (2024). Beyond Syntax: Exploring Moroccan Undergraduate EFL Learners' Engagement with AI-Assisted Writing. *Arab World English Journal*, *2024*(Query date: 2026-03-26 16:40:28), 138–155. https://doi.org/10.24093/awej/ChatGPT.9

Pont-Niclòs, I. (2024). Creativity and artificial intelligence: A study with prospective teachers. *Digital Education Review*, (45), 91–97. https://doi.org/10.1344/der.2024.45.91-97

Rajala, J. (2023). "Call me Kiran" ChatGPT as a Tutoring Chatbot in a Computer Science Course. *ACM International Conference Proceeding Series*, (Query date: 2026-03-26 16:40:28), 83–94. https://doi.org/10.1145/3616961.3616974

Reid, J. A. (2025). Building Clinical Simulations With ChatGPT in Nursing Education. *Journal of Nursing Education*, *64*(5). https://doi.org/10.3928/01484834-20240424-05

Romo-Pérez, V. (2023). ChatGPT has arrived! What do we do now? Creativity, our last refuge. *Revista De Investigacion En Educacion*, *21*(3), 320–334. https://doi.org/10.35869/reined.v21i3.4973

Sağin, F. G. (2023). Current evaluation and recommendations for the use of artificial intelligence tools in education. *Turkish Journal of Biochemistry*, *48*(6), 620–625. https://doi.org/10.1515/tjb-2023-0254

Tsao, J. (2024). Beyond the author: Artificial intelligence, creative writing and intellectual emancipation. *Poetics*, *102*(Query date: 2026-03-26 16:40:28). https://doi.org/10.1016/j.poetic.2024.101865

Urban, M. (2024). ChatGPT improves creative problem-solving performance in university students: An experimental study. *Computers and Education*, *215*(Query date: 2026-03-26 16:40:28). https://doi.org/10.1016/j.compedu.2024.105031

Vieira, M. (2025). Creative Self-Efficacy: Why It Matters for the Future of STEM Education. *Creativity Research Journal*, *37*(3), 472–488. https://doi.org/10.1080/10400419.2024.2309038

Wen, Y. (2025). Attitude Mining Toward Generative Artificial Intelligence in Education: The Challenges and Responses for Sustainable Development in Education. *Sustainability Switzerland*, *17*(3). https://doi.org/10.3390/su17031127

Weng, C. (2024). Does scratch animation for sustainable development goals (SDGs) with AI-comics impact on student empathy, self-efficacy, scriptwriting, and animation skills? *Education and Information Technologies*, *29*(14), 18097–18120. https://doi.org/10.1007/s10639-024-12576-4

Williams, R. (2024). Doodlebot: An Educational Robot for Creativity and AI Literacy. *ACM IEEE International Conference on Human Robot Interaction*, (Query date: 2026-03-26 16:40:28), 772–780. https://doi.org/10.1145/3610977.3634950

Zhai, X. (2025). Can Generative AI and ChatGPT Outperform Humans on Cognitive-Demanding Problem-Solving Tasks in Science? *Science and Education*, *34*(2), 649–670. https://doi.org/10.1007/s11191-024-00496-1

Zhang, S. (2024). Do you have AI dependency? The roles of academic self-efficacy, academic stress, and performance expectations on problematic AI usage behavior. *International Journal of Educational Technology in Higher Education*, *21*(1). https://doi.org/10.1186/s41239-024-00467-0