JLPH: Journal of Law, Politic and Humanities
E-ISSN: 2962-2816
P-ISSN: 2747-1985
https://dinastires.org/JLPH dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/jlph.v5i5

Collaborative Policing to Combat Cyber Crime in Banking Sector Modelling – a Systematic Literature Review

Wani Sabu[1], Albertus Wahyurudhanto[2], Puspitasari[3], Bambang Pratama[4].
[1]Sekolah Tinggi Ilmu Kepolisian - PTIK, Jakarta, Indonesia, nathalya.wani@gmail.com.
[2]Sekolah Tinggi Ilmu Kepolisian - PTIK, Jakarta, Indonesia, wrudhanto@gmail.com.
[3]Universitas Indonesia, Jakarta, Indonesia, mipuspita@gmail.com.
[4]Bina Nusantara University, Jakarta, Indonesia, bptama@binus.ac.id

Corresponding Author: nathalya.wani@gmail.com[1]

Abstract: This study addresses the increasing threats of cybercrime that endanger the stability of banking industry, driven by the rapid growth of digital financial transactions. The objective of this research is to formulate a collaborative policing model to effectively prevent and respond to cybercrime within the banking sector. The research was conducted through a comprehensive literature study that explored various aspects of cybersecurity, inter-agency collaboration, technology management, and the roles of actors in cyberspace. The findings indicate that an effective collaborative policing strategy requires the integration of multiple components such as initial conditions, motivation, key actors, emerging technologies, vulnerabilities, international legal frameworks, cyber diplomacy, collaborative processes, and outcome governance. The collaboration process must be built on open dialogue, strong commitment, mutual trust, and shared consensus to create adaptive and sustainable cyber resilience. The conclusion of this study is that a collaborative policing model can serve as a strategic approach to enhance the effectiveness of cybercrime prevention and response efforts in Indonesia's digital financial sector

Keyword: Collaborative Policing, Cybercrime, Banking Industry, Digital Resilience.

INTRODUCTION

The number of financial transactions using digital services in Indonesia has experienced significant growth. In October 2022, digital financial transactions were recorded at IDR 49.34 trillion. On the payment system side, the transaction value of the Quick Response Code Indonesian Standard or commonly known as QRIS increased by 298 percent from the beginning of the year to September 2022, reaching IDR 29.7 trillion. The value of electronic money transactions across all channels increased by 43.2 percent annually, reaching IDR 35.5 trillion. Meanwhile, the value of digital banking transactions increased by 30.9 percent annually, reaching IDR 9,002 trillion until November 2022. In 2024, QRIS was recorded to have experienced rapid growth of up to 194.06 percent annually in April 2024 with the number of users reaching 48.90 million and the number of merchants 31.86 million. In addition, in August

2024, QRIS transactions grew 217.33 percent annually with the number of users reaching 52.55 million and the number of merchants reaching 33.77 million.

In the era of rapidly developing digital transformation, the banking sector in Indonesia faces increasingly complex and significant cybercrime threats, including phishing attacks, hacking of funds, identity theft, and social engineering. With the dominance of digital transactions in several large banks, this industry is a prime target for cybercriminals, given its vital role as a pillar of national economic stability. In addition to causing significant financial losses, cybercrime also threatens the reputation and public trust in banking institutions, as well as creating new challenges in the regulatory and law enforcement framework. The absence of a clear legal framework, minimal cross-sector coordination, and limited resources in digital forensic investigations worsen this situation, so that only a small portion of the proceeds of crime can be recovered.

In this context, a collaborative policing approach, involving synergy between law enforcement officers, regulators, the community and the financial industry, becomes relevant as a strategic effort to prevent and combat cybercrime. This collaboration is not only important to improve the security of digital systems, but is also needed to build public trust, strengthen economic stability, and support the growth of the banking industry in Indonesia amidst the ever-evolving cyber threat landscape. For this reason, a collaborative policing model is needed that can overcome cybercrime.

METHOD

This research employs a systematic literature review method to identify, synthesize, and analyze studies related to collaborative policing efforts in combating cybercrime within the banking sector. The process was conducted with the aim of constructing a conceptual model that captures the dynamics of inter-agency and cross-sector collaboration relevant to cybercrime threats in financial institutions. Literature was sourced from two academic search engines, Scopus and Google Scholar, using a combination of keywords including “collaborative policing”, “cybercrime”, “banking sector”, “framework”, and “model”.

The search yielded a total of 320 documents, including journal articles, conference proceedings, and book chapters published between 2019 and 2024. Each article was screened through a three-step selection process. First, an initial screening based on titles and abstracts was carried out to eliminate duplicates and irrelevant studies, resulting in 114 articles. Second, full-text reviews were conducted on these selected articles to assess their relevance to the research objectives, leading to a final inclusion of 34 articles. These final studies were chosen based on their substantial discussion of collaborative mechanisms, cybercrime strategies, or specific case studies in the banking and financial sectors.

To ensure the quality of the review, only peer-reviewed academic publications written in English and accessible in full text were considered. Articles were excluded if they focused solely on technical detection systems without addressing institutional or collaborative frameworks, were published before 2019, or lacked clear relevance to the financial services context. Data extraction was performed manually, focusing on several key variables: actors involved in collaboration (e.g., police, computer emergency response team or CERT, private banks), types of cybercrime addressed (e.g., phishing, ransomware, digital fraud), level and scope of cooperation (e.g., national, regional, international), and conceptual or operational frameworks used to evaluate success or barriers.

The selected articles were analyzed qualitatively to identify patterns, challenges, and proposed models of collaboration. The review culminated in a synthesized conceptual model illustrating essential dimensions of collaborative policing within cybercrime response ecosystems in the banking sector.

RESULTS AND DISCUSSION

Base on previous research on collaborative governance in Indonesian police (Aditya & Kusumastuti, 2023), researcher looking for from the literature review to create a modelling for banking industry. And it was found that the components of collaborative policing to handle cybercrime in the banking industry are as follows:

1) Initial condition
   a) Antecedents
      Antecedents are an initial condition that shapes organization readiness in response to cyber crime activities that relate to their organization with components like motivation, actor, emerging technologies and vulnerabilities. Motivation in cybersecurity is shaped by threat perception and self-efficacy, where increased awareness through simulations or campaigns encourages protective actions like encryption and staff training (Al-Kumaim & Alshamsi, 2023) and also real life simulation to prepare staff like cyber attack simulation (Gerdenitsch et al., 2023). The role of key actors such as leaders, IT managers, and policymakers is critical in ensuring cybersecurity governance, alongside external contributors like consultants and government agencies (Pomerleau & Lowery, 2020b). Additionally, emerging technologies like AI and blockchain enhance detection and response capabilities, offering both efficiency and broader threat mitigation (Pomerleau & Lowery, 2020a).
   b) Externalities
      Externalities in cybersecurity refer to broader factors beyond internal organizational control that significantly influence how cyber threats are managed and mitigated. These include legal, political, and diplomatic dimensions that shape international coordination and policy responses. International law plays a crucial role in governing cross-border cyber activities, with frameworks like the Budapest Convention enabling nations to cooperate in preventing, detecting, and prosecuting transnational cybercrime (Y. Li & Liu, 2021). Alongside legal efforts, cyber politics and diplomacy serve as mechanisms for addressing global threats such as state-sponsored attacks and digital espionage. Through platforms like the United Nations Group of Governmental Experts on Information Security (UNGGE), countries engage in negotiations to establish norms, reduce tensions, and promote regulatory harmonization and multilateral trust in cyberspace(Y. Li & Liu, 2021).
2) Cyber space
   Cyberspace is an ecosystem that includes information technology networks, interconnected devices, and users who utilize digital platforms for various activities(McGregor et al., 2024). Cyberspace also includes social and legal dimensions, making it an arena of complex interactions that require strong regulation and security (Gunawan et al., 2021).
   a) Cyber threat vector
      In the context of cyber security and digital law enforcement, harmful activities in cyberspace can be categorized into several forms. Cyber deviance refers to unauthorized network exploitation or malware dissemination, often driven by economic or ideological motives (Martineau et al., 2023). Cyber crime includes online fraud, illegal trade, and the digital exploitation of children, threats that have escalated alongside rapid technological adoption (Lusthaus, 2024). More aggressive forms, such as cyber attacks, involve operations like distributed denial of service (DdoS) designed to disrupt institutional or governmental functions and often result in significant economic damage (Y. Li & Liu, 2021). Cyber terrorism leverages digital tools to instill public fear, for example by sabotaging transportation systems or spreading extremist propaganda (Pomerleau & Lowery, 2020a). Cyber espionage involves the theft of sensitive or strategic information, typically carried out by state actors targeting political or economic rivals (Ali et al., 2024). In extreme cases, this escalates into cyber war, where nations

engage in digital conflict targeting critical infrastructure such as power grids and health systems(Pratama & Bamatraf, 2021). Lastly, cyber disputes emerge from contractual violations or digital policy breaches, often requiring mediation or arbitration for resolution (Calliess & Baumgarten, 2020).

b) Human elements

Effective cyber defense relies on continuous education and awareness campaigns to enhance individual understanding of cyber threats (Bada & Nurse, 2021). Organizational responses are also shaped by cyber risk perception, as limited awareness can lead to poor resource allocation and increased vulnerability (McGregor et al., 2024). Strong technical capabilities, including firewalls, threat analytics, and intrusion detection systems, are essential for competent security teams (Y. Li & Liu, 2021). Additionally, workforce competencies, supported by training and certification, play a critical role in addressing complex security challenges (Martineau et al., 2023).

c) Managerial and organizational

Managerial roles in cybersecurity are essential for embedding security as a strategic priority and ensuring consistent implementation across organizational levels. Leadership must align values, objectives, and strategies to reflect cybersecurity as a core component of operational resilience (Oyeniyi et al., 2024). A well-formulated strategy should engage all departments, fostering a holistic security culture. Clear and structured policies further reinforce this by guiding employee behavior and clarifying responsibilities in safeguarding data and systems (Pomerleau & Lowery, 2020a). Additionally, managing fraud whether internal or external requires the integration of advanced digital surveillance tools and routine audits to detect anomalies and prevent security breaches (Y. Li & Liu, 2021).

d) Technical and infrastructure

Technological and infrastructural components are foundational to effective cybersecurity management. Robust physical infrastructure including servers, data centers, and communication networks must be designed for resilience, such as through geographically distributed backups to withstand cyberattacks (McGregor et al., 2024). Cybersecurity processes involve deploying tools like firewalls, antivirus software, and AI-based monitoring systems, alongside establishing internal policies and staff training programs (Tridgell, 2025). The rise of the Internet of Things (IoT) has expanded the attack surface, requiring measures like end-to-end encryption and device authentication to mitigate risks (Pomerleau & Lowery, 2020a). Blockchain technology contributes by providing decentralized security that ensures data integrity across financial transactions, supply chain systems, and secure digital voting (Pomerleau & Lowery, 2020a). Finally, Artificial Intelligence (AI) enhances proactive defense by detecting anomalies in network traffic and enabling automated threat responses through machine learning models that predict attacks before they occur (Pugnetti et al., 2024).

e) Cyber threat intelligence

Cyber Threat Intelligence (CTI) refers to the collection, analysis, and sharing of information related to current and potential cyber threats to enhance organizational readiness. CTI enables organizations to detect and respond to cyberattacks more effectively by leveraging shared insights into attack patterns and threat actor behavior. Crowd-sourced CTI platforms such as the Malware Information Sharing Platform (MISP) facilitate real-time exchange of threat data while maintaining strict data security protocols, thus fostering collaborative defense ecosystems (Jesus et al., 2024). By integrating CTI into their security operations, organizations can significantly improve their ability to preemptively mitigate threats and reduce incident response time.

f) Cyber resilience

Cyber resilience is the organization's capacity to anticipate, withstand, recover from, and adapt to adverse cyber incidents, and it has become a strategic imperative for modern enterprises, particularly in the financial sector (Papuashvili, 2023). As cyber threats evolve in frequency, complexity, and scope ranging from ransomware and DDoS attacks to data breaches and digital espionage, companies must move beyond traditional defense mechanisms toward integrated resilience frameworks that emphasize risk anticipation, adaptive response, and continuous recovery (Asakpa & Chaifetz, 2023). Investing in cyber resilience not only strengthens technical defenses through AI-based detection and zero trust architectures, but also fosters institutional stability, regulatory compliance, and public trust, ensuring that operations can continue even during active cyberattacks (Jooda et al., 2023).

3) Collaborative process
   a) Dialogue
   Effective dialogue is at the heart of the collaboration process. Open, transparent, and inclusive dialogue allows the parties involved to align perceptions, discuss differences, and find common solutions. Formal and structured forums are an important medium to ensure that this dialogue runs smoothly(Aditya & Kusumastuti, 2023).
   b) Commitment
   Commitment is the main foundation of successful collaboration. All parties involved need to demonstrate clear dedication, both formally through agreements and informally through shared value agreements. In this context, a history of positive working relationships can be an important asset for building initial trust. On the other hand, conflicts of interest or lack of clarity in motivation can be serious obstacles in ensuring the sustainability of cooperation(Hapsari & Meliala, 2022).
   c) Trust
   Trust is not only an important element, but also a catalyst in driving successful collaboration. Trust needs to be built through transparency, consistent communication, and concrete actions that demonstrate the good intentions of all parties involved. In inter-institutional collaboration, trust often grows from regular interaction and respect for each party's contribution(Feradinata, 2023).
   d) Relationship
   Strong relationships are the mainstay of sustainable collaboration. These relationships must be based on mutual respect, effective communication, and inclusiveness in decision-making. Horizontal relationship structures, where all parties are treated equally, are essential to encourage active participation from various sectors(M. Li, 2017).
   e) Consensus
   The process of reaching consensus requires active involvement from all parties involved. Consensus is not just about agreeing on a decision, but also about aligning shared values, goals, and expectations. This process often includes in-depth negotiations to resolve differences in perceptions and views(Ansell & Gash, 2008).
   f) Intermediate outcome
   Intermediate outcomes, such as the development of a strategic plan or the achievement of small agreements, are important indicators of the sustainability of the collaboration process. These outcomes validate the effectiveness of the approach taken and serve as motivation for all parties to continue the collaboration.(Ansell & Gash, 2008)
   g) Knowledge management
   Good knowledge management is a supporting pillar for successful collaboration. Sharing information systematically through digital platforms or data-based systems ensures that all parties have equal access to relevant information. This not only increases

transparency but also speeds up the decision-making process(Weerawardhana & Wijewardhana, 2024).

4) Outcome
   a) Governance
   Effective cybersecurity governance relies on structured procedures, regulatory frameworks, and legal mandates to ensure organizational resilience. Key procedures include penetration testing, attack simulations, and routine audits to identify vulnerabilities and assess compliance, alongside strict incident monitoring and timely reporting protocols (Calliess & Baumgarten, 2020). Regulations such as the GDPR provide critical guidance on data protection and user rights, while innovative legal tools like regulatory sandboxes and sunset clauses support adaptive governance in the financial sector(Calliess & Baumgarten, 2020). Complementing these are cybersecurity laws, such as the Cybersecurity Act, which empower government bodies to enforce digital security, impose penalties, and require transparency through mandatory incident disclosure(Atkins & Lawson, 2021).
   b) Capabilities
   Organizational cybersecurity capabilities consist of technical proficiency, service readiness, and ongoing competency development. Technically, cybersecurity teams must master essential tools such as firewalls, intrusion detection systems, and threat analytics software, while also preparing for future threats through investment in emerging technologies like quantum-based encryption (Sweetman, 2022). On the service side, effective capabilities involve real-time threat monitoring, forensic investigations, and post-incident recovery, along with providing consulting and training to ensure all employees understand security protocols(Atkins & Lawson, 2021). Enhancing these capabilities requires structured competency uplift through certifications like CISSP, which strengthen staff expertise in threat analysis, policy enforcement, and incident response (Pugnetti et al., 2024).
   c) Cyber response
   Effective cyber response encompasses immediate containment actions, system recovery, continuous support, and structured dispute resolution. Quick and accurate responses, such as isolating infected devices or blocking compromised network access, are essential to limit the impact of an attack (Calliess & Baumgarten, 2020). Recovery efforts involve restoring systems from backups, reinforcing infrastructure, and conducting thorough evaluations to identify exploited vulnerabilities(Pugnetti et al., 2024). Support mechanisms during and after incidents include deploying technical teams and maintaining clear communication with stakeholders to ensure business continuity(Pomerleau & Lowery, 2020a). Additionally, resolving conflicts stemming from cyber incidents often requires Alternative Dispute Resolution (ADR) methods like mediation or arbitration, which offer faster and more flexible outcomes than traditional litigation, especially in complex digital environments (Calliess & Baumgarten, 2020).
   d) Technology
   Technology plays a crucial role in strengthening an organization's cyber defense through continuous upgrades, adoption of innovations, and financial risk mitigation. Regular technology upgrades, such as patching security software and replacing outdated hardware, are essential to close newly discovered vulnerabilities and maintain operational security (Calliess & Baumgarten, 2020). Emerging technologies like quantum cryptography introduce advanced methods for securing data against increasingly complex threats, positioning organizations to stay ahead of cyber adversaries (Despotović et al., 2023). Complementing these technical efforts, cyber insurance provides financial protection against losses from cyber incidents such as data

breaches and recovery costs while also supporting better risk planning through insurer-led risk assessments (Calliess & Baumgarten, 2020).

5) Supporting technology
Supporting technologies play a vital role in enabling effective collaboration, particularly across institutional and sectoral boundaries. Information systems support structured inter-organizational cooperation by facilitating data collection, workflow coordination, and shared access to relevant intelligence essential for joint operations such as law enforcement collaboration(Zhao et al., 2006). Meanwhile, technologies for smart governance enhance broader-scale coordination by providing data management platforms, tech-enabled decision-making tools, and integrated systems that connect diverse stakeholders within environments like smart cities or cross-agency(Ruijer et al., 2023). These technologies help align efforts and improve efficiency in achieving collective goals.
6) Collaborative stakeholders
Collaborative stakeholder engagement is fundamental to the success of cyber policing initiatives in the banking sector, involving diverse actors such as banking institutions, the general public, law enforcement agencies, regulators, legislators, and judicial or alternative dispute resolution (ADR) bodies including mediators and arbitrators. These stakeholders interact through multi-party collaboration models that leverage the unique resources, expertise, and perspectives of each sector ranging from government agencies to civil society and private actors to address complex threats collectively(Pajón & Walsh, 2023). Community-based collaboration, such as Community-Oriented Policing (COP), promotes grassroots involvement by positioning citizens not merely as beneficiaries but as active partners in maintaining security(Docherty & Russell, 2022). Moreover, innovation-driven collaboration emphasizes co-creation, where stakeholders jointly participate in problem-solving from early identification to implementation, fostering creative and inclusive solutions to cybersecurity challenges(Torfing et al., 2023).
7) Proposed assessment
Metrics and assessment are important components in supporting successful collaboration. Both serve to ensure that the collaboration process is running according to the goals that have been set, by providing data-based feedback that can be used for evaluation and improvement.

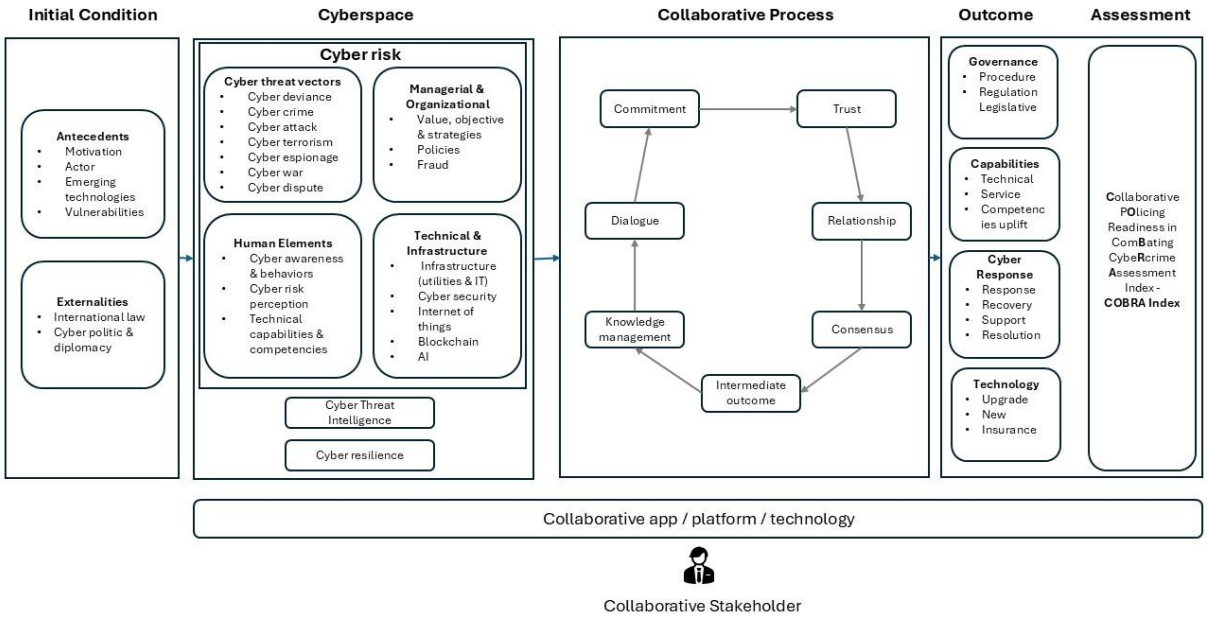

Figure 1. Conceptual Collaborative Policing to Combat Cybercrime in Banking Sector Modelling

CONCLUSION

This study concludes that collaborative policing is a strategic and necessary response to the growing threat of cybercrime within the digital banking sector. Through a systematic literature review, it was found that effective collaboration involves not only coordination between key stakeholders—such as law enforcement, regulators, the banking industry, civil society, and judicial institutions—but also requires the integration of technology, human competencies, legal frameworks, and shared governance mechanisms. The synthesis of research reveals that proactive communication, mutual trust, and shared responsibility are foundational to building adaptive and sustainable cyber resilience.

Furthermore, the proposed model highlights that combating cybercrime is not solely a technological challenge but also an organizational and institutional one. The collaborative approach offers a dynamic framework that integrates technical response capabilities, stakeholder engagement, and innovative tools such as cyber threat intelligence and smart governance systems. This contributes to strengthening not only cybersecurity performance but also the overall stability of the financial ecosystem. As a contribution to the field of industrial and policing studies, this model provides a basis for developing policy, guiding institutional practice, and enhancing collaborative governance in combating digital financial threats.

REFERENCE

Aditya, B. I., & Kusumastuti, R. (2023). Collaborative Governance in Police: A Review of Research, Managerial Implication and Agenda for Future Research. *Journal La Sociale*, *4*(5), 250–264. https://doi.org/10.37899/journal-la-sociale.v4i5.891

Ali, G., Mijwil, M. M., Buruga, B. A., & Abotaleb, M. (2024). A Comprehensive Review on Cybersecurity Issues and Their Mitigation Measures in FinTech. *Iraqi Journal for Computer Science and Mathematics*, *5*(3), 45–91. https://doi.org/10.52866/ijcsm.2024.05.03.004

Al-Kumaim, N. H., & Alshamsi, S. K. (2023). Determinants of Cyberattack Prevention in UAE Financial Organizations: Assessing the Mediating Role of Cybersecurity Leadership. *Applied Sciences (Switzerland)*, *13*(10). https://doi.org/10.3390/app13105839

Ansell, C., & Gash, A. (2008). Collaborative governance in theory and practice. *Journal of Public Administration Research and Theory*, *18*(4), 543–571. https://doi.org/10.1093/jopart/mum032

Asakpa, S. T., & Chaifetz, R. (2023). From Risk to Resilience: Strengthening Cyber Security in Financial Institutions. In *International Journal of Advance Research, Ideas and Innovations in Technology*. https://www.ijariit.com

Atkins, S., & Lawson, C. (2021). Cooperation amidst competition: cybersecurity partnership in the US financial services sector. *Journal of Cybersecurity*, *7*(1). https://doi.org/10.1093/cybsec/tyab024

Bada, M., & Nurse, J. R. C. (2021, June 14). Profiling the Cybercriminal: A Systematic Review of Research. *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2021*. https://doi.org/10.1109/CyberSA52016.2021.9478246

Calliess, C., & Baumgarten, A. (2020). Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective. *German Law Journal*, *21*(6), 1149–1179. https://doi.org/10.1017/glj.2020.67

Despotović, A., Parmaković, A., & Miljković, M. (2023). *Cybercrime and Cyber Security in Fintech* (pp. 255–272). https://doi.org/10.1007/978-3-031-23269-5_15

Docherty, K., & Russell, B. (2022). *Police Scotland and Local Government Collaborative Leadership Pilots Evaluation*. https://www.sipr.ac.uk/projects/targeted-rapid-research-call-evaluation-of-collaborative-leadership-pilots/

Feradinata, I. (2023). Collaborative Policing dalam Era Kontemporer untuk Memperkuat Harkamtibmas. *Jurnal Impresi Indonesia*, *2*(5), 468–477. https://doi.org/10.58344/jii.v2i5.2459

Gerdenitsch, C., Wurhofer, D., & Tscheligi, M. (2023). Working Conditions and Cybersecurity: Time Pressure, Autonomy and Threat Appraisal Shaping Employees' Security Behavior. *Cyberpsychology*, *17*(4). https://doi.org/10.5817/CP2023-4-7

Gunawan, A. B., Pratama, B., & Sarwono, R. (2021). Digital proxemics approach in cyber space analysis - A systematic literature review. *ICIC Express Letters*, *15*(2), 201–208. https://doi.org/10.24507/icicel.15.02.201

Hapsari, W., & Meliala, A. (2022). Collaborative Policing Model: Strategy for Maintaining Community Security and Order in Disaster Situations. *International Journal of Multidisciplinary Research and Analysis*, *5*(9). https://doi.org/10.47191/ijmra/v5-i9-29

Jesus, V., Bains, B., & Chang, V. (2024). Sharing Is Caring: Hurdles and Prospects of Open, Crowd-Sourced Cyber Threat Intelligence. *IEEE Transactions on Engineering Management*, *71*, 6854–6873. https://doi.org/10.1109/TEM.2023.3279274

Oyeniyi, L. D., Ugochukwu, C. E., & Mhlongo, N. Z. (2024). Developing Cybersecurity Frameworks for Financial Institutions: a Comprehensive Review and Best Practices. *Computer Science & IT Research Journal*, *5*(4), 903–925. https://doi.org/10.51594/csitrj.v5i4.1049

Li, M. (2017). Collaborative Governance and Partnerships in Policing. *Open Journal of Social Sciences*, *05*(12), 50–58. https://doi.org/10.4236/jss.2017.512004

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Lusthaus, J. (2024). *Annual Review of Law and Social Science Reconsidering Crime and Technology: What Is This Thing We Call Cybercrime?* https://doi.org/10.1146/annurev-lawsocsci-041822

Martineau, M., Spiridon, E., & Aiken, M. (2023). A Comprehensive Framework for Cyber Behavioral Analysis Based on a Systematic Review of Cyber Profiling Literature. In *Forensic Sciences* (Vol. 3, Issue 3, pp. 452–477). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/forensicsci3030032

McGregor, R., Reaiche, C., Boyle, S., & Corral de Zubielqui, G. (2024). Cyberspace and Personal Cyber Insurance: A Systematic Review. In *Journal of Computer Information Systems* (Vol. 64, Issue 1, pp. 157–171). Taylor and Francis Ltd. https://doi.org/10.1080/08874417.2023.2185551

Pajón, L., & Walsh, D. (2023). The importance of multi-agency collaborations during human trafficking criminal investigations. *Policing and Society*, *33*(3), 296–314. https://doi.org/10.1080/10439463.2022.2106984

Papuashvili, D. (2023). Cyber Resilience Implications for the Financial System. *Business Administration Research Papers*, *8*(a). https://doi.org/10.62232/barp.8.2023.6774

Pomerleau, P.-L., & Lowery, D. L. (2020a). *Countering Cyber Threats to Financial Institutions*. Springer International Publishing. https://doi.org/10.1007/978-3-030-54054-8

Pomerleau, P.-L., & Lowery, D. L. (2020b). The Evolution of Cybersecurity within the American Financial Sector. In *Countering Cyber Threats to Financial Institutions* (pp. 29–45). Springer International Publishing. https://doi.org/10.1007/978-3-030-54054-8_3

Pratama, B., & Bamatraf, M. (2021). Tallinn manual: Cyber warfare in Indonesian regulation. *IOP Conference Series: Earth and Environmental Science*, *729*(1). https://doi.org/10.1088/1755-1315/729/1/012033

Pugnetti, C., Björck, A., Schönauer, R., & Casián, C. (2024). Towards Diagnosing and Mitigating Behavioral Cyber Risks. *Risks*, *12*(7). https://doi.org/10.3390/risks12070116

Ruijer, E., Van Twist, A., Haaker, T., Tartarin, T., Schuurman, N., Melenhorst, M., & Meijer, A. (2023). Smart Governance Toolbox: A Systematic Literature Review. *Smart Cities*, *6*(2), 878–896. https://doi.org/10.3390/smartcities6020042

Sweetman, A. (2022). *Cyber and the City*. Springer International Publishing. https://doi.org/10.1007/978-3-031-07933-7

Jooda, T. O., Aghaunor, C. T., Kassie, J. D., & Peter Oyirinnaya. (2023). Strengthening cyber resilience in financial institutions: A strategic approach to threat mitigation and risk management. *World Journal of Advanced Research and Reviews*, *20*(3), 2166–2177. https://doi.org/10.30574/wjarr.2023.20.3.2424

Torfing, J., Sørensen, E., & Breimo, J. P. (2023). When Norway met co-creation: the import, diffusion, and onboarding of a magic concept in public administration. *International Public Management Journal*, *26*(5), 667–686. https://doi.org/10.1080/10967494.2022.2128127

Tridgell, J. (2025). Open or closing doors? The influence of 'digital sovereignty' in the EU's Cybersecurity Strategy on cybersecurity of open-source software. *Computer Law & Security Review*, *56*, 106078. https://doi.org/10.1016/J.CLSR.2024.106078

Weerawardhana, K. G. S. D., & Wijewardhana, B. V. N. (2024). Community-Oriented Policing: A Theoretical Exploration and its Implications for Building Safer Communities.

International Journal of Research and Innovation in Social Science, *VIII*(II), 15–21. https://doi.org/10.47772/IJRISS.2024.802002

Zhao, J. L., Bi, H. H., Chen, H., Zeng, D. D., Lin, C., & Chau, M. (2006). Process-driven collaboration support for intra-agency crime analysis. *Decision Support Systems*, *41*(3), 616–633. https://doi.org/10.1016/j.dss.2004.06.014