Jurnal Pustaka Cendekia Hukum dan Ilmu Sosial
Volume 3, No. 3, October 2025 - January 2026, pp. 724-737
E-ISSN: 2987-4475
https://pchukumsosial.org/index.php/pchs

Digital Competency Components Most Relevant To Police Intelligence For Cybercrime Prevention Systematic Literature Review

Salfiani Sari[1]*

[1]Management Science Doctoral Program, Halu Oleo University, Kampus Hijau Bumi Tridharma, Anduonohu, Kec. Kambu, Kota Kendari, Sulawesi Tenggara
salfianisari@gmail.com

Abstract

This study aims to map the most relevant digital competency components for police intelligence, identify intelligence technologies used for cybercrime prevention, and explain how these technologies affect the effectiveness of prevention through early detection, prediction, and response, considering the role of cybercrime dynamics as factors that can moderate or suppress the effectiveness of strategies. The method used was a systematic literature review with searches on Google Scholar and ScienceDirect using a combination of English and Indonesian keywords, as well as Boolean AND and OR operators. The study selection process is carried out through the stages of identification, screening of titles and abstracts, full text review, and determination of the final study based on inclusion criteria that emphasize relevance to law enforcement and police intelligence, discussion of digital competence or intelligence technology, novelty of publications, and quality of scientific sources. The selected studies were then summarized, extracted into a synthesis table, and analyzed using narrative synthesis and thematic analysis. The results of the study show that the dominant digital competencies include information literacy, technological proficiency, digital communication, critical and analytical thinking skills, ethical and legal awareness, and continuous adaptive learning. The most commonly identified intelligence technologies include artificial intelligence and machine learning, cybersecurity software, cloud computing, mobile forensics, integrated cyber investigation platforms, as well as blockchain exploration for data integrity and digital evidence. These technologies tend to improve the effectiveness of prevention by accelerating early detection, strengthening predictive analytics, and accelerating response coordination.
Keywords: Digital Competence, Police Intelligence, Cybercrime Dynamics

Abstrak

Penelitian ini bertujuan untuk memetakan komponen kompetensi digital yang paling relevan untuk intelijen kepolisian, mengidentifikasi teknologi intelijen yang digunakan untuk pencegahan kejahatan siber, dan menjelaskan bagaimana teknologi ini memengaruhi efektivitas pencegahan melalui deteksi dini, prediksi, dan respons, dengan mempertimbangkan peran dinamika kejahatan siber sebagai faktor yang dapat memoderasi atau menekan efektivitas strategi. Metode yang digunakan adalah tinjauan pustaka sistematis dengan pencarian di Google Scholar dan ScienceDirect menggunakan kombinasi kata kunci bahasa Inggris dan Indonesia, serta operator Boolean AND dan OR. Proses seleksi studi dilakukan melalui tahapan identifikasi, penyaringan judul dan abstrak, tinjauan teks lengkap, dan penentuan studi akhir berdasarkan kriteria inklusi yang menekankan relevansi dengan penegakan hukum dan intelijen kepolisian, pembahasan kompetensi digital atau teknologi intelijen, kebaruan publikasi, dan kualitas sumber ilmiah. Studi yang terpilih kemudian diringkas, diekstrak ke dalam tabel sintesis, dan dianalisis menggunakan sintesis naratif dan analisis tematik. Hasil penelitian menunjukkan bahwa kompetensi digital yang dominan meliputi literasi informasi, kemahiran teknologi, komunikasi digital, keterampilan berpikir kritis dan analitis, kesadaran etika dan hukum, dan pembelajaran adaptif berkelanjutan. Teknologi intelijen yang paling umum diidentifikasi meliputi kecerdasan buatan dan pembelajaran mesin, perangkat lunak keamanan siber, komputasi awan, forensik seluler, platform investigasi siber terintegrasi, serta eksplorasi blockchain untuk integritas data dan bukti digital. Teknologi-teknologi ini cenderung meningkatkan efektivitas pencegahan dengan mempercepat deteksi dini, memperkuat analitik prediktif, dan mempercepat koordinasi respons.
Kata kunci: Kompetensi Digital, Intelijen Kepolisian, Dinamika Kejahatan Siber

✉Corresponding author: Salfiani Sari
Email Address: salfianisari@gmail.com (Kampus Hijau Bumi Tridharma, Kota Kendari, Sulawesi Tenggara)
Received 01 January 2026, Accepted 07 January 2026, Published 13 January 2026

INTRODUCTION

Changes in information technology have shifted the way crime appears, spreads, and causes harm. Cybercrime no longer relies on geographical proximity, but on connectivity, anonymity, and automation that allow perpetrators to move quickly, target multiple victims, and cover their footprints more neatly (Wall 2024). This makes the police intelligence function even more important because effective prevention requires the ability to read signals early, connect fragments of information from multiple sources, and then turn them into timely action recommendations. In practice, relevant data is scattered across community reports, network logs, social media footprints, open sources, and other technical findings that are high in volume and in varying quality, so information management is key to avoiding late or inaccurate decisions.

On the other hand, police organizations are increasingly encouraged to utilize digital-based intelligence technology, such as data analytics, threat monitoring systems, investigation platforms, and forensic devices (Mantas and Patsakis, 2022). The goal is to speed up early detection, improve predictive capabilities, and strengthen response to incidents. However, the literature shows that technology investment alone is not enough if the digital competence of personnel is inadequate. Limited technical capacity can make the use of tools not optimal, while the ability to sort out valid information becomes increasingly critical amid a flood of data and potential misinformation (Akdemir et al., 2020). Therefore, research that combines digital competency components, police intelligence technology for cybercrime prevention, and cybercrime dynamics that can suppress the effectiveness of strategies is relevant and urgent to be studied in a more structured manner.

Digital competence is an organizational capability that determines whether digital data can be processed into meaningful intelligence. In the context of police intelligence, this competency includes information literacy to accurately search, assess, and use data from digital sources. The ability to distinguish trusted information from misleading information is crucial because the digital environment is full of manipulation, misinformation, and noise that can obscure threat signals (Barclay, 2018). Digital competence also requires critical and analytical thinking skills so that officers can interpret patterns, test the relevance between findings, and avoid bias when drawing conclusions. A number of studies confirm that analytical skills help read trends and anticipate potential crimes through the proper interpretation of data, not just information collection (Sinaga et al., 2021; Zakharevych & Hryhorenko, 2024). At the coordination level, digital communication competencies also determine the speed and quality of intelligence dissemination between units and external partners, including the strategic use of digital channels to expand the reach of information and community support (Mokhtari, 2023).

The next variable is police intelligence technology for cybercrime prevention. These technologies expand organizational capacity through automation, data correlation, and decision support. Artificial intelligence and machine learning are widely discussed for their capabilities in anomaly detection as well as predictive analytics, including large-scale data processing that accelerates the identification of threat patterns (Kim, 2021; Vishwanath, 2023). Cybersecurity software such as intrusion detection systems and firewalls help monitor suspicious activity while protecting systems and databases from unauthorized access (Razaque et al., 2021). Cloud computing supports cross-location storage, processing, and collaboration as data volumes increase and coordination is needed in real time (Kim, 2021; Klochko & Prokopenko, 2023). Mobile forensic tools play an important role in digging up evidence from mobile devices, while investigative platforms help integrate case management, analytics, and visualization so that work processes are more efficient (Akdemir et al., 2020; Alodhiani, 2023). Blockchain is also beginning to be explored to maintain the integrity of digital records and evidence through traceability and strengthening the authenticity of data (Razaque et al., 2021). Organizationally, all of these technologies function as accelerators, but the benefits depend heavily on the digital competence of personnel and the readiness of the work processes that support their utilization.

There are still research gaps related to the digital competency component that most determines the success of police intelligence in cybercrime prevention. Many studies view digital competence as a general concept or assess technology as a stand-alone factor, so the specific relationship between certain types of competencies and prevention outputs has often not been tested in detail in the context of police intelligence. In fact, in the field, it is often seen that organizations with similar technologies produce different prevention achievements. Empirical evidence suggests that skills limitations can limit the implementation of strategies, so success indicators are not solely determined by the availability of tools, but rather by the ability of personnel to operate, interpret, and apply findings consistently (Akdemir et al., 2020). Without proper component mapping, training risks becoming generic, technology investments becoming less appropriate, and intelligence processes difficult to standardize to produce stable performance.

Theoretical gaps also arise because many technology adoption frameworks emphasize acceptance, perception of ease, or intent of use, while the character of cybercrime is adversarial and adaptive. Threats evolve with technological innovation so that effective strategies can quickly become obsolete if organizations do not update their approaches, systems, and competencies (Dupont & Whelan, 2021). In addition, underreporting makes event data incomplete so that the analytical and prediction bases become weak, biased, and potentially misleading in the allocation of prevention resources. Commonly researched solutions often focus on the procurement of more sophisticated tools, general training in digital literacy improvement, or the formation of specialized units. However, this approach has not sufficiently answered when the effectiveness of the strategy weakens and what competencies play the most role in maintaining prevention performance in conditions of limited data, high anonymity, and rapid changes in tactics.

This research offers a mechanism that links digital competence with the use of intelligence technology, then lowers it to the effectiveness of prevention seen in early detection, prediction, and response. Information literacy allows officers to select credible sources and indicators, while analytical skills help process data into actionable intelligence through the assessment of threat patterns, linkages, and priorities (Zakharevych & Hryhorenko, 2024). Technological competence ensures that officers are able to operate AI, monitoring systems, investigation platforms, and forensic devices correctly so that system outputs can be understood, verified, and applied operationally (Akdemir et al., 2020). Digital communication competencies accelerate intelligence dissemination and cross-functional coordination, while ethical and legal awareness maintains compliance with privacy, data sharing protocols, and integrity of digital evidence so that rapid responses remain accountable (Reza et al., 2022). In this mechanism, technology increases capacity, while digital competence controls the quality of utilization as well as the quality of decisions taken.

Furthermore, this study places the dynamics of cybercrime as a moderator that can suppress or change the power of strategy influence. The evolution of attack modes can increase false positives and decrease detection accuracy when models are not updated and personnel adaptability is inadequate, resulting in deterrence performance declining even when tools are available (Dupont & Whelan, 2021). The anonymity and geographic mobility of perpetrators can slow down attribution and prolong response times, especially when searches require cross-jurisdictional coordination and rigorous technical proofing (Suarmita & Purnomo, 2024). Underreporting makes the patterns the system learns biased and weakens predictions, leading to inappropriate resource placement. The fragmentation of cross-agency collaboration can also hinder intelligence exchange and integrated responses, so that the benefits of technology and competence are not maximized at the broader security system level (Leenen et al., 2020). Thus, this research model explains not only whether competence and technology have an effect, but also why it affects through the quality of utilization, as well as when the influence is weakened due to the character of the threat.

The context of the study is in the police intelligence unit that focuses on cybercrime prevention, with the main characteristics of high data volume, the need for rapid analysis, and cross-unit coordination. This unit deals with a variety of digital information sources that must be combined to produce relevant intelligence, ranging from open sources, community reports, to technical data from systems and devices. At the same time, there is pressure to maintain the security of internal data, maintain the integrity of evidence, and meet accountability demands, especially when intelligence must be downgraded to operational actions or evidentiary support. Differences in personnel competency levels, variations in technology availability, and limited system integration can create gaps between the planned strategy and the implementation that occurs, so that testing the relationship between digital competencies, intelligence technology, and prevention effectiveness becomes highly contextual and of practical value for improving intelligence governance.

The objectives of the study were to identify the components of digital competencies that are most relevant to police intelligence, map the intelligence technologies used in cybercrime prevention, as well as analyze how they affect the effectiveness of prevention through early detection, prediction, and response. This study also aims to assess the role of cybercrime dynamics as a factor that can strengthen or suppress the effectiveness of strategies, so that the results of the study are able to explain the variation in performance between units or between organizations in the face of ever-changing and unpredictable threats. The expected theoretical contribution is the preparation of a more specific framework for the context of police intelligence with an explanation of the mechanisms of how digital competence activates the benefits of technology and how threat dynamics limit its effectiveness. His practical contributions include recommendations for more targeted training based on competency components, priority of technology investments that meet the needs of the intelligence cycle, as well as improvements in governance and procedures for intelligence dissemination so that prevention decisions are faster, more precise, and remain compliant with ethical and legal aspects.

METHODS

This research method uses a systematic literature review that focuses on mapping research concepts, findings, and gaps related to digital competence, police intelligence technology for cybercrime prevention, and the role of cybercrime dynamics on strategy effectiveness. Literature search was conducted through Google Scholar and ScienceDirect with a combination of English and Indonesian keywords such as digital competency, digital literacy, police intelligence, law enforcement intelligence, cybercrime prevention, threat intelligence, early detection, prediction, response, and cybercrime dynamics, and used Boolean AND and OR operators to expand and sharpen the results. Articles are then selected through the stages of identification, screening of titles and abstracts, full text review, and determination of final studies based on inclusion criteria such as direct relevance in the context of law enforcement or police intelligence, discussion of digital competency components or intelligence technology, publications in the latest year range, and quality of scientific sources; Meanwhile, the exclusion criteria include duplication, opinion articles without a methodological basis, or studies that are not related to cybercrime prevention. The selected studies were assessed for their quality in a concise manner through the examination of the clarity of objectives, methodological accuracy, and consistency of findings, and then the data were extracted in a synthesis table containing the concept definition, key indicators, technologies discussed, prevention outputs, and the form of threat dynamics. The final stage is a narrative synthesis and thematic analysis to group the components of digital competencies that are most relevant to police intelligence, map the technologies that are predominantly used for prevention, explain how technology influences early detection, prediction, and response, and identify the dynamics mechanisms of cybercrime that moderate or suppress the effectiveness of strategies, resulting in conceptual frameworks and evidence-based advanced research agendas.

RESULTS AND DISCUSSION

Results

What Components of Digital Competency are Most Relevant to Police Intelligence

The results of the thematic synthesis show that the most relevant digital competencies for police intelligence are consistently concentrated in six domains, namely information literacy, technological proficiency, digital communication competence, critical and analytical thinking skills, ethical and legal awareness, and continuous adaptive learning. Information literacy emerged as a foundation because intelligence work relies on the ability to identify, assess credibility, and use information from various digital sources that are large volumes and of non-uniform quality, so validation and verification are prerequisites before information is downgraded into intelligence products. In this framework, the accuracy of intelligence is determined not only by the amount of data, but by the quality of the selection, interpretation, and testing of information carried out during the analysis process.

Subsequent findings suggest that technological proficiency is required for personnel to be able to operate devices and platforms used in intelligence analysis, including databases, analytical devices, and information coordination tools. This skill relates to the organization's capacity to process data, strengthen work coordination, and improve the effectiveness of information management through the use of available tools. Digital communication competencies also emerge strong because intelligence dissemination, cross-unit information exchange, and collaboration with external partners require the ability to use digital channels safely and strategically, including the use of online platforms for public engagement and information gathering (Mokhtari, 2023). At the analysis stage, critical thinking skills and analytical skills are considered decisive because they help interpret data, identify patterns, and anticipate potential criminal activities that are relevant to prevention (Sinaga et al., 2021; Zakharevych & Hryhorenko, 2024).

In addition to these core competencies, the literature also emphasizes the importance of ethical and legal awareness, especially related to privacy, information sharing protocols, and limitations on the use of surveillance technology and data collection, as effective intelligence practices need to go hand in hand with regulatory compliance and the maintenance of public trust (Reza et al., 2022). At the same time, adaptive learning and continuous development are emerging as structural needs as technological changes and cybercrime modes are taking place rapidly, so personnel capabilities need to be constantly updated so that the use of tools and methods remains relevant.

In the technology dimension, the results of the study grouped police intelligence technology for cybercrime prevention into several main clusters that complement each other. Artificial intelligence and machine learning are widely positioned as key technologies for anomaly detection, large-scale data processing, and prediction support based on historical patterns and current signals (Kim, 2021; Vishwanath, 2023). Cybersecurity software such as intrusion detection systems and firewalls are seen as important to monitor suspicious activity and strengthen the protection of police systems and databases from unauthorized access (Razaque et al., 2021). Cloud computing stands out for providing scalable storage and processing resources and supporting cross-site collaboration in data management and digital evidence (Kim, 2021). Integrated cyber investigation platforms are also emerging as a solution to bring together case management, visualization, and real-time analytics to make workflows more efficient and response coordination faster (Alodhiani, 2023). Blockchain has also emerged as a technology that is being explored to maintain data integrity and authentication, especially related to digital evidence management and record traceability (Razaque et al., 2021).

Overall, the literature synthesis shows a consistent pattern of relationships, i.e. technology expands the capacity of detection, prediction, and response, while digital competence determines the quality of the use of such technologies in the intelligence cycle. More effective prevention outputs tend to be related to the ability of personnel to filter credible information, operate analytical and investigative tools appropriately, communicate intelligence through digital channels, and maintain ethical and legal compliance in data processing (Reza et al., 2022). Thus, the focus of the literature points to the need for alignment between the components of digital competence and the choice of intelligence technology so that cybercrime prevention not only relies on the sophistication of the system, but also the accuracy of intelligence-based interpretation and actions (Akdemir et al., 2020; S et al., 2024; Kim, 2021).

Table 1. Typology of Digital Competency in Police Intelligence

Areas of Competence	Description and Relevance to Intelligence Tasks	Main References
Information Literacy	A foundation for identifying, assessing credibility, validating, and verifying large-scale digital information before it is processed into intelligence products.	Irwin and Mandel (2019)
Digital Communication	Ability to use digital channels securely and strategically for intelligence dissemination, cross-unit information exchange, and public engagement.	Mokhtari (2023)
Critical Thinking & Analysis	Crucial skills at the analysis stage to interpret complex data, identify hidden patterns, and anticipate potential criminal threats.	Sinaga et al. (2021); Zakharevych & Hryhorenko (2024)
Ethical & Legal Awareness	Understanding of data privacy, digital surveillance regulations, and information sharing protocols to maintain legal legitimacy and public trust.	Reza et al. (2022)

What technologies are included in police intelligence technology for cybercrime prevention

The results of the literature synthesis show that police intelligence technologies for cybercrime prevention are generally concentrated in six complementary groups of technologies, namely artificial intelligence and machine learning, cybersecurity software, blockchain, cloud computing, mobile forensic tools, and integrated cyber investigation platforms. This technology group has emerged repeatedly in studies that discuss how law enforcement organizations are improving the capacity of detecting, analyzing, coordinating, and managing digital evidence in the face of rapidly evolving cyber threats. The findings indicate that the role of technology does not stand alone, but rather forms an ecosystem that connects monitoring, analytics, investigation, and case management functions so that prevention can be more proactive and response can be carried out faster and more structured.

The first group is artificial intelligence and machine learning, which are predominantly discussed due to their ability to run anomaly detection to catch unusual and potentially activity-related patterns of cyberattacks, especially when data is large and changes rapidly (Kim, 2021). The literature also links machine learning to fast processing and near-real-time response support, as models are able to filter out threat signals from massive data faster than manual checks (Kim, 2021; Vishwanath, 2023). In some studies, AI is positioned as the foundation of predictive analytics that leverages historical data to forecast trends or areas of risk, so intelligence units can direct preventive measures earlier before incidents develop. The second group is cybersecurity software, including intrusion detection systems and firewalls, which act as a layer of protection as well as monitoring, as they are able to detect suspicious traffic, block unauthorized access, and generate alerts for mitigation actions (Razaque et al., 2021).

The third group is blockchain which is discussed as a technology that supports data integrity and traceability of digital records, especially for the need to manage digital evidence so that the authenticity of data is better maintained and the risk of manipulation is lower (Razaque et al., 2021). The fourth group is cloud computing which has emerged as a capacity and collaboration solution, as it is able to provide scalable storage and processing resources, facilitate access to analytics tools from various locations, and support cross-unit and cross-agency work in handling cyber cases (Kim, 2021). The fifth group is mobile forensic tools which are positioned crucially considering that mobile devices are often the primary means of communication, transactions, and traces of offender activities, so the ability to extract and analyze digital artifacts can enrich intelligence, accelerate investigations, and strengthen evidentiary support (Akdemir et al., 2020). The sixth group is an integrated cyber investigation platform that combines case management, visualization, and real-time analytics to streamline workflows, improve team coordination, and reduce the fragmentation of handling processes (Alodhiani, 2023).

Table 2. Police Intelligence Technology Cluster and Its Functions

Technology Cluster	Key Functions in the Intelligence Ecosystem	Main References
Artificial Intelligence (AI) & Machine Learning	Massive data processing, anomaly detection (unusual activity patterns), and foundation for predictive analytics.	Kim (2021); Vishwanath (2023)
Cybersecurity Devices (IDS & Firewall)	Network traffic monitoring, unauthorized access detection, and protection of police infrastructure and sensitive data.	Razaque et al. (2021)
Cloud Computing	Provision of large-scale storage capacity and facilitation of collaboration of data access/analytics tools across locations/units.	Kim (2021)
Mobile Forensics Tools	Extraction and analysis of digital artifacts from the perpetrator's mobile devices to enrich intelligence and strengthen evidence.	Akdemir et al. (2020)
Integrated Cyber Investigation Platform	Unification of case management, data visualization, and real-time analytics to streamline operational workflows.	Alodhiani (2023)
Blockchain	Ensure data integrity, authentication, and traceability of digital footprints to maintain the authenticity of digital evidence (anti-manipulation).	Razaque et al. (2021)

Evaluating Prevention Effectiveness and the Suppressing Effects of Cybercrime Dynamics

The results of the literature synthesis show that the use of police intelligence technology has a direct effect on the effectiveness of cybercrime prevention through three main outputs, namely early detection, prediction, and response. In early detection, analytics-based and automation-based technologies expand the monitoring capabilities of large and diverse data, so that threat signals can be picked up faster than manual processes. Artificial intelligence-based modeling and machine learning have repeatedly been associated with anomaly detection capabilities, i.e. recognizing patterns of aberrant activity and potentially indicative of attacks, while cybersecurity software such as intrusion detection systems and firewalls strengthen early warning functions through network traffic monitoring and triggering alerts for suspicious activity (Kim, 2021; Vishwanath, 2023; Razaque et al., 2021). Literature findings also point to the fact that cloud computing support aids early detection when the need for cross-unit data consolidation increases as it speeds up access and processing, especially in organizations that handle many different cases and data sources (Kim, 2021; Klochko & Prokopenko, 2023).

In the prediction aspect, intelligence technology functions as a proactive capability enhancer by converting historical data and current intelligence data into trend estimates and risk priorities. Machine learning models in some studies have been positioned as the basis for predictive analytics that help identify recurrent patterns, map vulnerabilities, and support preventive decision-making before an incident occurs (Kim, 2021). However, the results of the study also show that predictions are very sensitive to the quality and completeness of the data, so predictive outputs are more accurately understood as decision support that increases preparedness, not certainty of events. When data is not representative or the threat environment changes rapidly, prediction accuracy tends to drop and the risk of misguided decisions increases, so organizations need continuous model updates and context-based verification (Dupont & Whelan, 2021).

In the response aspect, technology plays a role in accelerating coordination, improving case management, and strengthening the evidentiary dimension. Cyber investigation platforms that integrate case management, analytics, and visualization support more structured responses as workflows become more unified, task division is clearer, and findings are disseminated faster between units (Alodhiani, 2023). At the evidentiary level, mobile forensics tools are mapped as an important technology because they are capable of extracting and analyzing digital artifacts from mobile devices, which are often a central source of evidence in cyber cases, so that the response does not stop at technical mitigation but can be relegated to evidence-based law enforcement measures (Akdemir et al., 2020). In studies that discuss data integrity, blockchain also emerged as a technology that is explored to maintain the authenticity and traceability of digital records/evidence, thus potentially strengthening the accountability of the handling process (Razaque et al., 2021).

On the other hand, the literature consistently shows that the effectiveness of prevention strategies can be moderated or even suppressed by cybercrime dynamics. The ever-evolving threat landscape makes attack indicators change rapidly, giving rise to the phenomenon of drift models, and increasing the possibility of false positives and false negatives in detection and prediction systems if updates are not made regularly. This condition makes it difficult for organizations to maintain a proactive position because actors adapt to technological innovation and take advantage of cross-jurisdictional complexity, so that an effective strategy in one period can decrease its performance in the next period (Dupont & Whelan, 2021). In addition, the anonymity and geographic mobility of the perpetrators suppress effectiveness especially at the attribution stage, since the detected technical signals are not always easily connected to the actors that can be processed, so the response to enforcement can be delayed even if the initial detection has occurred (Suarmita & Purnomo, 2024).

Another powerful finding is underreporting that undermines the entire prevention cycle, especially in prediction and strategy planning. When incidents are not reported, incident data becomes incomplete and biased, so risk mapping and predictive analytics tend to be unrepresentative and can result in less targeted prevention priorities. Strategy effectiveness is also pressured by the challenges of internal implementation of the organization, particularly the skills gap and technological familiarity. The limitation of technical competence makes the use of advanced tools not optimal, both in configuration, output interpretation, and integration into work procedures, so that the benefits of technology are not fully converted into improved detection, prediction, and response (Akdemir et al., 2020). At the ecosystem level, fragmentation of multi-agency collaboration is also repeatedly cited as an obstacle because information exchange and coordination across agencies is slow, even though handling cybercrime often requires an integrated and rapid response (Leenen et al., 2020). In terms of organizational culture, strengthening cybersecurity culture is understood as a prerequisite for a sustainable prevention strategy, because changes in threats and technology require continuous learning and adherence to security practices; without such culture, strategies tend to be incidental and non-adaptive when threats change (Akdemir et al., 2020).

Table 3. The Impact of Technology on Prevention Outputs and Their Moderator Factors

Preventive Output	Contribution/Positive Impact of Technology	Inhibitor Moderator (Organizational Dynamics & Obstacles)
Early Detection	Automation analytics accelerate data monitoring; AI recognizes aberrant patterns; IDS provides early alerts.	The evolution of the attack indicator triggers the *drift model*, resulting in false *positive/negative* warnings if the model is not regularly updated.
Threat Prediction	Machine learning *models* turn historical data into proactive risk trend estimates before incidents spread.	The phenomenon of *underreporting* produces biased/incomplete data, so that predictions become unrepresentative and mistargeted.
Enforcement Response	Integrated platforms streamline task dissemination; Digital forensic tools transform mitigation into legal proof.	The anonymity of perpetrators and cross-jurisdictional mobility complicate legal attribution; The gap in personnel technical competence hinders the optimization of tools.

Discussion

Literature review shows that cybercrime prevention in the context of police intelligence is increasingly determined by the organization's ability to combine personnel digital competencies and appropriate intelligence technology. Cybercrime generates a massive, dispersed, and often mixed data trail between threat signals and noise. In these conditions, the results of prevention are not enough to be judged by the availability of tools, but by the ability of personnel to convert data into actionable intelligence and coordinate their actions quickly across units. These findings show a close relationship between the quality of information input, analytical capacity, and speed of intelligence dissemination with prevention effectiveness as reflected in early detection, prediction, and response.

The most relevant components of digital competencies for police intelligence appear consistent in six domains. Information literacy is foundational because it helps officers identify, assess the credibility, and use information from diverse digital sources, including open sources that are vulnerable to misinformation (Irwin and Mandel 2019). This competency serves as an initial filter that determines whether threat signals are truly valid before entering the analysis process. Technological prowess complements this foundation because intelligence work requires the ability to operate databases, analytical tools, and digital communication tools so that data can be efficiently managed, traced, and exchanged. Digital communication competence also emerges strong because intelligence dissemination requires not only reports, but also safe, fast, and relevant cross-unit and cross-partner information sharing mechanisms, including the use of online channels in public engagement and information collection (Mokhtari, 2023). Furthermore, critical thinking and analytical skills determine the quality of data interpretation, pattern identification, and threat prioritization to support tactical and strategic decisions (Sinaga et al., 2021; Zakharevych & Hryhorenko, 2024). Ethical and legal awareness affirms that data processing, digital supervision, and information exchange must be within the limits of privacy, procedures, and accountability in order for organizational legitimacy to be maintained (Reza et al., 2022;). Continuous adaptive learning becomes the last binder as changing technologies and modes of attack demand continuous skill renewal to keep competencies relevant.

In terms of technology, the literature maps police intelligence technology for cybercrime prevention into several groups that complement each other. Artificial intelligence and machine learning are often positioned as the primary enablers for anomaly detection and large-scale data processing, including the support of predictive analytics based on historical patterns and current signals (Kim, 2021; Vishwanath, 2023). Cybersecurity software such as intrusion detection systems and firewalls are positioned as important instruments for monitoring, prevention of unauthorized access, and provision of early warnings on suspicious activity (Razaque et al., 2021). Cloud computing is emerging as a supporting infrastructure that provides scalable storage and processing capacity while facilitating cross-location collaboration, especially as data volumes and coordination needs increase (Kim, 2021). Mobile forensic tools are mapped as a key technology because mobile devices are often the medium of activity of perpetrators and victims, so the extraction of digital artifacts helps with intelligence enrichment and evidentiary support (Akdemir et al., 2020). An integrated cyber investigation platform strengthens workflows by combining case management, visualization, and real-time analytics to make internal coordination more efficient (Alodhiani, 2023). Blockchain is also discussed as a technology that is explored to maintain the integrity and traceability of records, especially in the management of digital evidence (Razaque et al., 2021).

The impact of such technology on the effectiveness of prevention is evident in early detection. AI and machine learning help lift threat signals from massive data through the identification of anomalies and suspicious patterns, so intelligence units can build alerts faster than manual processes (Kim, 2021). IDS and firewalls add to early detection capacity through network traffic monitoring and notification of risky activities, while cloud support accelerates data consolidation across systems and across units (Kim, 2021). However, the literature also indicates that early detection can easily produce false positives if information literacy and analytical skills are not strong, as systems that detect "strangeness" still require contextual interpretation in order for signals to turn into valid intelligence (Zakharevych & Hryhorenko, 2024).

In the prediction aspect, the contribution of technology emerges through predictive analytics that help project attack trends, target vulnerabilities, or risk priorities based on historical data and current signals (Kim, 2021). Predictions serve to strengthen preparedness and more proactive resource allocation, but their quality is largely determined by data completeness, threat pattern stability, and model updates. The literature shows that when threats change rapidly, predictions can weaken as models lose match to field conditions, so predictions are more accurately seen as decision support that must be tested and adjusted on an ongoing basis (Dupont & Whelan, 2021). In the response aspect, technology has an effect through accelerating coordination and strengthening evidence. An integrated investigation platform helps with case management, clarifies workflows, and accelerates the dissemination of findings within the organization (Alodhiani, 2023). Mobile forensics strengthens response because it allows the tracing of evidence on relevant devices, including communication data, location, and application artifacts that are often key to handling cyber cases (Akdemir et al., 2020). Discussions about blockchain lead to the potential for strengthening evidence integrity and traceability of records, which can help with accountability of responses when digital evidence is debated (Razaque et al., 2021). However, a rapid response still depends on digital communication competencies and legal ethical frameworks so that coordination is not hampered and actions remain procedurally valid (Reza et al., 2022; Santos & Gomes, 2023).

The literature also confirms that the dynamics of cybercrime can moderate and even suppress the effectiveness of prevention strategies. The evolution of the threat landscape makes attack techniques and perpetrator infrastructure change rapidly, so that detection and prediction indicators are easily obsolete and organizations are pushed back to being reactive when updates do not take place quickly (Dupont & Whelan, 2021). Anonymity and geographic mobility suppress effectiveness especially on attribution and enforcement, as detected technical signals are not always easily linked to legally processable actors, so responses can be delayed (Suarmita & Purnomo, 2024). Underreporting weakens prediction and planning because event data is incomplete and biased, making risk mapping and strategy priorities less accurate. Effectiveness is also suppressed by skills gaps and technological familiarity that make advanced tools not optimally utilized, as well as by the fragmentation of cross-agency collaboration that slows down information exchange and integrated responses (Akdemir et al., 2020; Leenen et al., 2020). Therefore, the literature points to the need to strengthen cybersecurity culture and continuous learning so that strategies remain adaptive to face changing threats and ensure that technology truly improves early detection, prediction, and response (Akdemir et al., 2020; Dupont & Whelan, 2021).

CONCLUSION

The conclusion of this study shows that the effectiveness of police intelligence in cybercrime prevention is determined by the alignment between the digital competence of personnel and the use of intelligence technology. Information literacy, technological proficiency, digital communication, analytical skills, ethical-legal awareness, and adaptive learning serve as prerequisites for technologies such as AI, cybersecurity software, cloud computing, mobile forensics, investigative platforms, and blockchain to truly improve early detection, strengthen predictions, and accelerate responses. However, cybercrime dynamics such as threat evolution, anonymity of perpetrators, cross-regional mobility, and underreporting have proven to suppress strategy performance so that the technology-effectiveness relationship is not permanent and requires continuous updates and cross-actor collaboration to keep prevention proactive and responsive.

The practical implication is that police organizations need to prioritize the development of specific digital competencies according to intelligence functions, rather than general training, and ensure that data governance, intelligence dissemination procedures, and cross-agency cooperation mechanisms support the optimal use of technology. The limitations of this study lie in the dependence on the literature in various contexts of countries and institutions as well as the potential limitations of bibliographic information and variations in construct definitions, so generalizations need to be made carefully. Further research can develop a more operational conceptual framework with uniform indicator measurements for each competency component and each technology cluster, examine the role of moderators of cybercrime dynamics in more detail, and compare applications at different levels of intelligence units or jurisdictions to find the most effective combinations of competencies and technologies under different threat and resource conditions.

REFERENCES

Akdemir, N., & Lawless, C. J. (2020). Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach. *Internet Research*, *30*(6), 1665-1687.

Alodhiani, A. A. B. (2023). Financial Technology (Fintech) and Cybersecurity: A Systematic Literature Review

Barclay, D. A. (2018). *Fake news, propaganda, and plain old lies: how to find trustworthy information in the digital age*. Bloomsbury Publishing PLC.

Dupont, B., & Whelan, C. (2021). Enhancing relationships between criminology and cybersecurity. *Journal of criminology*, *54*(1), 76-92.

Irwin, D., & Mandel, D. R. (2019). Improving information evaluation for intelligence production. *Intelligence and National Security*, *34*(4), 503-525.

Kim, S., Chen, J., Cheng, T., Gindulyte, A., He, J., He, S., ... & Bolton, E. E. (2021). PubChem in 2021: new data content and improved web interfaces. *Nucleic acids research*, *49*(D1), D1388-D1395.

Klochko, A., & Prokopenko, A. A. (2023). Development of digital competence under the conditions of digitalization of education. *Scientific Journal of Polonia University*, *1*(56), 103-110.

Leenen, J. P., Leerentveld, C., van Dijk, J. D., van Westreenen, H. L., Schoonhoven, L., & Patijn, G. A. (2020). Current evidence for continuous vital signs monitoring by wearable wireless devices in hospitalized adults: systematic review. *Journal of medical Internet research*, *22*(6), e18636.

Mantas, E., & Patsakis, C. (2022). Who watches the new watchmen? The challenges for drone digital forensics investigations. Array, 14, 100135.

Mokhtari, F. (2023). Fostering digital literacy in higher education: Benefits, challenges and implications. *International Journal of Linguistics, Literature and Translation*, *6*(10), 160-167.

Razaque, A., Alotaibi, B., Alotaibi, M., Amsaad, F., Manasov, A., Hariri, S., ... & Alotaibi, A. (2021). Blockchain-enabled deep recurrent neural network model for clickbait detection. *IEEE Access*, *10*, 3144-3163.

Reza, S., Ferreira, M. C., Machado, J. J., & Tavares, J. M. R. (2022). A multi-head attention-based transformer model for traffic flow forecasting with a comparative analysis to recurrent neural networks. *Expert Systems with Applications*, *202*, 117275.

Sinaga, J. (2021). The effect of supply chain management practices and information and communication technology on competitive advantage and firm performance (Case study: Smes of processed food in Jakarta). *Journal of Business and Entrepreneurship*.

Suarmita, I. A., & Purnomo, H. (2024). Challenges of Hybrid Policing in Countering Online Fraud Networks: A Case Study from Sidrap Regency. *Al-Ishlah: Legal Scientific Journal*, *27*(1), 17-30.

Vishwanath, T., Shirwaikar, R. D., Jaiswal, W. M., & Yashaswini, M. (2023). Social media data extraction for disaster management aid using deep learning techniques. *Remote Sensing Applications: Society and Environment*, *30*, 100961.

Wall, D. S. (2024). *Cybercrime: The transformation of crime in the information age*. John Wiley & Sons.

Zakharevych, M., & Hryhorenko, V. (2024). Digital competence and digital literacy of higher education acquires. *Collection of Scientific Papers of Uman State Pedagogical University*, *1*, 119-129.