International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 8, 2025
https://theaspd.com/index.php

Strengthening Cyber Resilience Against Online Scamming Threats Through Optimizing Police Human Resources and Digital Literacy Campaigns

John Anderson Batara Aryasena[1]
[1]Akademi Kepolisian, Semarang, Indonesia
Corresponding author: john.anderson@ui.ac.id

Abstract: *This research is motivated by the increase in cybercrime in the digital era, which poses complex challenges for law enforcement, data security, and community protection. This problem is exacerbated by a lack of adequate regulation and technical constraints in law enforcement. This research is aimed at identifying and developing a model for optimizing the National Police's human resources through the establishment of special units and digital forensic training to strengthen law enforcement against online scamming crimes, and formulate effective digital literacy campaign strategies to increase public awareness of the threat of online scamming, in order to reduce vulnerability and support national cyber resilience. The analysis knife of this research uses Cyber Law Theory, Institutional Capacity Theory, Transnational Crime Theory, Digital Literacy Theory, and Multi-Stakeholder Collaboration Theory. This research is a literature study research that is descriptive-analytical. This approach allows for the identification of patterns, challenges, and opportunities in the handling of cybercrime, without involving the collection of primary data such as surveys or field interviews. Data analysis was carried out through the qualitative analysis content method. The results of this study show that the development of the National Police's human resource optimization model to deal with online scamming crimes involves the establishment of a special unit of the Ditressiber in each Regional Police, AI-based digital forensic training and big data analytics, as well as integration with various parties by adopting global best practices such as the Anti-Scam Command Singapore and IC3 AS to detect and handle phishing, deepfakes, and crypto transactions. Digital literacy strategies are implemented through social media, workshops, and technologies such as mobile applications, aimed at increasing public awareness, especially the elderly and MSMEs, to reduce vulnerability and financial losses and support national cyber resilience. The conclusion of this study is that handling cybercrime requires an integrated approach that involves cross-sectoral collaboration, strengthening regulations, and improving digital literacy. Law enforcement strategies must be supported by advanced technology and an adaptive cross-border legal framework, to minimize the risk of cybercrime and protect society in the digital age.*

Keywords : *cybercrime, online scamming, optimization, National Police human resources, digital literacy.*

1. INTRODUCTION

The rapid development of information technology has changed the way humans view and understand the world. In this era of globalization, cyberspace is an important need that connects humans across geographical boundaries (Rosmayati, 2023). Although intangible, the existence of cyberspace is a reality presented through the internet that connects computers, software, digital data, and human interaction and is supported by network infrastructure and technologies such as AI and IoT, which are governed by policies and regulations (Banjarnahor, et al., 2022). The existence of this cyberspace allows individuals to communicate, transact, and hide their identities, so that this can be used to commit cybercrimes that are transnational in nature and strengthened by international collaboration between perpetrators who share information, tools, and attack techniques (Tobing, et al., 2024).

According to Wibowo, Munawar and Hidayatullah (2024), cybercrime has a wide impact, not only harming the individuals who are victims, but also disrupting economic stability, national security, and social stability due to the decline in public trust in digital systems, such as banking services, e-commerce, and technology-based government platforms. Meanwhile, according to Saputra, Pratama and Ramadhani (2025), this type of crime is increasingly difficult to control due to the high accessibility of technology, the speed of digital transactions, and the lack of control on various online platforms.

One of the types of cybercrime that causes the most victims globally is online scamming (Drew and Webster, 2024). Online scamming is defined as the act of deliberately and knowingly deceiving a victim by misinterpreting, concealing, or omitting facts about goods, services, or other promised benefits and consequences that do not exist, are unnecessary, never intended to be given, or are deliberately distorted for the purpose of monetary gain, targeting organizations or individuals (Koning, Junger, and Veldkamp,

2023). Dada, et al., (2025), explain that online scamming is a term that is often used interchangeably to describe various acts of fraud, fraud, manipulation carried out deliberately to gain economic advantage, through different methods of communication, the channels used to do so, and the influence used to do so. According to Sai (2024), the type of online crime scamming is a big problem in the digital world. Kipngetich (2025), also explained that online scamming covers a broad spectrum with prohibited activities, ranging from phishing emails, identity theft, cryptocurrency fraud to ransomware attacks. These types of crimes often target individuals, small businesses, and even large corporations, causing significant financial and psychological losses.

Arnell and Faturoti (2023) state that cybercrimes such as online scamming are transnational, involving perpetrators from various countries. Although national and international regulations have existed, their complexity continues to increase, leading to less effective legal responses. Transnational and extraterritorial jurisdictional approaches are often used, but they are problematic because they violate state sovereignty, potentially infringe on individual rights such as privacy and justice, require complicated coordination and high costs, and are inconsistent with criminalization goals such as prevention and justice. They reject the normalization of this approach and recommend the strengthening of more effective territorial laws for the long term. AllahRakha (2024) states that cybercrime is transnational due to the borderless nature of cyberspace, with increased scale and complexity despite regulations such as the Budapest Convention, leading to less effective legal responses due to perpetrators, victims, and infrastructure spread across various jurisdictions. Transnational jurisdictional approaches, such as mutual legal assistance, face challenges in the form of legal fragmentation, cross-border data privacy and legality issues, delays in processes due to language and legal constraints, and technical limitations of law enforcement. International standards such as the Budapest Convention are not yet adequate for modern cybercrime. He then proposed an integrated approach with strengthening the international legal framework, improving technical capacity, efficiency of procedures such as evidence-sharing platforms, and protection of individual rights such as privacy and justice. Wang (2024) states that cybercrime is transnational, with increased complexity despite regulations such as the Budapest Convention, leading to less effective legal responses due to normative competition between countries and the absence of global consensus. The global approach is hampered by conflicts between state sovereignty and human rights, as well as the lack of a centralized law enforcement mechanism. The Budapest Convention as the main instrument has not sufficiently addressed the dynamics of modern cybercrime. Wang proposed strengthening international cooperation through inclusive negotiations to establish common norms, while respecting state sovereignty and protection of individual rights such as privacy and justice.

AllahRakha (2024) highlights the regulatory gap in handling online scams, especially in developing countries in Asia and Africa, which lack comprehensive cybercrime legislation. These weaknesses, coupled with limited digital infrastructure and a lack of dedicated cybercrime units, hinder the investigation and prosecution of cross-border scammers. In developed countries, despite regulations such as the Computer Fraud and Abuse Act (CFAA) and the General Data Protection Regulation (GDPR), these laws are often unable to keep up with advanced technological developments, such as artificial intelligence-based scams (deepfakes and phishing). The misalignment between the realities of modern cyber threats and the need for responsive laws, digital forensic training, and public education exacerbate vulnerability to online scams. In addition, differences in the definition of cybercrime and jurisdiction between countries also create loopholes that perpetrators take advantage of, while many countries still lack the resources and technology to effectively track and deal with such threats.

METHOD

This research is a descriptive-analytical literature study, focusing on the collection and analysis of secondary data from various written sources such as books, scientific journals, official reports from institutions such as the Criminal Investigation Branch of the National Police, OJK, and Kominfo, as well as international documents from INTERPOL and FATF. The data was collected through systematic searches in academic databases such as Google Scholar, Scopus, and official government websites, with key keywords including "online scamming", "cyber resilience", "optimization of police human resources", and "digital literacy". This approach allows for the identification of patterns, challenges, and opportunities in the handling of cybercrime, without involving the collection of primary data such as surveys or field interviews.

Data analysis is carried out through the qualitative analysis content method, where the collected sources are synthesized to formulate a model for optimizing the National Police's human resources and digital literacy campaign strategies. The results of the analysis were tested for validity through triangulation of sources to ensure accuracy and diversity of perspectives, resulting in concrete recommendations that can be applied in the national context. This research is expected to make a theoretical and practical contribution to strengthening the cybersecurity ecosystem in Indonesia.

2. FINDINGS AND DISCUSSIONS

3.1 Identification and development of a model for optimizing the National Police's human resources through the establishment of Special Units and Digital Forensic Training to strengthen law enforcement against online scamming crimes

Online scamming crime has become a major threat in Indonesia's digital ecosystem, with data from the National Police Criminal Investigation Branch recording 1.2 million case reports by mid-2025, causing financial losses of Rp 4.6 trillion until August 2025, as well as significant psychological impacts for victims. The complexity of these crimes, which utilize advanced technologies such as deepfake AI, phishing, and crypto transactions, coupled with the transnational nature and anonymity of the perpetrators, demands increasing the capacity of the National Police's human resources through a structured and technology-based approach. The identification and development of a model for optimizing the National Police's human resources through the establishment of special units and digital forensic training is crucial to strengthen law enforcement against cybercrime. This approach integrates Institutional Capacity Theory, Cyber Law Theory, and Multi-Stakeholder Collaboration Theory, by modeling best practices from countries such as Singapore, the United States, and Australia, to create an adaptive law enforcement ecosystem that supports national cyber resilience.

To identify and develop a model for optimizing the National Police's human resources in dealing with online scamming crimes, the first step is to conduct a comprehensive analysis of existing empirical data by considering the specific challenges and needs arising from the dynamics of cybercrime in Indonesia. This analysis focuses on four main aspects, namely:

a. Empirical data on the trends and impact of online scamming crime

Based on data from the National Police Criminal Investigation Branch until April 2025, online scamming is the most dominant type of cybercrime in Indonesia, with the highest frequency compared to other categories such as defamation, spreading hoaxes, or TPPU. Data shows that online fraud cases amounted to 15 in 2021, decreased to 12 in 2022, increased to 20 in 2023, then dropped again to 10 in 2024 and 6 in early 2025. Despite the decrease in frequency, the impact remains significant, with financial losses reaching Rp 4.6 trillion from 225,281 online fraud reports in the 10 months to August 2025, with an average of 800 reports per day, much higher than Singapore which recorded only 150 reports per day. This data shows an escalation of cyber threats that is not only limited to the number of cases, but also to the complexity and scale of economic and psychological losses.

The 2025 cyber threat prediction highlights an increase in advanced technology-based attacks such as phishing (128k reports through May 2025) and deepfake AI, which leverages social engineering techniques to exploit people's vulnerabilities. Low digital literacy, especially financial literacy, which only reached 49.68% in 2022, exacerbates the situation, as people are often unable to recognize fraudulent tactics such as phishing emails, identity disguise, or messaging application-based fraud (Fahrudin, 2024; Mahvitasari and Azzahrah, 2023). In addition, a report from the National Police Criminal Investigation Center noted that from January 1 to January 23, 2025, the National Police handled 1,062 cybercrime cases, with the Metro Jaya Police as the largest contributor (582 cases), indicating that cybercrime is concentrated in urban areas with high internet access. The trend of the last three years (2022–2024) also shows a significant increase, from 8,636 cases in 2022 to 13,913 cases in 2024, with a total of 32,073 reported and 29,067 victims until January 2025. This data underscores the urgency of strengthening the National Police's human resources to deal with the increasing volume and complexity of cybercrime.

b. Operational challenges of the National Police's human resources

The main challenges in optimizing the National Police's human resources to deal with online scamming include the following aspects:

a) The National Police faces limitations in technological equipment, such as digital forensic tools for big data analysis and temporary digital evidence tracking (Abdullah and Jahan, 2020). This is compounded by the complexity of AI-based attacks, such as deepfakes, which require specialized software

for anomaly detection and metadata analysis. The digital forensic laboratory at the Dittipidsiber Bareskrim of the National Police has met quality standards, but the distribution of these facilities has not been evenly distributed at the Regional Police level, limiting the rapid response in the regions.

b) The operational costs of dealing with cybercrime are very high, especially due to the need for investment in cutting-edge security technologies, such as AI and machine learning for threat detection, as well as personnel training (Yoganandham, 2024). Budget constraints hampered the procurement of tools, the recruitment of experts, and the expansion of cybercrime special units throughout the Regional Police. Data shows that the cost of recovery and compliance with regulations, such as GDPR in Europe, also increases the financial burden, which is relevant if Indonesia wants to harmonize international standards such as the Budapest Convention (Eling et al., 2023).

c) Although the National Police has established a Directorate of Cyber Crime (Dittipidsiber) in the Criminal Investigation Branch and eight Regional Police, this organizational structure is still limited to workload indexes, geographical conditions, and uneven resources. The handling of cybercrime at the Regional Police level was previously carried out by the Directorate of Special Criminal Investigation (Ditreskrimsus), which did not fully focus on cybercrime, resulting in less effective handling. The establishment of Ditressiber in eight Regional Polices in 2024 is a step forward, but it still requires stronger integration and coordination between units (Trunoyudo, 2024)

d) National Police human resources still lack special training in digital forensics, such as malware analysis, tracking crypto transactions, or deepfake attack detection. These limitations hinder the ability of the National Police to handle transnational crimes involving foreign servers and the anonymity of the perpetrators (Reznik et al., 2024). Existing training is often short-term and unsustainable, so it is not able to keep up with technological developments such as AI and blockchain used by scammers (AllahRakha, 2024).

e) Online scamming is often cross-jurisdictional, with perpetrators using offshore servers, VPNs, and social engineering techniques such as identity disguise or flexible fraud scripts to manipulate victims (Wilson et al., 2023). These challenges are exacerbated by the lack of effective international cooperation and differences in regulations between countries, which make it difficult to track perpetrators and recover assets (Simanjuntak, 2021). Data from INTERPOL shows that more than 60% of global respondents consider phishing, ransomware and online fraud to be the main threats, which often lead to money laundering, adding to the complexity of law enforcement.

c. The need for capacity development of the National Police's human resources

Based on the operational challenges of the National Police's human resources above, the needs for developing the capacity of the National Police's human resources can be identified as follows:

a) The National Police needs to expand the establishment of Ditressiber in more Polda, following Singapore's Anti-Scam Command model that coordinates law enforcement, cyber patrols, and public education (Octavia, 2025). This unit should have a specific focus on online scamming, with tasks including investigation, threat analysis, and cross-sector coordination. The unit structure should be supported by a dedicated budget allocation and the recruitment of digital forensic experts to handle high-tech-based cases.

b) The National Police requires a training curriculum that includes phishing detection, deepfake analysis, crypto transaction tracking, and cross-border investigations. This training can adopt the standards of the Budapest Convention, which emphasizes forensic capacity building and international cooperation (Situmeang, 2020). Training should be ongoing, with short-term (e.g., 1–2-month training) and medium-term (6–12-month programs) modules to ensure adaptation to new technologies such as AI and blockchain (Dwinugroho, 2024).

c) The National Police needs to invest in digital forensic tools, such as big data analysis software and AI-based anomaly detection systems, needed to support the National Police's human resources. For example, the use of technology such as that applied in the US through the FBI IC3 for rapid investigations can be adapted (Krause, 2025). This infrastructure should also include a digital forensic laboratory in each Police to support local evidence analysis.

d) The National Police needs to strengthen cooperation with the OJK, Kominfo, the private sector (such as ISPs and digital platforms), as well as international organizations such as INTERPOL and FATF. This collaboration is important for joint training, information exchange, and tracking of illegal fund flows, as Singapore is doing through public-private partnerships (Khan, 2023). International cooperation is also needed to deal with transnational crime, as recommended in the Transnational Crime Theory (Simanjuntak, 2021).

e) The National Police needs to allocate a special budget for technology procurement, training, and the expansion of special units is very important. The high cost of dealing with big data and advanced persistent threats (APTs) demands ongoing funding, as identified by Yoganandham (2024). The National Police can emulate the Australian model through the ACSC, which integrates budgets for technology and public education (Mishra et al., 2022).

f) In addition to forensic training, National Police human resources need to be trained in digital literacy to understand cyber risks, such as social engineering, and be able to educate the public. This is in line with Digital Literacy Theory, which emphasizes competencies such as content evaluation and knowledge preparation to detect false information (Usman et al., 2022).

Institutional Capacity Theory (Irawan, 2017; Ilato, 2016), these steps can be supported by identifying the need for optimizing the National Police's human resources through three levels:

a) Micro level (Individual), focusing on improving the quality of human resources through digital forensic training, data analysis skills, and understanding of social engineering techniques. For example, training to detect AI deepfakes or track crypto transactions will improve an individual's ability to handle scamming cases.

b) The meso level (Management System), through the establishment of a special unit such as the Ditressiber in each Police Department, with an integrated management system, including responsive leadership and a clear workflow for cyber investigations. This includes the development of SOPs for cyber patrols and threat analysis, such as those carried out by the Directorate of Cyber Crime Agency.

c) At the macro level (Institutional Reform), reform the organizational structure of the National Police to support cybercrime as a priority, with special budget allocations and cross-sector partnerships. For example, the establishment of integrated reporting centers such as the US IC3 or ACORN Australia to facilitate coordination and reporting (Krause, 2025; Mishra et al., 2022).

The next step after conducting a comprehensive analysis of the specific challenges and needs arising from the dynamics of cybercrime in Indonesia, the development of a model for optimizing the National Police's human resources to deal with online scamming crimes, can be carried out through:

d. Identify specific needs through qualitative content analysis

The first step in model development is to identify the specific needs of the National Police's human resources based on qualitative content analysis from empirical data and official reports. Data from the National Police Criminal Investigation Branch shows a significant escalation of online scamming cases, with 1.2 million reports by mid-2025, which includes financial losses of Rp 4.6 trillion in the 10 months to August 2025, with an average of 800 daily reports. This data shows an increase in the complexity of threats, especially with the rise of AI-based attacks such as deepfakes, which leverage advanced technology to deceive victims. In addition, a report from the National Police Criminal Investigation Center until January 2025 recorded 1,062 cases of cybercrime, with the Metro Jaya Police as the largest contributor (582 cases), indicating that cybercrime is concentrated in areas with high digital infrastructure.

Qualitative content analysis was carried out by evaluating official reports from the Criminal Investigation Branch of the National Police, OJK, Kominfo, as well as international documents from INTERPOL and FATF. The results of the analysis show that the main needs of the National Police's human resources include:

1. Digital forensics capabilities to detect and analyze AI-based threats, such as deepfakes, phishing, and crypto transactions used by scammers. It includes skills such as metadata analysis, IP address tracking through a VPN, and digital evidence investigation that is temporary.
2. Responsive organizational structure through the establishment of specialized units focused on cybercrime, with cross-agency coordination to expedite responses to reports.
3. Ongoing training to keep pace with technological developments, such as the use of blockchain and AI by scammers, which require regular skill updates.
4. Budget and technology infrastructure to support the procurement of digital forensic tools and cyber laboratories in each Regional Police.

The various steps above are in accordance with the perspective of Institutional Capacity Theory, which emphasizes strengthening capacity at the micro level (individuals/human resources through training) and meso (management systems such as special units) to overcome organizational gaps in the face of cyber dynamics (Irawan, 2017; Ilato, 2016). This empirical data shows that the low digital literacy of the public (49.68% for financial literacy in 2022) and the limitations of the National Police's technology exacerbate their vulnerability to scamming, thus emphasizing the urgency of human resource development.

e. Establishment of Special Units based on comparative studies

The National Police's human resources optimization model adopts the establishment of special units as a core component, inspired by global best practices such as the Anti-Scam Command in Singapore (Octavia, 2025). The unit is designed to deal with online scamming crimes in a focused manner, with tasks including cyber patrols, rapid investigations, threat analysis, and cross-sector coordination. The development of this special unit can be carried out through:

1) Establish an organizational structure Special Units, such as the Directorate of Cyber Crime (Ditressiber) in each Regional Police, should have the authority to handle scamming cases directly, with a team consisting of investigators, digital forensic analysts, and cross-agency coordinators. The structure emulates Singapore's Anti-Scam Command, which integrates police, internet service providers (ISPs), and digital platforms to cut off the flow of illegal funds and detect malicious content.

2) Coordinate across agencies, as this unit must work with the OJK to track illegal financial transactions, Kominfo to block scam sites (such as 2.6 million online gambling sites until July 2024), and the private sector to verify online entities. This collaboration reflects Singapore's harm-centric approach, which involves public-private partnerships to protect potential victims (Khan, 2023).

3) Focusing on anonymity and digital evidence, given that scammers often use offshore servers, VPNs, and social engineering techniques (Wilson et al., 2023), specialized units should be equipped with tracking technologies such as big data analysis and forensic software to address the anonymity of the perpetrator and the transient nature of digital evidence (Reznik et al., 2024).

4) The determination of the scale of implementation, where the establishment of the Ditressiber in eight Regional Polices in 2024 (Trunoyudo, 2024) is the first step, but it needs to be expanded to all Regional Police with special budget allocations for infrastructure, such as digital forensic laboratories, and the recruitment of cyber experts. The unit should also have a unified reporting hotline, similar to IC3 in the United States, to make it easier for people to report on it.

The formation of this special unit is in line with the meso level as described in the Theory of Institutional Capacity, which emphasizes the strengthening of the management system through a responsive and coordinated organization (Irawan, 2017). Comparative studies show that models such as Australia's ACORN and the US IC3 are effective in centralizing reporting and investigations, but the National Police needs to ensure transparency and follow-up of investigations to avoid weaknesses like those experienced by ACORN (Cross, 2018).

f. Implementation of AI and Big Data-based digital forensics training curriculum

The next component of the National Police's human resource optimization model to deal with online scamming crimes is the development of a comprehensive digital forensic training curriculum, based on AI technology and big data analytics, to equip National Police human resources with skills relevant to modern cyber threats. This curriculum is designed based on the recommendations of Dwinugroho (2024) and modules from the Budapest Convention (Situmeang, 2020), with a focus on the harmonization of transnational law and the handling of cross-border crimes. Curriculum details include:

1) Training modules:

a) Phishing detection and social engineering, which includes training to recognize phishing attack patterns, such as app-based emails or messages, and social engineering techniques such as impersonation or flexible fraud scripts. This module includes simulating an attack to train a quick response.

b) AI deepfake analysis, which contains skills training to detect and analyze deepfake content using AI software, such as video or audio metadata analysis to identify digital manipulation. This is important given that the 2025 report shows an increase in deepfakes in scamming.

c) Crypto transaction tracking, which contains training to track blockchain-based transactions, which perpetrators often use to hide illegal fund flows. This module includes the use of tools such as Chainalysis or Elliptic for the analysis of crypto transactions.

d) Cross-border investigations, which contain technical training to cooperate with international organizations such as INTERPOL and Europol, including joint legal assistance (MLA) and extradition procedures, are in line with Budapest Convention standards.

e) Big Data analytics, which contains training in the use of analytics tools such as Splunk or Palantir to manage large volumes of cyber data, enables real-time detection of anomalies and crime patterns.

2) Duration and format:

a) Short-term (Diklat), where an intensive training program lasts 1–2 months, focuses on basic skills such as phishing detection and the use of simple forensic tools, for basic level investigator personnel.

b) Medium-term (Continuing Program), where a 6–12-month program for senior personnel, includes in-depth analysis such as deepfakes and crypto transactions, with international certifications to meet global standards.
c) Simulations and field practices, which are carried out through training that include simulations of real cases, such as the investigation of deepfake cases revealed by Dittipidsiber in January 2025, to ensure practical application.
d) Collaboration with external parties is carried out by involving universities and technology companies such as Microsoft or Google to develop training modules. Partnerships with INTERPOL can provide access to global forensic training, such as the one conducted in Singapore (Khan, 2023).
e) Adjustment to nine capacity areas, where this curriculum is adjusted to nine capacity development areas according to Ilato (2016), such as human resource management (expert recruitment and training), transition management (adaptation to new technologies), and inter-organizational networking (collaboration with OJK and Kominfo).
This curriculum supports the micro-level of Institutional Capacity Theory, which emphasizes improving individual quality through technical and managerial training (Irawan, 2017). This approach is also aligned with Cyber Law Theory, which highlights the need for forensic training to handle digital evidence and cross-border dynamics (Husamuddin et al., 2024).
a. Integrasi dengan studi komparatif dan praktik terbaik global
This model of optimizing the National Police's human resources to deal with online crime scamming must also integrate best practices from countries with advanced cybersecurity approaches to ensure its relevance and effectiveness, which can be done through the adoption of specialized unit models such as Singapore's Anti-Scam Command that integrates AI technology for early detection, law enforcement, and public education through campaigns such as ScamShield. as well as the establishment of integrated reporting centers such as the US IC3 that leverages AI for rapid analysis of cyber reports and intensive forensic training for malware analysis and crypto transactions (Octavia, 2025; Krause, 2025). The National Police can also emulate Australia's ACSC and ACORN models to establish a national reporting hotline with transparent cross-sector collaboration, as well as adopt Aadhaar biometric verification from India and Nigeria to prevent identity misuse in scamming (Mishra et al., 2022; Singh et al., 2019; Ameen et al., 2016). In addition, the implementation of data protection standards from Article 32 of the European Union's GDPR will strengthen the training of National Police human resources in the management of secure digital data, reducing the risk of data breaches during investigations (Chiara, 2021). By integrating this approach, the National Police can establish a dedicated unit of the Directorate of Cyber Security supported by advanced technology, AI-based forensic training, and multi-stakeholder collaboration to improve the response to cybercrime and support national cyber resilience.
b. Implementation and evaluation
The implementation of the National Police human resource optimization model to handle online scamming crimes began with a pilot project at the National Police Criminal Investigation Department, training 500 digital forensic personnel in 6 months, with a focus on phishing and deepfake detection. The national expansion is carried out in stages, with the target of establishing a Ditressiber in all Regional Police within 2 years, supported by a special budget and technological infrastructure. The evaluation is carried out through the following indicators:
1) A decrease in underreporting to measure the increase in reports handled through an integrated reporting center, compared to 1.2 million cases in 2025.
2) The response time is the investigation time from an average of 30 days to 10 days for simple scamming cases.
3) The success rate of cases, which shows an increase in the number of cases resolved, such as the disclosure of 1,301 cases of Indonesian citizens related to scams abroad in 2025.
4) Public satisfaction, measured through public trust through post-implementation surveys, with a target of 20% increase in 1 year.

c. Impact and sustainability
This model of optimizing the National Police's human resources to handle online scamming crimes is expected to improve the ability of the National Police to detect and handle online scamming, reduce psychological and financial impacts on victims, and support public trust in the digital ecosystem. By integrating digital forensic training, special units, and cross-sector collaboration, the National Police can deal with transnational threats more effectively, as recommended by Transnational Crime Theory

(Simanjuntak, 2021). The sustainability of the model depends on a long-term commitment to funding, periodic evaluation, and adaptation to new technologies, as emphasized in Institutional Capacity Theory (Ilato, 2016). With successful implementation, this model will strengthen adaptive law enforcement and support Indonesia's vision for a secure and resilient cyber ecosystem.

The next step after developing a model for optimizing the National Police's human resources to handle online scamming crimes is to integrate with multi-stakeholders, which is in accordance with the view of the Multi-Stakeholder Collaboration Theory to strengthen cross-sector synergy, such as partnerships with the OJK, Communication and Informatics, and the private sector for joint training, this is also in accordance with the harm-centric approach Singapore involving ISPs and digital platforms (Khan, 2023). In Cyber Law Theory, this model emphasizes forensic training to adapt investigative procedures with digital evidence, as stipulated in the ITE Law and the accession plan to the Budapest Convention, to address transnational jurisdiction and process delays (AllahRakha, 2024; Husamuddin et al., 2024). Development involves the creation of specialized units such as the US IC3 (Krause, 2025), which focuses on FBI investigations with AI detection, adapted for the National Police through the recruitment of forensic experts and a dedicated budget for tools such as data analysis software. Collaboration with INTERPOL and the FATF, as recommended by Transnational Crime Theory, allows for the exchange of information for hybrid policing training (Febriawan and Marisa, 2024; Simanjuntak, 2021), reduces impunity for scammers.

Effective digital literacy campaign strategy to increase public awareness of online scamming threats, to reduce vulnerability and support national cyber resilience

An effective digital literacy campaign strategy must be comprehensively designed, data-driven, and involves multi-stakeholder collaboration can be implemented to raise public awareness of online scamming threats, reduce vulnerabilities, and support national cyber resilience. Based on data from the National Police Criminal Investigation Branch until August 2025, online scamming crimes recorded 1.2 million reports with losses of IDR 4.6 trillion, exacerbated by the low digital literacy of the Indonesian people, which only reached 49.68% for financial literacy in 2022. Threats such as phishing, deepfake AI, and social engineering exploit people's lack of understanding of digital technology, so digital literacy campaigns must focus on education that is easily accessible, relevant, and technology-based. This strategy integrates Digital Literacy Theory, Behavior Change Theory, and global best practices, such as the ScamShield campaign in Singapore, to create sustainable impact. This campaign targets vulnerable groups such as the elderly and rural communities, as well as digitally active users such as young people and MSMEs, with the aim of reducing financial losses, such as Rp 1,200 trillion from online gambling-related scamming in 2024, and the psychological impact on victims.

The digital literacy campaign strategy is designed based on Digital Literacy Theory (Usman et al., 2022), which emphasizes three pillars: access to information, critical evaluation, and knowledge preparation. Its main components are:

a. Specific content-based education:

a) The introduction of cyber threats with educational materials includes types of scamming such as phishing (128 thousand reports until May 2025), deepfakes, fraudulent investment fraud, and social engineering. For example, the public is taught to recognize phishing emails through features such as suspicious links or requests for personal data.

b) Digital security practices that teach practical steps, such as the use of strong passwords, two-factor authentication (2FA) activation, and verification of website authenticity via HTTPS or official domains.

c) Digital financial literacy, which educates the public on how to protect digital transactions, such as checking the authenticity of banking applications or avoiding transfers to unknown accounts, considering the low level of financial literacy (49.68% in 2022).

b. Segment-specific approach:

a) Vulnerable groups that focus on groups with low digital literacy, such as the elderly, rural communities, and new internet users, are often targeted for scamming (Mahvitasari and Azzahrah, 2023). For example, seniors can be trained through simple face-to-face sessions on how to spot phone scams.

b) Young people and professionals who target active users of social media and digital apps through interactive content, such as short videos or quizzes on platforms like TikTok and Instagram.

c) Business actors provide special training for MSMEs on the security of e-commerce transactions, such as payment verification and customer data protection.

c. Media and delivery channels in digital literacy campaigns can leverage social media such as Instagram, TikTok, and YouTube for educational videos and infographics, traditional media such as

radio, television, and banners to reach rural communities, as well as workshops in schools, villages, and religious communities by engaging community leaders to increase trust and participation.

d. Multi-stakeholder collaboration in digital literacy campaigns involves collaborating with Kominfo to block scam sites and spreading messages through the Cyber Patrol application, OJK through the "OJK Sikapi" program for digital financial education, the private sector such as Google and Gojek to provide educational tools such as the local version of the ScamShield application and 2FA promotion, as well as NGOs and local communities to reach marginalized groups through training at posyandu and arisan groups.

e. Supporting technologies for digital literacy campaigns include the development of mobile apps with interactive quizzes, phishing simulations, and digital security guides similar to ScamShield Singapore, the use of AI-based chatbots to answer digital security questions in real-time like in Australia, as well as the integration of push notifications in banking apps and social media to alert users to the latest cyber threats.

The implementation of the campaign is carried out in stages: Phase 1 (0–6 months) involves needs analysis based on data from the National Police and INTERPOL Criminal Investigation Department, simple content design, and pilot projects in areas with high cases such as Polda Metro Jaya (target of 10,000 people). Phase 2 (6–18 months) expands the campaign to a national scale (50 million people) through training of 5,000 facilitators and social media campaigns with hashtags such as #AmanDariScam. Phase 3 (18 months and above) launches a national app, integrates digital literacy into the school curriculum, and updates content every 6 months based on cyber threat trends. Best practices from the U.S. FBI IC3 (use of AI for education) and India's Aadhaar (biometric verification) are adapted to strengthen the campaign (Krause, 2025; Singh et al., 2019).

The campaign evaluation measured the decrease in scamming reports (target 20% from 1.2 million cases), the increase in digital literacy (15% from 49.68%), and the participation of public reporting (30% in 1 year), using triangulation of data from Bareskrim, Kominfo, and public surveys. Long-term impacts include reducing financial losses, increasing national cyber resilience, and empowering the community to support law enforcement by the National Police Directorate. Sustainability is ensured through integration into national policies, dedicated budgets, and periodic updates, ensuring campaigns remain relevant against evolving cyber threats, such as deepfakes and IoT-based fraud.

3. CONCLUSION

Based on the results of the discussion above, it can be concluded that the development of a model for optimizing the National Police's human resources to deal with online scamming crimes, which recorded 1.2 million reports with losses of Rp 4.6 trillion until August 2025, requires the establishment of a special unit of the Directorate of Cyber Intelligence in each Regional Police and AI-based digital forensic training and big data analytics, which integrates Institutional Capacity Theory, Cyber Law Theory, and global best practices such as the Anti-Scam Command Singapore and IC3 US, to improve the ability of the National Police to detect phishing, deepfakes, and crypto transactions, as well as accelerate investigative responses through collaboration with the OJK, Kominfo, and INTERPOL. In addition, an effective digital literacy campaign strategy, based on Digital Literacy Theory and Behavior Change Theory, must utilize social media, community workshops, and technologies such as mobile applications and AI chatbots to increase public awareness of scamming threats, targeting vulnerable groups such as the elderly and MSMEs, with the aim of reducing vulnerability, reducing financial losses such as Rp 1,200 trillion by 2024, and supporting national cyber resilience through relevant education and multi-stakeholder collaboration.

Recommendations

Based on the above conclusion, the following recommendations were given:

1. Expanding the establishment of Ditressiber in all Police Departments within 2 years, equipped with digital forensic laboratories and integrated reporting hotlines, with special budget allocations for technologies such as Splunk and Chainalysis, adopting the Singapore Anti-Scam Command and IC3 US models.
2. Developed a training program based on the Budapest Convention, covering phishing detection, deepfake analysis, and crypto transaction tracking, with short and medium duration, involving universities and technology companies such as Microsoft for international training and certification modules.

3. Strengthen partnerships with the OJK, Kominfo, the private sector, and INTERPOL for joint training, information exchange, and blocking of scam sites, by establishing dialogue forums such as SATSPAM 2025 for cross-sectoral coordination.
4. Launched a digital literacy campaign using social media, traditional media, and community workshops, targeting 50 million people in 18 months, focusing on vulnerable groups such as the elderly and MSMEs, and developing an AI-based digital literacy application similar to ScamShield.
5. Allocating funds through the State Budget for the procurement of forensic software, analytics servers, and cyber infrastructure in each Regional Police, as well as ensuring technology updates every 6 months to compensate for threats such as deepfakes and IoT.
6. Conducting periodic evaluations using indicators such as a decrease in scamming reports, investigation response times, and increased digital literacy, as well as integrating digital literacy into school curricula and MSME training for long-term sustainability.

REFERENCES

1. Abdullah, A.T.M., & Jahan, I. (2020). Challenges of Cyber Policing in Response of Cybercrime to Reduce Victimization. International Journal of Research and Innovation in Social Science (IJRISS), 4(5).
2. AllahRakha, N. (2024). Cross-Border E-Crimes: Jurisdiction and Due Process Challenges. Adliya: Jurnal Hukum dan Kemanusiaan, 18(2), 153–170.
3. AllahRakha, N. (2024). Global Perspectives on Cybercrime Legislation. Journal of Infrastructure, Policy and Development, 8(10), 6007.
4. Ameen, A.O., et al. (2016). Design and development of a unified subscribers' SIM registration platform using top-down approach. African Journals Online Information Technologist (The), 13(2).
5. Anggraeni, D.C.H., Wismanto, Y.B., & Susetyo, D.P.B. (2023). Stres Kerja Anggota Satlantas Polrestabes Semarang Ditinjau dari Kepribadian Multikultural dan Hubungan Interpersonal dengan Rekan Kerja. Philanthropy: Journal of Psychology, 7(1), 73–89.
6. Ansell, C., & Gash, A. (2008). Collaborative Governance in Theory and Practice. Journal of Public Administration Research and Theory, 18, 543–571.
7. Arnell, P., & Faturoti, B. (2023). The Prosecution of Cybercrime-Why Transnational and Extraterritorial Jurisdiction Should be Resisted. International Review of Law, Computers & Technology, 37(1), 29–51.
8. Banjarnahor, A.R., et al. (2022). Transformasi Digital dan Perilaku Organisasi. Jakarta: Yayasan Kita Menulis.
9. Boateng, O.N., et al. (2022). A Fraud Prevention and Secure Cognitive SIM Card Registration Model. Indian Journal of Science and Technology, 15(46), 2562–2569.
10. Bruinsma, G. (2015). Histories of Transnational Crime. New York: Springer.
11. Chiara, P.G. (2021). The Balance Between Security, Privacy and Data Protection in IoT Data Sharing: A Critique to Traditional "Security&Privacy" Surveys. European Data Protection Law Review, 7(1), 18–30.
12. Cross, C. (2018). Expectations Vs Reality: Responding to Online Fraud Across the Fraud Justice Network. International Journal of Law, Crime and Justice, 55, 1–12.
13. Dadà, C.B., et al. (2025). Uncovering Vulnerability to Fraud and Scams Among Adult Victims in Online and Offline Contexts: A Systematic Review. Computers in Human Behavior, 172, 108734.
14. Dwinugroho, Y.B. (2024). Transformation Strategy: Indonesian National Police in Coordinating Crime in The Digital Era. International Journal of Integrated Science and Technology (IJIST), 2(5), 374–383.
15. Eling, M., Elvedi, M., & Falco, G. (2023). The Economic Impact of Extreme Cyber Risk Scenarios. North American Actuarial Journal, 27(3), 429–443.
16. Emami, C., Smith, R.G., & Jorna, P. (2019). Online Fraud Victimisation in Australia: Risks and Protective Factors. AIC Reports Research Report.
17. Fahrudin, A., et al. (2024). Online Gambling Addiction: Problems and Solutions for Policymakers and Stakeholders in Indonesia. Journal of Infrastructure, Policy and Development, 8(11), 9077.
18. Fajrin, Y.A., et al. (2022). Critical Analysis of The Republic of Indonesia Police in The Implementation of Cybercrime Law in Indonesia. Journal Equity of Law and Governance, 4(1).
19. Febriawan, D., & Marisa, H. (2024). Understanding Indonesia's Cyber Security Policies: Opportunities and Challenges in The Digitalization Transformation Era. Journal of Election and Leadership (JOELS), 5(1), 13–21.
20. Husamuddin, M.Z., et al. (2024). Hukum Acara Pidana & Pidana Cyber. Medan: PT Media Penerbit Indonesia.
21. Ilato, R. (2017). Capacity Building Pemerintah Daerah Menuju Good Governance: Upaya Mewujudkan Keseimbangan Politik, Akuntabilitas Pemerintah, dan Pertanggungjawaban Pemerintah Lokal. Gorontalo: Ideas Publishing.
22. Irawan, B. (2016). Kapasitas Organisasi dan Pelayanan Publik. Jakarta: Publica Press.
23. Jiow, H.J. (2013). Cyber Crime in Singapore: An Analysis of Regulation based on Lessig's four Modalities of Constraint. International Journal of Cyber Criminology, 7(1), 18–27.
24. Khan, A.A. (2024). Reconceptualizing Policing for Cybercrime: Perspectives from Singapore. Laws, 13, 44.
25. Kipngetich, A. (2025). A Review of Online Scams and Financial Frauds in the Digital Age. GSC Advanced Research and Reviews, 22(01), 302–329.
26. Koning, L., Junger, M., & Veldkamp, B. (2023). Risk Factors for Fraud Victimization: The Role of Socio-Demographics, Personality, Mental, General, and Cognitive Health, Activities, and Fraud Knowledge. International Review of Victimology, 30(3), 443–479.
27. Krause, D. (2025). The Rise of Online Scams and Consumer Protections: A Comparative Analysis of the U.S. and Singapore. Journal of Economic Literature Classification System, G28, K22, D18, O33, L51, H11.

28. Laksana, T.G., & Mulyani, S. (2024). Faktor-faktor Mendasar Kejahatan Siber Terhadap Kemanusiaan. Sejarah Artikel, 11(2), 136–160.
29. Mahvitasari, I., & Azzahrah, S. (2023). Regulatory Gaps in Addressing the Dark Side of Online Loans and Online Gambling in Indonesia. Next Policy, 2 November 2023.
30. May, C. (2017). Transnational Crime and the Developing World. Global Financial Integrity.
31. Mishra, A., et al. (2022). Attributes Impacting Cybersecurity Policy Development: An Evidence from Seven Nations. Computers & Security, 120, 102820.
32. Octavia, J. (2025). Online Fraud and Scams in Singapore. Safer Internet Lab Research Report.
33. Oladipo, F.O., Abdu, H., & Obansa, A.A. (2018). Integrated Subscriber Identification Module Registration. International Journal of Science and Engineering Investigations, 7(75).
34. Purba, R.E., et al. (2024). Peranan Hukum Positif dalam Mengatur Cyberspace Untuk Menghadapi Tantangan dan Peluang di Era Digital. MANDUB: Jurnal Politik, Sosial, Hukum dan Humaniora, 2(2).
35. Reznik, O., et al. (2024). Strategies and Challenges of Combating Cyber-Financial Fraud: An Analysis of Ukraine's Experience During the Military Conflict. Library Progress International, 44(3), 21444–21457.
36. Rosmayati, S. (2023). Tantangan Hukum Dan Peran Pemerintah dalam Pembangunan E-Commerce. Koaliansi Cooperative Journal, 3(1), 9.
37. Sai, K.S. (2024). The Threat of Online Scams: Examining Tactics, Impacts, and Effective Defences. International Journal of Research Publication and Reviews, 5(11), 5233–5240.
38. Shalhoub, Z., & Qasimi, L. (2010). Cyber Law and Cyber Security in Developing and Emerging Economies. USA: Edward Elgar Publishing Limited.
39. Simanjuntak, E.L. (2021). Hukum Pidana Khusus dan Kejahatan Transnasional Pengantar dan Konsep Penegakan Hukum Lintas Yuridiksi. Jakarta: Perpustakaan Nasional.
40. Singh, A., Srivastva, R., & Singh, Y.N. (2019). Prevention of Payment Card Frauds using Biometrics. International Journal of Recent Technology and Engineering (IJRTE), 8(3S).
41. Situmeang, S.M.T. (2020). Cyber Law. Bandung: CV. Cakra.
42. Stiftung, H.B., & Schönfeld, R. (2013). Transnational Organized Crime Analyses of a Global Challenge to Democracy. Berlin: The Deutsche Nationalbibliothek.
43. Thangavel, V. (2025). Global Identification of Smart Card Technologies-Safe and Secure: A Research. Journal of Research and Development, 13(1), 1000283.
44. Tobing, C.I., et al. (2024). Globalisasi Digital Dan Cybercrime: Tantangan Hukum dalam Menghadapi Kejahatan Siber Lintas Batas. Jurnal Hukum Sasana, 10(2), 105–123.
45. Usman, et al. (2022). Literasi Digital dan Mobile Learning. Sulawesi Selatan: IAIN Parepare Nusantara Press.
46. Vitus, E.N. (2023). Cybercrime and Online Safety: Addressing the Challenges and Solutions Related to Cybercrime, Online Fraud, and Ensuring a Safe Digital Environment for All Users-A Case of African States. Tijer-International Research Journal, 10(9), 975–989.
47. Wang, X. (2024). Global (re-)framing of Cybercrime: An Emerging Common Interest in Flux of Competing Normative Powers? Leiden Journal of International Law, 1–27.
48. Wangke, H. (2011). Transnasional di Indonesia dan Upaya Penanganannya. Jakarta: Pusat Pengkajian, Pengolahan Data dan Informasi (P3DI) Sekretariat Jenderal DPR Republik Indonesia.
49. Wibowo, M.S.I., Munawar, A., & Hidayatullah. (2024). Kendala Teknis dan Hukum dalam Proses Penyidikan Tindak Pidana Siber di Indonesia. Rewang Rencang: Jurnal Hukum Lex Generalis, 5(7).
50. Wilson, S., et al. (2023). A Holistic Qualitative Exploration on the Perception of Scams, Scam Techniques and Effectiveness of Anti-Scam Campaigns in Malaysia. Journal of Financial Crime, 1359–0790.
51. Wright, D., & Kumar, R. (2023). Assessing the Socio-Economic Impacts of Cybercrime. Societal Impacts, 1, 100013.
52. Yoganandham, G. (2024). Economic Consequences of Cyber Fraud in Online Banking and Credit Card Transactions-A Theoretical Assessment. Gis Science Journal, 11(10).
53. Yoganandham, G., & Kalaivani, M. (2024). Economic Impact of Cyber Crime on Society and Sustainable Economic Development in Tamil Nadu With Reference to Trends, Challenges, and Consequences - A Comprehensive Assessment. International Journal of Early Childhood Special Education (INT-JECSE), 16(4).