Policy, Law, Notary and Regulatory Issues
https://ojs.transpublika.com/index.php/POLRI
Online ISSN 2809-896X

https://doi.org/10.55047/polri.v4i4.1821

Original Article

Public Education as a Strategy for Human Resource Development in Preventing Cybercrime in Indonesia

Ega Satya Nugraha[1*], Chairul Muriman Setyabudi[2], Muhammad Ezra Aminanto[3]

[1,2]Police Science Study Program, School of Strategic and Global Studies, Universitas Indonesia, Indonesia
[3]Universitas Indonesia, Indonesia
Email: [1)] egasn5399@gmail.com , [2)] cak_iir1966@yahoo.com, [3)] erza.aminanto@ui.ac.id

Received : 26 June - 2025
Accepted : 29 July - 2025
Published online : 30 July - 2025

Abstract

Cybercrime has escalated significantly in Indonesia over the past five years, with offenses such as online gambling, fraud, and data manipulation increasing in both frequency and sophistication. This study investigates the role of public education, particularly the National Digital Literacy Movement (GNLD), in addressing these challenges by applying a descriptive qualitative design that relies on literature review as the primary method. Data were drawn from secondary sources, including Bareskrim cybercrime reports from 2020 to 2024 and digital literacy assessments issued by the Ministry of Communication and Informatics. The analysis focuses on suburban and semi-rural regions where digital vulnerability remains high despite broader program outreach. Findings indicate a structural disconnect between the expanding scale of digital literacy initiatives and the persistent weakness of the "Digital Safety" pillar, which consistently scores lowest on the national index. This gap suggests that general awareness alone does not ensure behavioral change or online protection. The study concludes that cybercrime prevention efforts must move beyond surface-level education and adopt targeted, behaviorally informed strategies that align with actual regional threat patterns. Strengthening this approach is essential to building meaningful digital resilience, especially in communities facing the greatest risks.

Keywords: Cybercrime, Cybersecurity Strategy, Digital Literacy, Human Resource Development, Public Education.

1. Introduction

Digitalization, in theory, was supposed to be humanity's great leap forward. And to be fair, in many ways, it is. We can talk across continents in seconds, run businesses from our bedrooms, connect entire cities with a tap. But there's something most people don't really want to talk about. Not in conferences, not in glossy tech ads, not even in policy papers until it becomes urgent. Beneath all this excitement about progress, a different kind of economy has quietly been growing. One that doesn't produce or innovate, but instead feeds on speed, ignorance, and weak systems. The World Economic Forum estimates cybercrime could cost the world about $10.5 trillion every year by 2025. That number is enormous. Hard to picture, maybe, until you imagine hospitals locked out of their systems, state agencies losing control of data, or someone's life savings disappearing after a single click. The Global Cybersecurity Outlook 2025 explains this isn't some unfortunate side effect. It is the result of how we adopted technology faster than we trained people to use it wisely. Deloitte CTI (2025) points out ransomware is still the biggest threat, now made even worse by Ransomware-as-a-Service.

That means anyone, even someone with no coding skills, can launch an attack with the right kit. What used to be celebrated as technical brilliance anonymity, decentralization, encrypted tunnels now also help criminals vanish without trace. Likewise, since no one owns the internet, no one really governs it. What scholars like Buçaj and Idrizaj (2024) try to call a "risk ecosystem" might sound like a technical label, but honestly, that feels too neat. The way things look right now, it's not really a system at all. It's scattered, unstable, and nobody seems to be really steering the wheel. There's no shared playbook. Just a lot of exposed entry points, vague responsibility, and actors moving faster than the rules can catch up. Calling it an ecosystem almost makes it sound natural, but nothing about it feels under control.

As one of the fastest-growing internet markets in the world and the largest digital economy in Southeast Asia, Indonesia is experiencing a surge in both the volume and sophistication of cyberattacks (Dalimunthe et al., 2022). According to the Criminal Investigation Agency, one in three internet users in the country has fallen victim to cybercrime, resulting in economic losses of IDR 23.4 trillion over the past five years. Phishing and ransomware remain the most common threats, with 82% of phishing incidents targeting individuals with low digital literacy (Fazlurrohman et al., 2024). The 2024 data breach at BPJS Health, which exposed 279 million medical records, illustrates how digital attacks now carry systemic consequences. The "open and borderless" nature of cyberspace, while fostering greater interaction and collaboration across regions, also leaves individuals and institutions increasingly exposed to transnational digital threats, especially those who lack the knowledge or tools to defend themselves.

Cybercrime is no longer a niche concern confined to IT specialists or law enforcement; it has become a tangible threat that affects ordinary people in their everyday lives. Online scams, identity theft, and digital harassment are now commonplace, often targeting individuals who are unaware they are even at risk. Fazlurrohman et al. (2024) note that the consequences include violations of privacy, emotional distress, and significant financial harm. Vulnerable groups, such as women with limited digital access, suburban residents, and digital MSME operators, are disproportionately affected (Kusumawardhani et al., 2023). Even seemingly harmless online activities, shopping, accessing public services, or sharing family updates, can become entry points for cyberattacks. In this paradox, cyberspace both connects us more than ever and simultaneously deepens our exposure to digital vulnerability. If cyberattacks continue to escalate, the crucial question is: how prepared is the Indonesian public to navigate the digital world? Unfortunately, the answer remains far from ideal. While internet penetration has risen sharply, digital literacy levels have not kept pace. According to Kominfo, Indonesia's Digital Literacy Index stands at just 3.54 out of 5, a moderate score that still leaves many citizens vulnerable. This gap is exacerbated by a lack of awareness regarding basic cybersecurity practices such as password hygiene, hoax detection, and caution toward suspicious links (Agustini, 2023). As Halim et al. (2022) observed, humans are inherently social beings driven to connect, but without sufficient literacy, that desire becomes an open invitation to exploitation. In this light, digital ignorance is not merely a technological issue; it represents a new form of social vulnerability.

Public education thus emerges as a strategic solution to bridge the gap between connectivity and protection. Compared to reactive and costly approaches such as law enforcement or forensic technologies, public education is preventive, inclusive, and cost-effective. Sunyoto (2015) emphasizes that human resources are both physical and non-physical assets that can be developed through education and training. As this capacity grows, so does society's resilience to digital threats. Halim et al. (2022) further argue that education does not merely transmit knowledge, it shapes risk-aware behavior. Public education not only

enhances technical skills but also empowers individuals to act as human firewalls, the first line of defense against cyberattacks (Sunyoto, 2015).

Nevertheless, the implementation of public education faces significant challenges. Several Indonesian studies have evaluated the effectiveness of digital literacy interventions, but most remain limited to one-way socialization efforts. Supanto et al. (2023) for example, examined literacy programs among Muhammadiyah community leaders in Klaten and found an increase in awareness, though not a lasting behavioral change. Kusumawardhani et al. (2023) also highlight digital skill gaps in the public sector, especially among policy implementers, which result in weak institutional support for community education. National literacy indices reveal that digital safety remains the lowest-scoring dimension. These facts suggest that although public education holds promise, it cannot succeed as a one-off campaign, it must be continuous, participatory, and context specific.

There seems to be a gap in the current research, although it's not always obvious at first glance. Many existing studies have tried to address digital education, yes, but few of them have made a clear connection between real cybercrime trends and the needs of the communities most exposed to those risks. Especially in suburban or semi-urban areas where people use the internet daily but don't always have the tools to understand the risks. Supanto et al. (2023) conducted a relevant study, but they didn't appear to link their findings with national-level data from Bareskrim or even with broader patterns of digital literacy tracked by Kominfo. As a result, their approach, while useful in parts, doesn't fully respond to how cybercrime has changed on the ground in Indonesia. That's a problem, because without understanding the actual threat patterns, education efforts tend to repeat the same general advice. What's needed instead is something more layered. A model that blends theory and actual field data, and that looks closely at different groups not just by age or income, but by how they engage with digital space in their everyday lives.

This study is trying to fill part of that space. It looks at cybercrime data published by Bareskrim from 2020 to 2024 and combines that with literacy indicators reported by Kominfo in 2023. The goal isn't to produce a one-size-fits-all solution, but to design digital education modules that are more adaptive especially for suburban communities, where infrastructure and access vary greatly. The modules won't only teach things like how to detect phishing, though that's important. They'll also try to build a sense of risk awareness. Not just what to do, but how to think when something online feels off. If this works, it could become a foundation for more targeted approaches that match the way different groups live and experience digital life.

2. Literature Review

2.1. Human Resource Development Theory and Digital Literacy

Cyber resilience rarely appears in older human capital theories. Most of them, including Becker's, focus on formal education as a driver of productivity. That makes sense in a traditional economy. But when digital skills are often picked up informally, like through YouTube tutorials or advice from friends, the theory starts to feel limited. In Indonesia, this gap becomes even more noticeable. Wibowo and Basri (2020) points out that many people gain digital knowledge not in classrooms, but through trial, error, and social learning. So the usual model that treats education as an economic investment needs to be adjusted. Maybe cybersecurity should be viewed like health. Schultz (1961) once said that staying healthy keeps people productive. The same might apply to being digitally safe. Without it, even skilled workers can become vulnerable.

The government has tried to respond, although the results are uneven. The National Digital Literacy Movement (GNLD) claims to have reached over 12 million people. That sounds impressive at first, but the outcomes vary widely depending on where and how the training happens. In Eastern Indonesia, completion rates for webinars are barely nine percent according to Kominfo. Meanwhile, when the format shifts to local storytelling and discussion-based sessions, participation can jump above seventy percent. That difference is too big to ignore. It suggests that delivery methods may matter just as much as the material itself. Another issue is how success is measured. Most of it depends on self-assessment. Zahra (2023) found that 83 percent of participants believed they could recognize scams, yet many of them failed practical tests. The gap between confidence and competence is real. Nawaz and Kundi (2010) had warned about this. They argued that access alone is not enough. Halim et al. (2022) also noted that behavior, not just knowledge, is what helps people detect phishing. And behavior is harder to teach.

There's a framework by Eshet (2005) that goes further than most. It includes not just technical understanding, but also emotional and ethical aspects of digital behavior. That broader scope might explain why it was effective in certain contexts. Scam incidents dropped by forty percent. Still, even with promising results like that, most digital literacy programs don't seem connected to real-time threat patterns. They often feel general, and sometimes outdated. That disconnect matters. When threats evolve but training stays the same, people are left unprepared. This research tries to address that. It combines data from Bareskrim's cybercrime reports with local learning strategies, hoping to build models that actually reflect the risks people deal with in their everyday digital lives.

2.2. The Role of Public Education in Cybercrime Prevention

Despite growing thicknesses of digital protection such as firewalls, rules, and network monitoring software, many cyberattacks still begin with something far less exotic: a misstep by a human. It could be an email that is just convincing enough or a website that is remarkably similar to an official website. Solis-Diaz (2023) reports that more than 90 percent of digital breaches originate in the misstep of humans, more than the failure of the technological system. In Indonesia, this pattern is more than evident. In one case, a rural cooperative in the province of Central Java became the victim for Rp 1.2 billion for a phishing scam in the year 2023. The scam didn't rely upon technological savvy. It was successful because someone clicked the wrong thing at the wrong time. In suburban and rural regions, where digital sophistication is low, this type of blunder is more common (Halim et al., 2022; Zahra, 2023). Surfing the internet is different from understanding the landscape it opens.

In order to address this chronic weakness, the government came up with Gerakan Nasional Literasi Digital (GNLD), a nationwide movement designed to train 50 million individuals in digital skills and ethical behavior by 2024 (Andriani et al., 2024). The goal was ambitious and, at a glance, commendable. But the challenge lies in implementation beyond the culmination of the trainings. Only 18 percent of the trainees recalled how to execute simple protection measures like enabling the two-factor authentication. One number is enough in itself to engender concern. Additionally, the roll-out of the program divulges an unmistakable disconnect with local realities. In Sumba, for example, the attendance rate in the GNLD webinars was not more than nine percent. But when the same content was translated into local storytelling activity or interactive role-playing exercise, attendance reached 74 percent. The implication is obvious and yet typically overlooked. Information is not sufficient for people. They must get the right medium, language, and cultural context so that they understand what information they receive.

These findings reveal the limitations of one-size-fits-all approaches. GNLD's reliance on centrally trained facilitators unfamiliar with local dialects has alienated many users, especially in suburban areas where 82% disengaged (Zahra, 2023). In contrast, Singapore's Cybersafe program builds local ownership by training informal community leaders as digital ambassadors, something GNLD has yet to replicate.

The case for shifting toward prevention is not only behavioral but also economic. Training-based interventions are ten times more cost-effective than post-attack responses. Indonesia's Rp 23.4 trillion loss to cybercrime could fund GNLD for 27 years. To increase impact, educational campaigns must evolve into precision-education strategies that align threat data with localized digital literacy gaps, a model this study aims to advance.

2.3. Previous Research

Numerous researches carried out in Indonesia explored digital literacy and how it intersects with cybercrime awareness. Inspection, however, identifies a recurring pattern: the majority of the interventions increase short-term awareness or knowledge, but most of them do not entail robust methods for tracking behavioral changes, context-level adaptation, nor integration with real-time threat intelligence. This disconnects marks a significant empirical divide, between taught and needed for enduring cyber resilience.

Various research efforts attempted to put a number on the effectiveness of digital education programs conducted within school or community settings. Isnaini et al. (2024) reported a measurable digital literacy score improvement, from 17.49 to 30.77, upon targeted cyber hygiene education in schools and universities. These findings validate the effectiveness of well-designed, well-measured education programs in making cognitive and behavioral responses more resistant to online threats.

But other studies introduce depth and scope constraints. Marwati and Astofa (2024), in making PKBM learners aware of phishing, could not establish whether the learned knowledge translated into daily digital behavior. These examples are characteristic of the broader pattern in Indonesian digital literacy research: measurement stops short at surface level, and is unsuccessful at taking account of longer-term modification or practical avoidance of risk.

Even at the national level, programs like GNLD are criticized in the same manner. Despite ambitious targets and broad coverage, GNLD was criticized for poor granular measurement and poor local adaptation (Zahra, 2023). Referenced previously, training millions is commendable, but without tracking how many apply these lessons when faced with a phish link, the impact is questionable.

Another important gap is between cybersecurity education programming and crime statistics. While cybersecurity threats get more geographically specific and targeted, such as province-specific phishing rackets or population-specific data breaches, public education remains broadly standardized and non-adaptive. Kominfo's Digital Literacy Index is still largely based upon measures of access and content consumption, while Bareskrim's annual reports on cybersecurity crimes show obvious hotspots and behavioral patterns that are not reflected in education and training programming.

Filling these chasms requires the shift toward data-driven education design. This entails the use of data on patterns of cybercrime, for example the spread of phishing in the suburbs or the MSME operators' threat, and literacy segmentation for creating place-based, adaptive education modules. Defense courses against phishing could thus be prioritized in the regions with the highest number of incidents, while modules on digital ethics could be focused on youth segments who are most at risk for cyberbullying. This precision-education approach transforms blanket campaigns into targeted interventions based on real risk profiles.

Besides, Khairunnisak et al. (2024) show that practice-based programs, behavioral signals, and loops for feedback fare better than transfer-based programs for passive information. The takeaway is clear: cyber literacy should transcend the rigid checklist and become an adaptive system of practice guided by risks, assessed and refined at all times.

In short, the empirical reality of digital education in Indonesia presents hope, but identifies a critical strategic blind spot. Without rigorous evaluation, behavioral tracking, and alignment with threat intelligence, even the most well-intentioned programs cannot build genuine resilience. To address this gap, this research attempts to interoperate national trends in cybercrime (Kepolisian Negara Republik Indonesia, 2024) with Kominfo's digital literacy profiles in an effort to promote an adaptive, evidence-based framework for public education for Indonesia's most vulnerable populations.

3. Methods

This study applies a descriptive qualitative approach using a literature review as the primary method. The research draws on secondary data gathered from various publicly accessible sources, particularly cybercrime trend reports published by Bareskrim Polri from 2020 to 2024, and digital literacy assessments compiled by the Ministry of Communication and Informatics (Kominfo). These include annual reports from the GNLD (Gerakan Nasional Literasi Digital) program as well as Digital Literacy Index data segmented by region and demographic indicators. Additional references were collected from academic journals, policy documents, and national survey data to enrich the comparative perspective.

To ensure transparency in data collection, sources were selected based on three criteria: public availability, institutional credibility (e.g., government or peer-reviewed sources), and thematic relevance to cybercrime prevention and digital education. The focus of the analysis centers on suburban and semi-rural communities, chosen purposively due to the recurring pattern of low digital literacy and high exposure to online risks in those areas. Content analysis was used to identify trends in cybercrime incidents, assess the effectiveness of digital education programs, and explore gaps in community-level outreach strategies. Validity of findings was strengthened through source triangulation, by comparing patterns and conclusions across government data, academic literature, and independent evaluations of the GNLD initiative. Although fieldwork was not conducted, the study aims to offer grounded insights that can inform future empirical research or policy development in similar contexts.

4. Results and Discussion

4.1. Cybercrime Trends in Indonesia (2020–2024)

Based on statistical reports from the Criminal Investigation Department of the Indonesian National Police (Bareskrim Polri), the evolution of cybercrime in Indonesia over the past five years reveals not only a growing volume of incidents, but also an increasingly diverse and complex threat landscape. As society becomes more digitally interconnected, the types of cyber offenses reported have shifted, highlighting how the nation's exposure to digital risks is no longer confined to isolated technical breaches, but extends into social, economic, and psychological domains.

Figure 1 below presents the annual distribution of five major categories of cybercrime reported between 2020 and 2024. These categories were selected based on their consistent prominence in national law enforcement data and their strategic relevance to public digital safety and governance.

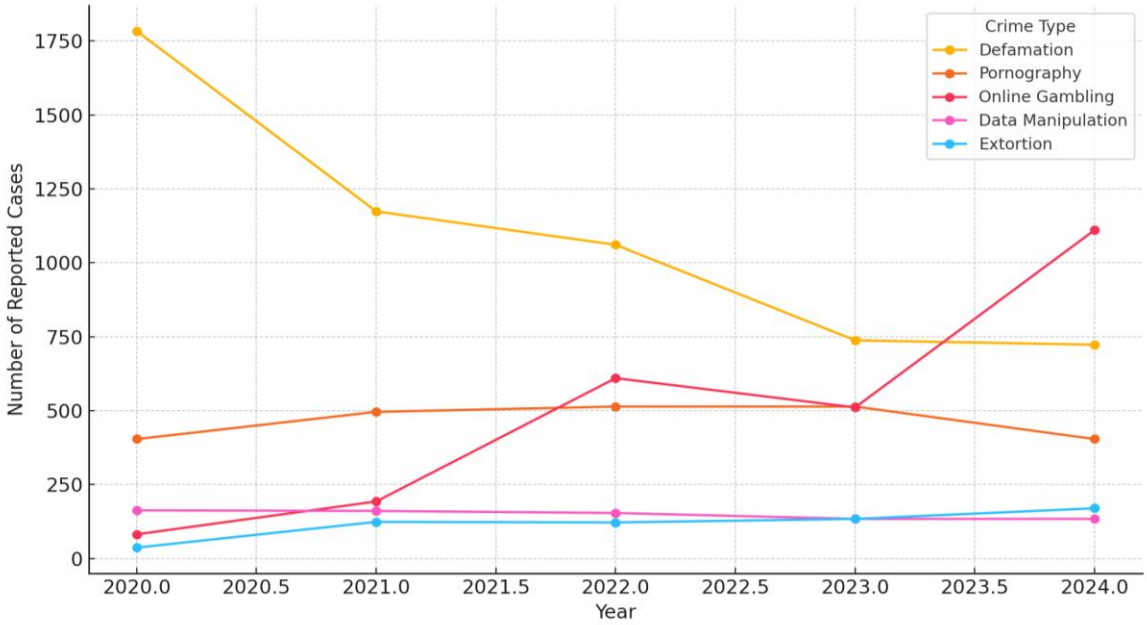

Figure 1. Cybercrime Trends in Indonesia

As shown in Figure 1, online defamation was the leader back in the year 2020 with an astonishing 1,800 reported cases. But this gradually slowed down for the following years, all the way down to 723 cases in the year 2024. While still massive, the declining trend could be due to the change in behavior among the public, the reaction in policies, or increasing digital literacy among users. In contrast, online gambling expanded explosively. Whereas the number was as few as 82 in the year 2020, the figures ballooned into 1,111 by the year 2024, growing more than thirteen times. The explosive growth is an indication of rising availability of illicit sites, possibly triggered by financial incentives and weak digital controls.

Crimes involving pornography remained flat over the five-year period, though always voluminous in number. In the same time frame, digital extortion and data manipulation reported moderate but consistent case numbers reflecting ongoing challenges with data privacy and cybersecurity potency.

Generally, these evolving trends suggest that the cybersecurity situation in Indonesia is systematically decreasing focus on socially inclined crimes (e.g., defamation) and is advancing toward economy-driven and technically advanced offenses. This new course necessitates more data-driven, specialized public awareness campaigns aligned with digital values and new threat realities.

The real spike is in online gambling. In 2020, cases were still under 100. But by 2024, it exploded past the thousand marks. This is not a minor jump but a shift in behavior. This is due to it there is something to do with how accessible these platforms have become. Some of these platforms, they do not even look like gambling at first. They appear like games or pop up in our social media feed, maybe even shared in group chats by someone we know. With all the encryption stuff and anonymous payments, they just sort of sneak by unnoticed. Further, when we mix that with people still recovering financially, especially after the pandemic, it is not hard to see why some take chances online. Not always because they want to. Sometimes, it feels like they do not have many options left.

Meanwhile, crimes involving digital extortion, data manipulation, and pornography have persisted. They are present year after year, albeit they do not usually surge sharply. The problem is that they frequently go unreported. Victims may be too ashamed, uncertain about where to go, or fearful of being held accountable. Additionally, cases are invisible when they are not included in official reports. Therefore, we are probably just seeing a portion of what is happening when we look at the statistics.

Now, looking at this through a legal system lens helps clarify some of the bottlenecks. Using Lawrence Friedman's framework, we can break it down into three elements: substance, structure, and culture. The laws? They are mostly in place. We have got the ITE Law, revisions to the Criminal Code, and several cyber-related regulations. But that was just the first layer. The bigger issues lie in the structure, which how these laws are applied, who enforces them, and whether the institutions are up to the task. Some areas have cyber units, while others do not. Some officers get training; others are left guessing.

Legal culture might be the trickiest piece. In a lot of areas across Indonesia, especially those far from big cities, it's still kind of blurry where the line is between what's just "normal" online behavior and what the law considers a crime. People might share hoaxes, explicit content, or even defamatory posts without thinking twice, and honestly, it is not always clear whether they know it could lead to legal trouble. Sometimes the rules feel vague, or maybe they are just not reaching the people who need to hear them. But in some countries, using dubious apps or going to gambling websites are accepted online practices rather than crimes. In addition to ignorance or disinterest, the lack of readily available, context-specific education is the primary cause of the issue. People find it challenging to recognize ethical boundaries in the digital sphere when social settings mainstream such behavior because of the uncertainty that results. That kind of mindset means that it does not really shift overnight. Moreover, when it sticks around, what happens is the authorities come in a bit too late. Damages already exist, and by then, it is harder to clean up. GNLD and similar programs initiatives are a good step, no doubt. But on their own? Probably not going to fix much. Real change needs more than just materials or one-time talks. It has to come from real discussions, ones that actually click with people, stuff that makes sense in their world, not just ours.

All of this tells us that cybercrime in Indonesia is not just about bad actors exploiting tech. It is also about institutions trying to catch up with problems that keep evolving. Criminals are adapting fast which sometimes faster than the state can regulate. Laws matter, sure, but unless the systems that support them grow in capacity and public trust improves, the problem will keep recurring in different shapes. The point isn't to fix everything overnight. But maybe it is time to rethink how we define progress which not just in terms of how many rules we write, but in how much those rules matter in real life.

4.2. Digital Literacy Index in Indonesia

Over the past four years, Indonesia has made consistent progress in improving digital literacy among its population. Government initiatives have played a key role in preparing citizens for the challenges of the digital era. Official data from the Ministry of Communication and Informatics (Kominfo) shows the country's Digital Literacy Index growing from 3.47 points in 2020 to 3.65 points in 2023, using a standardized five-point measurement system. What's particularly interesting is how this index breaks down. Rather than being a single metric, it actually assesses four distinct but interconnected areas: technical Digital Skills, responsible Digital Ethics, positive Digital Culture, and crucial Digital Safety awareness - giving us a comprehensive picture of how Indonesians are adapting to the digital world.

Figure 2 below indicates the increase in the digital literacy index every year for Indonesia for the period 2020-2023. The data were procured using the national digital literacy survey conducted annually among over 10,000 respondents with multistage random sampling across the country.

Figure 2. Indonesia's Digital Literacy Index (2020–2023)
Source: Ministry of Communication and Informatics (Kominfo), 2023.

Although the general upward trend is encouraging, a closer examination reveals a critical weakness: the "Digital Safety" pillar has consistently scored the lowest among the four dimensions. This suggests that while Indonesians may increasingly understand how to use digital tools, they remain less equipped to protect themselves from digital threats such as phishing, fraud, and data breaches.

The dissonance between rising index values and the persistent vulnerability to cybercrime points to a gap between digital perception and practical capability. In other words, the increase in self-reported or assessed digital literacy may not yet translate into tangible improvements in digital resilience, particularly in communities with limited access to formal digital education or real-world cyber hygiene practices.

This disconnect is especially concerning when juxtaposed with the rising trend of cybercrime in the same period, as discussed earlier. The data imply that existing digital literacy initiatives, while broad in scope, may require recalibration to better target critical awareness and threat-specific competencies, rather than just general digital engagement.

4.3. Digital Literacy Index in Indonesia

One of Indonesia's flagship initiatives in digital capacity building is the Gerakan Nasional Literasi Digital (GNLD) program, launched in 2021 and coordinated by the Ministry of Communication and Informatics (Kominfo). As of 2023, the GNLD has reached an impressive cumulative total of nearly six million participants, with year-over-year growth showing significant acceleration. Table 1 below presents the number of participants from 2021 to 2023, based on official government records and national progress reports.

Table 1. GNLD Program Participants in Indonesia (2021–2023)

Year	Participants
2021	1.800.000
2022	3.200.000
2023	5.801.436

Source: Kominfo, LAKIP 2023

Although the general upward trend is encouraging, a closer examination reveals a critical weakness: the "Digital Safety" pillar has consistently scored the lowest among the four dimensions (Tomczyk & Eger, 2020). This suggests that while Indonesians may increasingly understand how to use digital tools, they remain less equipped to protect themselves from digital threats such as phishing, fraud, and data breaches.

The dissonance between rising index values and the persistent vulnerability to cybercrime points to a gap between digital perception and practical capability. In other words, the increase in self-reported or assessed digital literacy may not yet translate into tangible improvements in digital resilience, particularly in communities with limited access to formal digital education or real-world cyber hygiene practices.

This disconnect is especially concerning when juxtaposed with the rising trend of cybercrime in the same period, as discussed earlier. The data imply that existing digital literacy initiatives, while broad in scope, may require recalibration to better target critical awareness and threat-specific competencies, rather than just general digital engagement.

4.4. Discussion

The study's findings lay bare a compelling contradiction at the heart of Indonesia's digital evolution. While national efforts to boost digital literacy have grown in both reach and ambition, this momentum hasn't translated into a corresponding drop in cybercrime. If anything, the opposite appears true. As Section 4.1 reveals, reported cases of online gambling, data manipulation, and digital fraud have surged between 2020 and 2024. These developments echo the warnings of Fazlurrohman et al. (2024) and Bareskrim (2024), who argue that cybercriminals are becoming increasingly adept at navigating regulatory gaps and exploiting the grey areas within Indonesia's evolving digital governance landscape.

This apparent disjunction between outreach and impact echoes patterns previously noted in several Indonesian digital literacy interventions. For instance, Supanto et al. (2023) documented how interactive digital awareness campaigns among community leaders increased surface-level knowledge but failed to produce durable behavioral changes in risk mitigation. This study confirms and extends those findings by showing that even large-scale national initiatives such as the GNLD, with over 5.8 million participants in 2023 which struggle to produce meaningful cybersecurity resilience when divorced from behaviorally anchored pedagogies and localized threat modeling.

Moreover, the consistent underperformance of the "Digital Safety" pillar in the national Digital Literacy Index (as presented in Section 4.2) reinforces critiques made by Zahra (2023) and Bulya and Izzati (2024), who caution against overreliance on quantitative participation metrics. Our findings align with Zahra's analysis of "competency illusions," wherein 83% of GNLD participants claimed to recognize scams yet failed in practical phishing simulations. This exposes a cognitive-behavioral gap in digital training—a phenomenon that Eshet (2005) anticipated in his multidimensional literacy model, which argues that true digital competence must integrate not just technical and cognitive skills but also ethical and emotional literacies.

By juxtaposing these earlier studies with current data, a critical insight emerges: the prevailing digital literacy strategies have emphasized scale over specificity. While Kioskli et al. (2023) demonstrated that structured cyber hygiene training can yield measurable improvements in controlled educational settings, our study suggests that these effects do not generalize across diverse geosocial contexts, especially suburban and semi-rural populations with limited infrastructural access and different cultural idioms of learning.

The GNLD's strong outreach to impoverished regions highlighted in Section 4.3 which should be lauded for its commitment to inclusive development. However, as Bulya & Izzati (2024) argue and this study affirms, such reach is only valuable if the content delivered is transformational rather than informational. Without behavioral scaffolding, culturally adaptive modules, and post-training feedback loops, digital literacy may remain performative, raising awareness but not enabling defense.

In contrast to earlier studies that treated digital threats as generic and uniformly distributed, our research introduces the need for data-driven segmentation in public education design. Drawing on Bareskrim's regional cybercrime analytics, we argue that training modules must be geographically and demographically tailored. For instance, phishing training should be intensified in suburban zones with high fraud incidence, while modules on data ethics may be prioritized in urban youth populations vulnerable to cyberbullying. This precision-education paradigm is largely absent in prior literature and represents a key contribution of this study.

Furthermore, our findings suggest that previous interventions have rarely been evaluated through a longitudinal lens. Marwati and Astofa (2024) succeeded in raising phishing awareness among informal learners but did not monitor daily digital practices. In contrast, this study not only maps the rise of cybercrime over time but also triangulates it with literacy trends, revealing a dangerous parallel growth rather than an inverse correlation.

Finally, this study expands on theoretical frameworks by extending Becker's and Schultz's human capital theory into the realm of cybersecurity. In line with Wibowo and Basri (2020), we reconceptualize digital safety as a form of economic preservation, where failing to educate citizens on digital risk becomes a threat not only to individual privacy but to national productivity. By proposing the integration of cybercrime intelligence into literacy planning, we operationalize the often-theoretical call for anticipatory governance in digital policy (Buçaj & Idrizaj, 2024).

In summary, this study confirms, extends, and critiques previous literature. It confirms the short-term gains and long-term limitations of awareness campaigns. It extends the discourse by incorporating empirical cybercrime data into literacy frameworks. Further, it critiques the assumption that digital literacy equals digital safety, a fallacy that must be addressed if Indonesia is to build a digitally resilient society.

5. Conclusion

This study shows that even though Indonesia has already done a lot to improve public digital literacy, especially with programs like GNLD, the effect on cybercrime prevention still seems quite limited. A lot of people have participated in these programs, but the number of cybercrime cases keeps going up, mainly in suburban and semi-rural areas where people don't have strong awareness about digital threats. From the findings, it becomes clear that knowing how to use digital tools is not the same as knowing how to stay safe online. That's why the way we do digital education needs to change, not just teaching general stuff but really focusing on the real risks people face out there on the internet.

There are a few important implications that can be taken from this research. First, for the government, it would be better if digital literacy programs were made based on the actual kinds of cybercrime that are happening in each region. That way, the material can be more useful and not too general. Second, for people or institutions who run the training, it's important to adjust the teaching methods so they fit the local culture and how people learn best, especially in areas with poor internet access. Third, this study also reminds us that building human resources in this digital age isn't just about giving people access to technology, but also helping them build the right mindset and habits to protect themselves online.

Lastly, since this research only used secondary data, future studies should try to go directly to the field. It would be interesting to see how people actually behave after they join a digital literacy program. Do they really change how they act online? Do they become more careful or alert when facing digital threats? Those kinds of questions are important to answer if we want to make digital literacy programs truly effective.

6. References

Agustini, P. (2023). Indeks Literasi Digital Indonesia Kembali Meningkat Tahun 2022. *Aptika. Kominfo. Go. Id*.

Andriani, A. D., Fitri, S. A., & Muchtar, K. (2024). Model Komunikasi Literasi Digital Dalam Mengatasi Ujaran Kebencian Di Media Sosial. *Interaksi: Jurnal Ilmu Komunikasi*, *13*(2), 439–464.

Buçaj, E., & Idrizaj, K. (2024). The need for cybercrime regulation on a global scale by the international law and cyber convention. *Multidisciplinary Reviews*, *8*(1), 2025024.

Bulya, B., & Izzati, S. (2024). Indonesia's Digital Literacy as a Challenge for Democracy in the Digital Age. *The Journal of Society and Media*, *8*(2), 640–661.

Dalimunthe, S. R., Pujawati, S. A., & Sitorus, A. S. A. (2022). Technical Security In ITE Law And Copyrights Of Devices And Systems. *POLICY, LAW, NOTARY AND REGULATORY ISSUES*, *1*(2), 27–36. https://doi.org/10.55047/polri.v1i2.124

Eshet, Y. (2005). Thinking skills in the digital era. In *Encyclopedia of distance learning* (pp. 1840–1845). IGI Global Scientific Publishing.

Fazlurrohman, M. A., Nita, S., & Aminanto, M. E. (2024). Comparative Studies On Trends And Strategies For Combating Cybercrime Between Indonesia And Developed Countries. *POLICY, LAW, NOTARY AND REGULATORY ISSUES*, *3*(4), 498–515. https://doi.org/10.55047/polri.v3i4.1512

Halim, E., Fitriani, M. N., Kurniawan, Y., & Husni, H. S. (2022). The Impact of Human Capital on Digital Literacy Index. *Proceedings of the 3rd Asia Pacific International Conference on Industrial Engineering and Operations Management, Johor Bahru, Malaysia, September 13-15, 2022*, Halim, E., Fitriani, M. N., Kurniawan, Y., Husni.

Isnaini, K. N., Rahmatullah, H. F., & Suhartono, D. (2024). Literasi Digital: Cyber Security di Dunia Pendidikan untuk Meningkatkan Perlindungan Data. *Jurnal Mengabdi Dari Hati*, *3*(1), 7–18.

Kioskli, K., Fotis, T., Nifakos, S., & Mouratidis, H. (2023). The Importance of Conceptualising the Human-Centric Approach in Maintaining and Promoting Cybersecurity-Hygiene in Healthcare 4.0. In *Applied Sciences (Switzerland)* (Vol. 13, Issue 6). https://doi.org/10.3390/app13063410

Kusumawardhani, N., Pramana, R., Saputri, N. S., & Suryadarma, D. (2023). Heterogeneous impact of internet availability on female labor market outcomes in an emerging economy: Evidence from Indonesia. *World Development*, *164*, 106182.

Marwati, F., & Astofa, A. (2024). Pentingnya Edukasi Cyber Security Untuk Menjaga Keamanan Data Pribadi dari Serangan Cyber Phishing Bagi Siswa/Siswi PKBM INTAN Tangerang Selatan. *AMMA: Jurnal Pengabdian Masyarakat*, *2*(12), 1508–1514.

Nawaz, A., & Kundi, G. M. (2010). Digital literacy: An analysis of the contemporary paradigms. *Journal of Science and Technology Education Research*, *1*(2), 19–29.

Schultz, T. W. (1961). Education and economic growth. *Teachers College Record*, *62*(10), 46–88.

Solis-Diaz, C. J. (2023). *Education as a Solution to Combat Rising Cybercrime Rates against Children and Teenagers* [California State University, San Bernardino]. https://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=2993&context=etd

Sunyoto, D. (2015). Manajemen dan pengembangan sumber daya manusia. *Yogyakarta: Center for Academic Publishing Service*.

Supanto, S., Ismunarno, I., Parwitasari, T. A., Budyatmojo, W., Fitriono, R. A., & Widiyanti, S. (2023). Pencegahan Dan Penanggulangan Kejahatan Teknologi Informasi Di Wilayah PDM Kabupaten Klaten Melalui Metode Sosialisasi Interaktif. *Gema Keadilan*, *10*(3), 170–182.

Tomczyk, & Eger, L. (2020). Online safety as a new component of digital literacy for young people. *Integration of Education*, *24*(2). https://doi.org/10.15507/1991-

9468.099.024.202002.172-184

Wibowo, A., & Basri, B. (2020). Literasi dan Harmonisasi Sosial: Desain Literasi Digital Berbasis Kearifan Lokal pada Masyarakat Pedesaan. *NALAR: Jurnal Peradaban Dan Pemikiran Islam*, *4*(2), 106–121.

Zahra, N. (2023). *Meningkatkan Inklusi dalam Indeks Literasi Digital Nasional: Dari Pengukuran hingga Pemberdayaan*. Center for Indonesian Policy Studies. https://repository.cips-indonesia.org/media/publications/565200-meningkatkan-inklusi-dalam-indeks-litera-a669d7c3.pdf