LAPORAN PENELITIAN

Comparative Analysis of Digital Literacy Effects on Cybercrime Awareness: Evidence from Generations Y and Z

Ketua Tim Peneliti:

Aris Subagio, M.Si

(NIDN: 0311028006)

Anggota Peneliti:

Rahmad Syalevi

(NUPTK: 4255769670130353)

Suhendra Saputra Jaya
(NIM: 123106151)

Universitas Paramadina

Juli 2025

HALAMAN PENGESAHAN

Penelitian dengan judul:

Comparative Analysis of Digital Literacy Effects on Cybercrime Awareness: Evidence from Generations Y and Z

Ketua Peneliti : Aris Subagio, M.Si (NIDN: 0311028006)
Jabatan Fungsional : Asisten Ahli
Program Studi : Ilmu Komunikasi
Nomor HP : 081311104867
Email: aris.subagio@paramadina.ac.id

Anggota Peneliti 1: Rahmad Syalevi (NUTPK: 4255769670130353)
Anggota Peneliti 2: Suhendra Saputra Jaya (NIM: 123106151)

Tahun Pelaksanaan : Tahun ke **1** dari rencana **1** tahun
Biaya penelitian: Rp 1.500.000,00

Jakarta, 21 Juli 2025

Penyusun Laporan,	Mengetahui,	Menyetujui,
Aris Subagio, M.Si	Dr. Tatok Djoko Sudiarto, MIB	Dr. Sunaryo
Ketua Peneliti	Dekan FFP	Direktur LPPM

ABSTRACT

This study aims to examine the influence of digital literacy and its dimensions - technical, cognitive, and social-emotional - on cybercrime awareness among university students, with a comparison between Generation Y and Generation Z. Adopting a quantitative approach, data were collected from 108 respondents through an online questionnaire using purposive sampling. Regression analysis revealed that all dimensions of digital literacy significantly affect cybercrime awareness, with the technical dimension having the most substantial impact. The generational comparison revealed that digital literacy had a significant influence on Generation Z, but no significant effect on Generation Y. These findings underscore the importance of adopting a multidimensional and generation-responsive approach to developing digital literacy and enhancing cybersecurity awareness.

Keywords: digital literacy, cybercrime, social media, Generation Z, Generation Y

1. Introduction

The swift evolution of digital technologies has profoundly reshaped various aspects of human life, influencing how people communicate, retrieve information, work, and engage socially. Social media has emerged as a hallmark of this digital era, offering unparalleled convenience in networking and real-time information sharing. Recent data indicate that in 2024, Indonesia recorded over 167 million active social media users, positioning it among the nations with the highest global social media penetration (Ramadhany et al., 2025).

The Digital 2025: Indonesia report published by DataReportal and We Are Social reveals that 91.7% of internet users aged 16–64 in Indonesia use WhatsApp, making it the most popular social media platform in the country, followed by Instagram (84.6%), Facebook (83.0%), TikTok (77.4%), and Telegram (61.6%). Other platforms such as Messenger (50.5%), X/Twitter (50.3%), and Pinterest (33.6%) also contribute significantly to the Indonesian digital ecosystem (DataReportal, 2025).

While social media offers numerous advantages, its rapid growth has also introduced significant challenges, particularly the escalation of cybercrime. Threats on social media platforms include phishing, online scams, account takeovers, malware infections, and unauthorized data exploitation. These threats underscore that digital literacy today goes far beyond technical abilities and requires critical comprehension, heightened security awareness, and ethical conduct in online contexts (Rodríguez-de-Dios et al., 2016).

Digital literacy encompasses a range of knowledge, skills, and attitudes that enable individuals to utilize digital technology safely, effectively, and critically (Ng, 2012). Specifically, in social media contexts, digital literacy encompasses the skills to assess information validity, secure personal data, detect cyber risks, and understand the legal and ethical implications of online behavior. Research suggests that, although younger groups are widely regarded as digital natives, many remain highly vulnerable to various forms of

cybercrime (Wilson, 2024).

Generational groups, such as Millennials or Generation Y (1981–1996) and Generation Z (1997–2012), each possess distinct digital backgrounds and characteristics. Millennials matured during the internet's expansion and became early adopters of social media. Meanwhile, Generation Z grew up in an entirely digital environment, making them highly adaptive to technological innovations (Rahardyan et al., 2023).

Nevertheless, recent findings show that frequent social media or internet usage does not necessarily equate to strong digital literacy. Many in Generation Z appear to be more susceptible to manipulation, phishing schemes, and social engineering due to their excessive trust in online content and inadequate information verification skills (Rodríguez-de-Dios et al., 2016; Umeugo, 2023). Wilson (2024) also revealed that numerous Generation Z employees require additional training to enhance their digital literacy, thereby ensuring safer and more efficient performance in digital workspaces.

In Indonesia, a series of recent cyber incidents highlights the urgent need to enhance digital literacy. A prominent example is the ransomware attack on the Temporary National Data Center (PDNS) 2 in June 2024, which severely disrupted public services and resulted in the leakage of sensitive data (CNN Indonesia, 2024). Another significant breach affected Bank Syariah Indonesia (BSI), where approximately 1.5 terabytes of customer data—impacting about 15 million people—were exposed online. Likewise, major e-commerce platforms such as Tokopedia, Bukalapak, and Lazada have faced similar breaches, further highlighting the fragility of Indonesia's cybersecurity infrastructure (Ramadhany et al., 2025).

Furthermore, in May 2025, Indonesia's Ministry of Communication and Digital Affairs temporarily suspended Worldcoin (rebranded "World") and WorldID operations due to the unauthorized collection of iris biometric data, violations of electronic system provider regulations, and public concerns over transparency (Komdigi). This case highlights that the

misuse of emerging digital identity tools can erode public trust and exacerbate cyber risks.

Additionally, the National Cyber and Crypto Agency (BSSN) documented over 403 million anomalous traffic incidents in 2024, revealing the magnitude of cyber threats in Indonesia. High social media penetration, coupled with inadequate digital literacy, raises users' vulnerability to cybercrime. A recent survey found that more than 60% of Indonesians lack a comprehensive understanding of how to protect personal data on social media and often share sensitive information publicly (Ramadhany et al., 2025).

Considering these realities, advancing digital literacy is crucial as a proactive measure to mitigate cybercrime risks, particularly on social media. Digital literacy equips individuals with critical thinking skills, risk identification capabilities, and the initiative to secure their digital data. Moreover, it helps build psychological resilience against manipulation and disinformation, which have become increasingly common on social media platforms (Tomczyk & Eger, 2020).

Therefore, this study aims to investigate and analyze the role of digital literacy as a pivotal factor in enhancing cybercrime awareness on social media, with a specific focus on generational differences between Generation Y and Generation Z in Indonesia. Accordingly, the study seeks to achieve the following objectives:

1. To analyze the overall effect of digital literacy on cybercrime awareness.
2. To analyze the influence of the technical dimension of digital literacy on cybercrime awareness.
3. To analyze the effect of the cognitive dimension of digital literacy on cybercrime awareness.
4. To analyze the impact of the social-emotional dimension of digital literacy on cybercrime awareness.
5. To compare the influence of digital literacy on cybercrime awareness between

Generation Y and Generation Z.

2. Literature Review

2.1 Digital Literacy

The concept of digital literacy has evolved significantly over the past two decades, moving beyond basic technical skills to encompass a complex set of abilities necessary to function effectively in a digitally saturated society. Digital literacy encompasses a blend of technical, cognitive, and socio-emotional skills that equip individuals to engage with digital technologies in a safe, effective, and ethically responsible way (Ng, 2012).

2.1.1 Technical Dimension

The first core dimension identified by Ng (2012) is the technical dimension. It refers to the operational skills required to effectively use information and communication technologies (ICT) in both learning and daily life contexts. A digitally literate individual in this dimension should be able to operate various hardware (e.g., computers, mobile devices, interactive whiteboards) and software applications with confidence. These skills include connecting peripheral devices, troubleshooting technical problems, managing file structures and data storage, and configuring settings for social media and communication tools. Ng (2012) emphasizes that mastery of these technical aspects allows individuals to engage comfortably with a range of digital tools, enabling them to perform tasks like downloading applications, using collaboration platforms, and managing digital content independently.

2.1.2 Cognitive Dimension

The cognitive dimension centers on critical thinking skills associated with searching for, evaluating, and creating digital content. According to Ng (2012), this dimension requires individuals to analyze and synthesize information gathered from various digital sources effectively. It involves the ability to choose appropriate tools and software for specific learning or creative purposes, while also understanding ethical and legal implications, such as

plagiarism and copyright. Moreover, this dimension demands multiliteracies skills, including linguistic, visual, audio, spatial, gestural, and multimodal literacies. These skills allow individuals to interpret and produce content in diverse formats, ranging from text and images to videos and interactive media.

2.1.3 Social-Emotional Dimension

The third dimension, the social-emotional dimension, addresses the ability to engage responsibly and ethically in digital social environments. This includes adhering to online etiquette (netiquette), protecting personal privacy, and recognizing and appropriately responding to potential online threats. Ng (2012) argues that social-emotional literacy is essential for safe participation in online communities, whether for learning, social interaction, or professional collaboration. This dimension also encompasses the ability to support and collaborate with peers, as well as the capacity to assess the intentions behind digital communications critically.

Studies emphasize that digital literacy refers to a person's capability to navigate complex online spaces, detect potential dangers, and defend themselves from harmful activities (Tomczyk & Eger, 2020). Therefore, digital literacy serves as a protective mechanism against cyber-related risks.

2.2 Cybercrime Awareness

Cybercrime awareness refers to the level of understanding, perception, and knowledge individuals possess about online threats, as well as their ability to identify, avoid, and mitigate risks during their digital activities (Arpaci & Aslan, 2023). Cybercrime includes a broad spectrum of illegal acts such as phishing, identity theft, data breaches, scams, cyberbullying, and ransomware attacks.

According to Umeugo (2023), the lack of adequate cybercrime awareness is a significant contributing factor to individuals becoming victims in online spaces. The rapid

growth of social media use has expanded the pool of targets for cybercriminals, making awareness an essential line of defense.

Additionally, cybercrime awareness is dynamic; it evolves continuously as new cyber threats and technological changes arise. For this reason, constant learning and adaptation are critical to maintaining adequate levels of protection. Increasingly, scholars and policymakers recommend embedding cybercrime awareness within broader digital literacy education frameworks.

2.3 Generational Differences in Digital Behavior

The theory of generational cohorts suggests that individuals born during similar time frames share everyday experiences, values, and exposure to technology, which shape their behaviors and attitudes (Rahardyan et al., 2023). In the sphere of digital technology and social media, these generational differences significantly influence how people consume content, assess online risks, and manage their digital identities.

2.3.1 Generation Y (Millennials)

Millennials, or Generation Y (born 1981–1996), matured during the internet expansion and were among the first to engage with social media actively. They are known for their flexibility in embracing new technology and their willingness to share personal information online. However, this enthusiasm can sometimes come at the cost of reduced attention to privacy and a lack of critical scrutiny of online information (Rahardyan et al., 2023).

2.3.2 Generation Z

Generation Z (born 1997–2012) represents a cohort that has been surrounded by digital technology from early childhood. While they are highly skilled in using various digital tools and navigating social media, research indicates that many in this group lack key critical digital literacy skills required to judge online risks accurately (Wilson, 2024).

Wilson (2024) found that Generation Z employees in higher education settings, despite being adept at adopting new technology quickly, often face difficulties when it comes to verifying information, safeguarding privacy, and practicing responsible online behaviors. This gap between high technical usage and weaker critical evaluation underscores the importance of developing specialized digital literacy training for this group.

2.4. Social Media and Cybercrime

Platforms like Facebook, Instagram, Twitter, and TikTok have become deeply ingrained in everyday routines, particularly for younger generations. These platforms enable widespread information exchange, social networking, and community building. However, they also create ample opportunities for cybercriminal activities.

Existing research shows that social media users are especially susceptible to threats like phishing, online fraud, and identity theft due to the personal details they frequently share publicly (Tomczyk & Eger, 2020). Cybercriminals can exploit this publicly available data to tailor personalized attacks, thereby increasing their chances of success.

In light of the theoretical framework and previous empirical studies, this research aims to investigate the impact of digital literacy on individuals' awareness of cybercrime. Considering that digital literacy encompasses multiple dimensions—technical, cognitive, and social-emotional—this study aims to explore both the overall and dimensional impacts of digital literacy on awareness of cybercrime. Moreover, the role of generational differences is considered by comparing the effects across Generation Y and Generation Z. The following hypotheses are proposed:

H1: Digital literacy significantly influences cybercrime awareness.

H1a: The technical dimension of digital literacy significantly influences cybercrime awareness.

H1b: The cognitive dimension of digital literacy significantly influences cybercrime awareness.

H1c: The social-emotional dimension of digital literacy significantly influences cybercrime awareness.

H2: There is a difference in the effect of digital literacy on cybercrime awareness between Generation Y and Generation Z.

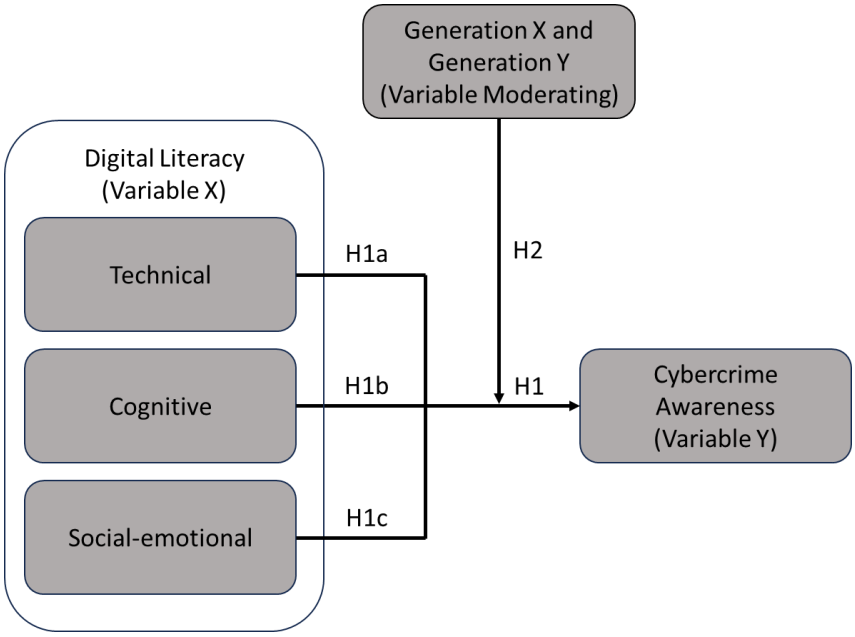

Figure 1: Theoretical Framework

Table 1 presents the key variables employed in this study, along with their conceptual definitions and the supporting references. These definitions provide the theoretical foundation for measuring and analyzing each construct within the research framework.

Table 1. Variables dan Definitions

Variable/ Dimension	Definition	Source
Digital Literacy	Digital literacy refers to the ability to effectively use digital tools and platforms to search, access, evaluate, manage, and create information; to communicate meaningfully with others; and to participate actively in digital environments.	Rodríguez-de-Dios et al. (2016); Ng (2012)
Technical	Refers to the ability to efficiently operate various digital tools and technologies, such as computers, smartphones, and software, in daily and professional contexts.	Rodríguez-de-Dios et al. (2016); Ng (2012)

Cognitive	The capacity to critically search, interpret, assess, and synthesize digital content, enabling individuals to make informed decisions in complex online environments.	Ng (2012); Tomczyk & Eger 2020
Social-emotional	Involves responsible and ethical behavior in digital spaces, including protecting one's privacy, engaging respectfully with others, and managing digital identity and emotions.	Ng (2012); Eshet-Alkalai (2004)
Cybercrime awareness	Represents an individual's awareness and understanding of cybercrime threats on social media, including the skills to recognize, avoid, and respond to online scams, phishing, identity theft, and digital fraud.	Arpaci & Aslan (2023); Umeugo (2023)

3. Research Method

3.1 Sample

This study utilized purposive sampling, focusing on students at Universitas Paramadina. Data were gathered through an online questionnaire distributed via Google Forms during the research period from June to July 2025. A total of 108 valid responses were collected. The respondents' demographic characteristics are outlined in the table below, covering four main aspects: generational group, gender, ownership of social media accounts, and frequency of daily social media usage.

Table 2. Respondent Description

Question	Answer	Frequency	Percentage
Generational Group	Generasi Y	36	33.3%
	Generasi Z	72	66.7%
Gender	Male	38	35.2%
	Female	70	64.8%
Social Media Account Ownership	Instagram	106	22.8%
	LinkedIn	45	9.7%
	Telegram	30	6.5%
	Threads	1	0.2%
	Tiktok	76	16.4%
	WhatsApp	102	22.0%
	X (Twitter)	57	12.3%
	Youtube	2	0.4%
	Facebook	45	9.7%
Daily social media access	More than 5 times	95	88.0%
	5 times	6	5.6%

	4 times	2	1.9%
	3 times	5	4.6%

Based on the demographic data, the majority of respondents belong to Generation Z, comprising 66.7% of the total, while Generation Y accounts for 33.3%. Respondents' sample is predominantly made up of younger individuals who are generally more digitally active and adaptive to technological trends. In terms of gender distribution, female respondents represent a larger proportion at 64.8%, compared to males at 35.2%. This higher representation of women could influence the overall trends in social media usage and digital behavior found in the study.

Regarding social media account ownership, Instagram and WhatsApp emerge as the most widely used platforms among respondents, with 22.8% and 22.0% respectively. These are followed by TikTok at 16.4% and X (Twitter) at 12.3%, indicating a preference for visual content and instant messaging applications. LinkedIn and Facebook are each used by 9.7% of respondents, while Telegram is used by 6.5%. Platforms like YouTube and Threads are the least popular, with only 0.4% and 0.2% of users, respectively. These findings reflect a strong inclination toward social media platforms that emphasize dynamic content sharing and quick communication.

When it comes to daily social media access, a significant majority (88.0%) of respondents reported accessing social media more than five times per day. Only small proportions access it five times (5.6%), three times (4.6%), or four times (1.9%) daily. This high frequency indicates a very intensive level of engagement with social media in everyday life, suggesting that for most respondents, social media has become an integral part of their daily routines.

3.2 Measurement

The research utilized a structured questionnaire developed based on prior literature concerning digital literacy and cybercrime awareness. This instrument comprised 32 items and

employed a Likert scale for response measurement. The digital literacy construct was adapted from the measurement index proposed by Ng (2012), encompassing a total of 10 items distributed across three key sub-dimensions: six items represented the Technical Dimension, two items assessed the Cognitive Dimension, and the remaining two measured the Social-Emotional Dimension. Meanwhile, the measurement of cybercrime awareness followed indicators established by Arpaci and Aslan (2022), consisting of 22 items in total.

Table 3. Variable Measurement

Variable	Dimension	Indicator	Statement	Source
Digital Literacy (X)	Technical (X_1)	Ability to solve technical problems independently (X_{11})	I know how to independently solve technical problems when using digital media.	Ng (2012)
		Ability to learn new technology easily (X_{12})	I can easily learn new technologies.	
		Awareness of emerging technologies related to digital safety (X_{13})	I keep up with important technology developments related to digital security.	
		Knowledge of commonly used digital technologies (X_{14})	I am aware of various types of commonly used digital technologies.	
		Skills in using ICT for content creation (X_{15})	I have the technical skills to use ICT in creating social media content.	
		Skills in managing account security (X_{16})	I have good ICT skills to protect the security of my social media accounts.	
	Cognitive (X_2)	Confidence in searching and evaluating online information (X_{21})	I am confident in searching for and evaluating information from the internet.	
		Understanding of digital risks and critical issues (X_{22})	I understand important issues related to online activities, such as cybersecurity,	

			plagiarism, and misinformation.	
	Social-Emotional (X_3)	Ability to collaborate and seek help online (X_{31})	I often seek help from friends via the internet (e.g., WhatsApp, Instagram, or video conferencing) to solve issues related to social media apps.	
		Safe and productive digital collaboration (X_{32})	Digital technology helps me collaborate with friends in a safe and productive way.	
Cybercrime Awareness (Y)		Awareness that hacking social media accounts without consent is a criminal act (Y_1)	Hacking someone else's social media account without permission is a crime.	Arpaci & Aslan (2022)
		Awareness that sharing others' personal data without consent is illegal (Y_2)	Sharing personal data with third parties without the owner's knowledge is a crime.	
		Awareness of legal consequences for data privacy violations (Y_3)	I know that there are penalties for violating data confidentiality on social media.	
		Awareness that promoting harmful substances on social media is a crime (Y_4)	Promoting the use of harmful substances on social media is a crime.	
		Awareness that supporting terrorism through social media posts is a criminal offense (Y_5)	I know that posting support for terrorist organizations on social media is a criminal act.	
		Awareness that posting unverified political or military content is a legal violation (Y_6)	Posting unverified political or military content on social media is a legal violation.	
		Awareness that selling illegal (fake/stolen) products via social media is a crime (Y_7)	Selling illegal (fake or stolen) products through social media is a crime.	

Awareness that linking to illegal websites via social media is a criminal act ($_{Y8}$)	Redirecting people to illegal websites via links on social media is a criminal act.
Awareness that conducting illegal betting/gambling on social media is a criminal offense (Y_9)	Conducting illegal gambling/betting activities on social media is a crime.
Awareness that distributing copyrighted works without permission is a legal offense (Y_{10})	Sharing copyrighted works without permission on social media is a legal offense.
Awareness that using insulting language on social media is a criminal act (Y_{11})	I know that using offensive language on social media is a crime.
Awareness that unauthorized audio/video recordings are criminal (Y_{12})	Recording videos or audio on social media without permission is a criminal act.
Awareness that disclosing confidential professional information via social media is a crime (Y_{13})	Disclosing confidential work-related information via social media is a crime.
Awareness that benefiting unfairly from illegal uploads is a criminal offense (Y_{14})	I know that gaining unfair profit from illegal uploads on social media is a crime.
Awareness that harassment through social media is a criminal offense (Y_{15})	I am aware that harassing others on social media is a form of crime.
Awareness that cyberbullying constitutes a legal violation (Y_{16})	I am aware that cyberbullying on social media is a legal offense.
Awareness that sexual content is prohibited on social media (Y_{17})	I am aware that sexual content must not be shared on social media.
Awareness that sharing violent imagery is a crime (Y_{18})	Sharing violent images on social media is a crime.

Awareness that distributing malware via social media is a criminal offense (Y_{19})	I know that spreading malicious software (malware) via social media is a crime.
Awareness that privacy breaches should be legally reported (Y_{20})	Legal reporting is required against those who violate personal privacy on social media.
Awareness that spreading fake news (hoaxes) is a criminal act (Y_{21})	I am aware that spreading fake news on social media is a crime.
Awareness that sharing unlicensed software is a legal violation (Y_{22})	Sharing unlicensed software on social media is a legal offense.

This study employed a quantitative approach to examine the influence of digital literacy, including its three dimensions—technical, cognitive, and social-emotional—on cybercrime awareness among university students. To address the research objectives, a series of statistical tests were conducted using SPSS version 23.

The analysis began with descriptive statistics to summarize the demographic characteristics of respondents and their perceptions of each variable, using measures such as mean and standard deviation. Next, validity and reliability tests were conducted to ensure that the questionnaire items met acceptable standards of internal consistency and construct validity.

To assess the relationships between variables, Pearson correlation analysis was used to determine the strength and direction of associations between the dimensions of digital literacy and cybercrime awareness. Following this, simple linear regression analysis was performed to examine the individual effect of each digital literacy dimension on the dependent variable.

Additionally, to explore generational differences in the influence of digital literacy on cybercrime awareness, split-group regression analysis was applied, comparing results between

Generation Y and Generation Z. All statistical tests were conducted at a significance level of 5% ($\alpha = 0.05$).

4. Results and Discussion

4.1 Results

4.1.1 Validity and Realibility

Based on the validity test results using item-total correlation, all items in the Digital Literacy dimension (10 items) and the Cybercrime Awareness dimension (22 items) showed correlation coefficients (r value) greater than the critical r table value (0.188) with a significance level of $p < 0.05$. This validity indicates that all items in both dimensions are valid and can be used to accurately measure their respective constructs.

The reliability test using Cronbach's Alpha yielded a value of 0.762 for the Digital Literacy dimension, which falls into the acceptable category, and 0.926 for the Cybercrime Awareness dimension, which is categorized as excellent. These results demonstrate that both instruments have good to excellent internal consistency.

4.1.2 Mean Test

From the results of the mean analysis, each dimension and indicator within the studied variables reflects differing levels of perception among respondents. On the Digital Literacy variable, the Cognitive dimension holds the highest average score (4.10), indicating that respondents generally perceive themselves as having strong cognitive abilities when dealing with digital information. Conversely, the Social-Emotional dimension scores the lowest (mean = 3.81), suggesting that emotional and social awareness in digital contexts may be perceived as less dominant.

Within the Technical dimension, the indicator “I can easily learn new technologies” (X_{12}) achieved the highest mean score of 4.23, showing that respondents strongly recognize adaptability to new digital tools. Meanwhile, the indicator “I have good ICT skills to secure

my social media account" (X_{15}) received the lowest in this dimension, with a mean of 3.82, indicating a potential gap in cybersecurity practices.

In the Social-Emotional dimension, the indicator "I often seek help through online communication to solve technical issues" (X_{31}) recorded the lowest mean (3.32). At the same time, "I understand critical digital issues such as cyber security and fake news" (X_{32}) reached the highest mean (4.29), showing that although awareness exists, confidence in social interaction via digital tools remains relatively low.

Turning to the Cybercrime Awareness variable, the overall mean score was relatively high (4.60), reflecting strong awareness among respondents regarding digital threats. Among the 22 indicators, the item "I am aware of the risk of cybercrime when using social media" (Y_1) achieved the highest mean (4.87), indicating strong baseline awareness. Other indicators such as "Sharing personal data with third parties without the owner's knowledge is a crime" (Y_2), "I know that posting support for terrorist organizations on social media is a criminal act" (Y_5), and "Conducting illegal gambling/betting activities on social media is a crime" (Y_9) also scored above 4.70. On the other hand, indicators such as "Posting unverified political or military content on social media is a legal violation" (Y_6) (mean = 4.19), "Sharing violent images on social media is a crime" (Y_{18}) (mean = 4.29), and "Sharing unlicensed software on social media is a legal offense" (Y_{22}) (mean = 4.40) showed comparatively lower perceptions, which may point to areas where digital crime prevention messaging could be improved.

These descriptive results not only highlight the dimensions that are perceived positively but also reveal areas requiring further attention.

Table 4. Mean Test Results

Variable	Dimension	Indicator	Mean	Mean Dimension	Mean Variable
Digital Literacy (X)	Technical (X_1)	X_{11}	4.09	4.05	4.01
		X_{12}	**4.23**		
		X_{13}	4.07		
		X_{14}	4.19		

		X_{15}	**3.82**		
		X_{16}	3.90		
	Cognitive (X_2)	X_{21}	**4.10**	**4.10**	
		X_{22}	**4.10**		
	Social-emotional (X_3)	X_{31}	**3.32**	**3.81**	
		X_{32}	**4.29**		
Cybercrime Awareness (Y)		Y_1	**4.87**	**4.60**	4.60
		Y_2	4.81		
		Y_3	4.61		
		Y_4	4.66		
		Y_5	4.78		
		Y_6	**4.19**		
		Y_7	4.72		
		Y_8	4.70		
		Y_9	4.81		
		Y_{10}	4.57		
		Y_{11}	4.44		
		Y_{12}	4.40		
		Y_{13}	4.44		
		Y_{14}	4.43		
		Y_{15}	4.74		
		Y_{16}	4.70		
		Y_{17}	4.63		
		Y_{18}	4.29		
		Y_{19}	4.68		
		Y_{20}	4.56		
		Y_{21}	4.68		
		Y_{22}	4.40		

4.1.3 Correlation Between Digital Literacy and Cybercrime Awareness.

The Pearson correlation test yielded a coefficient value of 0.271, with a significance level of $p = 0.005$ ($p < 0.01$), indicating a significant connection between overall Digital Literacy (Xtot) and Cybercrime Awareness (Ytot) scores. This result indicates a positive and significant association, albeit classified as weak. Individuals with higher digital literacy tend to demonstrate increased awareness of cybercrime.

4.1.4 Determination Coefficient of the Digital Literacy Variable on Cybercrime Awareness.

The results of the data analysis show that the unstandardized regression coefficient (B) for the Digital Literacy variable is 0.607, with a standard error of 0.209, and a standardized coefficient (Beta) of 0.271. The t-value is 2.900, and the significance level is 0.005. The result indicates that Digital Literacy has a significant influence on Cybercrime Awareness.

To test the influence of the independent variable on the dependent variable, a t-test was conducted. The hypothesis tested in this study is as follows:

H_1: Digital literacy significantly influences cybercrime awareness.

Based on the distribution table with a significance level (α) of 5%, the critical t-value is approximately 1.982. Since the calculated t-value (2.900) is greater than the t-table value and the significance level is less than 0.05 ($p = 0.005$), the hypothesis is accepted. Therefore, it can be concluded that Digital Literacy has a statistically significant influence on Cybercrime Awareness.

Furthermore, the constant value in the regression model is 76.739, representing the predicted value of Cybercrime Awareness when Digital Literacy equals zero. Thus, the simple linear regression equation can be estimated as follows:

$Y = 76.739 + 0.607X$

where Y is Cybercrime Awareness and X is Digital Literacy. This result implies that for every one-unit increase in Digital Literacy, Cybercrime Awareness increases by 0.607 units, assuming other factors remain constant.

4.1.5 Correlation Between the Technical Dimension of Digital Literacy and Cybercrime Awareness.

The results of the Pearson correlation analysis indicate a statistically significant relationship between the technical dimension of Digital Literacy and Cybercrime Awareness.

The correlation coefficient (r) is 0.221 with a p-value of 0.021, based on a sample size of 108 respondents. This result confirms a positive and weak correlation between the two variables. Since the p-value is less than 0.05, the correlation is considered significant at the 5% level. This result implies that as individuals' technical digital literacy increases, their level of awareness regarding cybercrime also tends to increase, although the strength of this relationship is relatively low.

In summary, the findings support the notion that technical competencies in using digital tools and platforms are meaningfully associated with higher levels of cybercrime awareness. However, given the modest strength of the correlation, it is likely that other factors also contribute significantly to cybercrime awareness.

4.1.6 Determination Coefficient of the Technical Dimension of Digital Literacy on Cybercrime Awareness

The results of the regression analysis demonstrate that the unstandardized coefficient (B) for the technical dimension of Digital Literacy is 0.718 with a standard error of 0.308, and the standardized coefficient (Beta) is 0.221. The corresponding t-value is 2.336, and the significance level is 0.021. The result suggests that the Technical dimension of Digital Literacy exerts a statistically significant effect on Cybercrime Awareness.

To assess the impact of the independent variable, a t-test was employed. The formulated hypothesis for this test is:

H1a: The technical dimension of digital literacy significantly influences cybercrime awareness.

Referring to the t-distribution table at a 5% significance level, the critical value is approximately 1.660. Since the computed t-value of 2.336 exceeds the critical threshold and the p-value (0.021) is less than 0.05, the hypothesis is accepted. The hypothesis confirms that the technical skills related to digital literacy significantly contribute to the level of Cybercrime Awareness.

Additionally, the constant in the model is 83.629, which represents the expected value of Cybercrime Awareness when the technical dimension score is zero. Based on this, the regression equation can be expressed as:

$Y = 83.629 + 0.718X$

where Y denotes Cybercrime Awareness and X denotes the technical dimension of Digital Literacy. This equation indicates that a one-unit increase in technical digital literacy skills is associated with a 0.718-unit increase in Cybercrime Awareness, holding other variables constant.

4.1.7 Correlation Between the Cognitive Dimension of Digital Literacy and Cybercrime Awareness.

The Pearson correlation analysis reveals a statistically significant relationship between the Cognitive dimension of Digital Literacy and Cybercrime Awareness. The correlation coefficient (r) is 0.203 with a p-value of 0.035, based on data from 108 respondents. It indicates a positive but weak correlation between the two variables.

Since the p-value is below the significance threshold of 0.05, the relationship is considered statistically significant. The result suggests that individuals with higher cognitive digital literacy tend to have a greater awareness of cybercrime threats.

Although the strength of the correlation is relatively modest, the results support the assumption that cognitive competence in the digital domain contributes to an individual's ability to recognize and respond to cyber threats. This finding highlights the importance of developing critical thinking and information evaluation skills as part of digital literacy education to foster cybercrime awareness.

4.1.8 Determination Coefficient of the Cognitive Dimension of Digital Literacy on Cybercrime Awareness

The results of the linear regression analysis indicate that the unstandardized coefficient (B) for the Cognitive dimension of Digital Literacy is 1.701, with a standard error of 0.797, and a standardized coefficient (Beta) of 0.203. The calculated t-value is 2.136, and the significance level is 0.035, which implies a statistically significant relationship between the two variables.

To assess the effect of the independent variable, a t-test was conducted. The hypothesis under investigation is:

H1b: The cognitive dimension of digital literacy significantly influences cybercrime awareness.

Using a 5% significance level, the critical t-value is approximately 1.660. Since the obtained t-value (2.136) is greater than the critical value and the p-value (0.035) is less than 0.05, the hypothesis is accepted. This result suggests that cognitive skills—such as the ability to critically assess, interpret, and apply digital information—have a significant influence on an individual's level of cybercrime awareness.

Furthermore, the constant value of 87.135 represents the expected value of Cybercrime Awareness when the Cognitive dimension score is zero. Therefore, the estimated linear regression equation is as follows:

$Y = 87.135 + 1.701X,$

where Y refers to Cybercrime Awareness and X to the Cognitive dimension of Digital Literacy. This indicates that for each one-unit increase in cognitive digital literacy score, Cybercrime Awareness is expected to increase by approximately 1.701 units, assuming all other factors remain constant. This highlights the importance of developing critical thinking and evaluative skills in promoting cyber awareness in digital environments.

4.1.9 Correlation Between the Social-emotional Dimension of Digital Literacy and Cybercrime Awareness.

The Pearson correlation test shows a statistically significant association between the Social-Emotional dimension of Digital Literacy and Cybercrime Awareness. The correlation coefficient (r) is 0.196, with a p-value of 0.042, based on a sample of 108 respondents. This result indicates a weak positive correlation between the two variables.

Given that the p-value is less than 0.05, the correlation is considered significant at the 5% level. It suggests that individuals with stronger social-emotional digital literacy—such as awareness of online behavior, empathy in digital interactions, and ethical decision-making—tend to be more aware of cybercrime risks.

Although the strength of the correlation is relatively low, the finding highlights the importance of emotional intelligence and responsible digital engagement in increasing one's awareness of online threats. Integrating social-emotional competencies into digital literacy training may contribute to building more resilient and cyber-aware individuals.

4.1.10 Determination Coefficient of the Social-emotional Dimension of Digital Literacy on Cybercrime Awareness

The regression analysis reveals that the unstandardized coefficient (B) for the Social-Emotional dimension of Digital Literacy is 1.340, with a standard error of 0.651, and a standardized coefficient (Beta) of 0.196. The resulting t-value is 2.059, and the associated significance level is 0.042, indicating a statistically significant effect of this variable on Cybercrime Awareness.

To evaluate the influence of the independent variable, a t-test was conducted to test the following hypothesis:

H1c: The social-emotional dimension of digital literacy significantly influences cybercrime awareness.

With a significance level (α) of 0.05, the critical value for t is approximately 1.660. As the calculated t-value (2.059) exceeds the critical threshold and the p-value (0.042) is below 0.05, the hypothesis is accepted. It signifies that the ability to navigate online interactions with empathy, ethical reasoning, and emotional regulation has a significant influence on individuals' awareness of cybercrime threats.

The regression model also includes a constant of 90.891, representing the predicted value of Cybercrime Awareness when the Social-Emotional dimension is zero. Therefore, the estimated simple linear regression equation can be expressed as:

$Y = 90.891 + 1.340X,$

where Y is Cybercrime Awareness and X is the Social-Emotional dimension of Digital Literacy. This equation suggests that for every unit increase in the social-emotional competency score, Cybercrime Awareness is expected to rise by approximately 1.340 units, assuming other variables remain constant. These findings underscore the importance of emotional intelligence and responsible digital engagement in enhancing cyber-awareness among users.

4.1.11 Comparison of the Determination Coefficient of Digital Literacy on Cybercrime Awareness Between Generation Y and Generation Z.

To explore generational differences in the influence of Digital Literacy on Cybercrime Awareness, separate regression analyses were conducted for Generation Y and Generation Z. The results demonstrate distinct outcomes across the two groups.

For Generation Y, the unstandardized regression coefficient (B) for Digital Literacy is 0.405, with a standard error of 0.360 and a standardized Beta of 0.189. The t-value is 1.125, and the significance level is 0.268. Since the t-value does not exceed the critical value at $\alpha = 0.05$ and the p-value is greater than 0.05, the effect of Digital Literacy on Cybercrime Awareness among Generation Y is not statistically significant.

In contrast, for Generation Z, the unstandardized coefficient (B) is 0.700, with a standard error of 0.257 and a standardized Beta of 0.310. The t-value is 2.723, and the significance level is 0.008. These results indicate that Digital Literacy has a statistically significant and moderately positive impact on Cybercrime Awareness among Generation Z. The regression model suggests that an increase of one unit in Digital Literacy leads to an approximate increase of 0.700 units in Cybercrime Awareness for Generation Z, assuming all else is constant.

The following hypotheses were tested:

H2: There is a difference in the effect of digital literacy on cybercrime awareness between Generation Y and Generation Z.

Given that Digital Literacy significantly influences Cybercrime Awareness in Generation Z ($p = 0.008$), but not in Generation Y ($p = 0.268$), the data support Hypothesis H2. This suggests that the role of digital literacy in shaping awareness of online threats is more pronounced among Generation Z than Generation Y.

These generational differences reflect the greater digital exposure and dependence among Generation Z, who have grown up in a digital environment that is largely devoid of traditional media. In contrast, Generation Y may have developed digital skills later in life, which may contribute to the weaker relationship observed in their cohort.

The regression models for both generations had no issues with multicollinearity, as indicated by tolerance values of 1.000 and Variance Inflation Factors (VIFs) of 1.000.

In conclusion, the findings underscore the importance of tailoring cybercrime prevention strategies to individual generational digital experiences. Educational efforts aimed at enhancing cyber-awareness may be more impactful when generational characteristics and digital literacy profiles are taken into account.

4.7 Discussion

The findings of this study emphasize the crucial role of digital literacy in enhancing cybercrime awareness, particularly across different generational cohorts. The results indicate that digital literacy has a significant influence on cybercrime awareness, with the most substantial effect observed in Generation Z. This finding supports the growing body of literature that affirms digital competence as a foundational defense mechanism against online threats (Ramadhany et al., 2025).

The regression analysis revealed that among the three measured dimensions—technical, cognitive, and social-emotional-each had a statistically significant, albeit modest, impact on cybercrime awareness. The technical dimension, with a standardized Beta of 0.221 ($p = .021$), highlights the importance of practical skills such as managing privacy settings, identifying phishing attempts, and protecting personal devices. This aligns with the indicators outlined in the DigComp framework, which include the ability to distinguish between malware emails, create strong passwords, and utilize security tools such as antivirus applications (Vuorikari et al., 2022; Ameliah et al., 2022).

Similarly, the cognitive dimension—comprising critical thinking and information evaluation—demonstrated a significant positive relationship with cybercrime awareness (Beta = 0.203, $p = .035$). This finding aligns with the literature emphasizing the importance of evaluative skills in filtering digital content, recognizing misleading information, and identifying social engineering tactics (Restianty, 2018; Saputra, 2023). The ability to assess the credibility of online information is increasingly vital in preventing manipulation and fraud attempts, especially as digital platforms proliferate.

The social-emotional dimension also had a significant yet weaker relationship with cybercrime awareness (Beta = 0.196, $p = .042$), indicating that empathy, ethical behavior, and

emotional regulation in digital environments play a contributory role. While often underestimated, this dimension supports safer digital behavior and mitigates the spread of harmful content or interactions online (Ameliah et al., 2022). Integrating socio-emotional awareness into digital literacy curricula, therefore, strengthens holistic digital resilience.

Crucially, this study revealed generational differences in how digital literacy affects cybercrime awareness. For Generation Y (born 1981–1996), digital literacy showed a positive but statistically insignificant influence on cybercrime awareness ($p = .268$). In contrast, Generation Z (born 1997–2012) exhibited a more substantial and statistically significant effect (Beta = 0.310, $p = .008$). This supports prior research suggesting that Generation Z, often referred to as digital natives, are more immersed in technology and more responsive to digital learning environments (Ker Yuek Li, 2021).

Generation Z's enhanced responsiveness can be attributed to their early and frequent engagement with digital media, mobile platforms, and social technologies, which makes them more adept at integrating technical, cognitive, and emotional skills in digital contexts (Kozinsky, 2017; Mathur & Hameed, 2016). Their familiarity with multitasking and real-time digital interaction fosters a deeper understanding of online risk and protection strategies, as also discussed in the Road to Digital Literacy framework (Kominfo, 2020).

Meanwhile, the lesser influence observed in Generation Y may stem from their transitional exposure to digital technology. Although many in this group are proficient users, they often acquired their digital skills later in life. They thus developed them in narrower contexts, such as for work-related tasks rather than holistic engagement. Research by Anckar et al. (2023) also points to gaps in cybersecurity awareness among Gen Y and Gen Z, with Gen Y often reporting lower confidence in managing digital threats.

These findings reinforce the argument that digital literacy must be cultivated not only as a technical skill but also as a multidimensional capacity that encompasses ethical reasoning,

critical thinking, and socio-emotional awareness. Ramadhany et al. (2025) emphasize the integration of these pillars as essential in reducing vulnerability to cybercrime and promoting sustainable digital behavior across all age groups. Their study shows that community-based digital education initiatives, especially those incorporating the DigComp and Kominfo frameworks, can effectively enhance digital resilience.

Additionally, cybercrime prevention must consider generational characteristics to design effective interventions. As shown in previous studies, awareness programs tailored to digital habits and cognitive styles of specific age groups lead to more impactful outcomes (Ismailova & Muhametjanova, 2023; Zayid & Farah, 2023). For example, Generation Z may benefit more from gamified learning modules or social media–based campaigns. At the same time, Generation Y might require workplace-oriented training programs with an emphasis on cybersecurity policy and device protection.

Ultimately, this research contributes to a growing consensus that digital literacy is not a one-size-fits-all construct, but rather a dynamic and evolving skill set shaped by generational experience, social context, and technological fluency. Strengthening digital literacy, therefore, should be prioritized not only in formal education but also in national cybersecurity strategies, especially as cyber threats continue to escalate in scale and complexity (BSSN, 2024; CNN Indonesia, 2023).

5. Conclusion

This study examined the influence of digital literacy and its key dimensions—technical, cognitive, and social-emotional—on cybercrime awareness among university students, with particular attention to generational differences between Generation Y and Generation Z. The findings indicate that digital literacy plays a significant role in shaping individuals' awareness of cybercrime, with the effect being more prominent among Generation Z. All three dimensions

of digital literacy were found to have a positive and statistically significant impact on cybercrime awareness. However, the magnitude of their influence varied.

Among the three, the technical dimension emerged as the strongest predictor, emphasizing the critical importance of practical skills such as safeguarding personal information, identifying online threats, and navigating digital environments securely. The cognitive dimension also made a meaningful contribution, highlighting the relevance of critical thinking and information evaluation in recognizing cyber risks. While the social-emotional dimension showed a slightly weaker relationship, it nonetheless underscored the value of ethical and empathetic digital behavior in promoting safe online practices.

A noteworthy finding is the generational disparity in the influence of digital literacy. For Generation Z, digital literacy showed a stronger and statistically significant effect on cybercrime awareness, whereas for Generation Y, the relationship was comparatively weaker and not statistically significant. This comparison suggests that Generation Z, having grown up immersed in digital environments, is better equipped to apply their digital competencies in identifying and responding to cyber threats.

These results suggest that digital literacy should be understood as a dynamic and multi-faceted competency, rather than a one-size-fits-all construct. Educational institutions are encouraged to design and implement digital literacy programs that are tailored to the specific needs, experiences, and learning styles of different generational groups. Integrating such multidimensional digital literacy frameworks into higher education curricula could serve as a proactive strategy for enhancing students' awareness of cybercrime and fostering greater digital resilience.

Despite its contributions, this study has certain limitations. The sample was restricted to university students, which may limit the generalizability of the findings to broader populations, particularly older age groups or individuals outside academic contexts.

Additionally, the reliance on self-reported questionnaire data may introduce response bias. The use of a cross-sectional design also restricts the ability to establish causality or examine temporal changes.

Future research should consider longitudinal approaches to track the development of digital literacy and cybercrime awareness over time. Broadening the scope to include more diverse demographic groups—across age, educational background, and geographical location—would enhance the applicability of future findings. Moreover, exploring potential mediating or moderating variables such as digital confidence, online behavior, or social influence could offer deeper insights into the mechanisms underlying the relationship between digital literacy and cybercrime awareness.

In conclusion, enhancing digital literacy in all its dimensions is essential for promoting greater awareness of cybercrime, particularly in light of generational differences. Continued research and well-targeted educational strategies are crucial for equipping individuals with the competencies necessary to navigate an increasingly complex and vulnerable digital landscape.

References

Ameliah, R., Negara, R. A., Minarto, B., Manurung, T. M., & Akba, M. (2022). *Status literasi digital di Indonesia 2022*. Kominfo. https://satudata.kominfo.go.id

Anckar, B., Kuusela, H., & Niemelä-Nyrhinen, J. (2023). Digital confidence across generations: Findings from Finnish working professionals. *Journal of Cybersecurity Education, Research and Practice*, 2023(1), 1–15.

Arpaci, I., & Aslan, A. (2023). Investigating cybercrime awareness in social media: A structural equation model approach. *Computers in Human Behavior Reports, 9*, 100271. https://doi.org/10.1016/j.chbr.2022.100271

BSSN. (2024). *Lanskap Keamanan Siber Indonesia 2023*. Badan Siber dan Sandi Negara. https://www.bssn.go.id

CNN Indonesia. (2024, Juni). *PDNS 2 diretas: Dampak dan investigasi kebocoran data nasional*. https://www.cnnindonesia.com

DataReportal. (2025). *Digital 2025: Indonesia*. We Are Social & Kepios. https://datareportal.com/reports/digital-2025-indonesia

Eshet-Alkalai, Y. (2004). Digital literacy: A conceptual framework for survival skills in the digital era. *Journal of Educational Multimedia and Hypermedia, 13*(1), 93–106.

Ker Yuek Li. (2021). Eye on digital media literacy from the perspective of Generation Z. In E. R. Anshari (Ed.), *Proceedings of the 9th International Conference on Educational Technology of ICT-Based Learning in Asia* (pp. 221–226). European Publisher. https://doi.org/10.15405/epsbs.2021.06.02.33

Kominfo. (2020). *Roadmap Literasi Digital Nasional*. Kementerian Komunikasi dan Informatika Republik Indonesia.

Ng, W. (2012). Can we teach digital natives digital literacy? *Computers & Education, 59*(3), 1065–1078. https://doi.org/10.1016/j.compedu.2012.04.016

Rahardyan, A., Setiawan, A. M., & Sari, M. (2023). Generational patterns in digital literacy and security behaviors: A comparative study of Indonesian millennials and Gen Z. *Jurnal Ilmu Komunikasi, 21*(1), 56–71. https://doi.org/10.1234/jik.v21i1.567

Ramadhany, A. F., Damayanti, N. E., Rahmania, L. A., & Inawati. (2025). Digital literacy as a cyber crime defense and prevention strategy. In *Proceedings of the 9th International Seminar on Recent Advances in Educational Technology (ISRM)* (pp. 778–785). NST Proceedings. https://doi.org/10.11594/nstp.2025.47116

Restianty, D. (2018). Literasi digital dan kesadaran keamanan siber di Indonesia. *Jurnal Keamanan Siber dan Sains Informasi, 3*(1), 23–30.

Rodríguez-de-Dios, I., Van Oosten, J. M. F., & Igartua, J. J. (2016). A study on the relationship between digital literacy and online risk among adolescents. *Computers in Human Behavior, 58*, 140–148. https://doi.org/10.1016/j.chb.2015.11.039

Tomczyk, L., & Eger, L. (2020). Educational cyber defense: Exploring the relationship between digital literacy and cyberbullying in the Czech Republic and Poland. *Cyberpsychology, Behavior, and Social Networking, 23*(3), 189–193. https://doi.org/10.1089/cyber.2019.0379

Umeugo, C. (2023). Digital safety behavior among digital natives: An empirical study of cybercrime vulnerability in Nigerian youth. *International Journal of Cyber Criminology, 17*(1), 85–100. https://doi.org/10.5281/zenodo.7654321

Vuorikari, R., Punie, Y., Carretero, S., & Van den Brande, G. (2022). *DigComp 2.2: The Digital Competence Framework for Citizens*. European Commission. https://joint-research-centre.ec.europa.eu

Wilson, T. (2024). Bridging the digital divide in Generation Z: Cybersecurity training in higher education. *Journal of Digital Behavior and Learning, 12*(1), 44–59.

Zayid, A., & Farah, N. (2023). Cybercrime awareness on social media: A comparison study. *International Journal of Network Security & Its Applications, 15*(2), 25–36. https://doi.org/10.5121/ijnsa.2023.15203