International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

The Cybercrime in the Philippines: A Literature Review

Laarni C. Cortes[1], Rowela Cartin-Pecson[2]

Abstract

The research presents a systematic analysis of cybercrime in the Philippines, examining its prevalent types, underlying causes, impacts, and the effectiveness of existing legal frameworks. Using the PRISMA 2020 framework, 200 studies were identified from multiple scholarly databases and other web tools, of which 51 studies met the inclusion criteria after rigorous screening and risk-of-bias assessment. Findings reveal that hacking, identity theft, phishing, online fraud, cyber libel, malware attacks, cyberbullying, ransomware, and cyberespionage are the most frequent documented types of cybercrime in the country. The review highlights significant economic, psychological, social, legal, and national security impacts, including financial losses, emotional trauma among victims, weakened public trust in digital systems, enforcement challenges, and threats to critical infrastructure. Contributing causes were categorized into technological vulnerabilities, low empathy and behavioral risk, and socioeconomic factors. Although Republic Act No. 10175 or the Cybercrime Prevention Act of 2012, constitutes a foundational legal guideline, enforcement gaps, jurisdictional issues, and limited public awareness hinder its full effectiveness.

Keywords: criminal justice, cybercrime, Cybercrime Prevention Act of 2012, PRISMA 2020, literature review, law enforcement, Philippines

1. Introduction

The Philippines has a wide range of cybercrimes, such as identity theft, internet fraud, hacking, and child exploitation. The frequency and complexity of cyber-attacks continue to rise, with small and medium-sized enterprises being particularly targeted, often lacking adequate resources for defense (Chakraborty et al., 2024). Cyberscrimes have emerged as a significant threat in the digital era, affecting individuals, organizations, and societies worldwide (Loggen et al., 2024).

Cybercrime is an act committed exclusively on the internet and through the use of computers, as well as traditional crimes. Criminal acts committed using electronic communications and information systems are considered Cybercrime and encompass a range of offenses. It can be individual acts as well as state-sponsored Cybercrime (Khan et al., 2022). These acts can range from unauthorized access, data breaches, identity theft, phishing, to ransomware attacks, with far-reaching implications across jurisdictions (Payne, 2020).

Society relies on technology to support everyday activities due to the growing complexity of digitalization and interconnected cyber networks. Technology is increasingly central to public, social, and business operations, influencing everything from government services to everyday shopping (World Economic Forum, 2021). Hence, in the research study by Cartin-Pecson et al. (2025), digital threats are becoming more sophisticated as technology becomes essential to everyday life. Viraja and Purandare

(2021) also highlighted the corresponding increase in Cybercrime with the advent of platforms that utilize vast amounts of data worldwide.

Social media platforms are also experiencing tremendous growth, with almost everyone connected to at least one platform. The world is enjoying the benefits of cyberspace, and globalization is more prevalent than ever before (Varol et al., 2024). In the face of this growing threat, numerous studies have sought to better understand the nature and scope of cybercrime. Previous research has examined various aspects, including risk factors associated with the victimization and perpetration of cybercrimes (Guo & Wang, 2024).

As technology advances and becomes more accessible, criminals have leveraged these tools to carry out illegal activities in cyberspace (Vaddi et al., 2024). Cybercriminals now exploit tools such as encrypted messaging apps, anonymizing networks, and even artificial intelligence to commit financial fraud, identity theft, cyberstalking, phishing, ransomware attacks, and more. This trend underscores the urgent need for robust cybersecurity measures, updated legislation, and digital literacy to protect individuals, businesses, and institutions from these evolving threats. The complex, transnational nature of Cybercrime presents unique challenges for researchers and criminal justice professionals (Dunsin et al., 2024).

The rapid evolution of technology has consistently outpaced the development of legal frameworks, creating a disjuncture between cybercriminal capabilities and the tools available to law enforcement. This dissonance underscores the pressing need to adapt legal mechanisms to the dynamic nature of cyber threats, ensuring the criminal justice system remains agile in the face of rapidly changing technologies (Refaei, 2023). Issues such as artificial intelligence-driven attacks, blockchain-enabled fraud, and the dark web challenge traditional legal responses, urging lawmakers to adapt swiftly. To counteract technological advancements by cybercriminals, legal mechanisms must be adaptive and anticipatory (Jerome, 2020). Legislation that incorporates flexible definitions and provisions empowers law enforcement to keep pace with emerging threats while upholding due process and protecting individual rights.

Recognizing the global nature of cyber threats, international collaboration becomes imperative to combat Cybercrime effectively (Mphatheni & Maluleke, 2022). No single jurisdiction or nation can single-handedly scale or sophisticate cyber threats. The dynamic and fluid nature of the internet, coupled with the use of anonymization tools, enables cybercriminals to effectively obfuscate their location (Khalifa, 2020). The collective intelligence, resources, and expertise of multiple nations are essential to form a united front against cybercriminals. Global organizations play a crucial role in facilitating this collaboration.

Digital evidence is often complex, diverse, and difficult to collect, preserve, and analyze. The lack of standardization and protocols for handling it has hindered its admissibility as evidence in court (Quick & Choo, 2021). Establishing standard protocols and procedures for digital evidence collection and handling is essential to ensure its admissibility in court and to prevent wrongful convictions (Reith, 2022). Policymakers, law enforcement agencies, and digital forensics experts must work together to develop effective guidelines and legal frameworks that specifically address the unique challenges posed by Cybercrime (Brayne & Martin, 2021).

Cyberspace, which encompasses the infrastructure, connectivity among devices, the software that runs on those devices, and the information maintained within those infrastructures, is growing exponentially across all spaces (Varol et al., 2024). This growth is redefining the world, as traditional activities such

as communication, industrialization, social interaction, the military, education, transportation, and more are being adapted by cybertechnologies. These crimes have rapidly evolved from cyberbullying to online fraud and ransomware attacks, exploiting technological advancements and security system vulnerabilities (Patsakis et al., 2024).

The dark web is a part of the internet that contains hidden sites that users cannot find through conventional web browsers. Referring to the collection of encrypted online content on darknets that cannot be acquired through standard web browsers poses a major challenge for law enforcement agencies investigating and prosecuting cybercriminals, due to the inherent anonymity of darknets (Dunn & Zukowski, 2021). One investigation by Yashaswi and Pulijala (2021) examined the challenges of detecting Cybercrime in the context of the Internet of Things (IoT), a network of everyday physical objects embedded with sensors, software, and connectivity that enable data exchange.

Motivating nations to actively participate in establishing international legal frameworks and reevaluating current laws that inadequately address cyber resilience within the digital economy. As highlighted by Cartin-Pecson et al. (2025), this contributes to the crucial global discourse on cyber governance and digital law enforcement by examining each nation's approach to cyber legislation. It also guides stakeholders, legal experts, and policymakers in the unwavering pursuit of a safer, more secure cyberspace. This growth is redefining the world through cybertechnologies, as traditional activities such as communication, industrialization, social interaction, the military, education, transportation, and more have changed. This positions cyberspace as a crucial new element and central focus, to the point that it is considered the fifth domain of security and warfare (Varol et al., 2024).

The Cybercrime Prevention Act of 2012 marked a significant legislative effort to combat Cybercrime in the Philippines. However, its implementation raises questions about its adequacy and the balance between security and freedom of expression. Studies indicate that cybercriminals exploit vulnerabilities in both legal frameworks and societal structures, underscoring the need for a comprehensive understanding of these dynamics to inform effective policy interventions (Sosa, 2024). Moreover, as digital platforms proliferate, the demographics of cybercriminals and their methods have evolved, underscoring the need for targeted educational initiatives and preventive strategies (Chen et al., 2023).

One prevalent form of Cybercrime is identity theft, where unauthorized individuals gain access to social media accounts to impersonate users. in the Cybercrime Prevention Act of 2012 (Republic Act No. 10175), which criminalizes unauthorized access to computer systems, including social media accounts. Once a hacker gains access, they can deceive others into providing money or personal information, constituting both identity theft and online fraud (Respicio & Co, 2024).

Cyberbullying victims frequently report significant emotional trauma, which can lead to severe mental health issues, including suicidal ideation (Sosa, 2024). The stigma associated with being victimized online can also deter individuals from seeking help or reporting incidents, further compounding their psychological burden. The University of the Philippines has initiated professional courses on digital governance and cybersecurity to enhance the skills of government officials and other stakeholders (UP CIFAL, 2021). These programs are essential for building a knowledgeable workforce capable of addressing cybersecurity challenges.

The Cybercrime Prevention Act of 2012 (Republic Act No. 10175) serves as the cornerstone of the Philippines' legal framework against cybercrime. This act focuses on the prevention, investigation, and prosecution of cyber offenses, including identity theft, online libel, and data breaches (Department of Justice, 2024). Although this legislation provides a foundation for combating cybercrime, the Philippine

government is developing a national cybercrime strategy to enhance coordination among agencies and strengthen legal frameworks to address emerging threats effectively (Council of Europe, 2024).

Legislative bodies must adopt proactive approaches to address technological challenges. These involve periodic reviews and updates of existing laws to encompass new technologies and threats (Chauhan & Shiaeles, 2023). Collaborative efforts between lawmakers, technologists, and cybersecurity experts are vital to drafting legislation that is not only comprehensive but also future-proof. Legislative bodies must adopt proactive approaches to address technological challenges. As law enforcement agencies leverage sophisticated technologies for investigations, the line between legitimate surveillance and unwarranted intrusion becomes blurred, necessitating a careful examination of the boundaries between security imperatives and individual rights (Olukunleo et al., 2024).

The establishment of specialized units within law enforcement agencies, such as the National Bureau of Investigation's Cybercrime Division and the Philippine National Police's Anti-Cybercrime Group, has been bolstered through these training initiatives. These units are essential for implementing effective responses to cyber incidents and fostering collaboration with international counterparts (UNAFEI, 2023).

The Budapest Convention on Cybercrime, which the Philippines acceded to in 2018, serves as a foundational framework for international cooperation in combating cybercrime (Council of Europe, 2024). This treaty provides guidelines for member states to harmonize their national laws regarding cyber offenses and procedural rules for investigating and prosecuting these crimes. It also emphasizes the importance of mutual legal assistance and information exchange among countries, which are vital for effectively addressing transnational cyber threats.

The research objective is to provide a comprehensive and evidence-based systematic review of cybercrime in the Philippines. It seeks to identify the various types, causes, and impacts of cybercrime, as well as the effectiveness of existing legal frameworks. This study is urgent given the increasing severity of cybercrime in the Philippines and the country's accelerating digital transformation. These gaps will hinder a full understanding of cybercrime in the Philippines and limit the development of effective, evidence-based reforms.

Cohen & Felson's Routine Activity theory serves as a foundation for this research. The essence of this theory is that when an individual possesses characteristics that attract the offender and is made aware of the motivated offender, coupled with a lack of protection from the attacker, he or she is likely to become a crime victim. Since this theory is used to explain physical crime, it is unclear whether it can be applied to online crime (Junger et al., 2017). One issue plaguing cybercrime research is whether concepts and constructs from the physical world can be applied and interpreted similarly in a virtual environment (Leukfeldt & Yar, 2016).

One of the supporting theories is General Strain Theory by Robert Agnew, which emphasizes how social and economic pressures may push individuals toward criminal behavior. Agnew's revision, termed GST, creates a readily testable framework by positing that strain stems from three sources: failure to achieve positively valued goals, loss of positive-valued stimuli, and the presentation of negative stimuli (Parti & Dearden, 2024). Empirical tests of strain have largely supported GST. More recent refinements have enabled researchers to focus on strains more closely associated with crime. These include victimization, parental rejection, bullying, and discrimination (Craig et al., 2017).

A recent study by Zhou et al. (2024) provides empirical support for Social Learning theory in explaining cybercrime, showing that individuals' exposure to deviant behaviors through social interaction significantly predicts their participation in online offending. Most prior studies grounded in the

perspective of offending suggest that individuals who commit online deviance should have developed specialized attitudes and behaviors distinct from those of other forms of deviance (Nodeland & Morris, 2020).

The study is of great importance, as it offers legislators useful insights into how to improve and create cybercrime laws by identifying gaps in current legislation. These will serve as the basis for more effective legislation to combat cybercrime and promote safer internet browsing in the Philippines. Law enforcement agencies will also be better equipped to develop strategies for public awareness and law enforcement in response to the study's enhanced understanding of cybercrime.

These will help the Philippine government raise public awareness and effectively address cybercrime. It will mobilize support for cybercrime prevention by enabling local communities to take proactive measures to counter it. These also provide a solid foundation for future research, enabling scholars to explore cybercrime. Importantly, it will promote international cooperation by giving the international community and organizations a resource to develop policies addressing the global impact and causes of cybercrime. This research aligns with the United Nations (2023) SDG 16 – Peace, Justice, and Strong Institutions by promoting accountability of cybercrime offenders and presenting effective responses towards cybercrime violations.

2. Methods

This study utilized a systematic review guided by the PRISMA 2020 framework. Relevant studies were identified through database and manual searches, screened using eligibility criteria, and synthesized using a thematic-descriptive approach. Ethical considerations focused on transparency as no human participants were involved.

Research Subject

A total of 14 research databases and two search engines were used to retrieve relevant studies. A manual search of relevant literature was conducted using Google and Google Scholar to identify additional sources not captured in research databases. Search terms such as "cybercrime," "Philippines," "cyberhacking," "cyber libel," "cyber attack," "cybercrime law," and "cybercrime enforcement." Additionally, the researcher will use operators (AND, OR) to refine the searches. Studies were screened and manually searched to identify additional studies. These include "cybercrime in the Philippines OR cybercrime law in the Philippines", "cybercrime law AND cybercrimes". Filters were applied to include publications from 2015 to 2025 and to include only English-language studies, to narrow the search.

The data collected in this research, based on the objectives and eligible results, were recorded manually in Microsoft Excel. Of the 200 studies initially identified, only 51 were deemed eligible after careful screening and full-text assessment. These eligible studies were screened using a descriptive thematic analysis to extract information on the types, impacts, and effectiveness of the cybercrime law.

The researcher established eligibility criteria to ensure the selection of relevant data. The inclusion criteria primarily consist of accessible full-text published studies in English from 2015 to 2025. Eligible literature includes both local and foreign research on cybercrimes in the Philippines, such as hacking, phishing, identity theft, online fraud, cyber libel, cyber bullying, malware attacks, ransomware, and cyber espionage. Studies that explore the impacts, causes, contributing factors, and effectiveness of the law in the Philippines. The selected literature was limited to peer-reviewed journals, academic theses or sources, dissertations, systematic or literature reviews, and credible organizational publications. Exclusion criteria included publications before 2015 and those not written in English. Studies not related

to Cybercrime, enforcement, or policies excluded. Non–academic sources, such as editorial pieces, blog posts, personal websites, YouTube videos, podcasts, and any unpublished literature, were excluded.

Materials and Instruments

A self-developed checklist was created and utilized within Microsoft Excel to guide the identification, screening, and extraction of selected studies. This tool was adapted from PRISMA 2020 to align with the objectives of the review of cybercrimes in the Philippines. To ensure the quality of eligible studies, a self-developed risk-of-bias checklist was used, enabling the researcher to assess the transparency of each selected study. A self-developed tool was necessary to support contextual judgment in evaluating the specific study on cybercrimes, because none were available or suitable for the qualitative nature of the study. All extracted and collected data were recorded manually in Microsoft Excel, providing a flexible, more organized way to synthesize the selected studies.

Design and Procedure

This study employs a systematic review as its research design, which helped identify, select, and critically appraise existing relevant research on cybercrimes in the Philippines. Unlike traditional literature reviews, it follows a predefined protocol to avoid bias and ensure comprehensive, reliable findings. The Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 configuration approach is used as a guide to ensure transparency, replicability, and rigor in the literature review and selection process for the eligibility assessment of the text (Page et al., 2021). All relevant literature retrieved from the databases was recorded using Microsoft Excel for organization.

Data synthesis was executed qualitatively, summarizing the findings from the included studies. The researcher will be required to synthesize the structure around the following key areas: prevalent types of cybercrime, impacts of cybercrime, underlying causes of cybercrime, and the effectiveness of existing cybercrime laws. Thematic analysis was used to identify common themes and patterns across the studies, providing a comprehensive understanding of Cybercrime in the Philippines.

The researcher upheld the four qualitative pillars of credibility, transferability, dependability, and confirmability throughout the study to ensure trustworthiness. Credibility was established through a structured, systematic review guided by the PRISMA 2020 framework and the application of inclusion and exclusion criteria to ensure only eligible studies were selected. To ensure that the included literature aligned with the research objective, manual screening and the CASP Checklist were used to assess the risk of bias. Transferability was maintained by documenting the study's limitations and ensuring that exclusion criteria were applied. Dependability was addressed through transparent documentation and the consistent application of the screening process in Microsoft Excel. Lastly, confirmability was achieved through a clear auditing process that included full documentation of the academic database searched, the search terms used, and the eligibility criteria applied. This comprehensive approach ensures the integrity, transparency, and reliability of the study's synthesized results.

3. Results and Discussion

This section presents the findings of the systematic review on cybercrimes in the Philippines. It highlights the study selection process and thematic-descriptive analysis of the included literature. The researcher highlighted the types, causes, and impacts of cybercrime, providing deep insights into this issue.

A total of 200 studies were identified through academic databases and search engines. 7 duplicate studies were removed, and 193 records were screened for title and abstract. Meanwhile, 33 studies were

excluded for being non-academic, having an irrelevant topic focus, or being inaccessible. Moreover, 160 full-text studies were assessed for eligibility, of which 81 reports were excluded because they either did not focus on Cybercrime or were not primarily focused on the Philippines. A total of 28 studies underwent risk of bias assessment, resulting in the exclusion of 5 reports tagged as high risk and 23 as moderate risk, but not highly relevant to the study. Finally, 51 studies were included in the final synthesis of this systematic review.

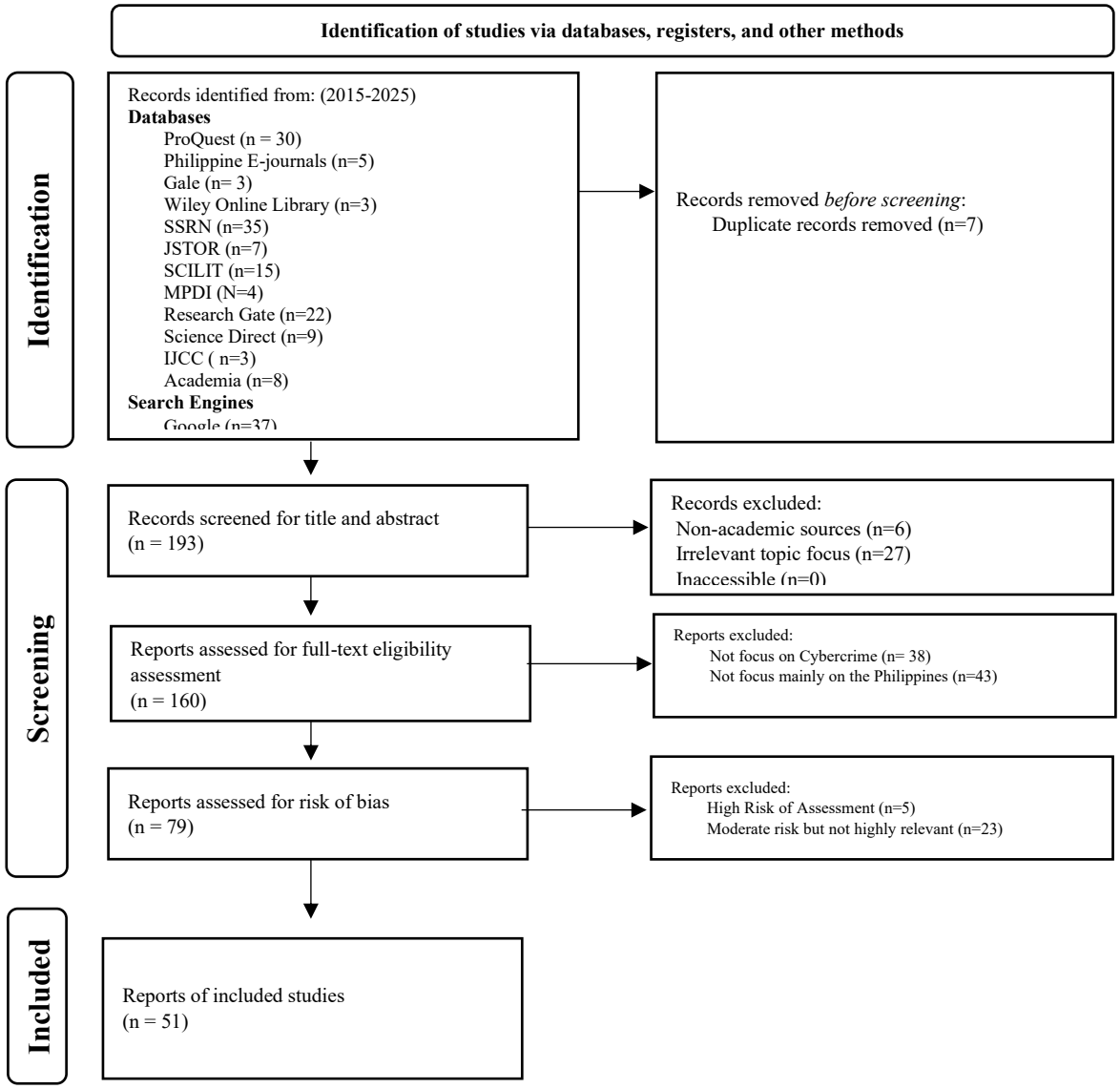

Figure 1. Study Selection Flow Diagram

In the risk of bias assessment, the researcher used the CASP General SR Checklist: Collation of critical appraisal responses. The checklist was divided into three sections: Are the review results valid? What are the results? Moreover, will the results help locally?. The questions are answered with Yes, No, or Cannot Tell. Through careful data collection, analysis, and evaluation, systematic reviews provide a comprehensive overview of the current evidence on a topic.

Table 1: Risk of Bias Assessment Tool
(CASP General SR Checklist: Collation of critical appraisal responses)

Yes	Checklist question	Can't tell	No
A. Are the results of the review valid?			
	1. Did the review address a clearly focused question?		
	2. Did the authors look for the right type of papers?		
	3. Do you think all the important, relevant studies were included?		
	4. Did the review's authors do enough to assess quality of the included studies?		
	5. If the results of the review have been combined, was it reasonable to do so?		
B. What are the results?			
	6. What are the overall results of the review?		
	7. How precise are the results?		
C. Will the results help locally?			
	8. Can the results be applied to the local population?		
	9. Were all important outcomes considered?		
	10. Are the benefits worth the harms and costs?		

Types of Cybercrime

This section presents the first major theme of the research: nine primary types of Cybercrime in the Philippines were identified. Out of the 51 included studies, 43 were under this theme. The following synthesis provides the key findings from the included studies under each category.

Table 2. Distribution of Studies by Types of Cybercrimes

Types of Cybercrime	Number of Studies
Hacking	11
Phishing	7
Identity Theft	8
Online Fraud	2
Cyber Libel	4
Cyber Bullying	5
Malware Attacks	3
Ransomware	2
Cyber Espionage	1

Hacking

According to the study by Brucal et al. (2025), the evolution of digital threats in the Philippines has necessitated a robust legal and institutional response. However, significant gaps remain in addressing the sophistication of modern hacking. According to the study of Suminig et al. (2025), the Cybercrime

Prevention Act was enacted as a strategic response to the proliferation of digital offenses such as identity theft, cybersex, and online libel, aiming to align national policy with international standards and restore public trust in digital transactions. However, according to Reyes (2024), legal scholars have identified critical limitations within the law, specifically its reliance on vague terminology; for instance, while the law penalizes "illegal access," it omits the specific term "hacking," despite the latter being the synonymous descriptor for unauthorized system entry in contemporary discourse. This lack of terminological precision complicates the legal pursuit of individuals who exploit network resources to access private communications or monitor third-party systems without authorization (Li, 2021).

The practical reality of Cybercrime in the Philippines was characterized by its increasing frequency across the government, private, and academic sectors, intensifying the demand for improved infrastructure (Rufino, 2025). Furthermore, in the study by Fajardo et al. (2025), these threats are often carried out through sophisticated techniques, including the exploitation of system vulnerabilities and the interception of private communications. Also, according to Pasia (2025), this trend is characterized by a deteriorating global crisis in which computers serve as both tools and targets of financial fraud and harassment. Moreover, the vulnerability of the citizenry is compounded by social media behaviors, where the routine sharing of personal data and imagery exposes users to hacking, defamation, and various forms of online abuse (Rufino et al., 2025).

In response to these pervasive risks, the Department of Justice (DOJ) has implemented specialized ethical hacking training for law enforcement to bolster the defense of state and commercial sites (Villamin, 2015). Despite these initiatives, the rapid pace of technological advancement continues to hinder the efficacy of criminal investigations. According to Custodio's (2025) study, the complexity of modern hacking methods, often orchestrated by highly sophisticated organized crime networks, creates a significant gap between detectives' capabilities and cybercriminals' evolving tactics. Consequently, while hacking is a multifaceted activity, it becomes a severe legal and social liability once leveraged for unauthorized access within these organized criminal frameworks.

Phishing

In the Philippines, the digital landscape presents unique vulnerabilities due to high social media penetration. In the study of Li (2021), it is noted that platforms like Facebook, with its massive user base, have become primary hunting grounds for malware invasion, phishing, and even sexual predation. To increase the efficacy of these attacks, criminals have transitioned to using advanced, automated tools. Pasia (2025) observes that integrating AI-based malware with machine learning models enables attackers to simulate genuine user activity and execute highly targeted phishing campaigns that are difficult for traditional security systems to detect.

Recent studies, most notably Jaspio (2025), emphasize that modern cyberattacks are no longer purely technical endeavors; they are sophisticated operations that dissect the anatomy of human trust. By exploiting both system vulnerabilities and psychological triggers, attackers create scenarios where victims essentially "open the door" themselves. This is particularly evident during times of global instability. Rufino (2025) highlights how crises ranging from the COVID-19 pandemic to climate-related emergencies serve as catalysts for fraud. Criminals leverage these high-stress periods to target the altruism of individuals and charities, using the emotional weight of these events to mask financial scams and phishing attempts.

Despite increasing digital literacy, significant behavioral gaps remain, especially among the youth. While Toso et al. (2023) suggest that older senior high school students possess a baseline awareness of

cyberbullying and basic scams, they still lack the advanced knowledge required to navigate complex issues like digital reputation, media literacy, and reporting protocols. This gap is evidenced by Abuda et al.'s (2020) findings, which showed that 59% of students in a survey still clicked on phishing links after opening the email, indicating a strong correlation between demographic factors and susceptibility. Furthermore, Rufino (2025) warns that unhealthy social media habits, such as oversharing personal data and engaging with unverified links, actively encourage reckless behavior that even the most informed student's defenses cannot withstand, leading to identity theft and persistent threats.

Identity Theft

The consistent rise in financially driven and data-centric offenses, particularly online scams and identity theft, underscores an urgent need for stronger digital security measures, enhanced public digital literacy, and more robust law enforcement strategies (Jaspio, 2025). This urgency is reflected in regional data, such as in 2019 when Region 1 (Ilocos) recorded the highest number of cybercrime victims due to SMS fraud, with over 113,000 cases; specifically, Pangasinan has been flagged as a hotspot for romance scams, fake job offers, and investment schemes (Rufino, 2025). Broadly defined, identity theft involves obtaining another person's personal or financial information to commit fraud, such as unauthorized transactions. Toso et al. (2023) emphasize that while social media is essential for modern communication, failing to safeguard personal information such as names, phone numbers, and addresses can lead to the creation of false identities and severe personal risk.

The scale of this issue in the Philippines is substantial, with the country recording over 19,000 cybercrime incidents in 2023 alone, an average of 53 cases daily, encompassing sextortion, online threats, and scams (Mahinay & Mamasalagat, 2025). Furthermore, the Philippines is recognized as one of the most susceptible countries in Southeast Asia, with an estimated 124 million accounts compromised since 2004, ranking it second in the region and increasing the prevalence of extortion (Pasia, 2025). These vulnerabilities are often exploited through targeted attacks using social engineering and customized malware to gain unauthorized access to sensitive data (Villamin, 2015). In response to these evolving threats, the Cybercrime Prevention Act of 2012 was enacted to address digital offenses, including child exploitation and cyber defamation (Suminig et al., 2025). This legal framework aims to criminalize a wide range of activities, from data interference to cyber libel, to punish offenders and deter potential criminals (Brucal et al., 2025).

Online Fraud

The OOC has conducted Basic Cybercrime Ethical Hacking Training for law enforcers as a countermeasure against hacking and network security threats to government and business firm sites. It was attended by the NBI-CCD operatives and PNP-ACG officers. Further, OOC committed to placing digital forensic equipment, surveillance equipment, and other equipment to enhance the capabilities of the Cybercrime Division of the NBI and Anti-Cybercrime Group of the PNP (Villamin, 2015). In order to criminalize and punish an extensive range of cybercrimes, going from unauthorized access and data interference through cyber libel, identity theft, and online fraud, to dissuade potential criminals (Brucal et.al, 2025).

Cyber Libel

The landscape of digital offenses in the Philippines has seen a notable shift, with cyber libel experiencing a significant uptick in 2024. According to Jaspio (2025), this trend underscores the persistent issue of defamation and abuse across social media platforms. These offenses typically involve the dissemination of false or defamatory statements that target a wide range of victims, including

journalists, public figures, and private citizens (Mahinay & Mamasalagat, 2025). Beyond defamation, technical offenses are also on the rise; illegal access reports surged from a single case in 2022 to 7 in 2024, signaling an escalating threat of unauthorized system intrusions (Jaspio, 2025).

At the center of the nation's policy response is the Cybercrime Prevention Act of 2012 (Republic Act No. 10175). This principal legislation was designed to combat a range of online crimes, including identity theft, child exploitation, and fraud, while establishing protocols for the collection of electronic evidence and for international cooperation (Rufino, 2025). The act has been instrumental in high-profile legal actions, such as the cyber libel conviction of Maria Ressa and the 2023 raid on a POGO facility in Las Piñas. However, the application of this law remains a subject of intense debate. Brucal et al. (2025) note that provisions on cyber libel are particularly contentious, as they raise concerns about potential abuse and a "chilling effect" on freedom of expression. This ongoing friction highlights the difficult balance the Philippine government must strike between modern cybersecurity requirements and the protection of fundamental civil liberties.

Cyber Bullying

Cyberbullying may take place on social media posting and messaging platforms that are aimed at spreading or posting embarrassing photos and videos, and sending hurtful, abusive, and threatening messages via messaging platforms (Thukral, 2022). This encompasses cyberbullying, online harassment, gender-based violence, grooming, and sexual exploitation, with especially harmful effects on vulnerable groups (Mahinay & Mamasalagat, 2025). Also, it is a symptom of increasingly polarised societies and should be situated in a broader political context. The Thai and Philippine governments manipulate cyberspace to consolidate power while exacerbating social divisions (Sombatpoonsiri, 2018). Additionally, females may be more likely to seek help or support when facing cyberbullying or online harassment situations (Zhu et al., 2021).

On the other hand, males might exhibit different patterns of behavior and risk perceptions regarding Cybercrime. They may be more prone to engaging in risky online activities or taking part in confrontations or cyberbullying incidents. It is essential to address these tendencies and provide education that emphasizes responsible online behavior, empathy, and respectful communication to ensure a safe and inclusive digital environment for all students (Cortesi et al., 2020).

Malware Attacks

A software firm has already released a report that stated more and more. Filipinos are falling victim to online criminal activities and other malicious attacks every year. Filipinos have fallen victim to a variety of attacks, which include, among others, malware invasion, online or phishing scams, and "sexual predation. For individual users, social networking services, particularly Facebook, which has at least 16 million users in the Philippines, are among the most vulnerable areas to these crimes (Li, 2021).

Enabling further cybercrimes such as man-in-the-middle attacks through traffic monitoring, phishing through password theft, identity fraud through data capture, and malware injection into network traffic (Silvestre & De Ocampo, 2023). Hackers may try to change, manipulate, or tamper with computer data and systems to accomplish their nefarious goals, including altering financial records, installing malware, or disrupting vital infrastructure. The PNP may face difficulties in confirming the legitimacy and dependability of digital evidence since cybercriminals can quickly generate, alter, or remove electronic documents (Fajardo et al., 2025).

Ransomware

Ransomware remains widespread and poses a serious threat to vital services and corporate infrastructure

worldwide. By using this malicious software, cybercriminals encrypt all of their victims' important data. Ransomware assaults are on the rise as more people access the internet. On the other hand, the S&R Membership Shopping also experienced a case of ransomware attack. On Nov. 14, 2021, S&R Membership Shopping experienced a ransomware attack on its membership system, affecting the personal data of 22,000 individuals, including date of birth, contact number, and gender (Blancaflor et al., 2023). 31% of these attacks target small businesses, which are attractive targets. Consumers remain vulnerable to ransomware and mobile threats, particularly on the Android platform (Villamin, 2015).

Cyber Espionage

Cyberespionage attacks or intellectual property theft are considered a major threat that increasingly affects the manufacturing sector and small businesses, with a 42% surge in 2012 compared to 2011. Research indicates that 31% of cyberattacks specifically target small businesses, which are viewed as highly attractive targets because they typically have fewer security resources. Furthermore, individual consumers face persistent risks from ransomware and mobile-based threats, with the Android platform being particularly susceptible to these vulnerabilities (Villamin, 2015).

Impacts of Cybercrime

This section presents the first major theme of the research, identifying five primary impacts of Cybercrime in the Philippines. Out of the 51 included studies, 30 were under this theme. The following synthesis provides the key findings from the included studies under each category.

Table 3. Distribution of Studies by Impacts of Cybercrime

Impacts of Cybercrime	Number of Studies
Economic	14
Psychological	2
Social	6
Legal	6

Economic

At a global level, Chen et al. (2023) discuss the worldwide landscape of Cybercrime, identifying prominent drivers such as economic disparities and technical accessibility as the primary impetus for growth. Nationally, Cybercrime is recognized as a grave threat to security and economic stability. Attacks on critical infrastructures and classified defense systems weaken fiscal stability, reduce the country's capacity to respond to foreign invasions, and compromise confidential data (Li, 2021). Furthermore, illegal data acquisition, hacking, and website defacement in the health, banking, and education sectors directly undermine the government's efforts to deliver public services (Li, 2021).

These attacks also target the private sector, specifically small and medium enterprises, which face significant economic losses due to their limited security infrastructure (Baker & Green, 2020). The consequences of financial Cybercrime go beyond immediate monetary theft; they diminish trust in online transactions, leading to lower uptake of digital services and slowing overall economic growth. Additionally, reputational harm to affected firms can lead to long-term customer losses and reduced investor confidence (Rufino et al., 2025).

The profile of the modern offender is shifting due to increased technical accessibility. As Grispos (2021) and Cohen et al. (2025) note, many offenders rely on ready-made malicious tools such as ransomware kits, phishing templates, and botnet rentals, which lower the barrier to entry for cyber offenses. This

democratization of cyber tools has expanded the population of potential offenders, making prevention and enforcement more complex (Ganguli, 2024). Sociodemographic factors such as age, education, and employment also influence these profiles; research indicates a prevalence of young males possessing moderate to advanced technical skills who are driven by limited economic opportunities (Songsrirote, 2025).

While the ICT sector in the Philippines is one of the fastest-growing in Southeast Asia, its large population of internet users makes it exceptionally susceptible to Cybercrime (Jing et al., 2019). Dubbed the "social media capital of the world," the Philippines sees millions of citizens spending hours daily on platforms like Facebook and TikTok. While these platforms have improved communication and economic activity in rural areas like Mountain Province, they have also become primary tools for cybercriminals (Fawas et al., 2025).

Economic pressure further compounds this risk, as households with few job options often turn to online work or small-scale digital trading, sometimes blurring the lines of digital safety (Fawas et al., 2025). This vulnerability is particularly acute among the youth. Due to youngsters' greater access to technology, Cybercrime is a worsening issue in the country (Szymkowiak et al., 2021). A lack of specific education regarding digital threats has led to numerous instances of children becoming involved in Cybercrime, either as victims or as perpetrators (Abuda et al., 2020).

Psychological

A psychological factor related to the development of violent behavior is having a low empathy level. Empathy can be defined using two dimensions: cognitive and affective. Cognitive empathy is the ability to communicate, tolerate, recognize, and perceive emotions, whereas affective empathy is the ability to perceive and share others' positive and negative emotions (Vezzali et al., 2017). A study showed that lower levels of empathy increased the development of violent or aggressive behaviors, while higher levels of empathy decreased the development of violent or aggressive behaviors. Since cyberbullying is considered to be a violent behavior, it is possible that empathy influences cyberbullying (Shechtman, 2017).

Social

The ASEAN region comprises 10 nations with diverse social and cultural heritages. These nations comprise a multitude of communities with rich traditions and value systems, influenced by the region's long history and diverse customs, religious beliefs, economic progress, innovation, and technological sophistication (ASEAN, 2021). Cyberbullying is a symptom of increasingly polarised societies and should be situated in a broader political context. The Thai and Philippine governments may manipulate cyberspace to consolidate power while exacerbating social divisions. Online bullies are instrumentalised by both the state and government supporters to silence dissent. The former reflects the autocratic backlash against civil society; the latter, a deeper crisis of social polarisation. The cases of Thailand and the Philippines reveal the interwoven relationship between these two aspects: autocratic and illiberal regimes can exploit existing social divides to consolidate power (Sombatpoonsiri, 2018).

The internet has many positive social effects and provides criminals with new, highly sophisticated technological tools. To prevent engaging in it or unintentionally creating illegal and punishable activities, they should be informed of the extent and restrictions of Cybercrime. As a result, policymakers, law enforcement, and international organizations face new challenges posed by emerging forms of Cybercrime (Toso et al., 2023). Furthermore, Cisco (2023) stated that Cybercrime is an illegal activity involving the internet, computers, and networks. Cybercriminals commit identity theft, phishing attacks,

spread malware, and instigate others and digital attacks, prejudicing others. Cybercrimes target any person, government, or property, leaving a significant financial and social impact on governments, businesses, and individuals, with the intent to damage them (Cisco, 2023). To sum up, digital technologies have enhanced individuals' lives by offering innovative solutions that improve productivity, communication, and accessibility across sectors. However, even as these digital technologies advance, challenges such as cybersecurity risks, privacy concerns, and social inequalities persist (Pasia, 2025).

Legal

According to Hagan (2021), a crime is an act that violates societal moral values and legal norms. Also, he highlights that criminality is socially constructed, meaning it is defined by society to determine wrongdoing. The same action may be considered a crime in one area but legal in another. The idea of deviance is frequently linked to crime. According to White & Haines (2021), deviance is behavior that disrupts social norms, while crime is nonconformity with codified law.

Current issues in the legal environment of Cybercrime are also being studied. Amoo et al. (2024) provide a thorough review of the challenges that arise in the criminal justice system, including emerging forms of Cybercrime and challenges in its prosecution. In the Philippines, Cybercrime has surged due to rising internet usage and the growing dependence on e-commerce and digital platforms. The Cybercrime Prevention Act of 2012 (Republic Act No. 10175) established clear parameters for prosecuting offenses such as illegal access and computer-related fraud, serving as a key legal pillar for law enforcement (Ajoy, 2022).

In the Philippines, the legal landscape, as outlined in instruments such as the Cybercrime Prevention Act and Republic Act 10175, establishes the framework for prosecuting cybercrimes. However, there is a dichotomy between legislative provisions and the practical challenges faced by law enforcement agencies, such as the PNP (Tarun, 2018). The national scenario mirrors global trends, where, despite the existence of preventive frameworks, there remains a prevailing vulnerability to cyber victimization, necessitating a re-evaluation of existing strategies and methodologies (Kikerpill, 2020).

Causes of Cybercrime

This section presents the first major theme of the research: three primary causes of Cybercrime in the Philippines were identified. Out of the 51 included studies, 9 were under this theme. The following synthesis provides the key findings from the included studies under each category.

Table 4. Distribution of Studies by Causes of Cybercrime

Causes of Cybercrime	Number of Studies
Technological	4
Psychological	2
Socioeconomic	3

Technological

In an article by Grzegorzek (2021), he explains that these technological advancements have been a breakthrough, opening many new opportunities by providing faster access to information and enabling faster analysis and data transfer. However, this advancement in technology and the opportunities it may bring to society still pose some threat to its users. Technological advancements bring convenience and faster transactions. However, according to The Asia Foundation (2022), people with extensive

knowledge of technology may be using it to take advantage of those engaged in it, for traffic analysis and information gathering.

The Philippines, due to its reliance on technology, is considered extremely vulnerable to cyberattacks and incidents (International Trade Administration, 2020). According to the Manila Times, there has been an increase in cyberattacks in the Philippines, specifically ransomware attacks, which accounted for 62% of incidents worldwide in 2020 (Manila Times, 2021).

Psychological

Research suggests that a lack of empathy is a significant psychological predictor of violent tendencies. According to Vezzali et al. (2017), empathy comprises two parts: cognitive, which involves identifying and understanding others' emotions, and affective, which involves actually feeling or sharing those emotions. Shechtman's (2017) study demonstrated an inverse relationship between empathy and aggression, in which greater empathetic capacity was associated with reduced violence. Given that cyberbullying is a form of digital aggression, an individual's level of empathy likely plays a role in their likelihood of engaging in such behavior.

Socioeconomic

The proliferation of Cybercrime hampers the reach of e-government and compromises the achievement of its national goals of creating an enhanced socioeconomic environment for its citizens. In essence, it is tantamount to becoming a grave threat to national security (Li, 2021). This democratization of cyber tools has expanded the population of potential offenders, making prevention and enforcement more complex (Ganguli, 2024). Sociodemographic factors such as age, education, and employment also influence offender profiles, with research indicating a prevalence of young males possessing moderate to advanced technical skills and limited socioeconomic opportunities (Songsrirote, 2025).

Effectiveness of Cybercrime Law in the Philippines

This section presents the first major theme of the research: the identification of nine primary types of Cybercrime in the Philippines. Out of the 51 included studies, 25 were under this theme. The following synthesis provides the key findings from the included studies under each category.

Table 5. Distribution of Studies by Effectiveness of Cybercrime Law in the Philippines

Effectiveness of Cybercrime Law	Number of Studies
Prevention	6
Awareness	13
Report/Cases	6

Prevention

According to Monroe Community College (2024), crime prevention is anticipating crime risk and taking action to reduce it. Crime prevention is a shared societal responsibility that requires community cooperation. Ortega Anderez et al. (2021) investigated how technology has taken center stage in crime prevention and discussed opportunities, challenges, and practitioner prospects for using technology to fight crime.

The Cybercrime Prevention Act of 2012 was enacted due to a growing number of digital offenses, including identity theft, online scams, child exploitation, and cyber defamation (Suminig et al., 2025). The law provides procedural measures to be undertaken by law enforcement authorities mandated to enforce and implement its provisions. To ensure that the technical nature of Cybercrime and its

prevention given focus and the procedures involved for international cooperation considered, law enforcement authorities specifically the computer or technology crime divisions responsible for the investigation of cybercrimes are required to submit timely and regular reports including pre-operation, post-operation and investigation results and such other documents as may be required to the Department of Justice (DOJ) forreview and monitoring (Villamin, 2015).

According to Pasia (2025), preventing Cybercrime will require addressing gaps, strengthening laws, implementing technological enhancements, and fostering societal awareness. By aligning international legal regimes, providing tools for more effective investigations, and improving digital literacy, stakeholders can act together on these fronts to mount a resilient defense against cyber threats. However, as pointed out by Vitus (2023), to create a safe digital environment, the stakeholders, that is, the government, law enforcement, the private sector, and the public at large, will need to engage in continued collaboration.

Public Awareness

In the study by Nagalingam et al. (2015), they revealed a low level of awareness of phishing attempts, with prime factors including overlooking, lack of awareness of online banking, and personal negligence. At the same time, Diaz et al. (2020) showed that, in a survey study, around 59% of students who opened the phishing email clicked the phishing link, and that several demographic factors were significantly associated with a student's susceptibility to phishing.

Available research on cybercrime awareness broadly covers other locations, such as Barangay 38 in Bacolod City and various senior high school students in other regions. However, there are no explicit, detailed studies focused on Pagadian City itself (Mahinay & Mamasalagat, 2025). In addition, the predominance of respondents with college-level education in cybercrime awareness studies aligns with findings that higher educational attainment is often associated with greater digital literacy and awareness of online risks (Nguyen, 2020).

Workplace and academic settings offer critical opportunities to implement cybercrime awareness programs, given the high exposure to and reliance on digital technologies in these environments (Jones et al., 2020). However, the presence of self-employed and unemployed respondents, though smaller in number, highlights the need for tailored cybersecurity education that addresses their unique challenges, such as less structured access to organizational resources and training (Kumar & Carley, 2021).

The mixed public perception of the Cybercrime Prevention Act of 2012 is reflected in various studies and observations that highlight both support and criticism of the law's effectiveness. While a majority of respondents express confidence in the law's capacity to address Cybercrime, substantial skepticism persists due to concerns about its enforcement, potential overreach, and its impact on fundamental rights such as freedom of expression (Robie & Abcede, 2015). This division underscores the complexity of balancing robust cybercrime prevention with protecting civil liberties, suggesting that the law’s practical outcomes vary across different segments of the population and may not yet fully meet public expectations or awareness levels (Li, 2021). Public education is a fundamental component of cybercrime prevention. RA 10175 promotes collaborative efforts among government agencies, educational institutions, and civil society organizations to raise cybersecurity awareness. Digital citizenship campaigns encourage safe online behavior and empower users to recognize and report threats (UNESCO, 2021).

In the study by Hawdon (2021), he explained that manipulative triggers, such as assignments or financial penalties, are not obfuscation but penalties. Such tactics are particularly effective against individuals

with lower cybersecurity awareness, underscoring the need for education and training to help them identify manipulative techniques. Shehu et al. (2024) in Kebbi State outline local bottlenecks affecting these efforts in crime prevention: limited law enforcement resources and low public awareness of cyber threats.

PNP-RACU 5 officers reported difficulties in prosecuting cases due to jurisdictional conflicts and procedural inefficiencies. At the same time, academic and victim groups noted a general lack of public awareness of cybercrime laws (Calupit, 2025). These observations align with studies by Rakhmanova & Pinkevich (2020), who argue that legal ambiguities create significant enforcement challenges and delay judicial processes in cross-border cases.

Report/ Cases

The Philippines has experienced a pronounced escalation in cybercrime incidents, as official data from the Philippine National Police (PNP) highlights a steep upward trend in criminal activity conducted through digital platforms. In 2023, the nation documented 19,472 cybercrime incidents an alarming 68.98% increase from 11,523 cases reported in 2022. This surge results in roughly 53 cybercrime cases per day nationwide, underscoring the increasingly persistent threat to both individuals and organizations (Tsakalidis & Vergidis, 2019). The Philippines is also among the most susceptible countries in Southeast Asia to cyber threats. From 2004, it was estimated that some 124 million accounts in the country had been infiltrated, ranking second in the region. High numbers of compromised accounts pose significant risks, such as identity theft and extortion. (Pasia, 2025).

In the Philippines, the Anti-Cybercrime Group recorded 4,469 cybercrime cases in the first quarter of 2024, up from 3,668 in 2023. According to ACG director Maj. Gen. Sidney Hernia. The top three crimes that contributed to the spike were online selling scams (990 cases), debit and credit card fraud (309), and investment scams (319). Possible causes of the rise in Cybercrime include increased online activity, sophisticated cybercrime tactics, and the public's lack of awareness. The growing reliance on online platforms for shopping, financial transactions, and investment opportunities has created a larger pool of potential targets for cybercriminals, Hernia noted (Tupas, 2024). Also, Pasia (2025) mentioned that according to the Cybercrime Investigation and Coordination Center (CICC), the latest data released during the Joint Anti-Bank Robbery and Cybercrime Coordinating Committee Second Quarter Meeting for 2023, held in Taguig City, showed that 6,250 cybercrime cases were recorded from January to June 2023. The CICC also noted that online scams almost tripled to 4,446, from 1,551 reported in the first half of 2022. With that, the Republic Act No. 10175, also known as the Cybercrime Prevention Act of 2012, took action against those apprehended.

According to Pasia (2025), 71% reported being targeted by digital fraud attempts across these communication channels, and 11% of all respondents fell victim during this period. Phishing (fraudulent emailsemails, social posts, websites, and QR codes) and smishing (fraudulent mobile text messages), both at 46%, were the most commonly reported fraud schemes experienced by Filipinos, followed by third-party seller scams at 33% and identity theft at 25%. Online scams have become the most significant and fastest-growing category of Cybercrime in the Philippines, accounting for the majority of reported incidents in recent years. The number of documented online scam cases nearly doubled in just twelve months, escalating from 7,208 cases in 2022 to 14,030 in 2023, a remarkable 94.64% increase (Palad et al., 2019).

4. Implications and Concluding Remark

This section provides the key implications and concluding remarks for the study. It highlights how the results can support stronger awareness and enforcement of cybercrime laws. These aims are to guide future research directions and practical solutions to improve cybercrime governance.

Implications for Practice

This study strongly advocates for urgent, actionable measures to address Cybercrime in the Philippines, from government officials and police to teachers and local business owners. With digital crimes like identity theft, phishing, and cyberbullying becoming part of our daily reality, it is clear that our current defenses need a major upgrade. To truly protect the public, agencies like the PNP and NBI cannot rely on old methods; they need better forensic technology, ongoing specialized training, and a much more unified approach to working together.

The staggering rise in phishing and identity theft makes it clear that we cannot just rely on laws to keep us safe; we need to start teaching people how to protect themselves. It means bringing cybersecurity education directly into our communities, schools, and offices becomes second nature for everyone. Since many people fall victim to scams simply because they are unaware of the red flags, our strategy needs to shift from just catching criminals to preventing crime in the first place. By focusing on proactive education, early intervention, and making it easier for the public to report suspicious activity, we can better protect students and other vulnerable groups who are often the primary targets of these digital attacks.

From a policy perspective, while the Cybercrime Prevention Act of 2012 provides a foundational legal framework, practical enforcement challenges, jurisdictional issues, and public skepticism suggest the need for periodic policy review and refinement. Policymakers must ensure clearer legal definitions, improved prosecution mechanisms, and safeguards that balance cyber regulation with the protection of civil liberties.

Implications for Future Research

Future researchers should conduct more localized and region-specific studies to generate precise data on cybercrime patterns, victimization trends, and reporting behaviors across different provinces and cities in the country. There is also a need to adopt more quantitative, mixed-method, and longitudinal research designs to provide empirical measurement of cybercrime prevalence, offender characteristics, and evolving digital crime trends.

Moreover, future research should critically evaluate the effectiveness of Republic Act No. 10175, the Cybercrime Prevention Act of 2012, by examining conviction rates, challenges to prosecution, evidentiary issues, and deterrence outcomes. Given the identified psychological and socioeconomic factors, future researchers will propose a deeper investigation into offender motivations, empathy levels, peer influence, unemployment, and digital exposure. Researchers should likewise explore emerging threats such as AI-driven phishing, ransomware-as-a-service, cryptocurrency-related crimes, and transnational cyber operations to anticipate future risks. Finally, intervention-based and interdisciplinary research is encouraged, particularly studies that test the effectiveness of cybersecurity awareness programs, digital literacy initiatives, and collaborative frameworks involving criminology, information technology, law, psychology, and public administration to strengthen evidence-based cybercrime prevention strategies in the Philippines.

Concluding Remarks

This study makes a significant contribution to the understanding of Cybercrime in the Philippines by sy-

stematically synthesizing existing research across legal, enforcement, awareness, and governance perspectives. Its primary impact lies in transforming fragmented findings into a coherent criminological framework that clarifies the nature, scope, and implications of Cybercrime within the Philippine context. The findings of this literature review reveal that Cybercrime in the Philippines is a complex, economically motivated, socially influenced, and technologically adaptive phenomenon that challenges traditional enforcement mechanisms. Strengthened capable guardianship, institutional capacity-building, legal refinement, and preventive education are essential to mitigating its impact. It strengthens the academic foundation of cybercrime studies in Criminal Justice Education and underscores the need to integrate digital crime prevention strategies into both law enforcement practice and educational curricula.

REFERENCES

1. Abuda, B., Rivera, K., & Norona, R. (2020). Predictive validity of a cybercrime awareness tool: The case of senior high school students in a Philippine secondary school. International Journal of IT-Based Governance and Business (IJITGEB), 2(1). https://doi.org/10.32664/ijitgeb.v2i1.63
2. Ajoy, B. (2022). Effectiveness of criminal law in tackling cybercrime: A critical analysis. Scholars International Journal of Law, Crime and Justice, 5(2), 74–80. https://doi.org/10.36348/sijlcj.2022.v05i02.005
3. Amoo, N. O. O., Atadoga, N. A., Abrahams, N. T. O., Farayola, N. O. A., Osasona, N. F., & Ayinla, N. B. S. (2024). The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system. World Journal of Advanced Research and Reviews, 21(2), 20–31. https://doi.org/10.30574/wjarr.2024.21.2.0456
4. ASEAN. (2021, May 2). Diverse ASEAN. Invest in ASEAN. http://investasean.asean.org/index.php/page/view/about-the-asean-region/view/707/newsid/930/diverse-asean.html
5. The Asia Foundation. (2022). Cybersecurity in the Philippines: Global context and local challenges. https://asiafoundation.org/publication/cybersecurity-in-the-philippines-global-context-and-local-challenges/
6. Baker, L. M., & Green, K. P. (2020). The economic impact of cybercrime on businesses: A case study approach. Journal of Business Security, 19(2),101–115. https://doi.org/10.1016/j.jbs.2020.05.004
7. Blancaflor, E., Daluz, J., Garcia, A., Monton, N., & Vergara, J. (2023). A literature review on the pervasiveness of ransomware threats and attacks in the Philippines. Semantic Scholar. https://pdfs.semanticscholar.org/e29a/63f5f4f27c684837ec6c63941961a948371b.pdf
8. Brayne, S., & Martin, K. (2021). Policing cybercrime: A collaborative approach. In M. Deflem (Ed.), The handbook of cybercrime (pp. 99–117). Wiley-Blackwell. https://doi.org/10.1093/socpro/spaa004
9. Brucal, A., Abante, M., & Vigonte, F. (2025). Cybercrime Prevention Act of 2012 in practice: Cybersecurity, controversy, and the future of digital rights in the Philippines. SSRN. https://doi.org/10.2139/ssrn.5275786
10. Calupit, P. (2025). Exploring the PNP Regional Anti-Cybercrime Unit 5 capability on cybercrime challenges: An empirical analysis. International Journal for Multidisciplinary Research, 7(1). https://www.ijfmr.com/papers/2025/3/43827.pdf

11. Chakraborty, E., Mombeshora, M., Clark, K. P., & Mbavarira, T. S. (2024). Understanding of cyber-attack vulnerabilities during natural disasters and discussing a cyber-attack resiliency framework. Southeast Con 2024, Atlanta, GA, USA. https://doi.org/10.1109/SoutheastCon52093.2024.10500233
12. Chauhan, M., & Shiaeles, S. (2023). An analysis of cloud security frameworks, problems and proposed solutions. Network, 3(3), 422–450. https://doi.org/10.3390/network3030018
13. Chen, S., Hao, M., Ding, F., Jiang, D., Dong, J., Zhang, S., Guo, Q., & Gao, C. (2023). Exploring the global geography of cybercrime and its driving forces. Humanities and Social Sciences Communications, 10(1). https://doi.org/10.1057/s41599-023-01560-x
14. Cohen, D., Te'eni, D., Yahav, I., Zagalsky, A., Schwartz, D., Silverman, G., ... & Makowski, J. (2025). Human–AI enhancement of cyber threat intelligence. International Journal of Information Security, 24(2), 99. https://doi.org/10.1007/s10207-024-00812-w
15. Cortesi, S., Hasse, A., Lombana-Bermudez, A., Kim, S., & Gasser, U. (2020). Youth and digital citizenship+ (plus): Understanding skills for a digital world (Berkman Klein Center Research Publication No. 2020-2). Berkman Klein Center for Internet & Society. https://doi.org/10.2139/ssrn.3547544
16. Council of Europe. (2024). Cybercrime policies/strategies-The Philippines. https://www.coe.int/en/web/octopus/country-wikiap/-/asset_publisher/CmDb7M4RGb4Z/content/philippines
17. Craig, B. M., Hays, R. D., Pickard, A. S., Cella, D., Revicki, D. A., & Reeve, B. B. (2017). Comparison of US panel vendors to online surveys. Journal of Medical Internet Research, 15(11), e260. https://doi.org/10.2196/jmir.2903
18. Custodio, K. (2025). Exploring the challenges faced by the Cavite Provincial Police Office in cybercrime investigation. Social Science and Humanities Journal, 9(6). https://doi.org/10.18535/sshj.v9i06.1889
19. Department of Justice. (2012). Cybercrime Prevention Act of 2012 (Republic Act No. 10175). LawPhil. https://lawphil.net/statutes/repacts/ra2012/ra_10175_2012.html
20. Diaz, A., Sherman, A. T., & Joshi, A. (2020). Phishing in an academic community: A study of user susceptibility and behavior. Cryptologia, 44(1),53–67. https://doi.org/10.1080/01611194.2019.1623349
21. Dunn, K., & Zukowski, L. (2021). The dark web and digital forensics: Challenges and solutions. Journal of Digital Forensics, Security and Law, 16(1), 15–28. https://doi.org/10.15394/jdfsl.2021.1691
22. Dunsin, D., Ghanem, M. C., Ouazzane, K., & Vassilev, V. (2024). Un análisis exhaustivo del papel de la inteligencia artificial y el aprendizaje automático en el análisis forense digital moderno y la respuesta ante incidentes [A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response]. Forensic Science International: Digital Investigation, 48, Article 301675. https://doi.org/10.1016/j.fsidi.2023.301675
23. Fajardo, M. et al., (2025). Challenges faced by PNP in resolving cybercrime cases. International Journal of Multidisciplinary: Applied Business and Education Research, 6(3), 1312–1333. https://doi.org/10.11594/ijmaber.06.03.23
24. Fawas, I., Fanasan, F., & Fanusan, F. (2025). The role of social media in the proliferation of cybercrime in Mountain Province. ORCID. https://orcid.org/0009-0002-4440-5942

25. Ganguli, P. (2024). The rise of cybercrime-as-a-service: Implications and countermeasures. SSRN. https://doi.org/10.2139/ssrn.4959188
26. Grispos, G. (2021). Criminals: Cybercriminals. In Encyclopedia of security and emergency management (pp. 84–89). Springer. https://doi.org/10.1007/978-3-030-06163-0_163
27. Guo, S., & Wang, Y. (2024). A literature review: Risk factors of being a cyber-criminal. Journal in Computer Virology, 2(1), 13–20. https://doi.org/10.1007/s11416-006-0015-z
28. Hagan, F. E. (2021). Introduction to criminology: Theories, methods, and criminal behavior (12th ed.).https://books.google.com/books/about/Introduction_to_Criminology.html?id=eKy-EAAAQBAJ
29. Hawdon, J. (2021). Cybercrime: Victimization, perpetration, and techniques. American Journal of Criminal Justice. https://doi.org/10.1007/s12103-021-09653-z
30. International Trade Administration. (2020). Philippine cybersecurity. https://www.trade.gov/market-intelligence/philippine-cybersecurity
31. Jaspio, V. (2025). Cybercrime trends, motivations, and challenges in Puerto Princesa City, Philippines. ETCOR Educational Research Center. https://doi.org/10.63498/etcor447
32. Jerome, B. (2020). Criminal investigation and criminal intelligence: Example of adaptation in the prevention and repression of cybercrime. Risks, 8(3), 99. https://doi.org/10.3390/risks8030099
33. Jerome, S., & Samoy, L. (2017). Industrial security management reviewer. https://kupdf.net/download/industrial-security-management-reviewer_598b0205dc0d60215a300d18_pdf
34. Jing, A. H. Y., Ab-Rahim, R., & Ismail, F. (2019). Information and communication technology (ICT) and income inequality in ASEAN-5 countries. International Journal of Academic Research in Business and Social Sciences, 9(9), 359–373. https://doi.org/10.6007/IJARBSS/v9-i9/6314
35. Jones, L., Smith, R., & Patel, K. (2020). Cybersecurity awareness in the workplace: Best practices and challenges. Journal of Information Security, 11(3), 145–158. https://doi.org/10.4236/jis.2020.113009
36. Junger, M., Montoya, L., Hartel, P., & Heydari, M. (2017). Towards the normalization of cybercrime victimization: A routine activities analysis of cybercrime in Europe. 2017 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA). https://doi.org/10.1109/CyberSA.2017.8073391
37. Khalifa, A. M. M. (2020). Overcoming the conflict of jurisdiction in cybercrime [Doctoral dissertation].
38. Khan, S., Saleh, T., & Dorasamy, M. (2022). A systematic literature review on cybercrime legislation. F1000Research, 11, 971. https://doi.org/10.12688/f1000research.123098.1
39. Kikerpill, K. (2020). The individual's role in cybercrime prevention: Internal spheres of protection and our ability to safeguard them. Kybernetes, 50(4),1015–1026.https://doi.org/10.1108/K-06-2020-0335
40. Kumar, S., & Carley, K. M. (2021). Cybersecurity behaviors among self-employed and unemployed populations: A comparative study. Cyberpsychology, Behavior, and Social Networking, 24(7), 448–455. https://doi.org/10.1089/cyber.2020.0288
41. Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. Deviant Behavior, 37(3),263–280. https://doi.org/10.1080/01639625.2015.1012409

42. Li, J. (2021). Cybercrime in the Philippines: A case study of national security. ProQuest. https://www.proquest.com/docview/2639753710
43. Loggen, J., Moneva, A., & Leukfeldt, R. (2024). A systematic narrative review of the pathways, desistance, and risk factors of financial and economic cybercrime. Computer Law & Security Review, 52, Article 105858. https://doi.org/10.1016/j.clsr.2023.105858
44. Mahinay, C., & Mamasalagat, M. (2025). Assessing cybercrime awareness and experiences among netizens: A study on the impact of R.A. 10175 in Pagadian City. International Journal of Research and Innovation in Social Science, 9(5). https://doi.org/10.47772/IJRISS.2025.905000216
45. The Manila Times. (2021, June 7). Cyberattacks threaten PH, other economies.https://www.manilatimes.net/2021/06/07/opinion/editorial/cyberattacks-threaten-ph-other-economies/1802184
46. Monroe Community College. (2024). What is crime prevention? https://www.monroecc.edu/depts/pstd/crime-prevention-information/
47. Mphatheni, M. R., & Maluleke, W. (2022). Cybersecurity as a response to combating cybercrime: Demystifying the prevailing threats and offering recommendations to the African regions. International Journal of Research in Business and Social Science, 11(4), 384–396. https://doi.org/10.20525/ijrbs.v11i4.1714
48. Nagalingam, V., Narayana, S., Ganthan, A., Rabiah, M., Nurazean, I., & Roslina, R. (2015). Identifying the level of user awareness and factors on phishing attempt among students. Advanced Science Letters, 21(10), 3243–3247. https://doi.org/10.1166/asl.2015.6520
49. Nguyen, M. H. (2020). The role of education in digital literacy and cybersecurity awareness. Journal of Cybersecurity Education, Research and Practice, 2020(1), Article 5. https://digitalcommons.kennesaw.edu/jcerp/vol2020/iss1/5
50. Nodeland, B., & Morris, R. (2020). A test of social learning theory and self-control on cyber offending. Deviant Behavior, 41(1), 41–56. https://doi.org/10.1080/01639625.2018.1519135
51. Olukunle, O. A., Akoh, A., et al. (2024). The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system. World Journal of Advanced Research and Reviews, 21(2), 438–448. https://doi.org/10.30574/wjarr.2024.21.2.0438
52. Ortega Anderez, D., Kanjo, E., Anwar, A., Johnson, S., & Lucy, D. (2021). The rise of technology in crime prevention: Opportunities, challenges and practitioners' perspectives. ResearchGate. https://www.researchgate.net/publication/349125315
53. Page, M. J., et al., (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. The BMJ, 372, Article n71. https://doi.org/10.1136/bmj.n71
54. Palad, E., Tangkeko, M., Magpantay, L., & Sipin, G. (2019). Document classification of Filipino online scam incident text using data mining techniques. 2019 19th International Symposium on Communications and Information Technologies (ISCIT), 362–367. https://doi.org/10.1109/ISCIT.2019.8905221
55. Parti, K., & Dearden, T. (2024). Cybercrime and strain theory: An examination of online crime and gender. Journal of Law and Criminal Justice, 13(1), 19–35. https://doi.org/10.6000/1929-4409.2024.13.19
56. Pasia, D. (2025). Cybercrime prevention initiative among the PNP affecting public trust and collaboration of the community. International Journal of Social and Applied Technology, 16(4).https://doi.org/10.71097/IJSAT.v16.i4.8517

57. Patsakis, C., Politou, E., Alepis, E., & Hernández-Castro, J. (2024). Cobrar criptomonedas: Estado de la práctica en el pago de rescates [Cashing out cryptocurrencies: State of the practice in ransom payments]. Revista Internacional de Seguridad de la Información, 23(2), 699–712. https://doi.org/10.1007/s10207-023-00766-z
58. Payne, B. K. (2020). Defining cybercrime. In The Palgrave handbook of international cybercrime and cyberdeviance (pp. 3–25). Palgrave Macmillan. https://doi.org/10.1007/978-3-030-22527-8_1
59. Pecson, R., Karsono, B., Sulastri, L., Rony, Z. T., & Chavez, C. B. (2025). Defending the digital domain: A critical look at cybercrime legislation in Indonesia and the Philippines. Academic Journal of Interdisciplinary Studies. https://doi.org/10.36941/ajis-2025-0040
60. Pulijala, Y., et al. (2021). Internet of Things forensics: A comprehensive survey. Journal of Network and Computer Applications, 18, Article 103037. https://doi.org/10.1109/COMST.2019.2962586
61. Rakhmanova, E., & Pinkevich, T. V. (2020). Digital crime concept. Modern Management Trends and the Digital Economy: From Regional Development to Global Economic Growth (MTDE 2020), 172–176. https://doi.org/10.2991/aebmr.k.200502.031
62. Refaei, M. D. M. (2023). Regulatory frameworks for autonomous robotics in NEOM's sustainable technology landscape. Migration Letters, 20(9), 228–258. https://doi.org/10.59670/ml.v20i9.5965
63. Respicio & Co. (2024). Unauthorized access to social media accounts for fraudulent purposes. https://www.respicio.ph/commentaries/cybercrime-in-the-philippines-unauthorized-access-to-social-media-accounts-for-fraudulent-purposes
64. Reyes, A. (2024). Rethinking the Cybercrime Prevention Act of 2012: Strengthening Philippine sovereignty in the digital age. Academia.edu. https://www.academia.edu/118169601
65. Robie, D., & Abcede, D. M. (2015). Cybercrime, criminal libel and the media: From 'e-martial law' to the Magna Carta in the Philippines. Pacific Journalism Review, 21(1), 211–229. https://doi.org/10.24135/pjr.v21i1.158
66. Rufino, C., Viray, M., Sindayen, R., Macaraeg, C., & Diaz, M. (2025). Five year empirical analysis of cybercrime victimization trends in Pangasinan, Philippines. International Journal of Research and Innovation in Social Science, 9(9). https://doi.org/10.47772/IJRISS.2025.909000355
67. Shechtman, Z. (2017). Group intervention with aggressive children and youth through bibliotherapy. International Journal of Group Psychotherapy, 67(1), 47–67. https://doi.org/10.1080/00207284.2016.1202682
68. Shehu, A., Kamba, M., & Faruk, A. (2024). Understanding the landscape of cybercrime in Kebbi State: Challenges and mitigation strategies. ResearchGate. https://www.researchgate.net/publication/384595100_Understanding_the_Landscape_of_Cybercrime_in_Kebbi_State_Challenges_and_Mitigation_Strategies/citations
69. Silvestre, A., & De Ocampo, J. (2023). Packet sniffing in the cyber threat landscape: Examining Wireshark capabilities, misuse, and policy options in the Philippines. International Journal of Research and Innovation in Social Science, 7(8). https://doi.org/10.47772/IJRISS.2023.7856
70. Sombatpoonsiri, J. (2018). Manipulating civic space: Cyber trolling in Thailand and the Philippines. German Institute of Global and Area Studies (GIGA). https://www.giga-hamburg.de/en/publications/giga-focus/manipulating-civic-space-cyber-trolling-in-thailand-and-the-philippines

71. Songsrirote, N. (2025). Socioeconomic determinants of cybercrime costs: A panel data analysis of OECD countries. Asian Journal of Applied Economics, 32(1), 30–57. https://ideas.repec.org/a/ris/apecjn/0109.html
72. Sosa, J. (2024). Country report on cybercrime: The Philippines. UNAFEI Resource Material Series No. 79. https://unafei.or.jp/publications/pdf/RS_No79/No79_12PA_Sosa.pdf
73. Suminig, A., Jr., Abante, M., & Vigonte, F. (2025). Safeguarding cyberspace: A comprehensive analysis of the Cybercrime Prevention Act of 2012 (RA 10175) and its role in Philippine digital governance. SSRN. https://doi.org/10.2139/ssrn.5270089wwwwwwwww
74. Szymkowiak, A., Melović, B., Dabić, M., Jeganathan, K., & Kundi, G. S. (2021). Information technology and Gen Z: The role of teachers, the internet, and technology in the education of young people.Technology in Society, 65, Article 101565. https://doi.org/10.1016/j.techsoc.2021.101565
75. Tarun, I. M. (2018). Legal consequences of social networking malpractices: Users' perspectives versus the reality of Cybercrime Prevention Act of the Philippines. Advanced Science Letters, 24(11), 8111–8114. https://doi.org/10.1166/asl.2018.12503
76. Thukral, P., & Kainya, V. (2022). How social media influence crimes. Indian Journal of Law and Legal Research, 4(2), 1–11. https://www.researchgate.net/publication/360540601_How_Social_Media_Influence_Crimes#fullTextFileContent
77. Toso, C. (2023). Cybercrime awareness among senior high school students. Mediterranean Journal of Basic and Applied Sciences, 7(2). https://doi.org/10.46382/MJBAS.2023.7218
78. Tsakalidis, G., & Vergidis, K. (2019). A systematic approach toward description and classification of cybercrime incidents. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49(3), 512–529. https://doi.org/10.1109/TSMC.2017.2700483
79. The United Nations Educational, Scientific and Cultural Organization. (2021). Digital citizenship education. https://www.unesco.org
80. University of the Philippines Centre International de Formation des Autorités etLeaders(2021). Professional course on digital governance and cybersecurity launched by UP-CIFAL Philippines. https://upepp.upd.edu.ph/academics/professional-course/
81. Vaddi, K. S., Kamble, D., Vaingankar, R., Khatri, T., & Bhalerao, P. (2024). Advancements in the world of digital forensic analysis. IAES International Journal of Artificial Intelligence, 13(1), 680–686. https://doi.org/10.11591/ijai.v13.i1.pp680-686
82. Varol, C., Rasheed, R., Karabiyik, U., Shashidhar, N., & Zhang, R. (2024). Cybercrime intention recognition: A systematic literature review. Information, 15(5), Article 263. https://doi.org/10.3390/info15050263
83. Vezzali, L., Hewstone, M., Capozza, D., Trifiletti, E., & Bernardo, G. A. D. (2017). Improving intergroup relations with extended contact among young children: Mediation by intergroup empathy and moderation by direct intergroup contact. Journal of Community & Applied Social Psychology, 27(1), 35–49. https://doi.org/10.1002/casp.2292
84. Villamin, D. (2015). Philippines 2014-2015 cybercrime report: The rule of law in cyberspace. Department of Justice. https://www.academia.edu/25773260
85. Viraja, V. K., & Purandare, P. (2021). A qualitative research on the impact and challenges of cybercrimes. Journal of Physics: Conference Series, 1964, Article 042004.

https://doi.org/10.1088/1742-6596/1964/4/042004

86. Vitus, E. N. (2023). Cybercrime and online safety: Addressing the challenges and solutions related to cybercrime, online fraud, and ensuring a safe digital environment for all users — A case of African states. TIJER - International Research Journal, 10(9). https://philarchive.org/archive/VITCAO
87. White, R., & Haines, F. (2021). Crime and criminology (9th ed.). Oxford University Press.https://books.google.com.ph/books?id=5rMa0AEACAAJ
88. Zhou, Y., Liu, W., Lee, C., Xu, B., & Sun, I. (2024). Traditional social learning predicts cyber deviance? Exploring the offending versatility thesis in social learning theory. Behavioral Sciences & the Law, 42(4), 417–434. https://doi.org/10.1002/bsl.2652
89. Zhu, C., Huang, S., Evans, R., & Zhang, W. (2021). Cyberbullying among adolescents and children: A comprehensive review of the global situation, risk factors, and preventive measures. Frontiers in Public Health, 9, Article 634909.https://doi.org/10.3389/fpubh.2021.634909