ETCOR Educational Research Center Inc.
SEC Reg. No. 2024020137294-00
Sta. Ana, Pampanga, Philippines
INTERNATIONAL MULTIDISCIPLINARY RESEARCH CONFERENCE
Website: https://etcor.org
iJOINED ETCOR
P - ISSN 2984-7567
E - ISSN 2945-3577
The Exigency
P - ISSN 2984-7842
E - ISSN 1908-3181

Cybercrime Trends, Motivations, and Challenges in Puerto Princesa City, Philippines

SFO1 Vilfred T. Jaspio, LPT [1, 2]
[1] Chief Administrative Section, Bureau of Fire Protection Dumaran Fire Station, Palawan, Philippines
[2] MSCJ Candidate, Philippine College of Criminology, Manila, Philippines
Corresponding Author e-mail: *vilfredjaspio@gmail.com*

Received: 05 August 2025 **Revised**: 07 September 2025 **Accepted**: 09 September 2025

Available Online: 10 September 2025

Volume IV (2025), Issue 3, P-ISSN – 2984-7567; E-ISSN - 2945-3577

https://doi.org/10.63498/etcor447

Abstract
Aim: This study examined the cybercrime trends, motivations, and challenges in Puerto Princesa City.
Methodology: Using a mixed-methods explanatory sequential design, quantitative surveys were conducted with 90 respondents, followed by qualitative interviews with three cybercrime offenders and three law enforcement officers.
Results: Findings revealed that technology, while beneficial for communication and productivity, also enables cybercrime through anonymity, rapid information flow, and weak enforcement. Offender motives centered on personal, financial, and behavioral factors, while law enforcers identified technical and resource constraints. Although limited to a small sample, the study provides key insights into the interaction between technology, human behavior, and institutional capacity.
Conclusion: The study concludes that strengthening public awareness, improving inter-agency coordination, and enhancing local enforcement capacity are critical to addressing cybercrime in Puerto Princesa City. These findings serve as a basis for future research and localized policy development.
Keywords: *Cybercrime trends, motivations, law enforcement, cybercrime challenges, Puerto Princesa City*

INTRODUCTION

Cybercrime is broadly defined as criminal activity that involves the use of computers, digital devices, or networks—either as the tool to commit the offense, the target of the crime, or both (Payne, 2020). As societies grow increasingly dependent on digital systems, cybercrime has emerged as one of the most pressing global security concerns. What distinguishes cybercrime from conventional crime is its ability to occur without physical contact, transcend geographical boundaries, and often remain undetected by victims until significant damage has been done (Caneppele & Da Silva, 2022). These characteristics make cybercrime uniquely complex to define, investigate, and prosecute.

Scholars and legal experts have developed various classifications to better understand the nature of cybercrime. One widely accepted framework divides cybercrime into two main categories: cyber-dependent and cyber-enabled crimes (Leppänen, 2024). Cyber-dependent crimes are offenses that exist only in digital spaces, such as hacking, malware deployment, distributed denial-of-service (DDoS) attacks, or illegal access to databases (Loggen et al., 2024). On the other hand, cyber-enabled crimes are traditional offenses that have been amplified through technology, such as fraud, identity theft, cyberbullying, extortion, and child exploitation (Akdemir & Lawless, 2020). These crimes, though rooted in pre-digital forms, have expanded dramatically with the advent of the internet, which provides broader reach, greater efficiency, and increased anonymity.

Increasingly, researchers view cybercrime as a sociotechnical phenomenon that cannot be understood solely through technological or legal perspectives. Kastner and Mégret (2021) argue that cultural practices, digital behaviors, and the inherent affordances of technology significantly shape the landscape of cybercrime. This perspective highlights how interactions on social media, the management of digital information, and everyday online habits influence both vulnerability to and participation in cybercriminal activities. Hallahan (2020) further emphasizes that cyberspace fosters new forms of social interaction and identity construction while blurring the boundaries

ETCOR Educational Research Center Inc.
SEC Reg. No. 2024020137294-00
Sta. Ana, Pampanga, Philippines
INTERNATIONAL MULTIDISCIPLINARY RESEARCH CONFERENCE
Website: https://etcor.org
iJOINED ETCOR
P - ISSN 2984-7567
E - ISSN 2945-3577
The Exigency
P - ISSN 2984-7842
E - ISSN 1908-3181

between public and private spaces (DeNardis, 2020). These conditions create an environment where deviant behaviors can thrive, requiring an analysis that accounts for both human and technological factors (Wall, 2024).

The evolution of cybercrime has closely followed the rapid advancements in information and communication technology. What began as isolated incidents of email fraud and basic hacking has grown into a complex array of attacks, including ransomware campaigns that cripple critical infrastructures and massive data breaches affecting millions of individuals (Riggs et al., 2023). As Ali (2024) and Amoo et al. (2024) observe, each technological innovation not only creates new opportunities for legitimate use but also introduces vulnerabilities that cybercriminals are quick to exploit, often staying ahead of legal and regulatory mechanisms.

The shift from physical to virtual crime spaces has fundamentally altered public safety and law enforcement paradigms. Crimes that once required physical presence, such as bank robbery or blackmail, can now be perpetrated remotely, often from entirely different jurisdictions. Wall (2021) notes that this transnational nature of cybercrime reduces the likelihood of apprehension for offenders while significantly amplifying their reach and impact. Such conditions demand international cooperation, but global responses often lag behind, hampered by jurisdictional complexities and inconsistent legal frameworks.

As digital systems become more integral to personal, business, and governmental operations, the stakes have grown exponentially (Iordache, 2024). Cloud services, mobile banking, telemedicine, and remote work platforms have created vast repositories of sensitive data that are prime targets for exploitation. Ali and Kollwitz (2025) highlight how these assets attract not only financially motivated criminals but also politically and ideologically driven actors. Consequently, cybercrime now extends beyond individual harm to threaten institutions, economies, and even national security.

Understanding the breadth of cybercrime requires not only functional classifications but also typologies based on actors and platforms. Offenders may range from lone individuals with limited technical skills to organized groups operating like transnational corporations, complete with hierarchical structures and specialized roles (Stoddart, 2022). Cybercriminal activities also differ by platform. On the surface web, scams, phishing, and social engineering schemes target the general public (Chaganti et al., 2021). Meanwhile, the dark web hosts more covert operations, including illegal markets for drugs, weapons, and stolen data, often enabled by cryptocurrency transactions that obscure financial trails (Kaur & Randhawa, 2020; Boyko et al., 2022).

Motivations for cybercrime are equally diverse. Financial incentives remain the most common driver, with schemes like credit card fraud, ransomware, and account takeovers dominating the landscape (Peersman et al., 2022). However, ideological motivations, often termed hacktivism, have also gained prominence, where actors seek to advance political or social causes by defacing websites or leaking sensitive information (Holt et al., 2021). State-sponsored cybercrimes represent another dimension, where digital tools are leveraged for espionage, sabotage, or disinformation campaigns, blurring the lines between crime, politics, and warfare (Baranovska et al., 2024).

Although there is no singular, unified "cybercrime theory," several traditional criminological theories have been widely applied and adapted to explain cyber-offending behavior. Among the most influential is the Routine Activity Theory, which posits that crime is likely to occur when three elements converge: a motivated offender, a suitable target, and the absence of a capable guardian (Schaefer, 2021). In cyberspace, these conditions are easily met. Offenders can access vast pools of vulnerable targets such as unprotected devices, poorly informed users, and unregulated digital environments. This theory is highly relevant to the context of Puerto Princesa City, where digital access is expanding, yet many individuals and institutions remain unaware of basic cybersecurity practices. Empirical studies, such as those by Yar and Steinmetz (2023), support the applicability of Routine Activity Theory in explaining online victimization and cybercrime proliferation.

Not all cybercriminals exhibit the same level of technical sophistication. 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). Socio-demographic 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 economic opportunities (Songsrirote, 2025; Dodel et al., 2020).

Emerging studies provide deeper insight into the structural and psychological aspects of cybercrime. Alkhalil et al. (2021) dissect the anatomy of phishing attacks, revealing how attackers exploit both technical vulnerabilities and human psychology. Similarly, Aslan et al. (2023) discuss critical system weaknesses and emphasize the need for layered defenses, including zero-trust architectures and AI-driven threat monitoring. Azubuike (2023) underscores

ETCOR Educational Research Center Inc.
SEC Reg. No. 2024020137294-00
Sta. Ana, Pampanga, Philippines
INTERNATIONAL MULTIDISCIPLINARY RESEARCH CONFERENCE
Website: https://etcor.org
iJOINED ETCOR
P - ISSN 2984-7567
E - ISSN 2945-3577
The Exigency
P - ISSN 2984-7842
E - ISSN 1908-3181

the geopolitical dimensions of cybercrime, framing state-sponsored attacks as instruments of power in modern conflicts and advocating for stronger international legal frameworks.

Legal responses and policing strategies are evolving to meet these challenges. Chimchiuri (2024) documents the global efforts to legislate against cybercrime but warns that laws often lag behind the rapid pace of technological change, creating enforcement gaps. Collier et al. (2022) recommend a market-focused approach to cybercrime policing, emphasizing adaptive strategies such as infiltrating illicit forums and fostering public-private collaboration to dismantle digital criminal infrastructures. These insights highlight the need for innovation, coordination, and sustained investment in digital forensics and intelligence-sharing mechanisms.

Finally, the human element remains a critical factor in both vulnerability and resilience. Proulx (2022) argues that anonymity fosters a sense of impunity, encouraging deviant behaviors, while Nobles (2022) highlights human error—such as cloud misconfigurations—as a primary source of data breaches. Tetteh (2024) draws attention to the vulnerabilities of small and medium-sized enterprises with limited resources, while Udoh (2024) examines how weak cybersecurity infrastructures undermine e-governance in developing nations. Together, these findings reinforce the need for a comprehensive approach that integrates technology, human behavior, governance, and education to effectively mitigate the escalating risks of cybercrime in an increasingly interconnected world.

Cybercrime in the Philippines reflects a complex interplay of technology, culture, and governance. Scholars note that trust, privacy, and social cohesion are being challenged by digital risks. Calatin and Pajo (2025) emphasize that data misuse and digital surveillance erode public confidence, heightening anxiety and disengagement from online platforms. Panalangin et al. (2025) highlight institutional gaps in cybersecurity preparedness but also point to opportunities for building resilient, localized systems such as regional CERTs. Cultural factors also play a role, as Regaro (2023) illustrates through the linguistic dynamics of "bardagulan," where multilingual hate speech and digital violence thrive. Similarly, San Miguel et al. (2020) show how widespread social media use among youth increases exposure to threats like identity theft and harassment, underscoring the need for proactive cybercrime education at schools and community levels. Toledano (2024) adds a national security lens, stressing that lapses in cybersecurity for critical infrastructure demand urgent institutional investments in risk management and awareness programs.

Legally, Republic Act No. 10175, the Cybercrime Prevention Act of 2012, provides a framework for addressing offenses ranging from system breaches to content-related crimes such as cyber libel, cybersex, and child exploitation (Brucal et al., 2025; Li, 2021). However, implementation challenges persist due to resource constraints and uneven internet access (Official Gazette, 2012). Critics, including Guison and Macalintal (2023), argue that the cyber libel provision threatens free expression, while Blancaflor et al. (2024) and Usman and Haryanto (2024) highlight the alarming prevalence of OSAEC crimes. Rising hacking incidents targeting government, private, and academic sectors (De Ramos & Il, 2022) have intensified calls for stronger infrastructure and coordinated responses. UNICEF Philippines (2021) reports that nearly half of adolescents experience online violence, linking it to adverse psychological and academic outcomes, while Ong and Tapsell (2022) reveal how fake news and digital manipulation shape public discourse. Experts agree that bridging gaps in awareness, literacy, and enforcement will require a collaborative, multi-sectoral approach to build sustainable resilience against cyber threats (Omorog & Medina, 2020).

Despite the growing body of literature on cybercrime in the Philippines, there is a significant research gap in the localized context of Puerto Princesa. Existing studies largely provide national or regional overviews (Calatin & Pajo, 2025; Panalangin et al., 2025; Regaro, 2023; San Miguel et al., 2020; Toledano, 2024), focusing on broader institutional, cultural, and legal dimensions of cybercrime. However, there is limited empirical data on the specific patterns, drivers, and impacts of cybercrime in Puerto Princesa, particularly regarding how local socio-cultural dynamics, digital literacy levels, law enforcement capacity, and community awareness influence cybercrime incidence and response. This lack of localized evidence hinders the development of targeted prevention and intervention strategies that reflect the city's unique technological landscape, governance structures, and community behaviors. Addressing this gap is critical for crafting context-sensitive policies and programs that not only enhance cyber resilience but also align with national efforts to strengthen cybersecurity under Republic Act No. 10175 (Brucal et al., 2025; Li, 2021).

Objectives

The researcher aimed to investigate the cybercrime trends, motivation, and challenges in Puerto Princesa City. Specifically, this sought:

1. To describe the historical trends and patterns in the reported cases of cybercrime in Puerto Princesa City from 2021 to 2024.
2. To describe the role of technology in increasing cybercrime risks in Puerto Princesa City in the following:

ETCOR Educational Research Center Inc.
SEC Reg. No. 2024020137294-00
Sta. Ana, Pampanga, Philippines
INTERNATIONAL MULTIDISCIPLINARY RESEARCH CONFERENCE
Website: https://etcor.org
iJOINED ETCOR
P - ISSN 2984-7567
E - ISSN 2945-3577
The Exigency
P - ISSN 2984-7842
E - ISSN 1908-3181

a. People,
b. Businesses, and
c. Government.

3. To examine the motivations and methods of cybercriminals in Puerto Princesa City.
4. To identify the challenges faced by law enforcement agencies in combating cybercrime in Puerto Princesa City.

METHODS

Research Design

This study utilized an Explanatory Sequential Mixed Methods Design, a two-phase approach in which quantitative data collection and analysis preceded qualitative inquiry to provide deeper context and explanation of initial results. This design was chosen for its strength in integrating numerical trends with rich narrative insights, ensuring a more comprehensive understanding of the research problem. The sequential process enabled the systematic identification of patterns through quantitative measures, which then informed the development of the qualitative phase to explore underlying meanings, perspectives, and experiences. The integration of methods enhanced the rigor and depth of the study, ensuring that the findings were both empirically grounded and contextually nuanced (Amihan et al., 2023).

Population and Sampling

The study engaged a total of 96 participants representing five key sectors to capture a comprehensive view of the role of technology in increasing cybercrime risks. These included respondents from the community (n = 30), business sector (n = 30), government agencies (n = 30), identified cybercrime offenders (n = 3), and law enforcement officers (n = 3) from the Philippine National Police in Puerto Princesa City. Clear inclusion criteria ensured relevance and consistency across groups: community members were residents with basic familiarity with digital technology and internet use; business participants included small to medium enterprise owners, IT personnel, or staff managing online transactions and customer data; and government participants were employees or officials from agencies delivering digital public services. Cybercrime offenders were individuals who had committed technology-related offenses and voluntarily consented to participate, while law enforcers were officers directly involved in cybercrime investigations. Quota sampling was applied to the community, business, and government groups to ensure equal representation for comparative analysis, while volunteer sampling was used for offenders and law enforcement officers given the sensitivity of their roles and the ethical need for voluntary participation. This structured sampling approach ensured balanced, relevant, and diverse perspectives to support both the quantitative and qualitative components of the research (Pangilinan, 2025).

Instrument

The study utilized a researcher-made instrument, grounded in existing literature and prior studies, to comprehensively assess the role of technology in increasing cybercrime risks across societal sectors in Puerto Princesa City. The tool, divided into five parts, combined quantitative and qualitative components to capture sector-specific insights. Part One focused on the community sector, using a 4-point Likert scale to measure perceptions of exposure to cyber threats via common digital platforms, while Part Two examined business-sector vulnerabilities, particularly among SMEs with limited cybersecurity resources. Part Three explored risks faced by government agencies as they increasingly relied on digital platforms, highlighting concerns about weak cybersecurity frameworks and their impact on public trust. Part Four consisted of open-ended questions for cybercrime offenders, aimed at uncovering motivations, targeting strategies, and exploitation of technological vulnerabilities, while Part Five gathered qualitative data from law enforcement personnel on challenges in detection, prevention, and prosecution of cybercrime. To ensure rigor, the tool underwent face and content validity testing, with expert validators from law enforcement, government, and academe yielding a perfect Content Validity Index (CVI) score of 1.00, confirming its relevance and appropriateness. Reliability testing using Cronbach's alpha produced a coefficient of 0.917, indicating high internal consistency and supporting the instrument's reliability for generating accurate, trustworthy, and actionable data for cybercrime risk assessment across sectors (Sanchez, 2025).

ETCOR Educational Research Center Inc.
SEC Reg. No. 2024020137294-00
Sta. Ana, Pampanga, Philippines
INTERNATIONAL MULTIDISCIPLINARY RESEARCH CONFERENCE
Website: https://etcor.org
iJOINED ETCOR
P - ISSN 2984-7567
E - ISSN 2945-3577
The Exigency
P - ISSN 2984-7842
E - ISSN 1908-3181

Data Collection

After securing the necessary approvals from the key institutions, data collection began with the distribution of the validated survey instrument to respondents across five sectors: community, business, government, cybercrime offenders, and law enforcement. To ensure accessibility, the survey was made available in two formats—online via Google Forms for participants with reliable internet access and printed copies for those in remote or underserved areas. Surveys were personally distributed to community members through local contacts, while links were shared via email and messaging platforms with government employees, business representatives, and professionals. Each respondent completed only the section relevant to their classification, ensuring accurate and sector-specific responses. Alongside the surveys, semi-structured interviews were conducted with three cybercrime offenders and three law enforcement officers to gather in-depth qualitative data. These interviews, conducted in focused sessions, explored offenders' methods and motivations as well as the operational challenges faced by investigators. All sessions were recorded, transcribed verbatim, anonymized, and prepared for thematic analysis. After completing the surveys and interviews, the researcher organized, encoded, and verified all responses, ensuring the data were ready for comprehensive quantitative and qualitative analyses (Pangilinan et al., 2025).

Treatment of Data

This study applied an integrated approach to data analysis, combining quantitative and qualitative techniques for a comprehensive interpretation of the findings. Quantitative data from the survey responses were analyzed using descriptive statistics, including frequency counts and median scores, to summarize perceptions of technology-related cybercrime risks across the three sectors: community, business, and government. Qualitative data, derived from key informant interviews with cybercrime offenders and Philippine National Police personnel, were examined using a thematic analysis approach. Thematic analysis was conducted by transcribing the interviews, organizing the data, and systematically coding the responses to highlight significant statements. Patterns and categories were then identified, from which key themes were developed. This process enabled a deeper understanding of offender motivations and the operational challenges experienced by law enforcement in addressing cybercrime (Sanchez, 2025).

Ethical Considerations

This research adhered to established ethical standards to protect the rights, dignity, and welfare of all participants. Formal approval was obtained from the participating offices and institutions, including government agencies, law enforcement, business entities, and community organizations. All participants received an informed consent statement embedded in the preliminary part of the data-gathering tool, clearly explaining the study's purpose, scope, and procedures, as well as their voluntary right to participate or withdraw at any time. In compliance with the Data Privacy Act of 2012 (RA 10173), respondents were assured of strict confidentiality, with no personally identifiable information disclosed in any report or publication. For interview participants, including cybercrime offenders and PNP personnel, additional verbal and written consent was obtained, and they were informed that their responses would be recorded, transcribed, and anonymized for analysis. Special care was taken when engaging with vulnerable participants to avoid coercion or discomfort, with interviews conducted in a safe and respectful setting. Throughout the process, the principles of voluntary participation, informed consent, confidentiality, and anonymity were consistently upheld. Lastly, no identifying information was reported in any part of the manuscript regarding the identity of the interview informants (Carvajal et al., 2025).

RESULTS AND DISCUSSION

Historical Trends and Patterns in the Reported Cases of Cybercrime in Puerto Princesa City from 2021 to 2024

Table 1. Historical Trends and Patterns in the Reported Cases of Cybercrime in Puerto Princesa City from 2021 to 2024

Types of Cybercrime	2021	2022	2023	2024	Total
Online Scam		6	8	6	20
Phishing					0
Identity Theft		2	8	6	16

ETCOR Educational Research Center Inc.
SEC Reg. No. 2024020137294-00
Sta. Ana, Pampanga, Philippines
INTERNATIONAL MULTIDISCIPLINARY RESEARCH CONFERENCE
Website: https://etcor.org
iJOINED ETCOR
P - ISSN 2984-7567
E - ISSN 2945-3577
The Exigency
P - ISSN 2984-7842
E - ISSN 1908-3181

Libel	1	4	1	6	12
Threat Online		2	1		3
Illegal Access		1		7	8
Anti-Photo and Video Voyeurism			1		1
Overall	1	15	19	25	60

From 2021 to 2024, reported cybercrime cases showed a clear and consistent upward trajectory, reflecting the growing prevalence of digital offenses within the community. Cases rose sharply from a single report in 2021 to 15 in 2022, 19 in 2023, and 25 in 2024. This steady increase not only signals greater reliance on digital platforms but may also indicate improved awareness and reporting mechanisms, highlighting cybercrime as an increasingly urgent local concern. Among the various types of cybercrime, online scams, identity theft, and cyber libel emerged as the most prevalent. Online scams were reported consistently from 2022 onward, accumulating the highest number of cases at 20, underscoring their persistent threat. Identity theft spiked in 2023 with eight cases and remained significant in 2024 with six, reflecting rising vulnerabilities in the protection of personal and financial data. Cyber libel, though fluctuating in frequency, also saw an uptick in 2024, pointing to the ongoing issue of online defamation and abuse on social media platforms. Other cybercrimes, though less frequent, displayed notable patterns. Illegal access surged to seven reported cases in 2024, up from a single case in 2022, highlighting escalating concerns over unauthorized system intrusions. Conversely, anti-photo and video voyeurism and online threats were reported only sporadically, suggesting these offenses may be underreported or harder to detect. Interestingly, phishing had no recorded cases throughout the period, possibly due to underreporting, misclassification under broader categories, or limited victim awareness. Over time, the range of reported cybercrimes expanded: while only a single cyber libel case was recorded in 2021, by 2024, nearly all categories—except phishing—had been reported, reflecting a broader understanding and recognition of cybercrime as awareness spreads (Yar & Steinmetz, 2023). The consistent rise in financially driven and data-centric offenses, particularly online scams and identity theft, underscores the urgent need for stronger digital security measures, enhanced public digital literacy, and more robust law enforcement strategies to address evolving cyber threats (Gulyamov & Raimberdiyev, 2023).

The qualitative findings on offender motivations complement the crime trend data, providing deeper insights into the behavioral and emotional factors driving local cyber offenses. Themes of cyber retaliation and emotional impulsivity help explain the persistence and escalation of cases such as cyber libel and identity theft, both of which saw significant increases between 2023 and 2024. Offenders often acted out of personal grievances or heightened emotional states, leveraging the anonymity and immediacy of digital platforms to retaliate or shame their targets, consistent with Wall's (2021) and Herman et al.'s (2024) observations on digitally mediated conflicts. The practice of public shaming as a form of digital vigilantism, tied to local online cultures like "bardagulan" (Regaro, 2023), also aligns with the surge of cyber libel cases, where reputational harm and humiliation are central to the offense. Coupled with the quantitative data showing rising reports of illegal access and identity theft, these findings indicate a dual dynamic of emotionally driven offenses and financially or data-centric crimes (Yar & Steinmetz, 2023; Gulyamov & Raimberdiyev, 2023). Together, they highlight the urgent need for interventions that not only enhance digital literacy and cybersecurity awareness but also address the socio-emotional and cultural dimensions of cybercrime in Puerto Princesa.

Role of Technology in Increasing Cybercrim Risks

Table 2. Role of Technology in Increasing Cybercrime Risks Among People, Businesses, and Government

Indicators	Median	Description
People	4	Very High Role
Businesses	4	Very High Role
Government	4	Very High Role

The overall results strongly emphasize the critical role of technology in increasing cybercrime risks across community members, businesses, and government agencies, reflecting how digital transformation has expanded opportunities for cybercriminal activities. Among community members, the rapid integration of technology into daily life—particularly the use of social media, smartphones, and online financial platforms—has created broader exposure to risks such as identity theft, fraud, cyberbullying, and misinformation. The rise of unregulated online engagement,

ETCOR Educational Research Center Inc.
SEC Reg. No. 2024020137294-00
Sta. Ana, Pampanga, Philippines
INTERNATIONAL MULTIDISCIPLINARY RESEARCH CONFERENCE
Website: https://etcor.org
iJOINED ETCOR
P - ISSN 2984-7567
E - ISSN 2945-3577
The Exigency
P - ISSN 2984-7842
E - ISSN 1908-3181

especially among youth and elderly groups, has amplified vulnerabilities to both opportunistic and targeted attacks. These findings mirror the observations of Alkhalil et al. (2021), who noted that widespread reliance on digital platforms often makes individuals easy targets for phishing and identity-related crimes, and Aslan et al. (2023), who highlighted the dangers posed by increasing sophistication of attacks in the absence of user education and protective measures. San Miguel et al. (2020) similarly emphasized that in the Philippine context, high social media use coupled with low digital literacy magnifies the potential for cyber victimization, demonstrating how technology, while empowering, also escalates risks in everyday online interactions.

In the business sector, technology plays a significant role in expanding the threat landscape, particularly through the integration of digital operations, cloud computing, and online transactions. The results show that most businesses recognize that digital platforms, while improving operational efficiency and competitiveness, have made them more susceptible to data breaches, ransomware, phishing, and system exploitation. This aligns with Nobles (2022), who observed that cloud service vulnerabilities and human errors make businesses primary targets for cybercriminals. However, Small and Medium Enterprises (SMEs) face a unique challenge: while they acknowledge these risks, limited budgets, outdated infrastructure, and lack of cybersecurity expertise leave them especially exposed. Tetteh (2024) highlights that SMEs are often prime targets due to weaker defenses, and Panalangin et al. (2025) similarly found that many Philippine businesses lack structured cybersecurity frameworks to manage evolving risks. These findings stress the urgent need for scalable and affordable security solutions, enhanced technical support, and collaborative industry-driven initiatives to reduce the widening risk gap between large corporations and smaller enterprises.

For government agencies, the findings reveal that technology-driven initiatives, including e-governance, online transactions, and digital records management, have significantly expanded their exposure to cybercrime risks. The transition to digital systems has created a larger attack surface for malicious actors, exposing sensitive public data and critical infrastructures to potential exploitation. The results indicate that cyber risks in this sector are compounded by outdated systems, inconsistent security protocols, and limited inter-agency coordination. These findings are consistent with Azubuike (2023), who stressed that digitized government systems are increasingly attractive to cybercriminals and state-sponsored actors, and Udoh (2024), who pointed out that the benefits of digital governance are often undermined by inadequate cybersecurity readiness in developing countries. Locally, Toledano (2024) observed that Philippine agencies frequently operate without comprehensive cybersecurity policies, leaving them vulnerable to data breaches and operational disruptions. This underscores the urgent need for government institutions to adopt robust cybersecurity frameworks, allocate adequate resources, and implement continuous training programs to strengthen defenses and ensure the security of digital public services.

Motivations and Methods of Cybercriminals in Puerto Princesa

Theme 1: Cyber Retaliation Due to Personal Offense

Cybercrime offenders in Puerto Princesa City frequently described their actions as deliberate acts of retaliation rooted in personal grievances such as betrayal, humiliation, or disrespect. Many admitted that their offenses—such as hacking, doxxing, or exposing private conversations—were committed to assert control or inflict emotional harm on individuals they felt had wronged them. Statements like, "He disrespected me, so I exposed his secret online" and "I wouldn't have done it if he hadn't hurt me first. What I did on social media was just revenge" illustrate this dynamic. These findings align with Wall's (2021) observation that personal vendettas are increasingly driving digital offending, particularly in contexts where individuals feel marginalized or disempowered by formal justice systems. The anonymity, accessibility, and immediacy of digital platforms create a perceived sense of empowerment, enabling offenders to retaliate without immediate repercussions. Similarly, Whyte (2020) highlights the rise of "digitally mediated revenge," where interpersonal conflicts are extended into digital spaces through harmful behaviors such as revenge pornography, cyberstalking, and harassment. Together, these perspectives underscore the emotional and relational underpinnings of cyber offending, highlighting the need for policies and educational interventions that address how technology amplifies interpersonal conflicts in the digital age.

Theme 2: Emotional Impulsivity Triggered by Betrayal or Conflict

Another recurring theme among offenders was the role of emotional impulsivity, where cyber offenses were committed in moments of intense anger, heartbreak, or humiliation. Many participants emphasized that their actions were unplanned, arising from overwhelming emotions triggered by personal betrayal or unresolved conflict. For example, one admitted, "I didn't mean to do it at first, but I was triggered, so I hacked his account." Another said, "I

ETCOR Educational Research Center Inc.
SEC Reg. No. 2024020137294-00
Sta. Ana, Pampanga, Philippines
INTERNATIONAL MULTIDISCIPLINARY RESEARCH CONFERENCE
Website: https://etcor.org
iJOINED ETCOR
P - ISSN 2984-7567
E - ISSN 2945-3577
The Exigency
P - ISSN 2984-7842
E - ISSN 1908-3181

did it because I was deeply hurt by what he did to me." Herman et al. (2024) argue that the immediacy and anonymity of online platforms amplify impulsive behaviors by reducing the social cues and accountability typically present in face-to-face interactions. In digital spaces, the lack of immediate consequences fosters environments where emotional triggers, coupled with low impulse control, can quickly escalate into cyber offenses. These findings point to the importance of interventions focused on emotional regulation, digital responsibility, and conflict resolution, as well as restorative approaches in the justice system that consider the emotional and cognitive drivers of impulsive online behaviors.

Theme 3: Public Shaming as a Means of Revenge

Public shaming also emerged as a prominent method of retaliation, where offenders deliberately exposed private conversations, images, or screenshots to humiliate their targets online. Such acts were often intended both as personal revenge and as public condemnation, with offenders stating, "I released screenshots so everyone would know how bad he is" and "I leaked information because I wanted him to feel the shame I went through." Others admitted, "I embarrassed him online." This reflects the concept of digital vigilantism described by Favarel-Garrigues et al. (2020), where individuals bypass formal legal systems and leverage digital platforms to exact informal justice. In the Philippine context, this aligns with the growing phenomenon of "online bardagulan"—a cultural practice characterized by confrontational, retaliatory exchanges on social media that often escalate into widespread public shaming (Regaro, 2023). While such actions may serve as outlets for emotional release or a means of asserting dominance, they contribute to significant harms, including reputational damage, psychological distress, and social polarization. The normalization of these practices underscores the urgent need for digital citizenship education that fosters empathy, respect for privacy, and responsible online conduct. Policy frameworks must also adapt to address the ethical and legal complexities of digital vigilantism, balancing accountability with the protection of individual rights in an increasingly connected society.

Challenges Faced by Law Enforcement Agencies in Combating Cybercrime in Puerto Princesa

The responses of law enforcement agencies in Puerto Princesa City reveal three key challenges in combating cybercrime: anonymity and technical evasion by offenders, limited public awareness and digital literacy, and enforcement gaps despite the existence of cybercrime laws. First, anonymity and technical evasion remain significant barriers to effective investigation and prosecution. Officers consistently highlighted the difficulty of identifying offenders who exploit fake profiles, aliases, VPNs, and encrypted platforms to mask their identities. As one officer explained, "Unlike street crimes, cybercriminals can hide behind fake accounts and anonymous profiles," while another noted, "It's hard to identify cybercriminals because they often use VPNs and fake names online." These experiences align with Proulx (2022), who emphasizes that anonymity tools such as VPNs and encryption technologies obscure digital footprints, complicating attribution and evidence collection. Heft (2023) adds that cyberspace, as a "disembodied" environment, disrupts traditional policing frameworks reliant on physical presence and localized jurisdiction, making transboundary offenses particularly difficult to address. This complex environment demands innovative investigative strategies, including investment in digital forensics, specialized cybercrime units, and cross-border collaborations. Without these advancements, law enforcement agencies remain at a disadvantage, unable to keep pace with offenders who increasingly view the digital space as a low-risk environment for illicit activities.

The second challenge involves limited public awareness and digital literacy, which exacerbate the community's vulnerability to cybercrime. Law enforcement personnel observed that many individuals remain unaware of basic cybersecurity practices, making them easy targets for phishing, scams, and other digital threats. As one officer stated, "Many people in the community still don't know the proper ways to stay safe online," while another remarked, "Because they don't understand the online risks, they become easy targets for cybercriminals." This reflects Guerrero's (2024) concept of "cyber risk naïveté," where users—especially those lacking formal digital education—underestimate the dangers of online spaces. Anderson and Agarwal further argue that such vulnerability stems from a critical knowledge gap rather than apathy. In the Philippine context, Calatin and Pajo (2025) note that cybersecurity campaigns are often concentrated in urban centers, leaving rural and marginalized communities with little access to accurate information or digital safety tools. This digital divide underscores the urgent need for inclusive, grassroots-level education tailored to local contexts, including community assemblies, radio broadcasts, and materials in local dialects. Partnerships with local leaders and schools can amplify these efforts, ensuring that

ETCOR Educational Research Center Inc.
SEC Reg. No. 2024020137294-00
Sta. Ana, Pampanga, Philippines
INTERNATIONAL MULTIDISCIPLINARY RESEARCH CONFERENCE
Website: https://etcor.org
iJOINED ETCOR
P - ISSN 2984-7567
E - ISSN 2945-3577
The Exigency
P - ISSN 2984-7842
E - ISSN 1908-3181

awareness campaigns reach those most at risk. Addressing this knowledge gap requires a multi-faceted approach that integrates education, infrastructure, and policy support to foster digital resilience across all sectors of society.

Lastly, enforcement gaps persist despite the presence of cybercrime laws such as the Cybercrime Prevention Act of 2012 (RA 10175). Law enforcers acknowledged that while the legal framework provides a foundation for prosecuting cyber offenses, practical implementation remains limited due to the inability to trace anonymous offenders and the complexities of handling digital evidence. As one officer explained, "Even if the law exists, it's hard to enforce it if you can't identify who's behind the crime," echoing Chimchiuri's (2024) argument that legislation often struggles to keep pace with rapidly evolving technologies. This mismatch between law and reality creates enforcement challenges and weakens deterrence, as offenders exploit legal loopholes and technical barriers. Collier et al. (2022) emphasize that meaningful cybercrime governance requires not just laws but also robust institutional capacity—especially in local enforcement units where technical expertise, advanced forensic tools, and standardized protocols are often lacking. These deficiencies result in delayed investigations, low conviction rates, and diminished public trust in the justice system. To close these gaps, a holistic approach is necessary: continuous capacity-building for law enforcement and the judiciary, regular updates to legal frameworks to match technological trends, and enhanced coordination across agencies and jurisdictions. By integrating modern digital infrastructure and fostering adaptive policies, authorities can better respond to the dynamic and complex landscape of cybercrime.

Globally, law enforcement agencies confront challenges similar to those in Puerto Princesa—namely, advancing cybercrime outpacing the capacity of existing legal and investigative structures. Europol's Internet Organised Crime Threat Assessment (IOCTA) highlights how the rapid evolution of cybercrime, particularly organized ransomware and crime-as-a-service models, continues to strain law enforcement resources and cross-border response mechanisms (Europol, 2023; Torres, 2025). These international patterns underscore the critical role of integrated intelligence-sharing, multi-jurisdictional task forces, public–private partnerships, and legal adaptation to keep pace with the dynamic and borderless nature of cybercrime.

Conclusions

In conclusion, the upward trend of reported cybercrime cases in Puerto Princesa City from 2021 to 2024 highlights the deepening integration of technology in daily life and its role in amplifying cyber-related risks. Offender motivations—ranging from personal retaliation and emotional impulsivity to public shaming for revenge—reveal how emotional and relational factors drive harmful online behaviors, often intensified by the anonymity and immediacy of digital platforms. At the same time, law enforcement faces significant barriers, including technical evasion by offenders, limited digital literacy within the community, and gaps in the practical enforcement of RA 10175, which collectively hinder timely investigations and prosecutions. These findings underscore the urgent need for a multi-pronged strategy that enhances technical capabilities and training for law enforcement, strengthens digital literacy and awareness campaigns at the grassroots level, and aligns local initiatives with national and global efforts to build a more adaptive and resilient cybersecurity framework for the community.

Recommendations

To address the rising cybercrime risks in Puerto Princesa City, a phased, multi-faceted approach with clear timelines and responsibility markers is recommended. In the short term (0–6 months), the Puerto Princesa City Police Office (PPCPO) Cybercrime Unit, in coordination with the PNP Anti-Cybercrime Group (ACG), should prioritize the enhancement of technical capabilities through advanced digital forensics training and the procurement of updated investigative tools. At the same time, the City Information Office and local schools should initiate community-wide digital literacy campaigns, using barangay assemblies, social media infographics, and local radio programs to teach safe online practices. These should focus on critical topics such as password security, phishing awareness, and basic data protection to build immediate awareness across different community sectors. For the medium term (6–18 months), the City Council and Legal Affairs Office, working closely with national cybersecurity agencies and local stakeholders, should lead the review and updating of local ordinances to align with technological advancements and ensure that the practical enforcement of RA 10175 remains effective. During this phase, public-private partnerships should also be strengthened. Local businesses, internet service providers, and civic organizations can collaborate on incident reporting mechanisms, data protection protocols, and training programs to create a stronger, unified response to cyber threats. In the long term (18–36 months), the Mayor's Office, in partnership with academic institutions, NGOs, and law enforcement agencies, should focus on scaling up initiatives like Project CYBERSAGIP. This expansion should include the development of youth-led advocacy programs, the establishment of incident reporting hotlines, and regular community drills on cyber awareness and threat reporting. Collaborations with

ETCOR Educational Research Center Inc.
SEC Reg. No. 2024020137294-00
Sta. Ana, Pampanga, Philippines
INTERNATIONAL MULTIDISCIPLINARY RESEARCH CONFERENCE
Website: https://etcor.org
iJOINED ETCOR
P - ISSN 2984-7567
E - ISSN 2945-3577
The Exigency
P - ISSN 2984-7842
E - ISSN 1908-3181

national agencies such as the Department of Information and Communications Technology (DICT) and global organizations like INTERPOL and Europol should also be formalized to promote cross-border intelligence-sharing, joint operations, and continuous capacity-building. These sustained efforts will ensure Puerto Princesa develops a secure, adaptive, and resilient digital ecosystem that keeps pace with the rapidly evolving landscape of cybercrime.

REFERENCES

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

Ali, M. D. J. (2024). Cybercrime and Cybersecurity: A critical analysis of legal frameworks and enforcement mechanisms. *Bharati International Journal of Multidisciplinary Research and Development, 2*(8), 137-154.

Ali, H., & Kollwitz, E. (2025). Cybercrime syndicates and their role in digital asset scams: A global threat.

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science, 3*, 563060.

Amihan, S. R., Sanchez, R. D., & Carvajal, A. L. P. (2023). Sustained quality assurance: Future-proofing the teachers for an ASEAN higher education common space. *International Journal of Open-access, Interdisciplinary and New Educational Discoveries of ETCOR Educational Research Center (iJOINED ETCOR),* 2(4), 276-286. https://etcor.org/storage/iJOINED/Vol.%20II(4),%20276-286.pdf

Amoo, O. O., Atadoga, A., Abrahams, T. O., Farayola, O. A., Osasona, F., & Ayinla, 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), 205-217.

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics, 12*(6), 1333.

Azubuike, C. F. (2023). Cyber security and international conflicts: An analysis of state-sponsored cyber attacks. *Nnamdi Azikiwe Journal of Political Science, 8*(3), 101-114.

Baranovska, T., Savitskyi, V., Serbov, M., Stoliar, Y., & Krutik, Y. (2024). The impact of cybercrime on state and institutional security: Analysis of threats and potential protection measures. *Economic Affairs, 69*, 33-42.

Blancaflor, E., Caberto, D. J., lara, C. G., & Mancilla, D. F. L. (2024, April). Guarding against phone scammers: An examination of gaining access to phone contacts through smishing social engineering exploits. In *Proceedings of the 2024 10th International Conference on Computing and Artificial Intelligence* (pp. 365-372).

Boyko, A., Dotscenko, T., & Dolia, Y. (2022). Patterns of financial crimes using cryptocurrencies. *Socio-Economic Relations in the Digital Society, 2*(44), 23-28.

Brucal, A., Abante, M. V., & Vigonte, F. (2025). *Cybercrime Prevention Act of 2012 in Practice: Cybersecurity, Controversy, and the Future of Digital Rights in the Philippines*. Controversy, and the Future of Digital Rights in the Philippines (May 19, 2025).

Calatin, M., & Pajo, P. (2025). Eroding trust, deepening isolation: Data misuse and the social disconnect in the digital Philippines.

Caneppele, S., & Da Silva, A. (2022). Cybercrime. In *Research Handbook of Comparative Criminal Justice* (pp. 243-260). Edward Elgar Publishing.

ETCOR Educational Research Center Inc.
SEC Reg. No. 2024020137294-00
Sta. Ana, Pampanga, Philippines
INTERNATIONAL MULTIDISCIPLINARY RESEARCH CONFERENCE
Website: https://etcor.org
iJOINED ETCOR
P - ISSN 2984-7567
E - ISSN 2945-3577
The Exigency
P - ISSN 2984-7842
E - ISSN 1908-3181

Carvajal, A. L. P., Fernandez, T. M., Pangilinan, A. M., Obod, M. M., Amihan, S. R., Sanchez, R. D., Sanchez, A. M. P., Sanchez, J. J. D. (2025). Future-Proofing Teachers in Reframing Teacher Education Curriculum in the Philippines: Basis for Policy Recommendations. *International Journal of Open-access, Interdisciplinary and New Educational Discoveries of ETCOR Educational Research Center (iJOINED ETCOR)*, 4(2), 235-252. https://doi.org/10.63498/nxz2st271

Chaganti, R., Bhushan, B., Nayyar, A., & Mourade, A. (2021). *Recent trends in social engineering scams and case study of gift card scam*. arXiv preprint arXiv:2110.06487.

Chimchiuri, L. (2024). The evolution of cybercrime legislation. *Scientific works of National Aviation University. Series: Law Journal" Air and Space Law", 2*(71), 221-227.

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.

Collier, B., Thomas, D. R., Clayton, R., Hutchings, A., & Chua, Y. T. (2022). Influence, infrastructure, and recentering cybercrime policing: Evaluating emerging approaches to online law enforcement through a market for cybercrime services. *Policing and Society, 32*(1), 103-124.

DeNardis, L. (2020). *The Internet in everything*. Yale University Press.

De Ramos, N. M., & II, F. D. E. (2022). Cybersecurity program for Philippine higher education institutions: A multiple-case study. *International Journal of Evaluation & Research in Education, 2252*(8822), 1199.

Dodel, M., Kaiser, D., & Mesch, G. (2020). *Determinants of cyber-safety behaviors in a developing economy: The role of socioeconomic inequalities, digital skills and perception of cyber-threats*. First Monday.

Europol (2023), *Internet Organised Crime Threat Assessment (IOCTA) 2023*. Publications Office of the European Union, Luxembourg.

Favarel-Garrigues, G., Tanner, S., & Trottier, D. (2020). Introducing digital vigilantism. *Global Crime, 21*(3-4), 189-195.

Ganguli, P. (2024). *The rise of cybercrime-as-a-service: Implications and countermeasures*. Available at SSRN 4959188.

Grispos, G. (2021). Criminals: Cybercriminals. In *Encyclopedia of Security and Emergency Management* (pp. 84-89). Cham: Springer International Publishing.

Guerrero, V. L. (2024). *Cyber threats, cyber risks, and cybersecurity responses: Modeling whole-of-nation strategy implementation for American organizations and citizens* (Doctoral dissertation, Clemson University).

Gulyamov, S., & Raimberdiyev, S. (2023). Personal data protection as a tool to fight cyber corruption. *International Journal of Law and Policy, 1*(7), 1-35.

Hallahan, K. (2020). Crises and risk in cyberspace. In *Handbook of Risk and Crisis Communication* (pp. 412-445). Routledge.

Heft, P. (2023). Virtual embodiment, or: when I enter cyberspace, what body will I inhabit?. *Cosmos and History: The Journal of Natural and Social Philosophy, 19*(1).

Herman, S., Barnum, T. C., Minà, P. E., Wozniak, P., & Van Gelder, J. L. (2024). Affect, emotions, and crime decision-making: Emerging insights from immersive 360 video experiments. *Journal of Experimental Criminology*, 1-34.

ETCOR Educational Research Center Inc.
SEC Reg. No. 2024020137294-00
Sta. Ana, Pampanga, Philippines
INTERNATIONAL MULTIDISCIPLINARY RESEARCH CONFERENCE
Website: https://etcor.org
iJOINED ETCOR
P - ISSN 2984-7567
E - ISSN 2945-3577
The Exigency
P - ISSN 2984-7842
E - ISSN 1908-3181

Iordache, A. (2024). The impact of digitalization on economic crimes. *Journal of Law and Public Administration, 10*(19), 22-28.

Kastner, P., & Mégret, F. (2021). International legal dimensions of cybercrime. In *Research Handbook on International Law and Cyberspace* (pp. 253-270). Edward Elgar Publishing.

Kaur, S., & Randhawa, S. (2020). Dark web: A web of crimes. *Wireless Personal Communications, 112*(4), 2131-2158.

Leppänen, A. (2024). *Networked responses to cyber-dependent crime: Developing policing in a changing security environment*. Tampere University.

Li, J. (2021). Cybercrime in the Philippines: A case study of national security. *Turkish Journal of Computer and Mathematics Education, 12*(11), 4224-4231.

Loggen, J., Moneva, A., & Leukfeldt, R. (2024). Pathways into, desistance from, and risk factors related to cyber-dependent crime: A systematic narrative review. *Victims & Offenders*, 1-32.

Nobles, C. (2022). Investigating cloud computing misconfiguration errors using the human factors analysis and classification system. *Scientific Bulletin, 27*(1), 59-66.

Official Gazette. (2012). *Republic Act No. 10175.*

Omorog, C. D., & Medina, R. P. (2020). *Internet Security Awareness of Filipinos: a survey paper*. arXiv preprint arXiv:2012.03669.

Ong, J. C., & Tapsell, R. (2022). Demystifying disinformation shadow economies: fake news work models in Indonesia and the Philippines. *Asian Journal of Communication, 32*(3), 251-267.

Panalangin, M. L., Mohamad, H. A., Abo, S. A., Cararag, A. S., & Reyes, A. R. L. (2025). Building a resilient computer emergency response team (CERT): A strategic approach using SWOT analysis and the CERT resilience maturity model for cybersecurity preparedness in the Bangsamoro Government, Philippines. *American Journal of Innovation in Science and Engineering, 4*(2).

Pangilinan, A. M. (2025). Challenges and Commitment to Teaching: A Quantitative Descriptive-Correlational Study of Filipino Teachers in Select Coastal Villages. *International Journal of Open-access, Interdisciplinary and New Educational Discoveries of ETCOR Educational Research Center (iJOINED ETCOR)*, 4(2), 1684-1692. https://doi.org/10.63498/etcor397

Pangilinan, A. M., Velasco, J., Punzalan, F. R. A., Sanchez, R. D., Sanchez, A. M. P., & Moldez, R. G. (2025). Artificial Intelligence in the Conduct of Research: Embracing its Promises and Avoiding the Pitfalls from the Lens of Research Practitioners. *International Journal of Open-access, Interdisciplinary and New Educational Discoveries of ETCOR Educational Research Center (iJOINED ETCOR)*, 4(3), 360-370. https://doi.org/10.63498/etcor432

Payne, B. K. (2020). Defining cybercrime. In The Palgrave handbook of international cybercrime and cyberdeviance (pp. 3-25). Cham: Springer International Publishing.

Peersman, C., Williams, E., Edwards, M., & Rashid, A. (2022). *Understanding motivations and characteristics of financially-motivated cybercriminals*. arXiv preprint arXiv:2203.08642.

Proulx, K. (2022). *Anonymity online and the perfect environment for cybercrime* (Master's thesis, Utica University).

ETCOR Educational Research Center Inc.
SEC Reg. No. 2024020137294-00
Sta. Ana, Pampanga, Philippines
INTERNATIONAL MULTIDISCIPLINARY RESEARCH CONFERENCE
Website: https://etcor.org
iJOINED ETCOR
P - ISSN 2984-7567
E - ISSN 2945-3577
The Exigency
P - ISSN 2984-7842
E - ISSN 1908-3181

Regaro, J. (2023). Linguistic Features of Multilingual Hate Speech in the Online "Bardagulan". *International Journal of English Language Studies, 5*(4), 120-139.

Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., ... & Sarwat, A. I. (2023). Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure. *Sensors, 23*(8), 4060.

Sanchez, R. D. (2025, August 24). To proceed forthwith: Basic rules, tips, and innovations in thesis and dissertation writing [PowerPoint slides]. https://www.facebook.com/share/p/1FUwVPnQv6/

San Miguel, C., Morales, K., & Ynalvez, M. A. (2020). Online victimization, social media utilization, and cyber crime prevention measures. *Asia-Pacific Social Science Review, 20*(4), 11.

Schaefer, L. (2021). *Routine activity theory*. Oxford University Press.

Songsrirote, N. (2025). Socioeconomic Determinants of Cybercrime Costs: A Panel Data Analysis of OECD Countries. *Asian Journal of Applied Economics, 32*(1), 30-57.

Stoddart, K. (2022). *Non and sub-state actors: Cybercrime, terrorism, and hackers. In Cyberwarfare: threats to critical infrastructure* (pp. 351-399). Cham: Springer International Publishing.

Tetteh, A. K. (2024). Cybersecurity needs for SMEs. *Issues in Information Systems, 25*(1).

Toledano, S. A. (2024). *Critical Infrastructure Security: Cybersecurity lessons learned from real-world breaches*. Packt Publishing Ltd.

Torres, A. (2025). *Working with INTERPOL and the world economic forum to continue driving cyber resilience in Latin America*. Fortinet.

Udoh, H. (2024). *E-governance performance in the context of developing countries* (Doctoral dissertation, University of Leicester).

UNICEF Philippines. (2021). *Online bullying remains prevalent in the Philippines, other countries*.

Usman, I. R., & Haryanto, A. (2024). Philippine and INTERPOL cooperation in addressing cybersex crime in the Philippines. *Journal of Social Political Sciences, 5*(2), 150-160.

Wall, D. S. (2021). Cybercrime as a transnational organized criminal activity. In *Routledge Handbook of Transnational Organized Crime* (pp. 318-336). Routledge.

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

Whyte, C. (2020). Beyond tit-for-tat in cyberspace: political warfare and lateral sources of escalation online. *European Journal of International Security, 5*(2), 195-214.

Yar, M., & Steinmetz, K. F. (2023). *Cybercrime and society*.