INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY: APPLIED BUSINESS AND EDUCATION RESEARCH
2025, Vol. 6, No. 3, 1312 – 1333
http://dx.doi.org/10.11594/ijmaber.06.03.23

Research Article

Challenges Faced by PNP in Resolving Cybercrime Cases

Maribel B. Fajardo, Mario N. Abragon, Lezeil Lopez Abuan, Justeofino M. Hinlayagan, Deodennis Joy Marmol, Anne B. Contreras, Rogelio Basbas Jr., Elizabeth B. Villa*

De La Salle University Dasmarinas

Article history:
Submission 31 February 2025
Revised 07 February 2025
Accepted 23 February 2025

**Corresponding author:*
E-mail:
esbuena@dlsud.edu.ph

ABSTRACT

The research examined the correlation between the level of challenges faced by the PNP-ACG and various demographic factors. Additionally, it examined the specific components of cybercrime offenses, which include offenses against the confidentiality, integrity, and availability of computer data and systems, as well as offenses related to computers, content, and other areas.

The findings indicated that the PNP-ACG faced roughly the same level of challenges as other law enforcement groups in the region. Interestingly, demographic factors such as age, length of service, educational attainment, and training attendance did not significantly affect the level of obstacles faced by the PNP-ACG personnel.

Moreover, the study revealed a significant relationship between the number of problems the PNP-ACG had and the types of privacy, honesty, and other crimes that happened during their digital forensic investigations and operations.

These findings suggest that the challenges faced by the PNP-ACG are more systemic in nature and not primarily driven by individual or demographic characteristics. The study ends with suggestions for how to improve the PNP-ACG in the region by doing a full organizational assessment, creating a strong digital forensic management system, running programs to build people's skills, and working together with other groups to deal with the problems that were found.

Keywords: *PNP Anti-Cybercrime Group (PNP ACG), Cybercrimes, Demographic Factors*

Background

Cybercrime is defined as the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy (Dennis, 2023). It is also known as "computer crime" wherein criminal activity is carried out by means of computer or internet. Nowadays, cybercrime is a growing concern to countries at

How to cite:
Fajardo, M. B., Abragon, M. N., Abuan, L. L., Hinlayagan, J. M., Marmol, D. J., Contreras, A. B., Basbas Jr., R., & Villa, E. B. (2025). Challenges Faced by PNP in Resolving Cybercrime Cases. *International Journal of Multidisciplinary: Applied Business and Education Research*. *6*(3), 1312 – 1333. doi: 10.11594/ijmaber.06.03.23

all levels of developments which affects essential services, businesses and individuals. As people become more reliant to communication and technology, criminals are also shifting their illegal activities.

The expansion in digital activities fades the way for escalation of cybersecurity concerns particularly for critical infrastructure. Cyberattacks usually target the most mission-critical industries, such as healthcare, or those that directly control a large amount of money, like financial institutions.

Moreover, cybercrime encompasses a range of diverse forms, each with its own distinct motivations for hackers, including financial gain, seeking recognition, or seeking retribution. Cybercrimes have the ability to transcend geographical boundaries and can take place on a worldwide scale. The incidence of particular categories of cybercrime may differ across countries, as it is influenced by factors such as economic conditions, levels of internet usage, and overall development. (Boussi et al., 2024).

In 2020, the United States of America (USA) received 791,790 cybercrime complaints, resulting in a total economic loss of 4.2 billion dollars. The most frequent internet crimes were phishing, scams, and extortion (World Economic Forum, 2021). However, cybercrime costs the United Kingdom's economy £27 billion annually. Cybercrime undermines the economic stability of the country and poses a threat to its national security (May, 2022). Similarly, the number of cybercrime offenses in China is rapidly increasing. From 2017 to 2021, more than 660,000 defendants were involved in cybercrime cases across the country; most of the defendants were aged between 18 and 40. Despite an array of laws and enforcement measures, cybercrime in China appears to be getting worse, and cybercriminals are becoming younger (Wyk, 2023). Globally, over 477 million internet consumers have been victims of cybercrime, with nearly 330 million cases in the past 12 months alone (Lim, 2021).

Phishing is a prevalent form of cybercrime that targets the financial sector in many countries. The strategies used may differ across industrialized and developing nations. Nevertheless, the constant influence of this phenomenon frequently results in financial losses. The authors investigation, employed a dataset containing 48 characteristics from 5,000 phishing webpages and 5,000 genuine webpages in order to forecast the status of websites as either phishing or legitimate. This method attained a remarkable accuracy rate of 98%. (Boussi et al., 2024).

Machine learning and present artificial intelligence (AI) techniques have been successfully employed in many practical applications (AlZu'bi et al., 2022) (Aqel et al., 2021). Several writers have made significant contributions to the field of predicting phishing websites and strengthening defenses against cybercrime.

In the digital age where technology infuses every aspect of society, cybercrime has emerged as a profound challenge, creating complex dilemmas for law enforcement agencies worldwide. The objective of enhancing security is to identify cyberattacks on the network using a soft computing environment, (Thomas et al., 2023). Nagunwaet al., (2022) proposes a machine learning-based approach for detecting phishing websites using a novel set of features. To enhance efficiency in anti-phishing techniques, Bahaghighat et al., (2023) presents an improved predictive model based on machine learning, utilizing six different algorithms and Warraich and Morsi (2023), focuses on cyberattacks related to fast-charging stations and introduces a machine learning-based approach for early detection. The encroachment of these digital delinquencies has necessitated a robust response from law enforcement agencies, such as the Philippine National Police (PNP), to safeguard societal integrity and security (Dupont, 2019).

Cyber offenders often conceal their identities behind their computers, making anyone worldwide a potential suspect. Hence, dealing with it requires police expertise and skills, as the global nature of the internet poses significant challenges to policing cybercrime. Previous studies illustrated that police officers lack the technical skills to fight against cybercriminals. Police forces continue to enhance their ability to stop cybercrime through specialized cybercrime units (AKDEMİR & Bürke, 2020).

When a crime occurs and injures a victim, it is the plaintiff who files a lawsuit and notifies

the judiciary. He files a criminal report or lawsuit, thus providing evidence of what happened and then the police and prosecution decide on his case. Investigating Internet Crimes is complicated. If a complaint received is about data found on a website the investigator needs to get clear and concise information as to the website involved in the complaint. Forensics comes into play after the commission of any kind of crime, depending on whether it is murder, rape, traffic offense, etc. Digital forensics refers to the scientific acquisition, analysis, and preservation of data contained in electronic media whose information can be used as evidence in a court of law. All evidence found is taken and examined in laboratories and other appropriate places, and if there is evidence of a criminal offense, a file is prepared. After collecting the entire file with evidence against the defendant, the investigation is transferred to criminal proceedings. (Arifi et. al., 2020).

As per Lexology, the Internet Organized Crime Threat Assessment Report ("the Report") from Europol's European Cybercrime Center (EC3) in 2019 talked about how cybercriminals do their work and how these crimes threaten society (Miralis & Miralis, 2020). The report talks about the five main problems: losing data or location; problems with national law systems; problems with working with other countries; and problems with public-private partnerships (Miralis & Miralis, 2020). Probably not, but prosecutors should learn how to understand digital evidence and use it in court. They don't need to learn how to find and keep digital evidence safe. This means that the costs of teaching lawyers how to use and collect digital evidence must be added to the costs of teaching police how to collect and store digital evidence. Cybercrime is also hard to police because police officers don't have the right skills. Investigating these kinds of crimes usually requires specialized technical knowledge and skills. At the moment, there aren't many signs that police have the right training and skills, but progress is being made, mostly by creating specialized officers and units (Steinmetz & Yar, 2019, p. 18).

UNCTAD says that of the 154 countries that have passed cybercrime laws, the pattern varies by area. Europe has the highest adoption rate (93%), while Asia and the Pacific has the lowest (55%). (UNCTAD, 2020).

Section 303b of the German Criminal Code talks about computer sabotage. It says that anyone who messes with someone else's data processing operations that are very important to them by destroying, damaging, making unusable, removing, or changing a data processing system or a data carrier can be jailed for up to five years or pay a fine. (German Penal Code, or Strafgesetzbuch, or StGB).

Specifically, article 278 of the "On damages" section says that anyone who gets data, written or electronic documents, computer media, or other items related to these things in order to find out a company secret, or who uses any of the tools or methods listed in Section 1 of Article 197, will be punished with two to four years in prison and a fine of twelve to twenty-four months (Criminal Code of the Kingdom of Spain, 1995 as of 2013).

Cybercrime is covered in Chapter 28: "Illegal Access to Computer Information." "Illegal access to legally-protected computer information, if this deed involved destroying, blocking, changing, or copying computer information, shall be punished with a fine of up to two hundred thousand rubles, or with corrective labor for up to one year, or with restricting freedom for up to two years, or with making the person work for free for up to two years, or with deprivation of freedom for the same amount of time" (The Criminal Code of the Russian Federation No. 63-Fz Of June 13, 1996, pp.135–136). It also talks about cybercrime in two other articles: "Article 274 Violating the Rules for Operation of the Facilities for Computer Information Storage, Processing and Transmittance and of Information-Telecommunication Networks" (The Criminal Code Of The Russian Federation No. 63-Fz Of June 13, 1996) and "Article 273 Creation, Use, and Dissemination of Harmful Computer Programs."

Some parts of Article 251 of the Criminal Code of the Republic of North Macedonia talk about cybercrime and using computer programs for bad things. It talks about "Damage and unauthorized entry into a computer system." This section says that someone can get a fine or up to three years in prison if they delete,

change, damage, hide, or otherwise make unusable computer data, a program, or a device for maintaining the information system. They can also get in trouble for using the computer system, data, program, or computer communication.

Other laws in the Criminal Code of the Republic of North Macedonia (2002) that deal with hacking are Article 251-a, which says "Making and importing computer viruses," and Article 251-b, which says "Computer fraud."

The United Nations Convention against Transnational Organized Crime (UNTOC) and its three protocols include the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, the Additional Protocol to the Convention on Cybercrime Concerning the Criminalization of Acts of a Racist or Xenophobic Nature Committed Through Computer Systems, the Inter-American Convention on Mutual Assistance in Criminal Matters, and the European Convention on Mutual Assistance in Criminal Matters. It is said that the Council of Europe agreement on Cybercrime and its Protocol is the most important agreement. Also, states are being told how to deal with these crimes by rules that are being made, and foreign cooperation is being used more and more.

The EU didn't have a program just for cybercrime until 2007. A communication from the European Commission in 2001 was about information security and fighting computer-related crime of that year. So, the European Union has taken steps to make sure that its member states can police crimes like child pornography, racism and xenophobia, attacks on computer systems, and terrorism that happen online.

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

More thoroughly, Philippines suffers from the same problems as many other countries in fighting cybercrime. Online scams were the most common type of cybercrime in the country. Other cybercrimes include illegal access, computer-related identity theft, ATM/credit card fraud, threats, data interference, anti-photo and video voyeurism, computer-related fraud, online libel, and unjust vexation (CNN Philippines, 2023). Undoubtedly, these cybercriminals not only damage the reputation of the Filipino people but also steal their identities and embezzle their money. The Bankers Association of the Philippines reports that cyber fraud cost more than P1 billion in 2021, as criminals exploited emails, text messages, and social media to trick people into revealing sensitive data or personal information for credit card and debit card hacking. The annual cost of global cybercrime is projected to reach $10.5 trillion by 2025 if not addressed properly (The Philippine Star, 2022).

In recent years, the Philippines has made significant advancements in both public and private sectors by adopting cutting-edge technologies. However, as gadgets and applications become increasingly complex, cyber dangers have also evolved. Between January and August 2023, the PNP-ACG documented a total of 16,297 instances of cybercrime. However, the number of individuals apprehended in connection with these crimes is just 2%, which amounts to 397 people (CNN Philippines, 2023). The data indicates that the PNP-ACG is facing challenges in resolving cybercrime cases. As per Alexander K. Ramos, the Undersecretary of the Cybercrime Investigation and Coordinating Center (CICC), the primary explanation for the limited success in solving cybercrimes is the country's insufficient understanding, resources, and expertise in combating such offenses (Inquirer.net, 2023).

Swindling or fraudulent schemes aimed at tricking someone for personal gain, is the top cybercrime in the Philippines, Philippine National Police (PNP) Chief Benjamin Acorda said.

In a press conference at Malacañang on Tuesday, the top cop said that online scams, particularly swindling are the most committed cybercrime in the Philippines, accounting for 15,000 incidents.

Swindling, also known as estafa, may be penalized from six months to six years imprisonment, according to the Revised Penal Code (RPC).

Following swindling, the top five cybercrimes in the country, according to Acorda, are:

Illegal access - 4,000 cases
Identity theft - 2,000 cases
Credit card fraud - Almost 2,000

Meanwhile, cyber libel, which is similarly defined under the Cybercrime Prevention Act and the RPC, also has 2,000 cases, according to the PNP chief. (Philstar, 2024).

The National Bureau of Investigation (NBI) Cybercrime Division (CCD) did a great job by catching a 21-year-old IT student who hacked into San Beda University's website and students' accounts. With a Warrant to Search, Seize, and Examine Computer Data (WSSECD), the NBI-CCD agents were able to search the subject's home and take things like Paymaya cards, Blank cards, a skimming device, a laptop computer, iPhones, an iPad, a router, and more. There was a violation of Section 4 (a)(1) Illegal Access, Section 4 (a)(3) Data Interference, and Section 4 (a)(4) System Interference under Republic Act No. 10175, also known as the Cybercrime Prevention Act of 2012. The Regional Trial Court in Pasig City gave the WSSECD in this case. There is a rule called A.M. No. 17-11-03-SC, which gives warrants for cybercrime. One of these warrants is a WSSECD. Law enforcement can use it as a procedure when they are looking into cybercrimes and cases where they need to collect electronic proof. (cybercrime.doj.gov.ph 2020).

The Philippines' Taguig City - On October 15, 2020, a woman who made materials for child sexual exploitation (CSEM), such as live video streams, was given reclusion perpetua, which is the same as a life term. This means that 15 people have been found guilty of sexually exploiting children online during the community quarantine. These results were helped by the International Justice Mission (IJM).

The person was found guilty by Judge Elisa R. Sarmiento-Flores of Taguig City Regional Trial Court Branch 163 of breaking R.A. 10175 (Cybercrime Prevention Act) and R.A. 9775 (Anti-Child Pornography Act). The criminal was given a life term in prison and told to pay a P2 million fine. She was also told to give each of her three victims 500,000 pesos in moral damages and 100,000 pesos in exemplary damages.

This is the 15th sentence that IJM helped get during the community quarantine.

An Australian Federal Police officer who caught a child sex offender in 2015 brought the case to our attention. The criminal said that he had watched CSEM and livestreams of the Filipino abuser sexually abusing children. www.ijm.org (2020).

Cybercrime cases are defined and penalized under Republic Act No. 10175 or the Cybercrime Prevention Act.

The Cybercrime Prevention Act has been flagged by United Nations Rapporteur for freedom of opinion and expression Irene Khan on February 3 as it brings a “chilling effect” to journalists instead of being utilized for other cybercrime offenses.

On January 31, the PNP Anti-Cybercrime group recorded 2,999 cases of cyber identity theft in 2023, which is a 12.2% rise from the 1,402 cases logged in 2022.

In response to the uptick in cybercrime cases, the Department of Interior and Local Government said that it would formally train local police officers in detecting and preventing cybercrimes by establishing National Cybercrime Training Institute.

In January 2023, the PNP announced its focus on tackling the increase in cybercrime incidents in the country, labeling it as the "fastest-growing transnational organized crime" globally. (Philstar, 2024).

This study aimed to scrutinize the challenges faced by the PNP in resolving cybercrime cases, thereby contributing to the limited body of literature on the practical impediments encountered by law enforcement agencies in the Philippines. While previous studies have delved into various aspects of cybercrime prevention, there remains a gap in understanding the specific obstacles that hamper the effectiveness of law enforcement agencies, such as the PNP, in the context of the Philippines (Kemp, 2023).

Exploring this avenue is imperative, as it not only enhances our understanding of the

prevailing challenges but also fosters the development of more nuanced and context-specific strategies to bolster the effectiveness of the PNP in combating cybercrimes. This study seeks to pave the way for more informed policy formulations and operational strategies through this investigation, thereby contributing to the broader goal of societal protection against the scourge of cybercrimes.

Statement of the Problem

The researchers sought in determining the challenges faced by the Philippine National Police Anti-Cybercrime Group of Region IV-A and IV-B in investigating cybercrime cases, specifically, it aims to answer the following questions:

1. What is the demographic profile of the respondents in terms of
   1.1 Age
   1.2 Trainings Attended
   1.3 Length of service in PNP-ACG
   1.4. Educational Attainment
2. What are the challenges faced by the Philippine National Police Anti-Cybercrime Group of Region IV-A and IV-B in addressing cybercrime offenses in terms of:
   2.1 Offenses against confidentiality, integrity and availability of computer data and systems;
   2.2 Computer-Related Offenses
   2.3 Content-Related offenses
   2.4. Other Offenses
3. What are the available digital forensic equipment in PNP-ACG Region IV-A and IV-B in terms of;
   3.1 Hardware
   3.2 Software
4. Is there a significant relationship between the demographic profile of the respondents and challenges faced by the PNP-ACG Region IV-A and IV-B in addressing cybercrime offenses in terms of offenses against confidentiality, integrity and availability of computer data and systems, computer-related offenses, content-related offenses and other offenses?
5. Is there a significant relationship between challenges faced by PNP-ACG Region IV-A and IV-B in addressing cybercrime offenses in terms of offenses against confidentiality, integrity and availability of computer data and systems, computer-related offenses, content-related offenses and other offenses?

Methods

This chapter focused on the discussion of the methods and procedures adhered to by the researchers. This chapter specifically explained the research design, research locale, research participants, research instruments, data gathering technique, ethical standards, and data analysis.

Research Design

Correlational studies sought to determine whether there are variations in the attributes of a community based on whether its individuals had been exposed to a specific occurrence in a real-life environment. Researcher/s limits control over the allocation of subjects into comparison groups or the administration of the intervention to specific groups. Alternatively, they establish a collection of factors, which includes a desired outcome, and thereafter examines the proposed connections between these variables. The result is referred to as the dependent variable, whereas the factors being examined for correlation are the independent variables. Correlational studies adopt an objectivist perspective, allowing for the definition, measurement, and analysis of variables to determine the presence of predicted relationships. Correlational studies encounter similar obstacles in research when it comes to their internal and external validity. The challenges of design decisions, selection bias, confounders, and reporting consistency are particularly significant. (Lau, 2017).

This study adopted a correlational research design. Research Questionnaire was used to obtain the data needed by the researchers. A quantitative correlation was deemed the most effective method for this research as it offered an objective approach and had the ability to identify statistically significant relationships or the strength of the association between the variables in the study. The goal of this study is to determine the challenges faced by the PNP-ACG Region IV-A and IV-B in investigating cybercrime cases as it existed at the time of the study.

Research Locale

This study was conducted in Police Regional Offices IV-A (CALABARZON) and IV-B (MIMAROPA).

Population and Sampling Technique

The respondents for this study were 60 uniformed personnel assigned to the Investigation Unit of the Philippine National Police in Regions IV-A and IV-B, for the reason that the said unit is responsible for investigating cybercrime cases in the aforesaid region.

This study made use of a purposive sampling technique to select the respondents. This study included PNP personnel assigned to the Investigation Unit as research participants, as these units were responsible for receiving complaints and conducting investigations related to cybercrime violations.

Research Instrument

The researchers in this study used a research-made questionnaire. The survey questionnaire used a 4-point Likert scale to obtain specific responses from the respondents. We will interpret the numbers on the Likert scale as "always," "often," "sometimes," and "never." The scale provided respondents with reliable information and consistent feedback.

Data Gathering Procedure

The following is the step-by-step process before, during, and after the survey. The researchers first issue informed consent to the participants, informing them of the procedures and conditions for answering the survey. Next, the researchers scheduled the survey administration for the respondents based on their availability. Third, the researchers decided to conduct the survey with the assurance that all researchers would be present during the actual data gathering. Furthermore, the respondents provided a survey questionnaire for review and preparation of their answers. Lastly, the researchers tallied the data gathered from the respondents' completed survey questionnaires.

Statistical Treatment of Data

The dissertation aims to address research questions. They have the potential to formulate original theories, elaborate on preexisting theories, or contribute to the current knowledge base in a particular discipline. Regardless of the objective, research questions are designed to tackle a research issue statement, which forms the core of a dissertation.

The insights that acquire from your research will assist you in formulating thoroughly supported responses to your inquiries. In order to obtain these findings, it is necessary to establish an investigation design for the dissertation.

The practice of systematically applying statistical or logical approaches to explain, demonstrate, summarize, and assess data is known as data analysis. The purpose of data analysis is to extract useful information from data and make decisions based on the analysis.

The data collected was interpreted and analyzed using fundamental statistical techniques. The respondents were categorized based on age, years of age, category of respondents, civil status, educational attainment, and training attended using frequency, percentage, and ranking. In addition, the average, which addresses the issues outlined in problems 2 and 3, was also utilized to interpret and analyze the respondents' responses regarding the level of challenges faced by the PNP Anti-Cybercrime Group in dealing with cybercrime offenses, specifically offenses related to the confidentiality, integrity, and availability of computer data and systems, computer-related offenses, content-related offenses, and other offenses. The problem statement 3 addresses the issue of the availability of hardware and software for the investigation of cybercrime and cyber-related offenses.

A one-way, or entirely randomized, experiment design is used when studying many levels of a factor and subjects are randomly assigned to these levels. ANOVA is a statistical method used to assess if the means of multiple populations are equal to test the significant difference to level of challenges faced by the PNP-ACG in addressing cybercrime offenses when grouped according to their demographic profile.

Moreover, the Pearson correlation coefficient can also be used to test whether the relationship among the challenges faced by PNP in

addressing cybercrime offenses against confidentiality, integrity and availability of computer data and systems, computer-related offenses, content-related offenses and other offenses is significant. A significance level of 0.05 alpha was set. The correlation between the compared variables was tested using the Pearson Correlation test.

Results and Discussions

This chapter presented, analyzed, and interpreted the collected facts and information. We presented the data in tabular form, providing textual explanations for each table. We presented the data in the order that addressed the specific study questions.

1. Socio-Demographic Profile of the Respondents

Table 1. Socio-Demographic Profile of the Respondents

Profiles / Variables		Frequency	Percentage
Age	21-30 years old	21	39.6
	31-40 years old	20	37.7
	41-50 years old	8	15.1
	51 years old and above	4	7.5
	Total:	**53**	**100**
Length of Service	Below 1 year	10	18.9
	1-5 years	36	67.9
	6-10 years	7	13.2
	Total:	**53**	**100**
Highest Educational Attainment	BS Criminology Graduate	29	54.7
	Computer Science Graduate	5	9.4
	IT Graduate	6	11.3
	BS Graduate	10	18.9
	Engineering/Master's Degree	3	5.7
	Total:	**53**	**100**
Trainings Attended	No Training	11	34
	1 -3 Trainings	6	11.3
	4-6 Trainings	29	54.7
	Total	**53**	**100%**

Table 1 presents the distribution of the fifty-three (53) respondents covered in this study with the corresponding socio-demographic profiles such as: age, length of service, highest educational attainment, and trainings attended.

The chosen respondents were diverse personnel of Philippine National Police (PNP) Anti-Cybercrime Group in various PNP stations.

Age: Almost four-fifths of the respondents belongs to the age range of 21 to 40 years old, which are comprised of 21 (39.6%) ages of 21-30 years old and 20 (37.1%) aged between 31-40 years old respectively. The rest which is lesser in number, 8 (15.1%) were in the age bracket of 41-50 years old, and the remaining 4 (7.5%) were on the age of 51 years old and above.

Length of Service: Majority 36 (67.9%) of the respondents has a tenure of 1-5 years at work, a fifth 10 (18.9%) served within a year, and a few 7 (13.2%) has a length of service of 6-10 years.

Highest Educational Attainment: Dominant 29 (54.7%) among the respondents has a BS degree in Criminology, followed by almost a fifth 10 (18.9%) were BS graduates. At least a tenth 6 (11.3%) were IT graduates and almost a tenth 5 (9.4%) were Computer Science graduate, and least in number 3 (5.7%) were Engineering graduates or had a Master's Degree.

Trainings Attended: More than half 29 (54.7%) of the respondents had attended at least 4 trainings and more, more than a third 18 (34%) had attended 3-4 trainings. Fewer in number 6 (11.3%) had no training. This showed that most of the PNP in charge of cybercrime offenses had enough trainings.

2. Level of Challenges Faced by the Philippine National Police Anti-Cybercrime Group in Addressing Cybercrime Offenses in Terms of Offenses Against Confidentiality, Integrity and Availability of Computer Data and Systems

Presented in table 2 was the level of challenges faced by the PNP Anti-Cybercrime Group in addressing cybercrime offenses in terms of offenses against confidentiality, integrity and availability of computer data and systems.

Considering the cybercrime offenses committed against confidentiality, integrity and availability of computer data and systems, the level of challenges encountered by the authorities was on a "Moderate" degree, with an overall mean score of 2.85. This middle category would represent the PNP facing a moderate level of challenges in resolving cybercrime cases. The difficulties and obstacles at this level were more substantial, requiring greater effort and resources to address the case.

Table 2. Level of Challenges Faced by the Philippine National Police Anti-Cybercrime Group in Addressing Cybercrime Offenses in Terms of Offenses Against Confidentiality, Integrity and Availability of Computer Data and Systems

STATEMENT INDICATORS	MEAN	VERBAL INTERPRE-
Offenses against confidentiality, integrity and availability of computer data and systems (*illegal access, illegal interception, data interference, system interference, misuse of device and cyber-squatting under Republic Act*		
Rapidly Evolving Technology: Cyber threats and techniques used by cybercriminals are constantly evolving. The PCRT needs to continuously update their knowledge and skills to keep up with these	3.34	Significant
Encryption and Anonymity Tools: Cybercriminals often use encryption and anonymity tools to hide their activities. This can make it	3.08	Significant
International Jurisdictional Issues: Cybercrimes can often be perpetrated from one country against targets in another. This can lead to jurisdictional challenges in investigating and prosecuting these	2.96	Moderate
Legislative and Legal Challenges: The legal framework related to cybercrimes may be complex and evolving. The PCRT may face challenges in interpreting and applying relevant laws and regula-	2.92	Moderate
Lack of Resources: This includes not only technological resources but also human resources. The PCRT may face challenges in acquiring and maintaining the necessary tools and personnel to ef-	2.79	Moderate
Collaboration and Information Sharing: Effective cybercrime investigation often requires collaboration and information sharing between different agencies and jurisdictions. Challenges may	2.77	Moderate
Digital Forensics Challenges: Investigating cybercrimes often involves digital forensics, which can be complex and time-consuming. The PCRT may face challenges in conducting thor-	2.74	Moderate
Capacity Building: Building and maintaining the capacity to respond to cybercrimes requires ongoing training and development. The PCRT may face challenges in ensuring that their personnel are	2.66	Moderate
Public-Private Partnership: Cybercrime prevention and response often require collaboration between the public and private sectors. The PCRT may face challenges in establishing and maintaining	2.64	Moderate
Awareness and Education: Many individuals and organizations may not be aware of the risks and preventive measures related to cybercrimes. The PCRT may face challenges in educating the public	2.60	Moderate
GRAND MEAN:	**2.85**	**Moderate**

Scale: 3.01 – 4.00 Significant
2.01 – 3.00 Moderate
1.00 – 2.00 Minimal

Among the 10 indicators, two of which gained a "Significant" level as assessed by the respondents. These were in the attributes related to Rapidly Evolving Technology (M=3.34) and Encryption and Anonymity Tools (M=3.08). This highest category would indicate the PNP faces significant, complex, and difficult challenges in resolving cybercrime cases. The obstacles at this level are substantial and may require major changes or enhancements to effectively overcome them.

On the other hand, the rest of the indicators had a "Moderate" level of predicaments faced with mean scores ranging from 2.60 to 2.96. Five areas which has the higher mean scores includes International Jurisdictional Issues (M=2.96), Legislative and Legal Challenges (M=2.92), Lack of Resources (M=2.79), Collaboration and Information Sharing (M=2.77) and Digital Forensics Challenges (M=2.74).

While three factors, which has the lowest scores, were in the areas of Capacity Building, Public-Private Partnership, and Awareness and Education, with mean ratings of 2.66, 2.64 and 2.60 respectively.

3. Level of Challenges Faced by the Philippine National Police Anti-Cybercrime Group in Addressing Cybercrime Offenses in Terms of Computer-Related Offenses

Shown in Table Three (3) is the level of challenges faced by the PNP Anti-Cybercrime Group in addressing cybercrime offenses in terms of computer-related offenses.

Table 3. Level of Challenges Faced by the Philippine National Police Anti-Cybercrime Group in Addressing Cybercrime Offenses in Terms of Computer-Related Offenses

STATEMENT INDICATOR	MEAN	VERBAL INTERPRETATION
Computer-Related Offenses		
Rapidly Evolving Technology: Cyber threats and techniques used by cybercriminals are constantly evolving. The PCRT needs to continuously update their knowledge and skills to keep up with these changes.	3.25	Significant
Encryption and Anonymity Tools: Cybercriminals often use encryption and anonymity tools to hide their activities. This can make it difficult for the PCRT to track and apprehend them.	3.11	Significant
International Jurisdictional Issues: Cybercrimes can often be perpetrated from one country against targets in another. This can lead to jurisdictional challenges in investigating and prosecuting these crimes.	2.96	Moderate
Legislative and Legal Challenges: The legal framework related to cybercrimes may be complex and evolving. The PCRT may face challenges in interpreting and applying relevant laws and regulations.	2.91	Moderate
Lack of Resources: This includes not only technological resources but also human resources. The PCRT may face challenges in acquiring and maintaining the necessary tools and personnel to effectively combat cybercrimes.	2.85	Moderate
Digital Forensics Challenges: Investigating cybercrimes often involves digital forensics, which can be complex and time-consuming. The PCRT may face challenges in conducting thorough and timely digital forensic investigations.	2.83	Moderate
Public-Private Partnership: Cybercrime prevention and response often require collaboration between the public and private sectors. The PCRT may face challenges in establishing and maintaining these partnerships.	2.72	Moderate
Collaboration and Information Sharing: Effective cybercrime investigation often requires collaboration and information sharing between different agencies and jurisdictions. Challenges may arise in establishing and maintaining these relationships.	2.70	Moderate
Awareness and Education: Many individuals and organizations may not be aware of the risks and preventive measures related to cybercrimes. The PCRT may face challenges in educating the public and raising awareness about these issues.	2.70	Moderate
Capacity Building: Building and maintaining the capacity to respond to cybercrimes requires ongoing training and development. The PCRT may face challenges in ensuring that their personnel are adequately trained and equipped.	2.66	Moderate
GRAND MEAN:	**2.87**	**Moderate**

Scale: 3.01 – 4.00 Significant
2.01 – 3.00 Moderate
1.00 – 2.00 Minimal

Collectively, in relation to the computer-related offenses, the level of challenges experienced by the uniformed personnel is on the 2.87 "Moderate" extent.

Two of the indicators gained a "Significant" nod among the respondents, these were in the categories of Rapidly Evolving Technology and Encryption and Anonymity Tools with the mean scores of 3.25 and 3.11 consequently.

All the rest of the statement indicators had a "Moderate" impression from the respondents: International Jurisdictional Issues (M=2.96), Legislative and Legal Challenges (M=2.91), Lack of Resources (M=2.85), Digital Forensics Challenges (M=2.83), Public-Private Partnership (M=2.72), Collaboration and Information Sharing (M=2.70), Awareness and Education (M=2.70), and Capacity Building (M=2.66).

4. Level of Challenges Faced by the Philippine National Police Anti-Cybercrime Group in Addressing Cybercrime Offenses in Terms of Content-Related Offenses

Displayed in table 4 is the level of challenges faced by the PNP Anti-Cybercrime Group in addressing cybercrime offenses in terms of content-related offenses.

Regarding the content-related cybercrime offenses made, the degree of challenges as tolerated by the respondents is on a "Moderate" level with the mean score of 2.83.

Again, two of the precept indexes acquired a "Significant" approval among the respondents, these were in the categories of Rapidly Evolving Technology and Encryption and Anonymity Tools with the mean scores of 3.21 and 3.06 accordingly.

The remaining touchstones had a "Moderate" impact on the respondents. These were on the statements: Legislative and Legal Challenges (M=2.91), International Jurisdictional Issues (M=2.89), Digital Forensics Challenges (M=2.83), Awareness and Education (M=2.75), Collaboration and Information Sharing (M=2.70).

Lack of Resources, Capacity Building and Public-Private Partnership got a 2.68 "Moderate" level imprint.

Table 4. Level of Challenges Faced by the Philippine National Police Anti-Cybercrime Group in Addressing Cybercrime Offenses in Terms of Content-Related Offenses

STATEMENT INDICATOR	MEAN	VERBAL INTERPRETATION
C. Content-Related Offenses *(Cybersex, child pornography, unsolicited commercial communication and libel under Republic Act 10175)*		
1. **Rapidly Evolving Technology**: Cyber threats and techniques used by cybercriminals are constantly evolving. The PCRT needs to continuously update their knowledge and skills to keep up with these changes.	3.21	Significant
2. **Encryption and Anonymity Tools**: Cybercriminals often use encryption and anonymity tools to hide their activities. This can make it difficult for the PCRT to track and apprehend them.	3.06	Significant
3. **Legislative and Legal Challenges**: The legal framework related to cybercrimes may be complex and evolving. The PCRT may face challenges in interpreting and applying relevant laws and regulations.	2.91	Moderate
4. **International Jurisdictional Issues**: Cybercrimes can often be perpetrated from one country against targets in another. This can lead to jurisdictional challenges in investigating and prosecuting these crimes.	2.89	Moderate
5. **Digital Forensics Challenges**: Investigating cybercrimes often involves digital forensics, which can be complex and time-consuming. The PCRT may face challenges in conducting thorough and timely digital forensic investigations.	2.83	Moderate
6. **Awareness and Education**: Many individuals and organizations may not be aware of the risks and preventive measures related to cybercrimes. The PCRT may face challenges in educating the public and raising awareness about these issues.	2.75	Moderate
7. **Collaboration and Information Sharing**: Effective cybercrime investigation often requires collaboration and information sharing between different agencies and jurisdictions. Challenges may arise in establishing and maintaining these relationships.	2.70	Moderate
8. **Lack of Resources**: This includes not only technological resources but also human resources. The PCRT may face challenges in acquiring and maintaining the necessary tools and personnel to effectively combat cybercrimes.	2.68	Moderate
9. **Capacity Building**: Building and maintaining the capacity to respond to cybercrimes requires ongoing training and development. The PCRT may face challenges in ensuring that their personnel are adequately trained and equipped.	2.68	Moderate
10. **Public-Private Partnership**: Cybercrime prevention and response often require collaboration between the public and private sectors. The PCRT may face challenges in establishing and maintaining these partnerships.	2.68	Moderate
GRAND MEAN:	**2.83**	**Moderate**

Scale: 3.01 – 4.00 Significant
2.01 – 3.00 Moderate
1.00 – 2.00 Minimal

5. Level of Challenges Faced by the Philippine National Police Anti-Cybercrime Group in Addressing Cybercrime Offenses in Terms of Other Offenses

Exhibited in table 5 is the level of challenges faced by the PNP Anti-Cybercrime Group in addressing cybercrime offenses in terms of other offenses.

In consideration to the other cybercrime offenses, it generally fared at a 2.85 "Moderate" level of perception amongst the respondents.

Rapidly Evolving Technology and Encryption and Anonymity Tools obtained a 3.25 and 3.09 "Significant" intensity as recognized by the respondents.

Whilst, the rest of the remaining assertions all got a "Moderate" appreciation from the respondents with mean scores ranging from 2.70 to 2.91. Legislative and Legal Challenges (M=2.91), International Jurisdictional Issues (M=2.83), Lack of Resources (M=2.79), Awareness and Education (M=2.74). Capacity Building, Digital Forensics Challenges and Public-Private Partnership all got a mean score of 2.72, and the least, Collaboration and Information Sharing got a 2.70 mean rating.

Table 5. Level of Challenges Faced by the Philippine National Police Anti-Cybercrim Group in Addressing Cybercrime Offenses in Terms of Other Offenses

STATEMENT INDICATOR	MEAN	VERBAL INTERPRETATION
D. Other Offenses *(Aiding/abetting in the commission of cybercrime and attempt in the commission of cybercrime under Republic Act 10175)*		
1. **Rapidly Evolving Technology**: Cyber threats and techniques used by cybercriminals are constantly evolving. The PCRT needs to continuously update their knowledge and skills to keep up with these changes.	3.25	Significant
2. **Encryption and Anonymity Tools**: Cybercriminals often use encryption and anonymity tools to hide their activities. This can make it difficult for the PCRT to track and apprehend them.	3.09	Significant
3. **Legislative and Legal Challenges**: The legal framework related to cybercrimes may be complex and evolving. The PCRT may face challenges in interpreting and applying relevant laws and regulations.	2.91	Moderate
4. **International Jurisdictional Issues**: Cybercrimes can often be perpetrated from one country against targets in another. This can lead to jurisdictional challenges in investigating and prosecuting these crimes.	2.83	Moderate
5. **Lack of Resources**: This includes not only technological resources but also human resources. The PCRT may face challenges in acquiring and maintaining the necessary tools and personnel to effectively combat cybercrimes.	2.79	Moderate
6. **Awareness and Education**: Many individuals and organizations may not be aware of the risks and preventive measures related to cybercrimes. The PCRT may face challenges in educating the public and raising awareness about these issues.	2.74	Moderate
7. **Capacity Building**: Building and maintaining the capacity to respond to cybercrimes requires ongoing training and development. The PCRT may face challenges in ensuring that their personnel are adequately trained and equipped.	2.72	Moderate
8. **Digital Forensics Challenges**: Investigating cybercrimes often involves digital forensics, which can be complex and time-consuming. The PCRT may face challenges in conducting thorough and timely digital forensic investigations.	2.72	Moderate
9. **Public-Private Partnership**: Cybercrime prevention and response often require collaboration between the public and private sectors. The PCRT may face challenges in establishing and maintaining these partnerships.	2.72	Moderate
10. **Collaboration and Information Sharing**: Effective cybercrime investigation often requires collaboration and information sharing between different agencies and jurisdictions. Challenges may arise in establishing and maintaining these relationships.	2.70	Moderate
GRAND MEAN:	**2.85**	**Moderate**

Scale: 3.01 – 4.00 Significant
2.01 – 3.00 Moderate
1.00 – 2.00 Minimal

6. Level of Challenges Faced by the Philippine National Police Anti-Cybercrime Group in Addressing Cybercrime Offenses as a Whole

Published in table 6 is the level of challenges faced by the PNP Anti-Cybercrime Group in addressing cybercrime offenses as a whole, considering above stated offense aspects.

Generally, the level of adversity being faced by our PNP Anti-Cybercrime Group personnel is on a "Moderate" level with a grand mean rating of 2.85.

With all of its 4 offense aspects also garnered a "Moderate" level with means ranging from 2.83 to 2.87, Computer-Related Offenses (M=2.87), Offenses Against Confidentiality, Integrity and Availability of Computer Data and Systems (M=2.85), Other Offenses (M=2.85), and Content-Related Offenses (M=2.83).

Table 6. Level of Challenges Faced by the Philippine National Police Anti-Cybercrime Group in Addressing Cybercrime Offenses as a Whole

STATEMENT INDICATOR	MEAN	VERBAL INTERPRETATION
Offenses Against Confidentiality, Integrity and Availability of Computer Data and Systems	2.85	Moderate
B. Computer-Related Offenses	2.87	Moderate
C. Content-Related Offenses	2.83	Moderate
D. Other Offenses	2.85	Moderate
OVERALL MEAN:	**2.85**	**Moderate**

7. Availability of Hardware and Software for the Investigation of Cybercrime and Cyber-Related Offenses

Laid out in Table Eight (8) is the availability of hardware and software as a tool for the investigation of cybercrime and cyber-related offenses.

Collectively, the availability of tools for cybercrime investigation, as recognized by the respondents, is at a mean rating of 2.65, which interpreted as "Moderately Available".

Out of the 14 resources, two of which has a "Highly Available" existence among the PNP Anti-Cybercrime Group offices. Prevalent availability of the following items: Alternative Recording Device (M=3.26) and Internet Connection (M=3.15).

While the rest of the 12 items were deemed to be "Moderately Available" per respondent feedback with the survey, with mean scores ranging from 2.19 to 2.98. Prevailing among the items were: Body Worn Cameras (M=2.98), Computer Systems (M=2.96), Video/CCTV Enhancement Software (M=2.83),

Cellebrite of UFED for Mobile Phones (M=2.74), and Storage devices for presentation of digital evidence in court (M=2.55) among others.

Three areas which got a lesser impact which also has a "Moderately Available" assessment were: Computer Forensics (Windows and Linux) UNCASE, Autopsy, FTK Imager (M=2.43), Anti-Static Containers (M=2.32), and Computer Forensics (Mac) (2.19).

The findings of the study denote that the PNP has access to a reasonable amount of specialized hardware and software tools that can be used to investigate and analyze various types of computer-related crimes, but these resources are not fully adequate or comprehensive.

Table 7. Availability of Hardware and Software for the Investigation of Cybercrime and Cyber-Related Offenses

Availability of Tools for Cybercrime Investigation	Mean	Verbal Interpretation
1. Alternative Recording Device	3.26	Highly Available
2. Internet Connection	3.15	Highly Available
3. Body Worn Cameras	2.98	Moderately Available
4. Computer Systems (desktop and notebook) used in the documentation of the investigation of cybercrime and cyber-related offenses	2.96	Moderately Available
5. Video/CCTV Enhancement Software	2.83	Moderately Available
6. Cellebrite of UFED for Mobile Phones	2.74	Moderately Available
7. Storage devices for presentation of digital evidence in court	2.55	Moderately Available
8. Other forensic tools that can be utilized for investigating cybercrime and cyber related offenses.	2.47	Moderately Available
9. Photo Enhancement Software	2.60	Moderately Available
10. Decryption Tools	2.53	Moderately Available
11. Network Analysis (Wireshark, etc.)	2.45	Moderately Available
12. Computer Forensics (Windows and Linux) UNCASE, Autopsy, FTK Imager	2.43	Moderately Available
13. Anti-Static Containers	2.32	Moderately Available
14. Computer Forensics (Mac)	2.19	Moderately Available
Grand Mean:	**2.65**	**Moderately Available**

Scale: **3.01 – 4.00 Significant**
2.01 – 3.00 Moderate
1.00 – 2.00 Minimal

Similarly, the PNP has some level of technological capabilities to conduct digital forensics, extract and analyze digital evidence, and utilize investigative tools for cybercrime cases, but the availability of these resources is not at an optimal level.

8. Significant Difference in the Level of Challenges Faced by the Philippine National Police Anti-Cybercrime Group in Addressing Cybercrime Offenses in Terms of Selected Profile

The following table presents the data with results of the number of scores of the compared variables using ANOVA, the sig-value, and a description that establishes whether the variable or the profile is significantly different in terms of the level of challenges faced. This is done in order to ascertain the significant difference in the level of challenges faced by the PNP-ACG region in addressing cybercrime offenses when grouped according to their demographic profile.

Table 8. Significant Difference in the Level of Challenges Faced by the Philippine National Polic Anti-Cybercrime Group in Addressing Cybercrime Offenses in Terms their Demographic Profile

Compared Variables	Mean	F-value	Sig-value	Remarks
Age:				
21-30 years old	2.78	0.585	0.628	Not Significant
31-40 years old	2.86			
41-50 years old	3.04			
1 years old and above	3.08			
Length of Service:				
Below 1 year	2.83	0.028	0.972	Not Significant
1-5 years	2.88			
6-10 years	2.86			
Highest Educational Attainment:				
BS Criminology Graduate	2.85	0.344	0.847	Not Significant
Computer Science Graduate	2.94			
IT Graduate	2.95			
BS Graduate	2.77			
Engineering/Master's Degree	3.18			
Relevant Trainings Attended:				
No Training	2.77	0.461	0.633	Not Significant
1-3 Trainings	2.97			
4-6 Trainings	2.92			

α = 0.05

Level of Challenges Faced and Age

Table 8 displayed the findings, which indicate that there was no statistically significant variation in the level of challenges encountered by PNP in dealing with cybercrime offenses based on age. It was evident from the F-value of 0.585 and sig-value of 0.628 that the results were not significant at the 0.05 alpha level. The outcome thus demonstrated that PNP faced comparable levels of difficulty.

Therefore, the null hypothesis—that there is no difference in the level of problems when respondents are classified according to age—was not rejected by the results.

Length of Challenges Faced and Length of Service

The results of the ANOVA, which were reflected in Table 9, indicate that there was no significant difference in the respondents' level of challenges when categorized based on length of service (F-value = 0.028, sig-value = 0.972). At the 0.05 threshold of significance, the result was not significant. As a result, it led the researcher to decide against rejecting the null hypothesis, which claims that the variables under comparison do not differ significantly.

The results suggested that respondents' perceptions of the degree of difficulties the PNP faces in combating cybercrime are not significantly influenced by their time of service.

Level of Challenges Faced and Highest Educational Attainment

The findings, as presented in Table 9, indicate that there was no statistically significant variation in the level of challenges when taking into account the respondent's highest educational attainment. The calculated F-value=0.344 and sig-value=0.847, which was higher than the 0.05 alpha level of significance, amply demonstrated this point and failed to reject the null hypothesis that there is no significant difference between the compared variables.

The results suggest that all group categories have the same degree of challenges meet, irrespective of the respondent's education.

Level of Challenges and Relevant Trainings Attended

Notably, the results of the ANOVA test on the same table (Table 9) showed that there was no significant variation in the respondents' level of difficulty in addressing cybercrime charges. The null hypothesis was not rejected, as evidenced by the computed F-value = 0.461 and sig-value = 0.633, which were not significant at the 0.05 alpha level. This further clarified why there was no variation in the respondent's assessment of the degree of difficulties faced with regard to the relevant trainings attended.

The challenges faced by the Philippine National Police (PNP) in resolving cybercrime cases appear to be consistent across different demographic and professional characteristics of the officers. This implies that the issues faced are systemic and not limited to specific groups within the PNP.

Correspondingly, the lack of significant differences across these grouping variables indicates that the challenges are widespread and not specific to certain age groups, levels of experience, or training backgrounds. This suggests that the issues are likely rooted in broader organizational, technological, or resource-related factors.

9. Significant Relationships among the Level of Challenges Faced by PNP Anti-Cybercrime Group in Addressing Cybercrime Offenses In Terms of Offenses Against Confidentiality, Integrity and Availability of Computer Data and Systems; Computer-Related Offenses; Content-Related Offenses and Other Offenses

Reflected in succeeding tables are the results of the correlation among the level of challenges encountered by PNP Anti-Cybercrime Group in addressing cybercrime offenses with respect to: Offenses Against Confidentiality, Integrity and Availability of Computer Data and Systems; Computer-Related Offenses; Content-Related Offenses; and Other Offenses.

Relationships between the Level of Challenges Faced And Confidentiality, Integrity and Availability of Computer Data and Systems

Table Nine (9) provides the association analysis between the level of Challenges Faced and Confidentiality, Integrity and Availability of Computer Data and System. In reference to Table 10, the outcome of r = 0.880 and sig-value=0.000 was highly significant at 0.05 alpha.

The result indicates that there is indeed a relationship among the two variables compared. The level of level of Challenges Faced and Confidentiality, Integrity and Availability of Computer Data and System, in some ways, has a relevant effect with each other.

Confidentiality Challenges: Cybercriminals may use sophisticated techniques to gain unauthorized access to sensitive data, such as hacking into computer systems, intercepting communications, or exploiting vulnerabilities.

The PNP may face difficulties in detecting, investigating, and gathering admissible evidence for these types of confidentiality breaches, especially as cybercriminals often cover their tracks and use advanced encryption methods.

Integrity Obstacles: Hackers may try to change, manipulate, or tamper with computer data and systems in order to accomplish their nefarious goals, which could include changing financial records, installing malware, or causing disruptions to 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.

Availability Challenges: Cybercriminals may use ransomware, denial-of-service attacks, or other forms of disruptions to deny access to computer systems and data to authorized users.

These availability assaults can seriously harm companies, governmental organizations, and individual users, therefore the PNP may find it challenging to react swiftly and minimize their effects.

The high correlation between these challenges suggests that the PNP is facing a complex, multifaceted problem that requires a comprehensive and coordinated response.

Addressing issues related to confidentiality, integrity, and availability often overlap and require a similar set of skills, tools, and resources.

Relationships between the Level of Challenges Faced And Computer-Related Offenses

In the same table, Table 9 provides the association analysis between the level of challenges faced and Computer-Related Offense.

In reference to Table 9, the outcome of r = 0.964 and sig-value=0.000 was highly significant at 0.05 alpha. The relationship between the level of challenges faced by the PNP and computer-related offenses was very high suggests that there was a strong, positive correlation between the difficulties and obstacles the PNP encounters in addressing cybercrime and the prevalence or volume of computer-related offenses.

As the level of challenges faced by the PNP increases, the incidence of computer-related crimes also tends to rise proportionally.

Relationships between the Level of Challenges Faced And Content-Related Offenses

Table 9 presents the correlation scrutiny between the level of challenges faced and content-related offenses. It showed that the overall result of r = 0.839 and sig-value =0.000 was significant at 0.05 alpha. The high correlation indicates that the challenges faced by the PNP in combating content-related offenses are directly linked to the perpetuation and expansion of these types of crimes.

The PNP's inability to effectively respond to and counter content-related crimes may be emboldening cybercriminals and allowing them to continue their illicit activities with minimal consequences.

Moreover, the challenges faced by the PNP, such as a lack of technical expertise, legal frameworks, or coordination with content providers, may be creating an environment that enables cybercriminals to engage in content-related offenses.

Relationships between the Level of Challenges Faced and Other Offenses

Shown in the same table was r = 0.916 and sig-value = 0.916. The result was highly significant at 0.05 level of significance, rejecting the null hypothesis of no relationships between these variables.

The highly significant correlation indicates that the challenges faced by the PNP in combating cybercrime were not limited to specific offense categories, but are broadly impacting their ability to address the overall landscape of computer-related criminal activities.

The PNP's shortcomings in responding to cybercrime are creating an environment that enables cybercriminals to diversify their illicit activities and target a wider range of victims and assets. The challenges faced by the PNP, such as a lack of specialized expertise, inadequate resources, or insufficient legal frameworks, may be allowing cybercriminals to exploit various vulnerabilities and engage in a wide array of computer-related offenses.

Table 9. Significant Relationship among the Level Challenges Faced by PNP in Addressing Cybercrime Offenses Against Confidentiality, Integrity and Availability of Computer Data and Systems, Computer-Related Offenses, Content-Related Offenses and Other Offenses

Compared Variables	r- value	Sig-value	Remarks
Level of Challenges Offenses Against Confidentiality, Integrity and Availability of Computer Data and Systems	0.880	0.000	Significant
Level of Challenges Computer-Related Offense	0.964	0.000	Significant
Level of Challenges Content-Related Offenses	0.839	0.000	Significant
Level of Challenges Other Offenses	0.916	0.000	Significant

$\alpha = 0.05$

Conclusions

The results and findings presented above lead to the following conclusions:

An insignificant level of challenges or barriers were experienced by the Philippine National Police - Anti-Crime Group (PNP-ACG) in Region 4 when they were attempting to carry out their duties and responsibilities. The fact that this is the case shows that the PNP-ACG encountered a number of important problems in that region; yet, these challenges were not of an extreme or severely in nature. The moderate degree of problems means that the Philippine National Police-Assistant Command Group in Region 4 was able to function and carry out its law enforcement duties in general, but they may have encountered hurdles that prevented them from being as effective and efficient as they could have been. It's possible that this could have resulted in certain gaps or restrictions in their capacity to deal with criminal activity and keep public safety in the region to the extent that they wished.

The fact that the level of availability of digital forensic equipment in the PNP-ACG was "Moderately Available" in terms of both hardware and software suggested that the PNP-ACG in the region has some access to the hardware and software that is required for conducting digital forensic investigations; however, there are likely gaps or limitations in the completeness and adequacy of these resources. This may make it more difficult for the Philippine National Police to adequately examine and handle digital evidence, which is becoming an increasingly critical area of focus in contemporary crime scenes. Within Region 4, the PNP-ACG has potential for development in terms of both the availability and the quality of the services.

As a result of the fact that demographic factors such as age, length of service, educational attainment, and training attended did not have a significant impact on the level of obstacles encountered, it can be inferred that the difficulties encountered by the Philippine National Police-ACG are not unique to that particular unit, but rather are likely indicative of wider issues or constraints within the larger law enforcement system or environment. It may be concluded that the challenges that are encountered are not a result of the personal traits or capabilities of the officers because the demographic aspects of individual personnel do not have a major influence on the level of difficulty that is encountered. However, the difficulties that the Philippine National Police-Agriculture Command (PNP-ACG) has encountered are most likely connected to structural, institutional, or resource-related concerns that are affecting law enforcement organizations in the region.

Given the strong correlation between the levels of issues and their components, it indicates that the challenges faced were not limited to specific areas but rather had a widespread

impact on the PNP-ACG's digital forensic skills and operations.

Recommendations

Based on the findings and conclusions cited from the study, the following recommendations are hereby recommended:

The substantial positive association between levels of problems and its components shows that the challenges faced were extensive, affecting all facets of the PNP-ACG's digital forensic skills and operations. It was highly recommended that the administrator conduct a full assessment faced by the PNP-ACG in Region 4, including resource constraints, operational difficulties, and coordination issues. Provide extra manpower resources and assistance to the PNP-ACG to help address the identified challenges. Provide more personnel, equipment, and funding; Enhance training and capacity-building programs; Improve coordination and information-sharing with other law enforcement agencies and implement measures to streamline operations, optimize processes, and enhance the overall effectiveness of the PNP-ACG in the region.

Considering that the PNP-ACG has a moderate level of access to digital forensic equipment in terms of both hardware and software, it is recommended that the PNP Headquarters modernize and increase the available digital forensic equipment for the region.

Ensure that the equipment using is up to date with the latest industry standards and best practices for digital forensic investigations. Train and improve the PNP-ACG staff's ability to use digital investigation tools and methods that work well.

The PNP-ACG together with Local Government Authorities may come up with a strategic action plan to deal with the systemic problems. This plan could include: Reviewing and improving how resources (people, tools, and money) are distributed across law enforcement units; Improving how law enforcement agencies work together, talk to each other, and share information; Making it easier for police officers to get training, grow professionally, and move up in their careers and build trust and work together between the PNP and ACG by doing more to involve the community and form partnerships.

Unit Heads may form partnerships with relevant stakeholders, like academic institutions, cybersecurity experts, and other law enforcement agencies, to use their knowledge and resources to improve the PNP-ACG's digital forensic capabilities.

References

Adopted by the State Duma on May 24, 1. A. (n.d.). The Criminal Code Of The Russian Federation No. 63-Fz Of June 13, 1996. Retrieved January 17, 2021

AlZu'bi, S., Aqel, D., & Lafi, M. (2022). An intelligent system for blood donation process optimization - smart techniques for minimizing blood wastages. *Cluster Computing,* 25(5), 3617–3627. https://doi.org/10.1007/s10586-022-03594-3

AKDEMİR, N., & Bürke , B. (2020). Retrieved from *International Security Congress Special Issue*, 113 - 134, 28.02.2020: https://dergipark.org.tr/en/pub/gbd/issu e/52738/695956#cited_by_articles

Aqel, D., Al-Zubi, S., Mughaid, A., & Jararweh, Y. (2021). Extreme learning machine for plant diseases classification: a sustainable approach for smart agriculture. *Cluster Computing*, 25(3), 2007–2020. https://doi.org/10.1007/s10586-021- 03397-y

Arifi, Dora & Arifi, Besa. (2020). Cybercrime: A Challenge to Law Enforcement. SEEU Review. 15. 42-55. 10.2478/seeur-2020-0016.

Back, S., & LaPrade, J. (2019). The Future of Cybercrime Prevention Strategies: Human Factors and A Holistic Approach to Cyber Intelligence. *The International Journal of Cybersecurity Intelligence and Cybercrime,* 2(2), 1–4. https://doi.org/10.52306/02020119kdhz8339

Bahaghighat, M., Ghasemi, M., & Ozen, F. (2023). A high-accuracy phishing website detection method based on machine learning. *Journal of Information Security and Applications,* 77, 103553.

https://doi.org/10.1016/j.jisa.2023.103553

Boussi, G. O., Gupta, H., & Hossain, S. A. (2024). A machine learning model for predicting phishing websites. *International Journal of Power Electronics and Drive Systems/International Journal of Electrical and Computer Engineering*, 14(4), 4228. https://doi.org/10.11591/ijece.v14i4.pp4228-4238

CNN Philippines. (2023, September 14). Retrieved from Around 2% of over 16,000 cybercrime cases probed led to arrests: https://www.cnnphilippines.com/news/2023/9/14/police-probe-cybercrime-cases.html

Criminal Code of the Republic of North Macedonia. (2002). Retrieved January 15, 2021, from Official Gazette of the Republic of Macedonia "No. 80/99, No. 4/2002, No. 43/2003, No. 19/2004, No. 81/2005, No. 60/06, No. 73/06, No. 7/08, No. 139 / 08, number 114/09, number 51/11, number 135/11, 185/.

Dupont, B. (2019). Enhancing the effectiveness of cybercrime prevention through policy monitoring. *Journal of Crime and Justice,* 42(5), 500–515. https://doi.org/10.1080/0735648X.2019.1691855

Europe, C. o. (2003, January 28). Additional Protocol to the Convention on Cybercrime. Retrieved January 18, 2021, from Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems: www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189

Europe, C. o. (2007). Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. Lanzarote: Council of Europe, Council of Europe Treaty Series-No. 201.

German Criminal Code Strafgesetzbuch – StGB. (n.d.). Retrieved from Criminal Code in the version published on 13 November 1998 (Federal Law Gazette I, p. 3322) as last amended by Article 2 of the Act of 19 June 2019 (Federal Law Gazette I, p. 844): https://www.gesetze-im internet.de/englisch_stgb/englisch_stgb.html

Inquirer.net. (2023, July 21). Retrieved from CICC: Protecting the Philippines from cyber threats: https://technology.inquirer.net/126198/cicc-protects-the-philippines-from-cyber-threats

Kemp, S. (2023). Exploring public cybercrime prevention campaigns and victimization of businesses: A Bayesian model averaging approach. *Computers and Security,* 127. https://doi.org/10.1016/j.cose.2022.103089

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

Lau, F. (2017, February 27). *Chapter 12 Methods for correlational Studies*. Handbook of eHealth Evaluation: An Evidence-based Approach - NCBI Bookshelf. https://www.ncbi.nlm.nih.gov/books/NBK481614/

Lim, J. (2021, July 20). www.techwireasia.com. Retrieved from Cybercrime is rising, and APAC users can do more to fight it: https://techwireasia.com/2021/07/cybercrime-is-rising-and-apac-users-can-do-more-to-fight-it/

Miralis, N. G., & Miralis, D. (2020, August 30). The 5 key challenges for law enforcement in fighting cybercrime. Retrieved January 17, 2021, from Lexology: https://www.lexology.com/library/detail.aspx?g=12513d17-cff3-4d8f-b7dccd91826f05d4

Nagunwa, T., Kearney, P., & Fouad, S. (2022). A machine learning approach for detecting fast flux phishing hostnames. *Journal of Information Security and Applications*, 65, 103125. https://doi.org/10.1016/j.jisa.2022.103125

Philstar.com February 6, 2024 Swindling tops list of cybercrimes in Philippines — PNP chief.

Secretariat, M. o.-G. (n.d.). Criminal codes - Criminal Code of the Kingdom of Spain

(1995 as of 2013). Retrieved January 16th, 2020, from Legislationline: https://www.legislationline.org/documents/section/criminalcodes/country/2/Spain/show.

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

Thomas, M., Gupta, M. V., Rajan, V. G., Rajalakshmi, R., Dixit, R. S., & Choudhary, S. L. (2023). Soft computing in computer network security protection system with machine learning based on level protection in the cloud environment. *Soft Computing*. https://doi.org/10.1007/s00500-023-08395-3

UNCTAD. (2020, April 02). UNCTAD. Retrieved January 17, 2021, from Cybercrime Legislation Worldwide: https://unctad.org/page/cybercrime-legislation-worldwide

Warraich, Z., & Morsi, W. (2023). Early detection of cyber–physical attacks on fast charging stations using machine learning considering vehicle-to-grid operation in microgrids. *Sustainable Energy Grids and Networks*, 34, 101027. https://doi.org/10.1016/j.segan.2023.101027

Wyk, B. v. (2023, August 23). China's cyber crime problem is growing. Retrieved from https://thechinaproject.com/2022/08/23/chinas-cyber-crime-problem-is-growing/

World Economic Forum. (2021, March 23). FBI report: How much internet crime cost the US in 2020. Retrieved from https://www.weforum.org/agenda/2021/03/fbi-report-shows-that-2020-was-the-worst-year-on-record-for-internet-crime/