INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH AND ANALYSIS

ISSN(print): 2643-9840, ISSN(online): 2643-9875

Volume 07 Issue 05 May 2024

DOI: 10.47191/ijmra/v7-i05-38, Impact Factor: 8.22

Page No. 2102-2106

Bridging the Gap between Criminology and Information Technology

Quimberly Rose P. Estrada[1], Dr. Kristine Soberano[2], Zillah R. Segue[3]

[1,2]State University of Northern Negros, Negros Occidental, Philippines

[3]Central Philippine State University, Negros Occidental, Philippines

ABSTRACT: This study aims to establish an essential connection between the fields of information technology and criminology, acknowledging the changing nature of crime in the digital era. Modern society is becoming increasingly dependent on technology, making it difficult for traditional criminological frameworks to understand and deal with the new types of cybercrime and digital deviance. The objective of this research is to study the relationship between criminology and information technology, with an emphasis on how technological improvements can be used to improve the knowledge of criminology students, prevention, and moderation of present-day criminal behavior. This study looks at the mutually beneficial connection between criminological theories and state-of-the-art information technology to offer a thorough and detailed framework for understanding the complexity of modern-day crime. It seeks to open up fresh possibilities for innovative ideas and remedies that successfully close the knowledge gap between criminology and the quickly changing field of technology-driven crimes.

KEYWORDS: information technology, cybercrime, criminology, innovation, gap

I. INTRODUCTION

The dynamic and significant aspect of the ever-evolving field of criminological studies is its relationship with information technology. The advantageous relationship that exists between these two domains possesses a great capacity to transform our understanding of criminal activity, its trends, and the effectiveness of preventive interventions. To improve knowledge, strengthen investigative techniques, and ultimately aid in the creation of stronger and more flexible tactics in the fields of criminal justice and law enforcement, this research aims to close the gap between criminology and information technology.

We leave digital footprints almost wherever we go because of the rapid advancements in information technologies, as well as the growing usage of mobile devices and sensors. Data are everywhere, mobile, and inexpensive today. They are not limited to spreadsheets that are rectangular anymore. The majority of websites that use data for different reasons have been affected by this. (Ozkan, 2019)

“Society and digital technology have become inseparable. The most developed countries are on the verge of true digitization: the Internet of Things, driverless vehicles, and smart cities, while even in the poorest of societies, mobile technologies are becoming ubiquitous.” (Colin, Davies & Murdoch, 2022). Indeed, we are living in a world where technology is evolving fast. Years ago, crimes may only have happened in the real world. Nowadays, crimes are even happening on the internet, also known as cybercrime. Who is authorized to stop or prevent these crimes from happening? They are the Philippine Anti-Cybercrime Group. The ACG is tasked with investigating and combating various forms of cybercrime, such as online fraud, hacking, identity theft, and other offenses related to information and communication technologies. And what related bachelor's degree should one take if he or she wants to be a part of this unit? Mostly those in the criminal justice field. However, the main focus of their program is mostly on the legal and ethical aspects of law enforcement and not information technology. So how can criminology students keep up with the fast evolution of technology in these modern times?

In 2018, according to Jaishankar, cyberspace was exploited by many fields of study; however, criminology was too late to explore this space and address the new form of criminality called cybercrime (p. 4). Cyberspace now has an extensive impact on many academic subjects due to the rapid expansion of technology and the internet in modern life. However, the expansion has surpassed the advancement of criminological and legal frameworks. Criminal justice did not keep up with the changing landscape of

cybercrime, whereas fields like cybersecurity, computer science, and information technology quickly arose to meet the difficulties of cyberspace.

"As the social web expanded, so too did the 'dark web' or 'deep web', a shorthand for the content on the Internet that is not indexed (and thus not searchable) by standard search engines and/or protected by layers of encryption and other security mechanisms." (Stratton et al., 2017) However, the fact that these deep networks are hidden creates the perfect setting for illegal content (such as material used to exploit children), criminal organizations (like terrorist or organized crime groups), and underground marketplaces (such as the trade of illegal drugs and viruses). To effectively combat these illegal activities on the internet, criminology students must also learn computer forensic techniques to investigate and analyze digital evidence, stay updated on cybersecurity threats and vulnerabilities, and understand the importance of data privacy laws and regulations. Given the rapid evolution of technology, criminology students must be encouraged to continue learning and staying updated on the latest developments in both criminology and information technology. By combining criminological knowledge with IT skills, students can better contribute to efforts aimed at combating cybercrime, particularly on the dark web.

Encouraging instructors to teach students about cybercrimes, rules and regulations, and investigations is one of the main obstacles to creating cybercriminology programs. The study of cyber criminology has grown significantly due to the advancements in computer science, information technology, and Internet science. The needs of the growing criminological field still need to be met by typical criminologists. They are not studying other subjects like Internet science and information technology, which also fall under the broad heading of cyber criminology. (Jaishankar, 2010)

As we study more thoroughly, it becomes clear that criminals' ways of operations are always being shaped by the rapidly changing technological world, which calls for a flexible and adaptable criminological framework. This research aims to provide insights to criminology students that not only improve their understanding of cybercrime but also inform the development of practical strategies and policies that address these digital dangers by addressing the gaps between criminology and information technology, and also for them to stay up to date with the most recent advancements in technology.

METHODS

Research and Design:

The researcher uses a descriptive quantitative research design to present how knowledgeable criminology students are when it comes to innovation and their gained knowledge about the basics of information technology and cybercrime.

Materials and respondents

45 Criminology students who had completed the cybercrime course assessed the instruments for their usability and it only lasted for a day. To collect information from criminology students, the researcher applies non-probability sampling. Based on the study's population and objective, it is selected. The target respondents can be easily reached in this scenario, which makes the sample useful.

Instrumentation

A modified survey was utilized to find out how much IT knowledge criminology students acquired. Sixteen questions covering the fundamentals of computers and the extent of their knowledge of cybercrime are included. The questions are evaluated from 1 (very unaware) to 5 (very aware).

Data Collection Procedure

Descriptive statistics like the mean are utilized to analyze the data collected. For the IT knowledge and cybercrime assessment, the range of the scale of interpretation for the variables measured was as follows;

4.20-5 – Very High
3.20-4.19 – High
2.60-3.39 – Moderate
1.80-2.59 – Low
1.79 – Very Low

RESULTS AND DISCUSSION

Knowledge of the Computer Basics

This part of the article presents the knowledge of criminology students with the basics of Information Technology. It demonstrates the respondents' perceptions of their level of IT knowledge.

To ascertain the respondents' familiarity with computer fundamentals, the students' IT knowledge was displayed, as shown in Table 1. Findings showed that the participants' awareness of computer basics is high (x=3.99, sd=.71). It shows that their awareness of the basic computer hardware is high (x = 4.44, sd =.58). It's interesting to notice that their awareness of fundamental software concepts is also high (x = 3.95, sd = .67), and their confidence in understanding computer security principles and measures is also high (x = 3.91, sd = .70). Moreover, their awareness regarding internet safety practices is very high (x = 4.2, sd =.72). In addition to this, their awareness of basic networking concepts (x = 3.8, sd =.72), familiarity with the basics of programming and coding (x = 3.4, sd =.89), awareness of common cyber threats (x = 4.1, sd =.64), and understanding of the concept of digital forensics (x = 4.73) are also high.

Table 1: Criminology student's knowledge of the basics of computers

Variable	SD	Mean (n=45)	Descriptive Interpretation
awareness of the basic computer hardware components such as CPU, RAM, and storage devices	0.58603	4.4444	HIGH
awareness of fundamental software concepts, including operating systems and common applications.	0.6727	3.9556	HIGH
confidence in the understanding of computer security principles and measures	0.70137	3.9111	HIGH
awareness regarding internet safety practices and precautions to protect personal information online	0.72614	4.2	VERY HIGH
awareness of basic computer networking concepts (e.g., IP addresses, routers, and protocols)	0.72614	3.8	HIGH
familiarity with the basics of programming and coding languages commonly used in cybersecurity	0.8933	3.4444	HIGH
awareness of common cyber threats such as malware, phishing, and ransomware	0.64979	4.1778	HIGH
understanding the concept of digital forensics and its role in investigating cybercrimes	0.73718	4.0444	HIGH
GRAND MEAN:	**0.711581**	**3.9972**	**HIGH**

Legend: Very Aware/Very High (4.20-5.00); Aware/High (3.40-4.19); Neither Unaware or Aware/Moderate (2.60-3.39); Unaware/Low (1.80-2.59); Very Unaware/Very Low (1.00-1.79)

The changing geography of modern society has placed the field of criminology at the center of innovative technical breakthroughs and classic investigative techniques. The study of criminal conduct, societal behaviors, and preventive measures is the main focus

of criminology; however, the integration of information technology (IT) has become increasingly vital in the fight for justice. Given the speed at, which technology is developing these days, criminology students cannot afford to disregard the importance of IT fundamentals. The ability of criminologists to solve and prevent crimes is improved by the integration of IT technologies and procedures, which makes data analysis, crime mapping, and digital forensics more effective.

Even though it might not be the main emphasis of criminology degrees, IT is an essential supporting element. To successfully navigate the complicated system of digital evidence, cybercrime, and surveillance technologies, criminology students need to brush up on their fundamentals in information technology. A solid foundation in information technology gives criminologists the ability to use technology ethically and responsibly, which helps them stay competitive in a field that is always changing. Educational programs may generate well-rounded individuals prepared to handle the complicated nature of modern crime by recognizing the close connection between criminology and IT. This will ultimately help to improve justice in our technologically-driven society.

Table 2: Criminology students' learning in the cybercrime course/subject

Variable	SD	Mean	Descriptive Interpretation
understanding of the lessons covered in the cybercrime course/subject	0.63802	4.1556	HIGH
understanding about how cybercrime ideas are used in actual applications	0.68165	4.1111	HIGH
familiarity with the software tools, web resources, and textbooks that are accessible for researching cybercrime	0.69048	3.9778	HIGH
understanding the present cybercrime course that tackles the difficulties and complications involved in the topic	0.68755	3.9333	HIGH
knowledge about resources available in assisting in overcoming obstacles related to studying cybercrime, such as counseling or tutoring services	0.65674	4.0222	HIGH
understanding of the cybercrime course's assessment techniques matches the learning objectives and your comprehension of the material	0.6727	4.0444	HIGH
satisfaction with the current teaching methods employed in the cybercrime course	0.67942	4.2444	VERY HIGH
awareness of technological challenges that can be faced during cybercrime studies, such as software issues, hardware limitations, or internet access problems	0.66058	4.1333	HIGH
GRAND MEAN:	**0.670893**	**4.0778**	**HIGH**

Legend: Very Aware/Very High (4.20-5.00); Aware/High (3.40-4.19); Neither Unaware or Aware/Moderate (2.60-3.39); Unaware/Low (1.80-2.59); Very Unaware/Very Low (1.00-1.79)

Table 2 presents the respondents' level of knowledge regarding the cybercrime course (subject).

The data indicates that their understanding of the cybercrime course/subject is high (x = 4.07, sd = .67). In its dimension, the respondents' understanding of the lessons covered in the cybercrime course/subject is high (x = 4.15, sd = .63). The same goes with their understanding about how cybercrime ideas are used in actual applications (x = 4.11, sd = .68); familiarity with the software tools, web resources, and textbooks that are accessible for researching cybercrime (x = 3.97, sd = .69); understanding the present cybercrime course that tackles the difficulties and complications involved in the topic (x = 3.93, sd = .68); knowledge about resources available in assisting in overcoming obstacles related to studying cybercrime, such as counseling or tutoring services (x = 4.02, sd = .65); understanding of the cybercrime course's assessment techniques match the learning objectives and your comprehension of the material (x = 4.04, sd = .67); and, awareness of technological challenges that can be faced during cybercrime studies, such as software issues, hardware limitations, or internet access problems (x = 4.13, sd = .66). While the respondents' satisfaction with the current teaching methods employed in the cybercrime course is very high (x = 4.24, sd = .66).

The digital world has completely changed the way that crime is seen, hence criminology students must learn more about cybercrime. With technology developing at an unprecedented rate, criminals have had to adjust their strategies to find new ways to take advantage of weaknesses in the virtual world. Cybercrime is the umbrella term for a variety of illegal behaviors, such as online fraud, identity theft, hacking, and cyberterrorism. For students studying criminology, understanding these digital risks is essential since it gives them the tools to stop and prevent modern criminal activity.

Cybercrime studies extend beyond the boundaries of traditional criminology, providing students with a broad understanding of the interconnection between the virtual and real worlds. Beyond geographical restrictions and legal borders, the digital environment serves as a refuge for illegal businesses. Students studying criminology need to understand the complexities of cybercrime to create tactics that will be useful in law enforcement, policy-making, and preventing crimes. Furthermore, because technology is used in criminal investigations, criminologists need to be knowledgeable about cybercrime to navigate the complicated world of digital evidence and ensure a complete and accurate understanding of illegal activity. All things considered, criminology students who want to address the changing face of criminal conduct in our more interconnected world need to have a solid understanding of cybercrime.

CONCLUSION

In summary, a promising and encouraging trend has been found in the research on bridging the gap between IT and Criminology at a university in Negros Occidental. The criminology students' impressive knowledge of IT and cybercrime abilities highlights the value of educational efforts that include digital in criminology curricula. In addition to giving students a comprehensive understanding of contemporary crime, the harmonious connection between IT and criminology prepares graduates as skilled professionals prepared to handle the challenges of the digital age.

The substantial level of IT proficiency among the criminology students in a university in Negros Occidental emphasizes how crucial it is for academic institutions to acknowledge and promote multidisciplinary collaboration. These students' combined knowledge of criminology and IT will surely help with more efficient crime prevention, investigation, and policy development when they enter the job. Institutions can expand on this accomplishment going forward by incorporating more IT elements into criminology curricula. This will ensure that upcoming generations of professionals are prepared to handle the dynamic difficulties presented by cybercrime in our rapidly changing technology environment.

REFERENCES

1) Colin, C. (2022, July). Bridging Information Security and Environmental Criminology Research to Better Mitigate Cybercrime.
2) JAISHANKAR. (2018, June). Cyber Criminology as an Academic Discipline: History, Contribution and Impact.
3) Stratton, G., Powell, A., & Cameron, R. (2017). Crime and justice in digital society: Towards a "digital criminology"? International Journal for Crime, Justice and Social Democracy, 6(2), 17–33.
4) Jaishankar, K. (2010). The Future of Cyber Criminology: Challenges and Opportunities1. International Journal of Cyber Criminology, 4(1/2), 26.
5) Ozkan, T. (2019, June). Criminology in the age of data explosion: New directions.