EXPLORING CHALLENGES IN CYBERCRIME INVESTIGATION AND PLAUSIBLE SOLUTION

AKMAL HAMDY BIN BAHARUDIN

UNIVERSITI TEKNOLOGI MALAYSIA

EXPLORING CHALLENGES IN CYBERCRIME INVESTIGATION AND PLAUSIBLE SOLUTION

AKMAL HAMDY BIN BAHARUDIN

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Master of Business Administration

Azman Hashim International Business School
Universiti Teknologi Malaysia

FEBRUARY 2022

DEDICATION

All praise and thanks is due to Allah SWT for His blessings, benevolence, and guidance at every stage of our life.

To my lovely mom and dad who have made endless sacrifices for the sake of my MBA completion,

To my beloved wife who is my pillar of strength and being understanding,

To my friends, and everyone who had contributed to this journey.

This research is dedicated to you..

ACKNOWLEDGEMENT

First and foremost, *Alhamdulillah,* I would like to thank God for His blessings throughout completing my research work successfully. I would like to express my heartfelt gratitude and appreciation to University Teknologi Malaysia (UTM) specifically Azman Hashim International Business School (AHIBS) for the opportunity given to me in carrying out my research project and finally I managed to complete my research with the guidance and encouragement from various individuals.

Secondly, I would like to thank my supervisor, Dr. Rafidah Othman for giving me the opportunity and trusted me to do my research and offered invaluable guidance and advice as well as willing to spend her valuable time with me despite her busy schedule throughout my journey in completing this thesis. I was profoundly influenced by her dynamism, motivation and spirit. Studying in her supervision was an honour and valuable experience. I am deeply thankful for what she has given me throughout the journey.

I would like to express my heartfelt gratitude to the entire officers of MCMC Investigation Department for their willingness to participate in my Action Research. Their assistance and support in data collection, as well as their participation and involvement in the department's intervention, means a lot to me.

Last but not least, I am forever thankful to both of my parents for their love and support, continuous care and unconditional prayers even though during the thesis completion journey, we were apart and barely see each other due to the pandemic. Also, I would like to thank all my siblings and families for their valuable and continuous support throughout this journey..

ABSTRACT

The rapid advancement of internet technology has led to an increase in cyber-crimes. In a typical scenario, online criminals manipulate loopholes within internet applications to commit crimes. There is also an ever-changing tactic employed by online criminals to avoid being detected or captured. Investigating Officers (IOs) of Malaysia Communication and Multimedia Commission (MCMC) also faced issues in cybercrime investigation such as unable to identify the culprit's due to anonymity, encryption, cross-border jurisdiction, quality of digital forensic and quality of witness. With this being said, this research aims to explore and understand these challenges at a deeper level within the cybercrime investigation sector. To achieve this research objective, this study employed a mixed method of qualitatively and quantitatively based on the research problems and gaps of research. The researcher has conducted a face-to-face interview with IOs and the manager at the Investigation Department of MCMC using semi-structured questionnaires. The potential contribution that can be made by this study is that it provides us with detailed knowledge of problems within cybercrime investigation. Understanding this aspect at a more conceptual level may clarify steps or the standard of procedures (SOPs) required to provide a plausible solution. As the intervention towards the quality of investigation has led the researcher to publish the handbook of cybercrime investigation namely "*Kesalahan Media Sosial: Manual Siasatan dan Pendakwaan*" in Cycle 1 and conducting the knowledge sharing session (technical training) for IOs to maximize the organisation knowledge-related effectiveness and achieve the research objective. This strategy could increase organizational performance and successfully shows significant impact towards IOs work efficiency. The potential managerial implication of this study is that - it enhances the quality of investigation procedures and ensures the output of tasks performed by IOs are in-line with the organizational stated Key Performance Index (KPI).

Keywords: Cybercrimes, Knowledge, Training

ABSTRAK

Kemajuan teknologi internet yang pesat menyebabkan peningkatan jenayah siber. Dalam senario biasa, penjenayah dalam talian memanipulasi aplikasi internet untuk melakukan jenayah. Terdapat juga taktik yang selalu berubah yang digunakan oleh penjenayah dalam talian untuk mengelakkan daripada dikesan atau ditangkap. Pegawai penyiasat Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) juga menghadapi masalah dalam menjalankan siasatan terhadap jenayah siber disebabkan oleh kesukaran untuk mengenal pasti penjenayah yang menyembunyikan identiti mereka, penyulitan, bidang kuasa rentas sempadan, kualiti forensik digital dan kualiti saksi. Dengan ini, kajian ini bertujuan untuk meneroka dan memahami cabaran ini pada tahap yang lebih mendalam dalam sektor penyiasatan jenayah siber. Untuk mencapai objektif kajian ini, kajian ini menggunakan kaedah campuran secara kualitatif dan kuantitatif berdasarkan masalah dan jurang penyelidikan. Kajian ini telah melakukan temuramah dengan pegawai penyiasat dan pengarah di Jabatan Siasatan SKMM. Potensi sumbangan yang dihasilkan melalui kajian ini adalah bahawa ia telah memberikan pengetahuan terperinci mengenai masalah dalam penyiasatan jenayah siber. Memahami aspek ini pada tahap yang lebih konseptual dapat menjelaskan langkah-langkah atau standard prosedur (SOP) yang diperlukan untuk memberikan penyelesaian yang munasabah. Bagi menghasilkan kualiti penyiasatan, kajian ini telah menerbitkan buku panduan penyiasatan jenayah siber yang bertajuk "Kesalahan Media Sosial: Manual Siasatan dan Pendakwaan" pada kitaran 1 dan mengadakan sesi perkongsian ilmu (latihan teknikal) kepada pegawai penyiasat untuk memaksimumkan keberkesanan dalam pengetahuan organisasi dan mencapai objektif penyelidikan. Strategi ini dapat meningkatkan prestasi organisasi dan mencapai kesan yang signifikan terhadap kecekapan kerja pegawai penyiasat. Potensi dalam kajian ini adalah - ia meningkatkan kualiti prosedur penyiasatan dan memastikan output dalam setiap tugasan yang dilakukan oleh pegawai penyiasat mencapai Indeks Prestasi Utama (KPI) dalam organisasi.

Kata kunci: Jenayah Siber, Pengetahuan, Latihan.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AGC	-	Attorney General Chambers
CMA 1998	-	Communications and Multimedia Act 1998
DPP	-	Deputy Public Prosecutor
EOA		Expert Opinion Analysis
FIR	-	First Information Report
I.O.	-	Investigating Officer
KPI	-	Key Performance Index
MACMA 2002	-	Mutual Assistance in Criminal Matters Act 2002
MCMC	-	Malaysian Communications and Multimedia Commission
MCO		Movement Control Order
NFA	-	No Further Action
SOP	-	Standard Operating Procedures
SPSS	-	Social Sciences Statistical Package

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Introduction

The internet has played a significant role in life. It created a paradigm for flexibility, creativity, and freedom to develop, expression, and information. Although information technology like the internet offers many benefits, it also has negative effects. When organisations and society become more technology-dependent and mass adoption of the internet, it will add various further dimensions to the problem. The rapid advancement of internet technology has led to an increase in cyber-crimes. In a typical scenario, online criminals manipulate loopholes within internet applications to commit crimes.

This chapter will cover the information about case company, problematic situation that occur in the organisation, research goals, research objective, research questions, the researcher's role, importance of the proposed research and term definition.

1.2 Information About the Company

The Malaysian Communications and Multimedia Commission (MCMC) is an agency under the Ministry of Communications and Multimedia, Malaysia which act as a regulator for communications and multimedia sector. The roles and responsibilities of MCMC is to implement and enforce the provisions under the Communications and Multimedia Act (CMA) 1998. The other primary functions of MCMC are supervising and monitoring social regulation on content-related issues.

Social media offences are part of cybercrimes and computer content crime which contravene the CMA 1998 such as sending obscene, offensive, menacing, false, and indecent material with intent to annoy, abuse, threaten or harass another person. The study explores with the aim of understanding cybercrime issues and the challenges of cybercrimes investigation faced by MCMC IOs.

It is important to study the MCMC practice of cybercrime investigation to achieve the research objective. Currently, there are only five IOs under Investigation Department of MCMC and 48 Authorised Officer in various departments in MCMC which involved in cybercrime investigation whereby their roles and tasks are dealing with all complaints received by the public based on the laws and regulations stipulated as well as the Standard Operating Procedures (SOP).

The process of investigation starts from receiving the First Information Report (FIR) as the written complaints made by public to MCMC to initiate an investigation. There are sufficient provisions of criminal laws like the Criminal Procedure Code and Evidence Act 1950 that allows IOs to acquire pieces of evidence from any person. (Nawawi, A. and Salin, (2018). For MCMC, the provision used is under section 254 of CMA 1998. IO will identify the culprits and seize the documentary or digital evidence under section 247 or 248 of CMA 1998. The telecommunication devices seized will be sent to the digital forensic lab for analysis to ensure whether the culprits have committed to an offense. Upon completion, IO will brief the case to the Deputy Public Prosecutor (DPP) from Attorney General Chambers (AGC) for decision whether to prosecute the culprits in court or vice versa.

1.2.1 External Environmental Analysis

PESTEL analysis has been used to analyze the organization external and internal perspectives of political, economic, socio-cultural, technology, environment and legal.

Table 1.1 PESTEL Analysis

PESTEL Analysis	
Politic	• Political instability in Malaysia due to the unexpected change of government has affected the organization structure and policy. The changing of leadership frequently will disrupt the vision and mission planned. • A group of individuals' dissatisfactions with the Malaysian government policies and regulations can lead to a net strike attack on government websites. • Conflicts between Malaysia and other countries may result in cyber warfare wherein the Malaysian hackers may take into Malaysian government websites under their control and post-inflammatory messages. • During an inter-national territorial conflict, hacker activists may use government websites to defame other countries or start a botnet attack.
Economy	• Economic espionage, theft of trade secrets is one of the biggest cybercrime challenges for the country. • Covid-19 has resulted in an Economic slowdown affecting many professionals who lose jobs and a significant amount of money in the stock market, leading professionals to resort to cybercrime. • Covid-19 pandemic has affected the economic stability and thus, the operational expenses such as training, facility and equipment budget become disorganized.
Social	• There are a lot of social cases investigated by MCMC such as sending obscene and offensive content through social media platform. • As the organization faced the financial implication and political instability, it will affect the investigative task which led to unsuccessful outcome. • Social media or social networking sites are used by multitude of people every day. It has become a massive platform for cybercriminals for hacking private information and stealing valuable data. • Fake online identities, mostly leading to cheating cases, cannot be controlled with cybercrime laws. • People may lose a sense of trust and safety from online mediums. • People do not report cyberbullying and harassment cases easily. • Online trafficking is another kind of cybercrime. Online trafficking may be in drugs, human beings,

PESTEL Analysis	
	arms, ammunition, weapons, and wildlife, etc. is challenging to track.
Technology	• The organization needs the current software and hardware to combat cybercrime issues. However, the price of the system is costly and mostly produced by oversea. • Besides that, the system cannot accessible by everyone, exposed to data intrusion and unethical behavior. • Cybercrime incidents may continue to increase with the advent of 5G technology and growth opportunities in the Internet of Things. • Cyber officers are required to be updated and experienced with the rapid adoption of machine learning and artificial intelligence tools with an increasing dependency on software, hardware, and cloud infrastructure.
Environment	• As MCMC IOs faced with various challenges while conducting investigation, there are safety and health risks that need to be emphasized. • Cybercrime can result in loss of control of critical equipment and warning systems and has the potential to cause damage to human health and the environment from catastrophic spills, waste discharges, and air emission.
Legal	• The existing laws and procedures of Communications and Multimedia Act 1998 are generally insufficient for MCMC to resolve the cybercrimes problems when it comes to cross-border jurisdiction. As most of the information operates outside the country, IOs needs to comply with the Mutual Assistance in Criminal Matters Act 2002 to get the information. • Security forces and Law enforcement personnel are not equipped to tackle high-tech crimes. • The private sector often holds the ability to provide law enforcement with crucial data to facilitate investigations and help to dismantle criminal infrastructures. Public-private collaboration is important yet there is no defining legal framework stating how the private sector shall cooperate with law enforcement while also maintaining the privacy or rights of their customers.

1.2.2 Internal Environmental Analysis

This study will identify problems by providing several steps to analyse causes of the problems, alternatives, assessment, and recommendations to be addressed. The increasing number of social media offenses shows the urgent need for MCMC to resolve cybercrime problems. Based on the observation found that MCMC IOs has strength of legal provision to investigate cybercrimes related to social media offenses as power provided under section 246 of CMA 1998 (Powers to investigate). However, there is a weakness whereby the outcome of the investigation doesn't meet the successful result and organizational stated Key Performance Index (KPI).

Table 1.2 SWOT Analysis

SWOT Analysis	
Strength	• MCMC IOs has the power to investigate under section 246 of CMA 1998. • The commitment of officers to the Department's mission and goals keeps the morale boosted. • There are expert officers who have years of experience in solving cybercrime. Their knowledge and expertise will help in the training and development of new officers.
Weakness	• Low rate of cybersecurity awareness and preparedness among the general public. • Lack of global investigation support services and global cybersecurity standards. • The funds allocated to MCMC are not enough to train personnel with the updated technology advancements. A low budget restricts the quality of training, hires more officers, and provides a well-developed facility with updated technology systems. • Collective reports of security breach or compromise incidents allow concerned authorities to develop new policies and procedures. However, many companies are reluctant to hand over or report breach details due to fear of commercial or legal liabilities. • Having no place of penalties in legislation about cyberbullying and harassment in social media

SWOT Analysis	
	platforms which are correspondences of crimes made in real life.
Opportunity	• By providing an educational platform in the field of cybersecurity and information system, more digital security start-ups may take the stage and develop innovative products and services that will reinforce online security. • Development of an internal leadership and management program aimed at developing current and future tech leaders. Also enhanced partnership with the community.
Threat	• There is not a definite timeline of the execution or progress of the investigation, which leads to piling up of cases due to which cybercriminals remain lose for a more extended period. • There is no clear evidence of cybercriminals. Only the source of a cyber-attack can be tracked, but the person responsible for it is difficult to track and detect. • Lack of clarity in regulations for constantly emerging technologies may create an obstacle for handling cybercrimes. • Cybercriminals use technology tactfully for every cyber-attack leaving little or no connection with multiple cyber-attacks.

1.3 Problem statement

The rapid advancement of internet technology has led to an increase in cybercrime. It has affected a large multinational organisation down to individuals (Solon and Hern, 2017). There is a lot of implications of cybercrimes against a person, national security, and financial system stability (Jayasekara, S.D. and Abeysekara, I., 2019). According to the 2019 Official Annual Cybercrime Report by Cybersecurity Ventures stated that cybercrime is one of the biggest problems which cost the world in over $6 trillion annually by 2021, up from $3 trillion in 2015. Cybercrime costs include damage and destruction of data, loss of money, data theft

pertaining to personal identification, intellectual property, steal financial and credit card account, fraud and hacking. For example, a global cyberattack of ransomware, known as the WannaCry has infected more than 230,000 computers in over 150 countries (Solon and Hern, 2017) and hit organizations worldwide including two Malaysian companies (The Star-News, 2017). Cybercrime related financial is a global threat today because money is the main motive of most criminals (Jayasekara, S.D. and Abeysekara, I. (2019).

Available evidence suggests there are a variety of impacts that can result from cybercrime. Cybercrime can cause the victims to lose of their hard-earned money. For businesses, the data loss, damage or sabotage of the information system caused to reputational damage, lack of trusts among customers and loss of revenue. (Furnell, S. and Dowling, S. 2019). There is also concern about the potential for misuse of the internet by terrorists (Broadhurst. R, 2006), and the UNGA in its resolution 51/210 stated the risk of cyber-terrorists by using electronic or wire communication systems (Redo, 2004). The rapid advancement of the internet also offers the opportunity to obtain criminal knowledge such as how to manufacture bombs and narcotic drugs (Gabrosky. P, 2000).

MCMC IOs also faced challenges while conducting a cybercrime investigation. Based on the Investigation Department of MCMC statistics shows that out of 807 FIR investigated from year 2018 until 2021, social media offenses are the highest cases investigated constitutes 71% (576 cases) from the total cases investigated. However, only 83 cases (16%) have successfully achieved the result either charged in court of compounded, but 449 cases (78%) were closed and decided to No Further Action (NFA). The balance of 58 cases (10%) cases is still under investigation and 26 cases (4.5%) resolved by administrative action. The NFA cases is surely affected the organisation KPI of 80% successful outcome and 70% meets prescribed timeline within 100 days. Besides, MCMC also received bad perception from public, especially from the complainant due to the ineffective action in investigation. This is similar as what Nawawi, A. and Salin (2018) stated that public perceptions affect the image of the government as a whole.

The ever-changing tactic by the criminal has brought problems to MCMC IOs. In a typical scenario, online criminals manipulate loopholes within cyber applications to commit crimes. Therefore, IOs is unable to identify the culprits due to the problem of anonymity and encryption. Lack of knowledge and expertise among IOs also is the factor that obstacle IOs to achieve a successful result. The existing laws and procedures are generally insufficient for MCMC to resolve the cybercrimes problems when it comes to cross-border jurisdiction. As most of the information operates outside the country, IO needs to comply with the Mutual Legal Assistance in Criminal Matters Act 2002 to get information. However, it depends on the cooperation given by the respective countries. Another problem faced by MCMC IOs is lack of cooperation from witnesses to assist the investigation. The incredibility of witness has affected the investigation and time-consuming. Delays in receiving the information will give more time for culprits to hide the evidence.

1.3.1 Problem Diagnosis

The problem diagnosis will identify the possible root cause of cybercrimes problems in a set of hypotheses, conducting analysis and synthesize the conclusion to explore the problems of cybercrime investigation and providing them with a plausible solution to ensure future investigation become effectively and efficient. It is stated that the anonymity is the major factor that obstacle the investigation to achieve successful result and meets organisation KPI.

Besides, the other factor that contributes to the cybercrime problems is because of encryption, quality of digital forensic, cross-border jurisdiction and lack of witness cooperation to assist investigation. Hence, the problem is further diagnosed by using a Fishbone (Ishikawa) Diagram. The diagram was generated with the aim of identifying and grouping the causes which generate a quality problem. Gradually, the process has also been used to group in categories the causes of other types of glitches or problem which an organization confronts with.

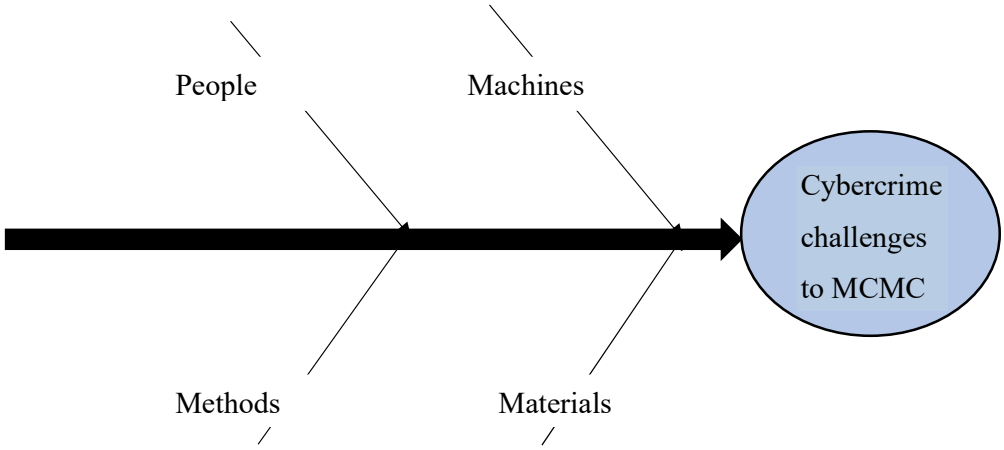

Figure 1.1 Fishbone Diagram Analysis for MCMC

- People – The experienced officers may not be updated with the latest technological advancements and cyber tactics of the cyber criminals. Inadequate training and shortage of officers affects the investigation process and resolving cases.
- Machines – The equipment used are computers with software, encryption tools, network tracking devices which are inadequate with changing criminal tactics.
- Methods – The MCMC rules, regulations and national laws dictates the cybercrime investigation process but the cross-border jurisdiction limits the information support and slows the investigation process.
- Materials- Data, records, and tracking results are the materials required for the investigation process. Any tampering or unreliable data can affect the investigation process.

1.3.2 Theoretical Gap

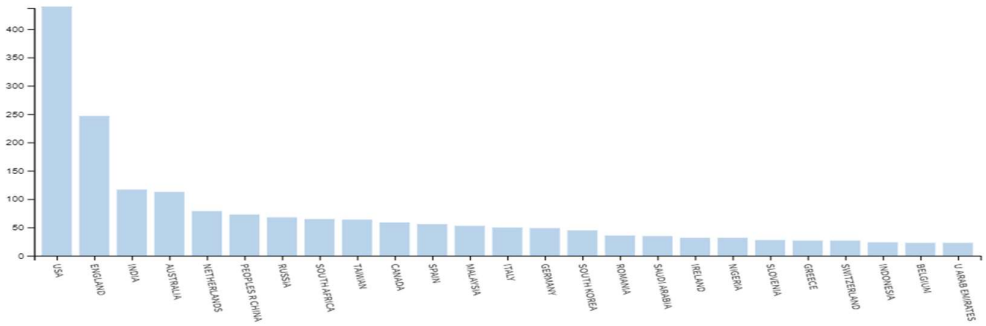

Figure 1.2 The bar graph analysis from Web of Science browser

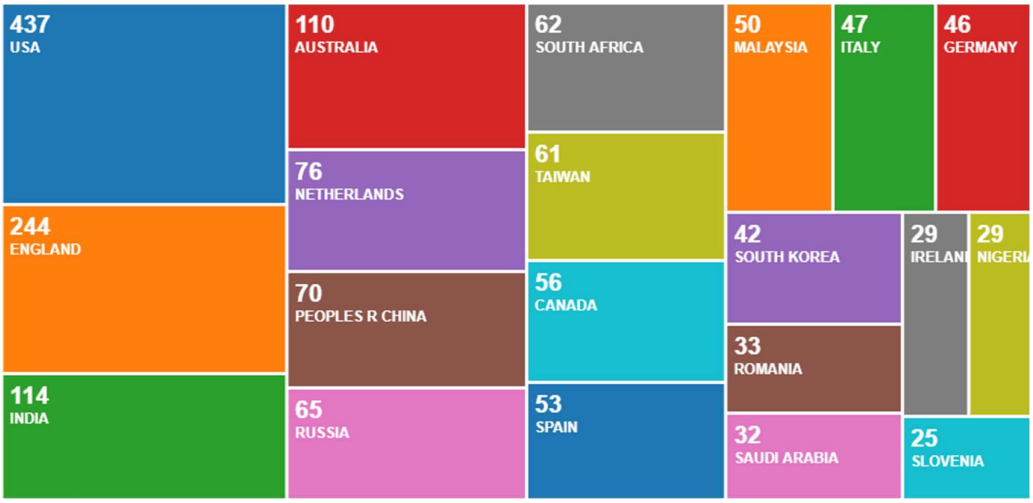

Figure 1.3 Tree Map Topic on cybercrimes

Based on the Figure 1.2 and Figure 1.3 shows the importance of the proposed study in the cybercrime field, based on the highest portion of the analysis box from the Web of Science browser. The topic in this study is relevant based on the highest total number of 1,952 record for the search of the study title. It means that the issues are significant globally and it is one of the major concerns for those who are involved in cybercrime investigation. However, in Malaysia, only 2.561% or 50 records of study title were found. In this regard, the cybercrime investigation knowledge needs to be explored further.

1.4 Research questions

This study is to explore and understand the cybercrimes investigation problems. The questions were prepared to be explained by the correspondents. More specifically, the study attempted to answer the following research questions:

Table 1.3 Research Question

Research Question	
RQ1	What are the main problems of cybercrimes investigation in MCMC?
RQ2	Do MCMC IOs have knowledge about cybercrimes investigation?
RQ3	What is the recommendation needed to resolve the problems?

Based on the outcome of the research questions, this study will implement an intervention that reliable can be resolving the problem of cybercrime. For Cycle 1, the researcher will publish the handbook of cybercrime investigation for IOs which will be assessed to ensure the effectiveness of the intervention. For Cycle 2, the researcher will conduct a knowledge sharing session (technical training) that can enhance IOs knowledge and skills, increase productivity, job performance, and achieve organisation KPI.

1.5 Research Objective

The research objective of the study is as follow:

Table 1.4 Research Objective

Research Objective	
RO1	To identify the main problems of cybercrime investigation in MCMC.
RO2	To measure the level of knowledge of MCMC IOs on cybercrimes investigation.
RO3	To provide the solution on cybercrime problems.

1.6 Researchers Role

This research will be using a mixed method of quantitatively and qualitatively based on the research problems and gaps of research. The research will be using an exploratory qualitative case study by using semi-structured questionnaires and conducting a face-to-face interview with the respondents from the manager and MCMC IOs whose can make the decision on the investigation processes that has potential to explain the issues at a deeper level. Based on the outcome of the research, this study will conduct the survey among the authorised officers of MCMC whose involved in cybercrime investigation to verify the issues raised. Furthermore, the research implements an intervention as a plausible solution that reliable can be resolving the problem of cybercrime. The intervention will be measured to ensure the effectiveness of the plan.

1.7 Importance of the proposed research

The potential contribution that can be made by this study is that it may provide detailed knowledge of problems within cybercrimes investigation and study the principles of training at a more conceptual level to clarify steps or the standard of procedures (SOPs) required to provide a plausible solution. This study can solve most of the country problems facing mankind – fraud, scam, fake news, child pornography and more. This study also can protect the people and online community while using the internet platform. Besides, the research will benefit MCMC as the regulator for internet service provider in Malaysia to create harmonious environment in online platform.

1.8 Definition of the term

To enhance understanding of this study, the definition was given for relevant terms as follows:

1. **Cybercrime:** crime committed against and through computer and internet to commit unlawful acts (Esposito, G. 2004)
2. **Anonymity:** unable to identify the real culprit which conceals the identity of the cyber-criminal (Laudon and Guercio Traver, 2004).
3. **Encryption:** method of converting the information (the plain text) or called as unencrypted data into the secret code (ciphertext) or called as encrypted data which hide the information (Bar-IIan, J,1996) such as encrypted messages and photographs (Maghaireh, Alaeldin Mansour Safauq (2009) by using the mathematical algorithm.
4. **IP Address:** An Internet Protocol address is a numerical address that is assigned to a computer and network to access the internet (Oerlemans, Jan-Jaap, 2017).

REFERENCES

Adelstein, F. (2006) 'Live Forensics: Diagnosing Your System Without Killing it First', Communications of the ACM, vol. 49, no. 2, p. 63-66.

Ajayi, Victor. (2017) Primary Sources of Data and Secondary Sources of Data. 10.13140/RG.2.2.24292.68481.

Bar-IIan, J. (1996) "Security issues on the Internet", The Electronic Library, Vol. 14 No. 1, pp. 37-42.

Bechara, F.R. and Schuch, S.B. (2020) "Cybersecurity and global regulatory challenges", Journal of Financial Crime, Vol. ahead-of-print No. ahead-of-print.

Bossler, A.M. and Holt, T.J. (2012) "Patrol officers' perceived role in responding to cybercrime", Policing: An International Journal, Vol. 35 No. 1, pp. 165-181

Bramley, P. (1989), "Effective Training", Journal of European Industrial Training, Vol. 13 No. 7

Braun, V., Clarke, V. (2006) Using thematic analysis in psychology. Qualitative Research in Psychology, 3, 77–101. doi:10.1191/1478088706qp063oa

Broadhurst, R. (2006) "Developments in the global law enforcement of cyber-crime", Policing: An International Journal, Vol. 29 No. 3, pp. 408-433.

Bryman, A., & Bell, E. (2015) Business Research Methods: Oxford University Press, USA.

Castillo-Montoya, M. (2016) Preparing for Interview Research: The Interview Protocol Refinement Framework. The Qualitative Report, 21(5), 811-831

Chave, D. (2017) "Proceeds of crime training: bringing it up to date", Journal of Financial Crime, Vol. 24 No. 3, pp. 437-448

Collis, J. and Hussey, R. (2003) Business Research: A Practical Guide for Undergraduate and Postgraduate Students, Palgrave Macmillan, Houndmills.

Comrey A, Lee H (1992) A first course in factor analysis. Hillsdale, NJ: Erlbaum.

Cohen, L., Manion, L., & Marrison, K. (2007) Research in education sixth edition. In: Newyork: Routledge.

Cranor, L. (1999) "Internet privacy", Communications of the ACM, Vol. 42 No. 2, pp. 29-31.

Ellen Nakashima, 'WhatsApp, most popular instant-messaging platform, to encrypt data for millions', The Washington Post, 19 November 2014 Available at: https://www.washingtonpost.com/world/national-security/whatsapp-worlds-most-popular-instant-messaging-platform-to-encrypt-data-for-millions/2014/11/18/b8475b2e-6ee0-11e4-ad12-3734c461eab6_story.html (accessed on 13 January 2021).

Esposito, G. (2004) "The Council of Europe Convention on cyber-crime: a revolutionary instrument?", in Broadhurst, R. (Ed.), Proceedings of the 2nd Asia Cyber Crime Summit, Centre for Criminology: University of Hong Kong, Hong Kong.

Etter, G.W. and Griffin, R. (2011) "In-service training of older law enforcement officers: an andragogical argument", Policing: An International Journal, Vol. 34 No. 2, pp. 233-245

Fayyad, F.A., Kukić, F.V., Ćopić, N., Koropanovski, N. and Dopsaj, M. (2020), "Factorial analysis of stress factors among the sample of Lebanese police officers", Policing: An International Journal, Vol. ahead-of-print No. ahead-of-print

Furnell, S. and Dowling, S. (2019) "Cybercrime: a portrait of the landscape", Journal of Criminological Research, Policy and Practice, Vol. 5 No. 1, pp. 13-26.

Gabrosky, P. (2000) 'Cybercrime and Information Warfare' in Australian Institute of Criminology Conference on Transnational Crime, Canberra, 9th Marc

Grabosky, P., Smith, R. and Dempsey, G. (2001) Electronic Theft: Unlawful Acquisition in Cyberspace, Cambridge University Press, Cambridge, p. 1.

Gritzalis, S. (2004) "Enhancing Web privacy and anonymity in the digital era", Information Management & Computer Security, Vol. 12 No. 3, pp. 255-287

Hart, Jeffrey. (2005) The G8 and the Governance of Cyberspace. 10.4324/9781315248035-9.

Hinduja, S. (2004) "Perceptions of local and state law enforcement concerning the role of computer crime investigative teams", Policing: An International Journal, Vol. 27 No. 3, pp. 341-357.

Jayasekara, S.D. and Abeysekara, I. (2019) "Digital forensics and evolving cyber law: case of BIMSTEC countries", Journal of Money Laundering Control, Vol. 22 No. 4, pp. 744-752

Jewkes, Y. and Yar, M. (2010) Handbook of Internet Crime, Willan Publishing, Cullompton.

Jilcha, Kassu. (2019) Research Design and Methodology. 10.5772/intechopen.85731.

Koksal, T. (2009) “The effect of police organization on computer crime”, PhD dissertation, Kent State University, Kent, OH

Levi, M. (2017) “Assessing the trends, scale and nature of economic cybercrimes: overview and issues”, Crime, Law and Social Change, Vol. 67 No. 1, pp. 3-20, doi: 10.1007/s10611-016-9645-3.

Liddicoat, J. and Doria, A. (2012) Human Rights and Internet Protocols: Comparing Processes and Principles, Internet Society, December, available at: www.internetsociety.org/doc/human-rights-andinternet-protocols-comparing-processes-and-principles (accessed 05 Jan 2021)

Maghaireh, Alaeldin Mansour Safauq, (2009) Jordanian cybercrime investigations: a comparative analysis of search for and seizure of digital evidence, Doctor of Philosophy thesis, Faculty of Law, University of Wollongong, 2009. https://ro.uow.edu.au/theses/3402

Mccarty, William & Zhao, Jihong & Garland, Brett. (2007) Occupational stress and burnout between male and female police officers: Are there any gender differences? Policing: An International Journal of Police Strategies & Management. 30. 672-691. 10.1108/13639510710833938.

Moitra, S. (2005) “Developing policies for cybercrime”, European Journal of Crime, Criminal Law and Criminal Justice, Vol. 13 No. 3, pp. 435-64

Nawawi, A. and Salin, A.S.A.P. (2018) "The influence of third party to the effectiveness of commercial crime investigation", Journal of Money Laundering Control, Vol. 21 No. 3, pp. 414-425

National Institute of Justice (2008) Electronic Crime Science Investigation: A Guide for First Responders, 2nd ed., NCJ 219941, Washington, DC

Nowacki, J. and Willits, D. (2019) "An organizational approach to understanding police response to cybercrime", Policing: An International Journal, Vol. 43 No. 1, pp. 63-76

Oerlemans, Jan-Jaap. (2017). Investigating Cybercrime. 10.13140/RG.2.2.19060.55686.

Ornelas, S. and Kleiner, B.H. (2003) "New developments in managing job related stress", Equal Opportunities International, Vol. 22 No. 5, pp. 64-70

Poulose, S. and Dhal, M. (2020) "Role of perceived work–life balance between work overload and career commitment", Journal of Managerial Psychology, Vol. 35 No. 3, pp. 169-183

Ramirez-Marin, J.Y., Barragan Diaz, A. and Acar-Burkay, S. (2020) "Is stress good for negotiation outcomes? The moderating effect of social value orientation", International Journal of Conflict Management, Vol. ahead-of-print No. ahead-of-print

Redo, S. (2000), "Crime as the growing international security threat: the United Nations and effective countermeasures against transnational economic and computer crime", UNAFEI Resource Material Series No. 55, Tokyo, Fuchu, Japan, pp. 117-39.

UNODC 2013 United Nations Office on Drugs and Crime (2013), 'Comprehensive Study on Cybercrime'

Rahi, Samar. (2017) Research Design and Methods: A Systematic Review of Research Paradigms, Sampling Issues and Instruments Development. International Journal of Economics & Management Sciences. 6. 10.4172/2162-6359.1000403.

Rider, B.A.K. (2001) "Cyber-Organised Crime — The Impact of Information Technology on Organised Crime", Journal of Financial Crime, Vol. 8 No. 4, pp

Ritella G, Rajala A. & Renshaw, P. (2020). *Using Chronotope to Research the space-time relations of learning and education: Dimensions of the Unit of Analysis.* Learning, Culture and Social Interaction. https://doi.org/10.1016/j.lcsi.2020.100381

Salifu, A. (2008) "The impact of internet crime on development", Journal of Financial Crime, Vol. 15 No. 4, pp. 432-443.

Solon, O. and Hern, A. (2017) "Petya' ransomware attack: what is it and how can it be stopped?", available at: www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attackwho-what-why-how (accessed 15 January 2021).

Tashakkori A, Creswell JW (2007) Editorial: The new era of mixed methods. Journal of Mixed Methods Research 1: 3-7.

The Star News (2017) "WannaCry strikes two Malaysian companies", available at: https://www.thestar.com.my/news/nation/2017/05/16/wannacry-strikes-two-

msian-companies-expert-first-organisation-infected-last-saturday/ (accessed 13 January 2021).

The 2019 Official Annual Cybercrime Report at https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report (accessed 15 January 2021).

US-CERT (2018) “Computer forensics”, United States Computer Emergency Readiness Team, Vol. 11 No. 28, available at: www.us-cert.gov/sites/default/files/publications/forensics.pdf

Wall, D.S. (2007b) “Policing cyber-crimes: situating the public police in networks of security withincyberspace”, Police Practice & Research: An International Journal, Vol. 8 No. 2, pp. 183-205

Westera, N.J., Kebbell, M.R. and Milne, B. (2011) "Interviewing witnesses: do investigative and evidential requirements concur?", The British Journal of Forensic Practice, Vol. 13 No. 2, pp. 103-113

Wiig, Karl Martin. (1993) Knowledge Management Foundations: Thinking about Thinking: How People and Organizations Create, Represent and Use Knowledge / K.M. Wiig.

Winkler, S. and Zeadally, S. (2015) "An analysis of tools for online anonymity", International Journal of Pervasive Computing and Communications, Vol. 11 No. 4, pp. 436-453

Yuvaraj, M. (2015), "Cloud libraries", Library Hi Tech News, Vol. 32 No. 8, pp. 19-23