STRATEGIES TO STRENGTHEN CYBERSECURITY PRACTICES IN OPEN-SOURCE INTELLIGENCE INVESTIGATIONS BY MALAYSIAN PHARMACY ENFORCEMENT OFFICERS

YAZID BIN KASANI

UNIVERSITI KEBANGSAAN MALAYSIA

STRATEGIES TO STRENGTHEN CYBERSECURITY PRACTICES IN OPEN-SOURCE INTELLIGENCE INVESTIGATIONS BY MALAYSIAN PHARMACY ENFORCEMENT OFFICERS

YAZID BIN KASANI

PROJECT SUBMITTED IN PARTIAL FULFILMENT FOR THE DEGREE OF MASTER OF CYBERSECURITY

FACULTY OF INFORMATION SCIENCE AND TECHNOLOGY
UNIVERSITI KEBANGSAAN MALAYSIA
BANGI
2024

STRATEGI MEMPERKUKUH AMALAN KESELAMATAN SIBER DI DALAM PENYIASATAN MAKLUMAT SUMBER TERBUKA OLEH PEGAWAI PENGUATKUASA FARMASI MALAYSIA

YAZID BIN KASANI

PROJEK YANG DIKEMUKAKAN UNTUK MEMENUHI SEBAHAGIAN DARIPADA SYARAT MEMPEROLEH IJAZAH SARJANA KESELAMATAN SIBER

FAKULTI TEKNOLOGI DAN SAINS MAKLUMAT
UNIVERSITI KEBANGSAAN MALAYSIA
BANGI

2024

DECLARATION

I hereby declare that the work in this thesis is my own except for quotations and summaries which have been duly acknowledged.

10 July 2024

YAZID BIN KASANI
P123139

ACKNOWLEDGEMENT

Praise to Allah the Almighty, the Most Merciful and Compassionate, for granting me the strength, perseverance, and guidance throughout this research journey.

I extend my heartfelt gratitude to my respected research supervisor, Dr. Rossilawati Sulaiman, for her invaluable guidance, unwavering support, and insightful feedback that have been instrumental in shaping this research.

I would like to express my sincere appreciation to all lecturers and instructors from Faculty off Information Science And Technology at Universiti Kebangsaan Malaysia and CyberSecurity Malaysia for providing the conducive research environment and resources necessary for the completion of this study.

I am deeply thankful to the Pharmacy Enforcement Branch Kuala Lumpur for their assistance and cooperation during the course of this research.

Special thanks to the financial sponsors, JPA under Hadiah Latihan Persekutuan (HLP) 2022, for their generous support, which has made this research possible.

I am indebted to all the postgraduate students of UKM Master of Cyber Security for their camaraderie, encouragement, and creating a supportive working atmosphere throughout my tenure at UKM.

Lastly, I extend my profound gratitude to my beloved wife, Ir. Nurfariza Jait for her undivided love, encouragement, and understanding throughout this journey. To my cherished mother, Cekgu Jah, I am forever grateful for all the prayers and blessings from afar, and to my dearest children, Natrah, Hannah, Arman, and Haris, I will make up for all the time I haven't been able to spend with all of you. To my late father, Kasani Yusuf, thank you for always being my endless source of motivation and inspiration. Al-Fatihah.

Thank you all for being a part of this journey. Amiin. Ya Rabbal Alamiin.

ABSTRAK

Ubat-ubatan yang tidak berdaftar dan palsu telah beredar dalam pasaran Malaysia selama beberapa dekad. Faktor-faktor seperti strategi penguatkuasaan undang-undang yang tidak berkesan, perkembangan teknologi internet, dan peningkatan permintaan ubat dan produk perubatan telah menyumbang kepada keadaan ini. Ini secara langsung telah mendedahkan pengguna di Malaysia kepada bahaya pengambilan ubat palsu dan tidak berdaftar yang boleh membawa kepada akibat yang berpotensi menyebabkan kematian. Agensi penguatkuasaan undang-undang yang bertanggungjawab untuk mencegah dan mengawal perdagangan ubat-ubatan yang tidak berdaftar dan palsu di Malaysia adalah Bahagian Penguatkuasaan Farmasi dengan sokongan Cawangan Penguatkuasaan Farmasi yang beroperasi di peringkat negeri. Salah satu usaha dalam memerangi perdagangan ubat tidak berdaftar dan palsu di Malaysia adalah dengan mengenal pasti dan menjejaki penjual produk tersebut agar tindakan undang-undang boleh diambil terhadap mereka. Salah satu teknik yang digunakan oleh pegawai penguatkuasa farmasi untuk menjejaki penjual adalah dengan membuat pemprofilan terhadap suspek dan juga dengan menggunakan kaedah Pengumpulan Maklumat Sumber Terbuka (OSINT). Pemprofilan oleh pegawai penguatkuasa farmasi dilaksanakan dengan merujuk kepada garis panduan yang dikeluarkan oleh Bahagian Penguatkuasaan Farmasi. Oleh kerana terdapat banyak kaedah dan teknik OSINT yang diterbitkan dalam tahun-tahun terkini, penyelidikan ini bertujuan untuk menilai amalan semasa Cawangan Penguatkuasaan Farmasi dalam penyiasatan OSINT berbanding model OSINT yang baru diterbitkan. Penyelidikan ini mengambil pendekatan kuantitatif dan kualitatif bagi mengumpul data melalui kajian susastera dan temu bual pakar. Model konsep proses kerja OSINT yang dihasilkan adalah berdasarkan bacaan piawai antarabangsa dan disemak bersama peraturan kerajaan dan garis panduan semasa. Komponen-komponen yang membentuk kitaran pengumpulan maklumat dan alur kerja dikenal pasti untuk disiasat. Data yang dikumpul melalui temu bual dianalisis menggunakan analisis frekuensi dan peratusan untuk mencapai peratus persetujuan pakar. Bergantung pada hasil analisis, model proses kerja OSINT dibangunkan dan dicadangkan berdasarkan komentar pakar, dengan fokus diberikan terhadap aspek keselamatan, termasuk ringkasan aliran kerja yang boleh digunakan oleh pegawai penguatkuasa farmasi. Model konsep proses kerja dan borang templat fasa persediaan yang dicadangkan ini membolehkan pengumpulan maklumat oleh pegawai penguatkuasa farmasi dilaksanakan secara lebih sistematik dan efektif, meminimumkan impak terhadap ancaman keselamatan

ABSTRACT

Unregistered and illegal medicines have been circulating in the Malaysian market for decades. Factors like ineffective law enforcement strategies, the expansion of internet technologies, and increasing demands for medicine and medical products have exacerbated the situation. This will directly expose consumers in Malaysia to the danger of consuming substandard and falsified medicines that can potentially have fatal consequences. The law enforcement agency that is responsible for preventing and curbing the trade of illegal medicines in Malaysia is the Pharmacy Enforcement Division, with the support of the Pharmacy Enforcement Branch, which operates at the state level. One of the efforts in combating the unregistered and illegal medicine trade in Malaysia is to identify and locate the sellers of such products so that legal action can be taken against them. One of the techniques employed by pharmacy enforcement officers in order to track the seller is by profiling the suspects and also by adopting Open-Source Intelligence (OSINT) methods. Currently, the profiling is done by referring to the guidelines issued by the Pharmacy Enforcement Division. As there are many OSINT methods and techniques that have been published in recent years, this research aims to situate the current practice of pharmacy enforcement officer in OSINT investigation among the recently established models of OSINT, especially in cybersecurity aspects. It is a common fact that OSINT investigators are more susceptible to cyber threats, especially if they are not equipped with the right skills and knowledge prior to initiating an open investigation. This research takes both quantitative and qualitative approaches and collects data through literature reviews and expert interviews. The OSINT model produced is based on international standard readings and is cross-checked against current government regulations and guidelines. The components and elements that shape the security aspects of the OSINT investigation are identified. Data gathered through expert questionnaire surveys are examined using frequency analysis and percentages to achieve expert consensus percentages. Based on the analytical results, an enhanced model of OSINT work process is developed and suggested depending on expert comments, incorporating preparatory phase in the current OSINT work processes adopted by Malaysian pharmacy enforcement officers. The establishment of this enhanced OSINT model and preparatory phase checklist template allows the intelligence gathering by pharmacy enforcement officers to be executed more systematically and effectively, while at the same time minimizing the impact on security threats.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF ILLUSTRATIONS

LIST OF ABBREVIATIONS

BIOS	Basic input/output system
CSM	Cybersecurity Malaysia
CBP	Certified Blockchain Professional
DCA	Drug Control Authority
DDOS	Distributed denial-of-service
GSEC	GIAC Security Essentials Certification
GCIA	GIAC Certified Intrusion Analyst Certification
ICT	Information and Communication Technology
ICTSO	Information and Communication Technology Safety Officer
IMPACT	International Medical Products Anti-Counterfeiting Taskforce
INTERPOL	International police
ISMS	Information Security Management System
MITM	Man in the middle
MCMC	Malaysian Communications and Multimedia Comission
MNMP	Malaysian National Medicines Policy
MOH	Ministry Of Health Malaysia
NACSA	National Cyber Security Agency
NGOs	Non-Government Organizations
NPRA	National Pharmaceutical Regulatory Agency
OSINT	Open-source intelligence
QUM	Quality Use of Medicine
UKM	Universiti Kebangsaan Malaysia
VM	Virtual Machine
VPN	Virtual private network
WHO	World Health Organization

CHAPTER I

INTRODUCTION

1.1 INTRODUCTION

The sharp increase in online sales of medicines in this age has been attributed to the expansion and rise of internet services such as e-commerce platforms (Pilus et al. 2021). This situation is exacerbated by the outbreak of the COVID-19 pandemic, in which medical products are in high demand (Zuryani, Zakuan, and Ismail 2021). The ever-increasing number of internet users translates into a higher number of online medicine sales transactions. In 2000, there were only 413 million internet users, while in 2016, the number of internet users increased to 3.4 billion. Consumers are also becoming more health conscious, taking more responsibility for their health and seeking alternatives to modern medicines. They tend to turn to health supplements to prevent or solve their health issue (Zuryani, Zakuan, and Ismail 2019). The conveniences of getting medicines and medical products online come with potentially undesirable consequences. This newly developed online purchasing behaviour, self-diagnosis, and online information seeking have opened the possibility of self-injury or even death, as it is usually done without proper consultation from healthcare professionals (Pilus et al. 2021).

According to the Malaysian Communications and Multimedia Commission (MCMC), with the expansion of internet service, Malaysians have the tendency to search for information regarding their health on the web (Fadhilah Ismail et al. 2020). The percentage of type of health information searched by Malaysians on the internet can be seen in Figure 1.1.

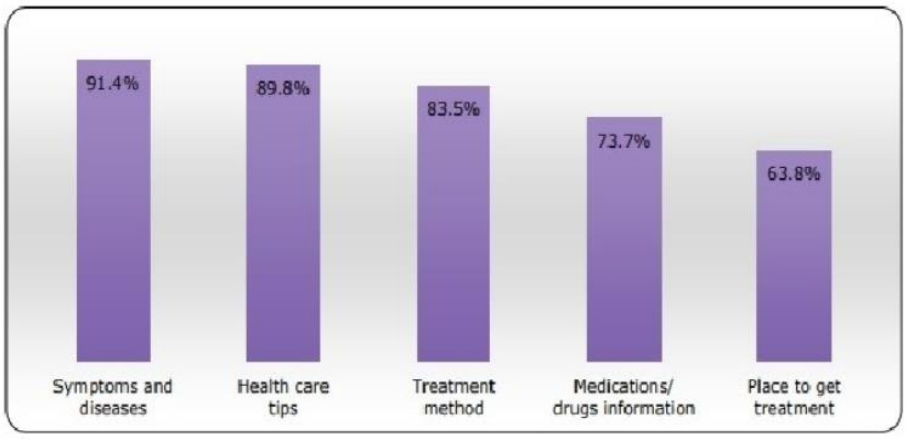

Figure 1.1 Percentage of type of health information searched by Malaysian on the internet

Source: Malaysian Communications and Multimedia Commission (MCMC) 2020

Consumers are also exposed to the possibility of obtaining substandard and falsified medicines due to the rise of online sales of medicines, as immoral traders were seen to be taking advantage of this situation by selling illegal and counterfeited medicines due to high demand. Criminals were given a newly discovered modus operandi and the opportunity to conduct criminal acts like selling illegal medicines as the result of rapid digital information (Kanta, Coisel, and Scanlon 2020). As a result, severe health risks such as toxicity, overdose, contraindication and adverse side effects will become a huge concern towards consumers (Pilus et al. 2021; Zuryani et al. 2021).

In parallel, law enforcement agencies are also affected by the rise of the digital world. On the positive aspect, law enforcement agencies can be equipped with newly developed technologies and solutions to combat criminal activities such as the illegal sale of medicines through online platforms. On the other hand, law enforcement agencies need to face the additional challenges created by the exploitation of new technologies adopted by criminals (Kanta et al. 2020). Law enforcement agencies must equip themselves with all the knowledge and skills to maintain their security while combating criminal activities. This research discusses the security measures that the enforcement agency can apply in their effort of combating the sale of illegal and counterfeit drugs in Malaysia.

1.2 PROBLEM STATEMENT

The digital world has been a 'double-edged sword' for law enforcement agencies in the twenty-first century. Digital technologies have the capability to deliver significant benefits to enforcement activities through the revolution of publicly available sources, i.e., open-source technology. However, information security is proven to possess some flaws and shortcomings that might affect the investigation process and law enforcer themselves. The rise of internet technology offers increased freedom and anonymity in communications to both law enforcers and criminals. The very same technologies that ensure anonymity for law enforcement activities also offer new ways for criminals to conceal their identity while conducting malicious activities. It is also acknowledged that due to cross border connection of computers via networks, risks that can be potentially faced by information security are more often than not of a global scope. This situation presents new issue with jurisdiction from law enforcement perspective as legal actions are often restricted by nationally bound borders (Akhgar, Saskia Bayerl, and Sampson 2018). United Kingdom Financial Conduct Authority emphasized the risks of criminals using open source intelligence (OSINT) for phishing attempts against law enforcement agencies Some of the criminals also were also known to move as trolling groups for examples 4chan group who notoriously employ OSINT techniques to harass, bully and intimidate websites and personal accounts of law enforcer This indicates that law enforcement agencies' OSINT processes need adjustments and safeguards (Saskia et al. 2022).

In Malaysia, the law enforcement agency responsible for combating the sale of unregistered and illegal medicines is the Pharmacy Enforcement Division, with the support of the Pharmacy Enforcement Branch, which operates at the state level. One of the initiatives of this agency to curb the crime of selling these illegal medicines especially via online mediums, is by locating and identifying the seller of such products. Pharmacy enforcement officers will conduct profiling towards the suspects to gather all the intelligence and information that is necessary for law enforcement agencies to locate and take legal actions towards the suspect. The profiling towards suspects is conducted using various OSINT techniques and methods, which eventually will produce a profiling report based on the guideline issued by Pharmacy Enforcement Division, titled

"New Media Profiling". The complete report that contains all the necessary intelligence will be evaluated by a senior pharmacy enforcement officer who will determine the status of the report and suggest the appropriate further action.

The latest document is enforced on 22nd February 2023 as an effort to upgrade the certification of Pharmacy Service Division to ISO 9001:2015. It is stated in the document that one of the requirements to produce a complete profiling report is to adopt the OSINT method in gaining intelligence. The guideline also has listed out free online OSINT tools that can be potentially used by Pharmacy Enforcement officers to gather intelligence along with the techniques of using Google Dork effectively. Google Dork or also known as Google Hack refers to the information search techniques by using Google to hack into vulnerable sites. It is usually employed to search for information that is not available in public search results. Google Dork custom queries utilises advanced search operators which include specific symbols or words in order to acquire a better targeted search results. However, there is no clear guidance for pharmacy enforcement officers to refer to on the security and preparatory measures that are necessary for them to take for self-protection prior to investigation.

The lack of guidance can expose them to any unwanted danger and exposure that suspects or other malicious actors might put on them. In order to mitigate and minimize the impact of security threats in this situation, there should be clear guidance for pharmacy enforcement officers to apply in their efforts to combat the online sale of illegal medicines.

1.3 RESEARCH QUESTIONS

This paper wishes to address these research questions.

1. What are the differences between the OSINT methodology of the Malaysian pharmacy enforcement agency and several relevant players in the global OSINT landscape?

2. What recommendations and suggestions can be made by the Malaysian pharmacy enforcement agency to help improve OSINT investigation security?

1.4 RESEARCH OBJECTIVES

The main objectives of this research are:

1. To identify security issues and challenges that can be potentially faced by pharmacy enforcement officers in producing quality intelligence using OSINT by comparing existing OSINT process with globally identified methodology.

2. To propose an enhanced OSINT methodology tailored to the requirements of the Pharmacy Enforcement Division, particularly emphasizing security aspects.

1.5 RESEARCH SCOPE

The scope of this research is to develop standard procedures and/or work processes for dealing with security threats associated with OSINT investigations conducted by pharmacy enforcement officers based on current standards and best practices. This research will explore the current practice of OSINT investigations and focus mainly on the preparatory phase of OSINT investigations. The procedures and/or work processes are developed without taking into consideration external issues like cost, time and skill.

This research only includes infrastructure that is reported in public sector assets or inventory registers. Due to the nature of technology, which is constantly evolving and changing, the material used for the recommendations and improvement suggestions for current OSINT practice is based on standards and best practices from at least five years ago to guarantee that the data and information are relevant and not outdated.

1.6 RESEARCH ARRANGEMENT

Chapter I discusses the background of the study on the security threat that can potentially face pharmacy enforcement officers in combating online sales of illegal

medicines. Furthermore, the study aims to examine the procedure and workflow involved in suspect profiling by pharmacy enforcement officers, which apply OSINT techniques and methods in achieving the objectives.

Chapter II will be a review of past literature, which aids in a better understanding of several areas of discussion that include Malaysian enforcement agencies and their activities in curbing the widespread selling of illegal medicines, OSINT techniques employed by law enforcement agencies and their challenges, and also a comparative study of existing guidelines and best practices in OSINT investigation, whose main focus is the security and preparatory phases of a security threat from a malicious actor.

Chapter III reviews and explains the methods used throughout the study in detail and sequence. The research design, data collection methods, and the development of survey questions to extract valuable input from experts and how the data was analyzed will be discussed thoroughly.

Chapter IV discusses the results and findings referring to the data analysis based on the outlined objectives. The data and input collected using methods in Chapter III will be used to develop and formulate an enhanced work process by applying a more secure preparatory phase of OSINT investigations for pharmacy enforcement officers. Percentage and frequency analysis will be used to analyze the input from expert opinion to get a clearer understanding of several elements of the survey distributed. This chapter will outline and suggest guidelines for a more secure OSINT investigation.

Chapter V refers to the summary, discussion, and further recommendations for future research.

CHAPTER II

LITERATURE REVIEW

2.1 INTRODUCTION

This chapter describes the literature review carried out on the subject matter studied. The literature study involved a semi-systematic evaluation process of past studies, which includes review books, scientific articles and other related sources. This provides a critical explanation, summary and assessment of past studies related to the research problems of this project. This chapter also dissected several current government circulars, policies, and guidelines to ensure this research outputs conform with local legislation and policies. This chapter consists of four (4) main phases that contain a detailed description of the topic: (1) the current situation of Malaysian illegal medicines trades, (2) the Malaysian pharmacy enforcement agency and its enforcement and regulatory activities, (3) OSINT methods and security challenges in conducting an open digital investigation, and (4) OSINT methodology adopted by pharmacy enforcement agency in Malaysia and comparative study of the published OSINT guidelines.

By identifying gaps and challenges in the current OSINT investigations methodology by pharmacy enforcement agencies in Malaysia, this chapter aims to lay the groundwork for proposing improvements that involve fundamental preparation for effective and more secure OSINT operations.

2.2 CURRENT SITUATION OF MALAYSIAN ILLEGAL MEDICINES TRADES

According to National Pharmaceutical Regulatory Agency (NPRA), a registered medicine is a “drug that is approved by the Drug Control Authority (DCA) for sale or to be used in Malaysia” which undergoes various evaluations and testing to establish its efficacy and safety. Unregistered drugs which include adulterated and counterfeit drugs

are harmful and pose a major threat to human health and safety worldwide, especially in a developing country like Malaysia where the percent of the contribution of unregistered drugs in the market is higher compared to other developed countries (Zulkifli et al. 2015). Studies show that counterfeit and unregistered drugs are not safe for human consumption as they are not manufactured under the same hygienic conditions as legitimate products. Illegal medicines were often contaminated with dangerous microbiology exceeding the permissible limits, representing a potential threat to consumer health (Pullirsch et al. 2014). International police (INTERPOL) estimates that the global trade in illicit pharmaceuticals is worth 4.4 billion dollars, which helps to picture the scope and effect of illegal online drug sales. For example, in Operation Pangea XV 2022 that was conducted by 96 INTERPOL members including Malaysia, on 23-30 June 2022, 7800 seizures of illicit medicines were made along with the removal of more than 4000 weblinks that advertised and sold illicit products (INTERPOL, 2022).

In Malaysia alone, Operation Pangea XV that was led by Pharmacy Enforcement Division seized more than RM5.2 million worth of unregistered pharmaceutical products. The operation involved multiple law enforcement agencies in Malaysia, including police, customs departments, and health enforcement agencies from various regions, to combat unregistered and counterfeit pharmaceuticals marketed and sold online. The operation also revealed that approximately 2,438 websites, including those from the dark web, were detected selling illegal pharmaceutical products worth RM2,652,500 (Teoh Pei Ying 2022).

2.2.1 Increasing Trend of Online Medicines Trade

The fast growth of information technology has transformed many traditionally operated businesses with premises into online businesses, and this involves medicines that, whether legal or illegal, are being sold over the internet, especially during the post-COVID era. There are many factors that contribute to this shift in consumer purchasing behaviour. General consumers are usually influenced by the notion that by purchasing medications online through websites, social media and mobile apps, the price offered will be much cheaper for most of the medications, and a prescription from a professional

medical practitioner is also not required. The convenience and confidentiality offered by online medicine purchases seem to attract consumers, as they are just one click away to get their much-needed medications without needing to visit their doctor and share their personal and sensitive health information. However, the conveniences do not come without consequences. The emergence of a big and vast market for online medications also attracts many rogue and unethical sellers to start selling unlicensed, substandard, and falsified medicines with various dubious medical claims (Lee et al., 2017). A study by Fittler A et al. (2022) also concluded that the online purchase of medications increased exponentially as the advancement of technologies in online shopping, like e-commerce, propelled the user's first online shopping experience. The study also found that respondents who are more educated and younger use the internet more frequently to shop online. This respondent's group is found to be more likely to purchase medications on the internet.

Consumer acceptance of online purchasing suggests that online transactions have been widely accepted as an alternative to physical store purchases for health supplements and medications. However, this acceptance must be accompanied by sufficient risk management by the consumers and effective enforcement and regulatory activities, as unregistered and substandard medicines have been flooding the Malaysian market (Ang et al. 2023). A study done by Pilus et al. (2021) that focuses on e-commerce platforms like Shoppe, found that 796 out of 852 (93.4%) prescription medicines samples were not registered with the DCA, Malaysia's Health Ministry. The types of unregistered medicines detected being sold on the platform are as follows: hormones that constitute (62.6%), antibiotics (4.8%), fertility drugs (2.2%), slimming pills (1.8%) and abortion pills (0.4%). This finding emphasizes that Malaysia should have rigorous and well-planned enforcement activities in place to manage and combat the online sales of unregistered drugs. The effort needs to be consistent, persistent, and ongoing.

2.3 PHARMACY ENFORCEMENT IN MALAYSIA

World Health Organization (WHO) proposes that the key to combating the plague of unregistered and substandard medicines in the online market are legislative and

regulatory infrastructure, regulatory implementation, enforcement, technology and communication. The effort should also be a collaborative venture between multiple sectors, such as pharmaceutical manufacturers, Non-Government Organizations (NGOs), regulatory and enforcement agencies. Thus, International Medical Products Anti-Counterfeiting Taskforce (IMPACT) was established by WHO in February 2006, which involves such sectors with the aim of creating a better network between countries and curbing the production and distribution of counterfeit drugs (Zulkifli et al. 2016).

One example of a successful operation is called Operation Pangea. By collaborating with other law enforcement agencies (custom and police), Internet Service Providers and private agencies that handle online payments (MasterCard, Paypal and VISA), Operation Pangea IX successfully targets some main aspects that are exploited by organized crime in trafficking medicines online like fraudulent domain name registrars, electronic payment systems and medicine delivery. (Lee et al. 2017)

In Malaysia, the Pharmacy Enforcement Division, formed on the 1st January 1976, is the enforcement agency mandated to enforce the legislation regarding pharmaceuticals. Currently, there are five subdivisions in Pharmacy Enforcement Division, as illustrated in Figure 2.1. All subdivisions serve their purpose in combating illegal and unregistered medicine (Zulkifli et al. 2016, Pharmaceutical Services Programme Annual Report 2021). The activities carried out by Pharmacy Enforcement Division include intelligence and operations, control of licensing and integrated monitoring and collaborative activities with stakeholders to reduce the demands for unsafe or hazardous products.

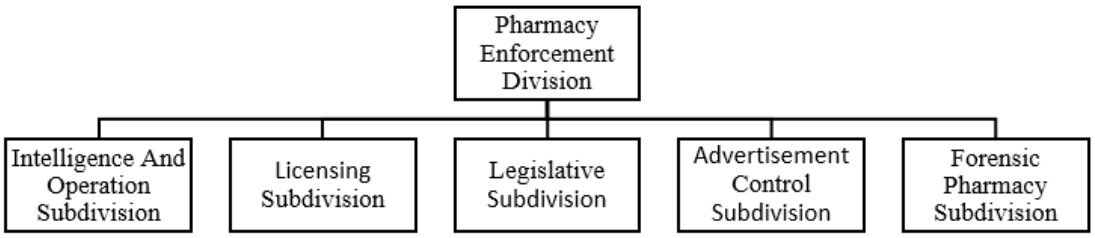

Figure 2.1 Pharmacy Enforcement Division Structure

Source: Pharmaceutical Services Programme Annual Report (2021)

A total of 15 Pharmacy Enforcement Branches in Malaysia operate at the state level. Pharmacy Enforcement Branch is divided into four sections that are Intelligence and Operation, Licensing, Legislative and Advertisement Control. Intelligence and Operation is further divided into four smaller units: Operation, Intelligence, Complaint, and Cyber Unit. The organization is illustrated in Figure 2.2.

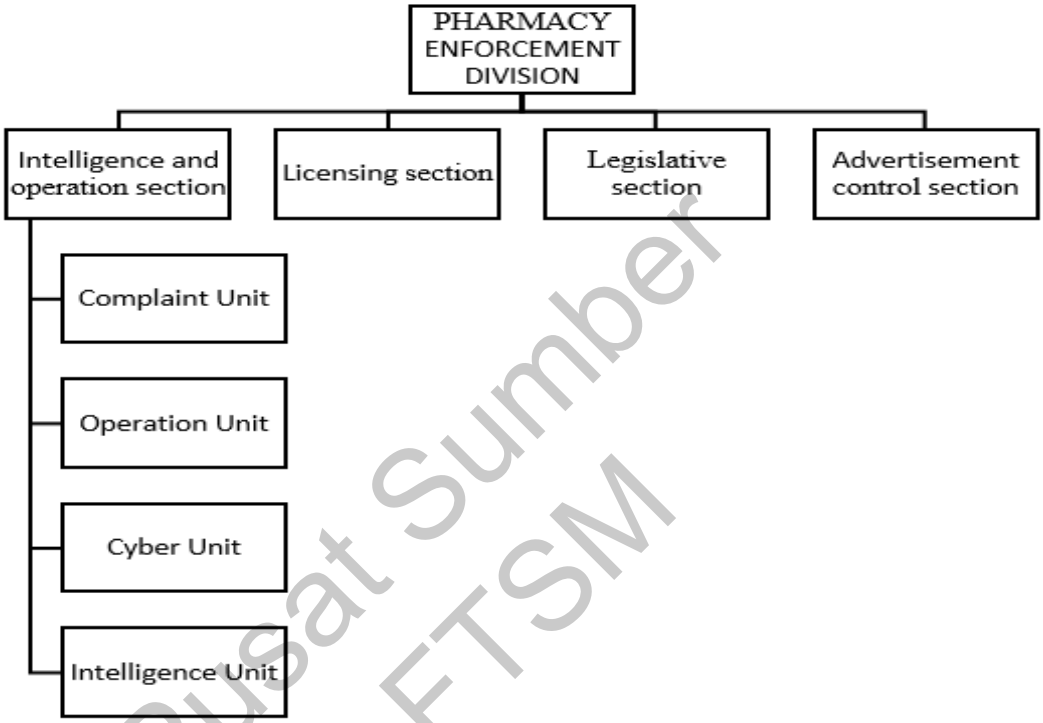

Figure 2.2 Pharmacy Enforcement Branch structure

Source: Pharmaceutical Services Programme Annual Report 2021

The pharmacy enforcement officer in the Cyber unit under Pharmacy Enforcement Branch job scope includes *"Screen and monitor the sale of pharmaceutical products in the new media and prepare profiling reports based on complaints in relation to the supply or sale of pharmaceutical products on the Internet as well as conduct digital forensics and data recovery to enable evidence to be brought to court"* (Pharmaceutical Services Programme Annual Report 2021)

2.4 ENFORCEMENT AND REGULATORY ACTIVITIES IN COMBATING ONLINE SALES OF ILLEGAL AND ILLICIT MEDICINES

A National Medicine Use Survey conducted in 2013 revealed that most Malaysians lack knowledge, especially about the correct use of medicines, the detrimental effects or side effects, and the interactions between medicines. As an important aspect of the national health system, Quality Use of Medicine (QUM) has been stipulated as one of the five components in the second edition of Malaysian National Medicines Policy (2nd MNMP) in 2012 by the Ministry of Health Malaysia. QUM was introduced with the intention of promoting the use of medicines in the correct, safe, and cost-effective way (Ministry Of Health Malaysia 2012)

In the report by Pharmacy Research Priorities in Malaysia issued by Pharmaceutical Services Programme in 2018 that was based on the 2nd MNMP, one of the research scope that has been addressed in the research priority is the Unregistered/Adulterated/Counterfeit Medicines as shown in Figure 2.3. The rationale behind the proposed scope is the rapid increase in the use of unregistered health products that are deemed dangerous and have the potential to be adulterated or in a substandard quality state. The suggested research area by the report is to discover the contributing factors that propelled the public to consume unregistered/adulterated/ counterfeit health products with the expected output of public protection against the hazardous use of such products (Pharmacy Research Priorities in Malaysia, 2018).

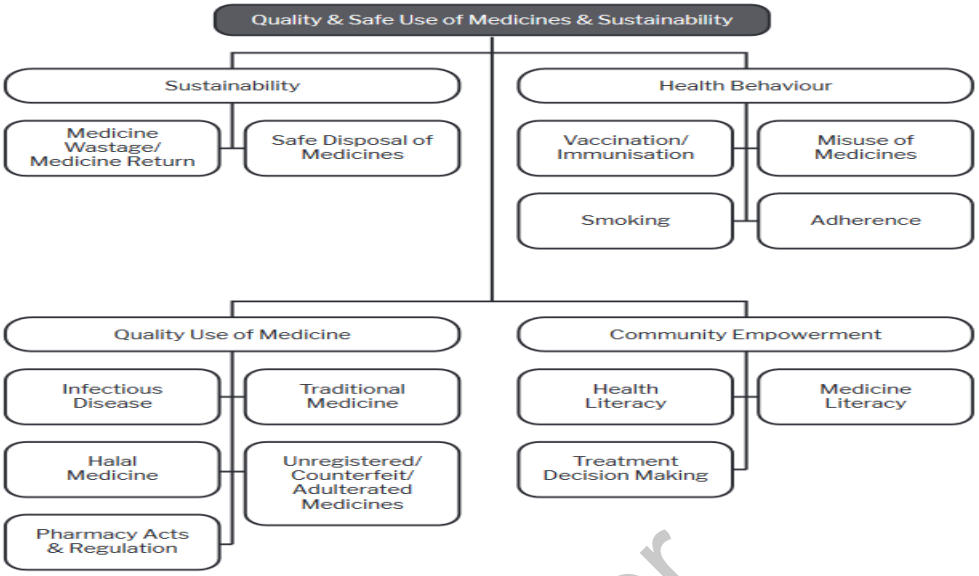

Figure 2.3 Research Priority Framework for 'Quality and Safe Use of Medicines and Sustainability

Source: Pharmacy Research Priorities In Malaysia 2018

In the latest and updated version of MNMP published in 2017 by Ministry of Health, one strategy proposed for ensuring medicines are of quality, safe and productive for consumers in Malaysia is by strengthening enforcement and regulatory activities under the relevant acts and regulations. The strategy includes ongoing activity like combating online sales of illegal and illicit medicines (3rd Malaysian National Medicines Policy 2017). The detail of the strategy is presented in Figure 2..

No.	Activities	Implementation Timeline	Indicator	Final Target	Stakeholder
2.1	Combating online sales of illegal and illicit medicines	On-going	Percentage of illegal and illicit medicines online sellers identified within 30 working days from profiling started	95%	Pharmacy Enforcement Division
		On-going	Number of actions taken on online sales of illegal and illicit medicines	400	Pharmacy Enforcement Division

Figure 2.4 Strengthening Enforcement and Regulatory Activities In Combating Online Sales Of Illegal And Illicit Medicines.

Source: Third (3rd) Malaysian National Medicines Policy 2017

This strategy is also reflected in the Pharmaceutical Services Programme Strategic Plan 2021-2025, where several initiatives have been proposed to strengthen the monitoring of sales and advertisement of unregistered and adulterated products to combat online sales of illegal medicines in Malaysia. “Broken Window” is one of the initiatives that includes producing quality intelligence information through careful implementation of the following steps shown in Figure 2.5.

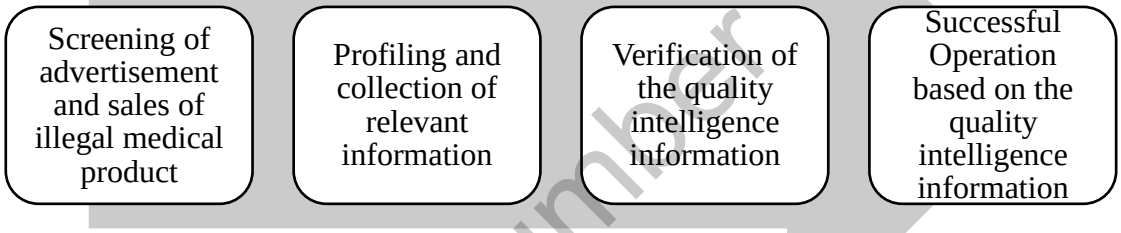

Figure 2.5 Broken Window Operation

Source: Pharmaceutical Services Programme Strategic Plan 2021-2025

The strategic plan target is that by 2025, 1000 quality intelligence information will be developed, and 80% of the operation will be successfully conducted based on the Broken Window information developed (Pharmaceutical Services Programme Strategic Plan 2021-2025, 2021).

2.5 OPEN SOURCE INTELLIGENCE (OSINT) OVERVIEW

Many definitions of open-source intelligence (OSINT) are available from published literature. Robert Steele (2006), in his book ‘Handbook of Intelligence Studies’, described an early definition of OSINT as “*Unclassified information that has been deliberately discovered, discriminated, distilled and disseminated to a select audience in order to address a specific question*”. Michael Hutchinson (2020) defined OSINT as *the activity of gathering intelligence and managing it. It involves finding, selecting, and obtaining information from publicly accessible sources, then analysing it to create useful intelligence*.

In recent years, with the rise of internet technology, OSINT has become one of the methods in law enforcement agencies' arsenal in combating crime. OSINT has helped to increase the effectiveness and efficiency of law enforcement activities at a relatively low cost with the abundance of publicly open information (Akhgar and Wells 2019)

OSINT offers a generous number of advantages to investigators in law enforcement agencies in their line of work in gathering intelligence. Hwang et al. (2022) have listed the advantages of OSINT in conducting open investigations as follows.

1. Real-time information collection: Through various online open-source platforms like YouTube, social media, articles, etc., OSINT collects information and data quickly in real time. The online world of the internet serves as a one-stop centre for OSINT investigators for prompt access to desired information rather than collecting it from one place.

2. Extensive acquisition of data: OSINT gives investigators the ability to collect extensive data in covert intelligence gathering through open sources. This data collection method yields meaningful and desired intelligence when processed in a proper manner. OSINT is accessible, legal, and offers relatively low-security risk, ensuring secure data acquisition.

3. Clarity of sources: In traditional intelligence gathering, the credibility of data collected can be questioned as the source of the information the agent obtains is ambiguous and vague. Through the validation process, data collected by OSINT ensures credibility because of the clarity of the open sources.

4. Convenience and ease of access: One factor distinguishing OSINT as a far greater means of obtaining intelligence is its openness. Data access rights only allow authorised users to access confidential and sensitive data, while in contrast, anyone can easily access information collected by OSINT and use data conveniently according to the user's requirement.

5. Low cost: OSINT provides the benefit of gathering data at a lower price, as opposed to the cost of training operatives in human sources and collecting data using cutting-edge technology.

As requirements vary from one organization to another, most organizations have their unique structure of OSINT that was developed according to their objectives and needs. Hwang et al. (2022) have proposed the basic structure of OSINT as shown in Figure 2.6.

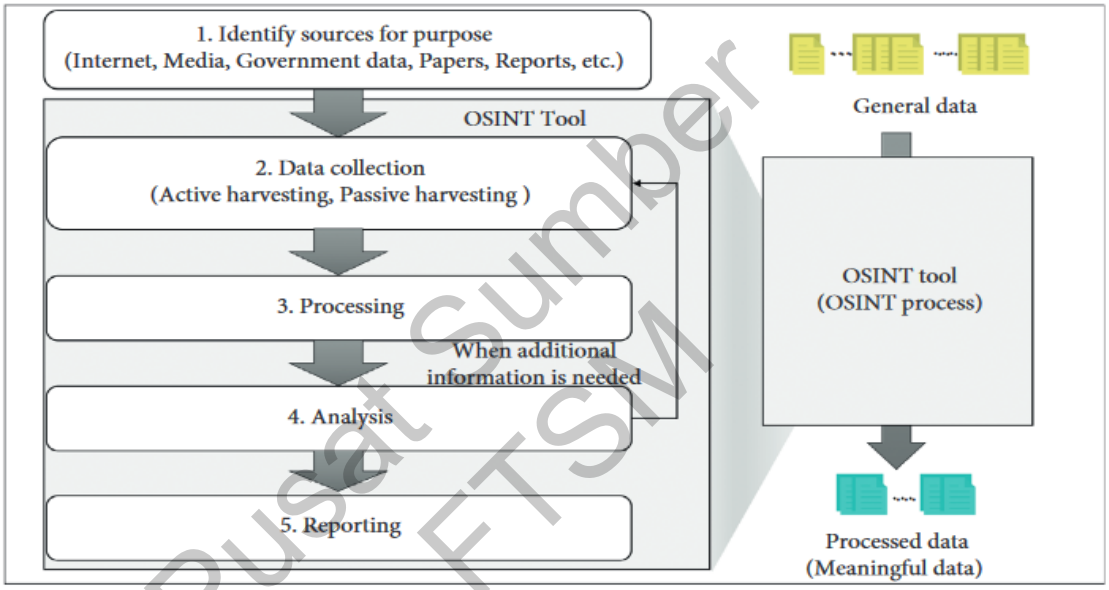

Figure 2.6 Basic OSINT Model

Source: Hwang et al. 2022

1. Identifying the source: Numerous data points should be identified where the investigator aims to extract the information, along with the methods of data extraction.

2. Data collection: This is the phase where relevant data will be accumulated from the sources. Depending on the method used for data gathering, there are two types of data collection methods: active and passive. In active data collection, information is directly harvested using software or script on the intended target. Because there is direct contact with the target, this type of data collection tends to leave logs behind. Contrary to active data collection, passive data collection

uses third-party programmes like Google, Whois, and other resources as its data point. Since there is no direct contact or access to the target, this method has the advantage of not leaving traces or logs behind.

3. Processing: All the data gathered from step 2 will be processed and refined to be converted into meaningful intelligence. This phase involves filtering a large amount of information, which is crucial to preventing information overload. It is also critical for investigators to map the association and connection between the data, and often investigators need to be equipped with sufficient experience for this stage as it is a highly challenging process that requires some expertise.

4. Analysis: Based on the objective of the investigation, the filtered and refined data is analyzed accordingly. If additional information is needed to achieve the objectives, steps 2 and 3 (data collection and processing phase) are repeated to derive meaningful intended intelligence.

5. Reporting: This is the phase where the findings of an investigation are recorded and compiled into writing. Each organisation has its format or way of reporting, and the report should be delivered, including the evidence and analysis report. To maintain the accuracy and credibility of the investigation, all the data sources should be listed and reported. The result of reporting should be a compilation of the relevant processed data that meets the criteria set by the organisation and investigator.

Apart from the basic OSINT model discussed, several OSINT methods have been published and compared in recent years. Tanabe (2022) has compared OSINT intelligence cycles, methods, and techniques of some relevant players in the global OSINT landscape. The OSINT methods compared in the paper include the Williams and Blum OSINT Cycle, the Berkeley Protocol OSINT Cycle, the Bellingcat OSINT Cycle, and Pastor-Galindo et al. OSINT approaches. He proposed a revised OSINT method that focuses on obtaining, transforming, and analysing information, as shown in Figure 2.7.

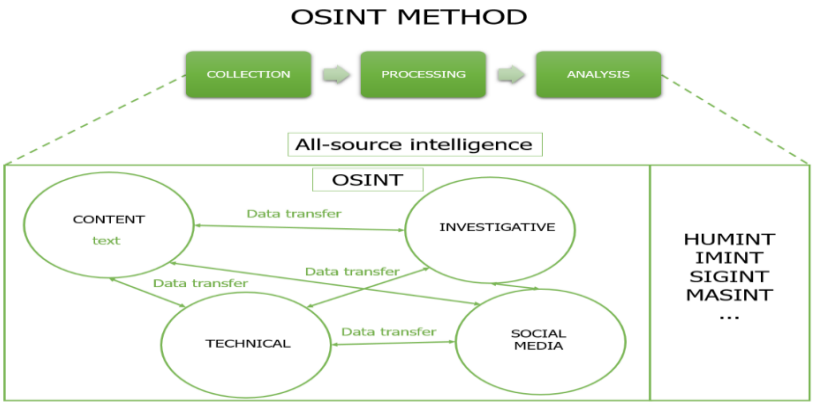

Figure 2.7 OSINT method

Source: Tanabe et al. 2022

Böhm and Lolagar (2021) have also studied different OSINT models where raw data will be transformed into quality intelligence. Among the models of the information cycle applied to OSINT addressed in the study is the model adopted by Gibson (2016) and Hassan and Hijazi (2018) where some adjustments have been made. Tabatabaei and Wells (2016) and Bohm and Lolagar (2021) discussed in detail the intelligence cycle, which contains six steps labelled Direction, Collection, Processing, Analysis, Dissemination, and Feedback. This model is also adapted by the Office of the Director of National Intelligence (2011) and Gibson (2016), as shown in Figure 2.8

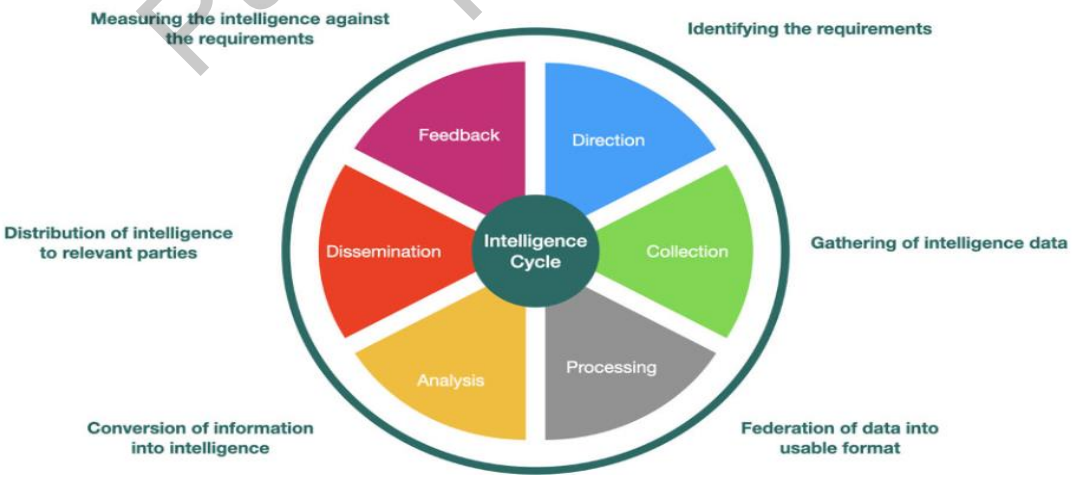

Figure 2.8 Intelligence Cycle

Source: Böhm and Lolagar 2021

2.6 SECURITY CHALLENGES IN OSINT

In the OSINT investigator line of work, there are many challenges and security threats that need to be addressed and managed properly. Bezzel (2021), in his book "*Open Source Intelligence Techniques: Resources for Searching and Analysing Online Information, Eighth Edition*" has demonstrated a situation where, more often than not, OSINT investigators tend to get into questionable websites and pages where the security threat like malware is much more prevalent in the course of an investigation. OSINT investigators also must bear the risk of counterintelligence, like entering the website of a malicious actor who has been monitoring the access and has the capability of backtracking the OSINT investigator.

OSINT has been known as a double-edged sword, especially for law enforcement agencies. Although its potential for empowerment of enforcement activities cannot be denied, it is also crucial to highlight its risks of unintended consequences. OSINT, drawing from publicly available information, offers valuable insights for decision-making and threat assessments. However, security concerns and privacy issues arise due to the openness of these sources. Hwang et al. (2022) illustrated how OSINT operations can be exposed to various threats that can lead to cybercrimes, as shown in Figure 2.9. This figure is a schematic diagram of the contents of cybercrimes that can occur through security threats by data dissemination, data privacy breaches, and data forgery and alteration that exist in the OSINT environment. Since anyone can access the data, a malicious actor can easily access the stored data and misuse it with malicious intent. Once the data is acquired, it can be disseminated to various target groups, which can be the basis for a larger cybercrime such as hacking, spearfishing, financial crimes, and malware spread. Data collected can also be contaminated and falsified, spreading fake information for crimes such as farce or inciting panic in society.

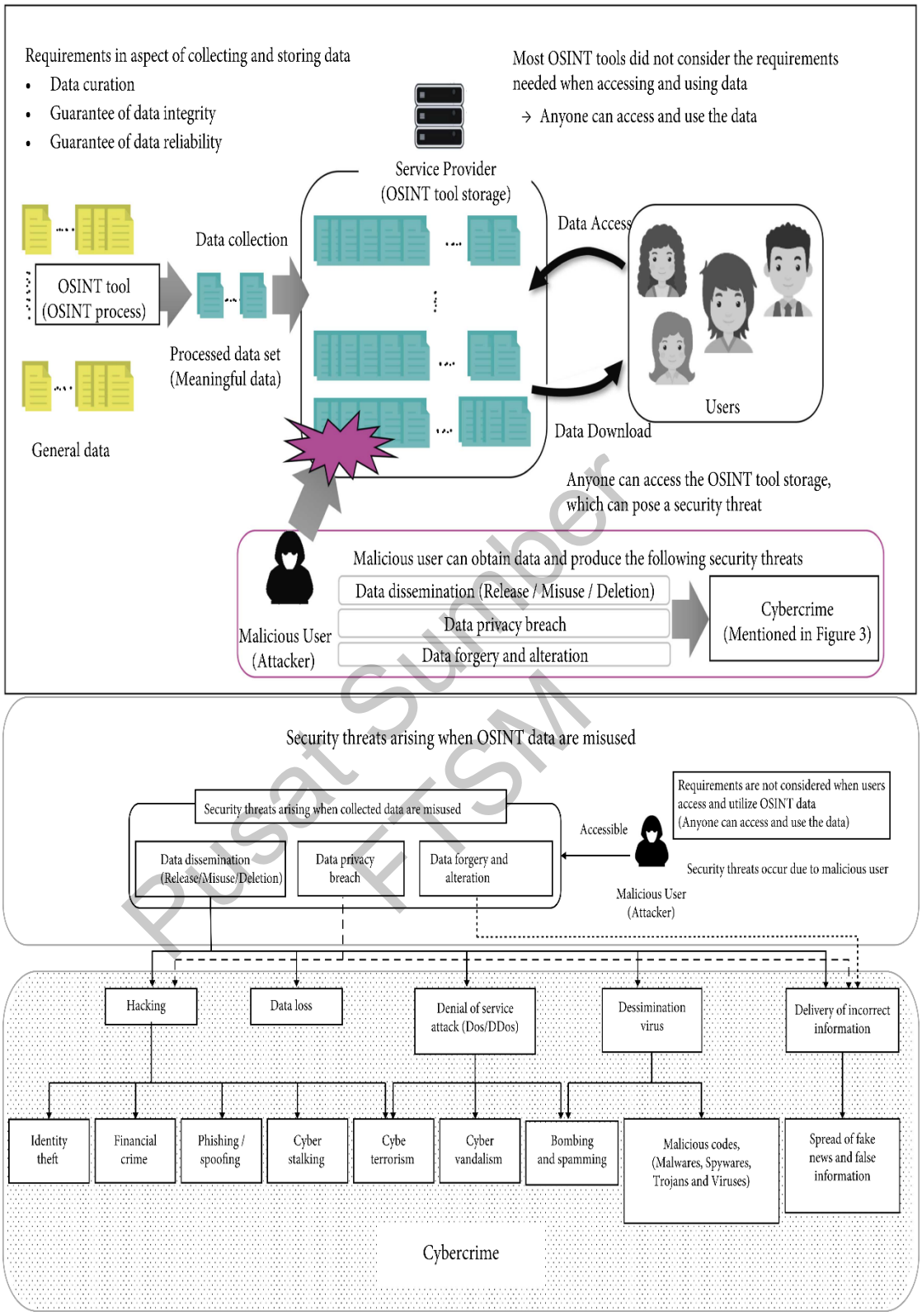

Figure 2.9 Schematic Diagram of Cybercrime in OSINT environment

Source: Hwang et al. 2022

2.6.1 Threats in OSINT Investigation

From a cybersecurity perspective, a threat is a potential danger or risk that can exploit vulnerabilities in a computer system, network, application, or other components, leading to unauthorised access, data breaches, disruption of services, or other harmful consequences. Threats are something that assets need to be protected against. Threats against an organisation or an investigation can come from the inside or the outside and can be carried out by individuals, other organisations, or groups. The main goal of cybersecurity is to identify, mitigate, and prevent these threats to safeguard the confidentiality, integrity, and availability of information and computing resources. United Nations for Human Rights Office of the High Commissioner (2022) in Berkeley Protocol proposed that OSINT investigators should be equipped with the skills and knowledge to predict, recognise and respond to following threats during investigation to safeguard themselves and their organization from cybercrimes.

1. Distributed denial-of-service (DDOS) attacks: DDoS attacks are the mechanisms used by criminals to disrupt legitimate access to a computer or network. Public-facing assets such as official websites are the most vulnerable assets exposed to this kind of attack if a system for mitigating such attacks is not implemented. For forensic purposes, a system to log incidents in the event of a DDoS attack should be put in place and used in the event of an attack to record all actions and the relevant actors.

2. Phishing attacks: Phishing is the fraudulent practice of posing as a legitimate source to acquire sensitive and confidential information from victims. Details such as usernames, passwords, and credit card information can be abused for monetary gain and pose a threat to victims and investigators. For this reason, it is highly recommended that OSINT investigator not use their account for intelligence gathering during investigation.

3. Man-in-the-middle attacks: It is a type of cyberattack in which malicious actors enter the talk or connection between two parties, impersonating them and intercepting the confidential information that both parties try to communicate.

Using a man-in-the-middle attack, a malicious actor can transmit and receive data intended for someone else or not intended to be sent. This is all done without the other party realising the actions of the attacker.

4. Social engineering: By conducting social engineering like spear phishing, victims of cyber-attacks can be psychologically manipulated to conduct potentially harmful actions for themselves, like revealing confidential information to malicious actors. Since social engineering techniques are always changing and evolving, OSINT investigators should get continual training to recognise and respond to this threat.

5. Malicious software: Computer programs that sneak into systems and harm without the user's knowledge. Malware comes in many forms, such as ransomware and spyware.

2.6.2 Vulnerabilities In OSINT Investigation

Vulnerabilities in cybersecurity, in general, refer to weaknesses or flaws in a system, network, application, or process that can be exploited by attackers to compromise the security and integrity of the information or infrastructure. These vulnerabilities can manifest at various levels within the digital ecosystem, and their exploitation can lead to unauthorised access, data breaches, service disruptions, or other malicious activities. When it comes to online activities, vulnerabilities could include a weakness in security protection measures that could be exploited to gain unauthorised access to an asset, security defects in software, insecure design, and over privileged users and code. Security vulnerabilities may come from external threats, such as new malware and viruses, of which investigators should be aware. A security mapping and risk assessment should consider these kinds of vulnerabilities.

United Nations for Human Rights Office of the High Commissioner (2022) in the Berkeley Protocol on Digital Open Source Investigations has listed the vulnerabilities that might be encountered by OSINT investigators, which they should also be aware of.

1. Cookies: It is a small file that is sent through a website and stored for use by a browser until it is deleted or expires. Cookies are used to store user preferences and details like user identity with the purpose of faster processing speed and reducing the need for repeated data entry. However, malicious actors have the potential to abuse cookies to gather sensitive and confidential data about visitors and can be centralised tools to capture users' browsing habits.

2. Trackers: It is a type of persistent cookie that has the ability to record a user's browsing habits and activities. It assigns a unique identity to a user's browser and links it to all subsequent browsing and search activities. Trackers are often integrated into online advertisements and can be abused by malicious actors to capture user activity across multiple websites. It exploits the ability of a browser to keep details of which web pages have been visited, which search criteria have been entered, etc. of their target. The overall data will help the owner of the tracker to build a detailed picture of users and their browsing habits. Users may unintentionally install trackers on their computers and have their future online behaviour monitored, even if they visit a website that is considered trustworthy.

3. Beacons: It is a small and unobtrusive element in a web page that is usually invisible and has the potential to track user activity and behaviour. When rendered by a browser, beacons will send details about the browser and the computer used to a third party. It is closely related to social media sites and can be used alongside cookies to trigger data collection and transmission, uniquely identify users, and record their browsing habits.

4. Codes and script: Downloadable small code is increasingly used by numerous websites to store and record details like visitor information and interactions. This type of code and script also influences the appearance of the websites. It can be misused by malicious actors to capture and store sensitive information through persistent collection and third-party transmission.

2.7 SECURITY CONSIDERATIONS IN CONDUCTING OSINT

By prioritising pre-investigation preparation and focusing on threat assessment and risk mitigation, OSINT investigators should be able to reduce the risk of harm during their course of investigation. When it comes to cybersecurity, harm can be defined as any bodily or psychological harm, injury to property, or destruction of digital, financial, legal, physical, or psychosocial aspects.

After recognising the impact of cyber threats on organizations' assets and resources, a holistic approach and security measures should be employed before initiating any open-source investigation. By incorporating independent auditing and evaluation and periodic updates to these security measures, an organization can create a resilient security framework, minimizing risks and protecting individuals, data, and assets throughout the open-source investigation process. United Nations for Human Rights Office of the High Commissioner (2022) proposes that the key to upholding security aspects for OSINT investigators can be viewed from two aspects: infrastructure-related security considerations and user-related security considerations.

2.7.1 Infrastructure Related Security Consideration

Ministry of Health, in its Guidelines On The Readiness Of Information And Communication Technology Infrastructure (ICT) In Agencies And Facilities Of Ministry Of Health Malaysia (MOH) issued in 2016, defines information and communication technology (ICT) infrastructure as infrastructure involving ICT hardware, ICT software and ICT network. For OSINT investigators, it refers to the structures, facilities, and systems needed to conduct open-source investigations. In order to protect and preserve an organization's assets and data from the harm and risk brought by open-source investigations, OSINT investigators should be provided with infrastructure that is equipped and armoured with sufficient security measures. United Nations for Human Rights Office of the High Commissioner (2022) has further categorised the infrastructure that is necessary for conducting effective and secure investigations with the minimum standard that it should be operated by, into three (3) categories: devices, internet connection and web browsers.

1. Devices: OSINT investigators must be provided with devices that can access online content with hardware secured with password-protected access and multifactor authentication. Any use of personal devices must always be avoided for investigation activities, as they could be linked back to investigators. OSINT investigators can use virtual machines to mask certain features during their investigations. When deemed necessary and feasible, virtual machines could allow OSINT investigators to destroy, recreate, configure, replicate, and preserve the virtual machine for future needs without compromising the actual machine being used.

2. Internet connection: When browsing online content, an OSINT investigator should have a strong, stable, and private internet connection. The use of public Wi-Fi in any open investigation should be avoided at all costs due to its insecurity and potential threats. OSINT investigators should be aware of the fact that personal and password-protected internet connections or hotspots are essential for secure online investigative activities. It is recommended that they use a virtual private network (VPN) for the purpose of masking their IP addresses and also creating encrypted channels for safe communications, with the caveat of having fail-safe mechanisms to protect their IP addresses in the event of lost connections. The limitation of using a VPN is that some of the available VPN services may be blocked by certain countries.

3. Web browsers: Browsers serve as the primary interface between investigators and the internet and are crucial tools in open-source investigations. However, due to their evolving nature and potential misuse, browsers can also be a source of risk for OSINT investigators. Through vulnerabilities within web browsers, sensitive and confidential data can be leaked to third parties. In addition to that, malicious scripts and code from dodgy websites can be downloaded and executed through web browsers, potentially altering digital content and the accessibility of data on target machines. By regularly patching web browsers and using appropriate software and plug-ins, OSINT investigators can minimize these risks.

2.7.2 User Related Security Considerations

Malicious actors are now focusing more on the person behind the computer as technical and infrastructural aspects of cybersecurity are constantly improving. It is acknowledged that one of the weakest points in any security framework is the users themselves. Security principles cannot be adhered to even with the implementation of flawless infrastructure without addressing faulty user behaviour through regular training and frequent supervision (Hughes-Lartey et al. 2021). Security in law enforcement agencies conducting open-source investigations should be a collective responsibility, and investigators should refrain from engaging in activities that could jeopardise data or persons without proper training on risk mitigation.

United Nations for Human Rights Office of the High Commissioner (2022) in Berkeley Protocol highlights the importance of OSINT investigators' awareness towards the security threats that open investigations could potentially bring. It also sets the minimum standard that every OSINT investigator must adhere to comply with security principles. Two of the most important aspects of user-related security consideration for OSINT investigators proposed by Berkeley Protocol are the ability to stay anonymous and mask the connection and machine used during investigations. It emphasizes the need for OSINT investigators to be familiar with the vulnerability of online activities to tracking by third parties, highlighting potential trace-back attempts targeting IP addresses, browsers, screen resolution, and user navigation patterns. OSINT investigators should receive sufficient training and guidance to assess the appropriate behaviour when conducting different online activities.

Several security measures are proposed to mitigate this risk, such as introducing the concept of virtual identity as a false online identity or profile that ensures secure investigative activities on social media and other web-based platforms. Open-source investigators are encouraged to create and use virtual identities to safeguard their real-life information from threat actors attempting to trace online activities. This approach protects investigators and enhances the security of individuals supporting an investigation. The importance of planning virtual profiles and maintaining records to explain activities conducted under this virtual identity should be stressed to the OSINT

investigator. Berkeley Protocol also emphasizes the significance of users' ability to mask connections and machines used in online investigations to protect themselves and their organizations' assets. The protocol warns against compromising this protection by revealing personal information on websites or using personal accounts for investigations.

2.8 OSINT APPLICATION BY MALAYSIAN PHARMACY ENFORCEMENT OFFICER

Despite many studies on OSINT investigation globally, this research failed to find any published study on the OSINT practice of Malaysian pharmacy enforcement agencies. Pharmacy enforcement officers adopt OSINT techniques in producing profiling reports based on the guidelines issued by the Pharmacy Enforcement Division on February 22, 2023, titled "Profiling in New Media" to gain intelligence for identifying and locating the sellers of illegal and illicit medicines. The suspects' profiling is done by combining information and data acquired from open online sources and close sources from several relevant agencies for verification purposes. The agencies that collaborate with the Pharmacy Enforcement Division and the information provided by them are listed in Table 2.1

Table 2.1 Agencies and their Close Source Information

Agency	Close source information
Telecommunication provider	Phone number ownership
Bank	Bank account ownership & online banking transaction
Companies Commission of Malaysia	Companies and enterprises ownership
Road Transport Department	Vehicle ownership
National Registration Department	Identity and family tree verification
E-Commerce Companies	Online account ownership and trasanctions

Source : Pharmacy Enforcement Division 2023

The guideline is developed by linking several procedures issued by Pharmacy Enforcement Division for certain work processes in suspect profiling. The procedures referred to in the development of this guideline include: 1) Procedure for Information Application from Telecommunications and E-commerce Agencies, and 2) Procedure for Information Application from the Banking Institute.

The guideline lists free online OSINT tools that can be potentially used by pharmacy enforcement officers to gather intelligence, along with the techniques of using Google Dork effectively. The document lists the knowledge requirements and sources for investigators to conduct suspect profiling in new media. This guideline's OSINT techniques and tools for open investigations do not include a statement of references that serves as a standard.

Table 2.2 Knowledge requirements and its sources for investigators to conduct profiling in new media

Knowledge requirement	Sources
Related Pharmacy Enforcement Law	Poisons Act 1952 and its regulation
Open Source Intelligence Technique and Tools (OSINT)	Dangerous Drugs Act 1952 and its regulation
Procedure for Information Application from Telecommunications and Ecommerce Agencies	Medicines (Advertisement and Sale) Act 1956 and its regulation
Procedure for Information Application from the Banking Institute	Sale of Drugs Act 1952 and its regulation
	Registration of Pharmacists Act 1951 and its regulation
	Guidelines on Offence Enforcement in New Media (2022 Edition)

Source: Pharmacy Enforcement Division 2023

The simplified workflow and brief description of the process to complete a profiling report are shown as Figure 2.10 and Table 2.3.

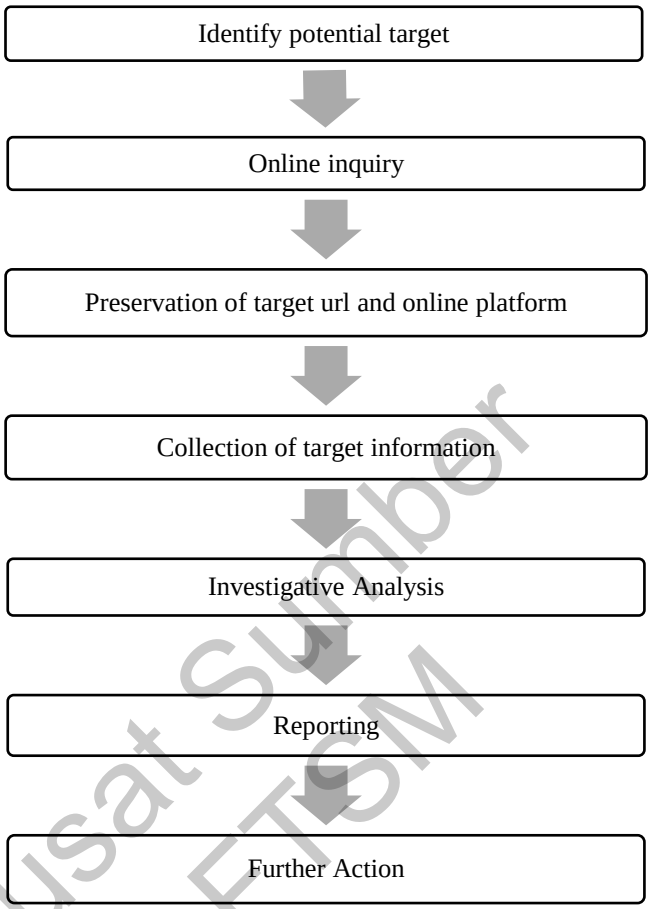

Figure 2.10 Workflow for Suspect profiling using OSINT

Source: Pharmaceutical Service Division 2023

Table 2.3 Description of Profiling

Process	Description
Identify potential target	Target to be profiled will be identified from complaint/information
Online inquiry	Perform online inquiry and identify online platform and URL that is suspected to break the law
Preservation of target url and online platform	Preserve the acquired target information according to "*Procedures for the Preservation of Content in New Media*"

to be continued…

…continuation

Collection of suspect information	Acquire and record any suspects information like phone number, email, account number, nick name, vehicle registration information, using OSINT tools. Extra information can be collected from close-source related agencies.
Investigative Analysis	Get the connection and relationship between other websites, social media and applications with suspect.
Reporting	Report all the findings and get the report checked by superior.
Further Action	Further action will be decided from the report findings. Further actions include: 1. Warning letter to suspect 2. The case will be forwarded to Intelligence Unit 3. The case will lead to direct raid. 4. Refer the case to other Pharmacy Enforcement Branch 5. No further action 6. Others.

Source: Pharmaceutical Service Division 2023

2.9 COMPARATIVE REVIEW OF OSINT WORK PROCESS

For this particular research, the Pharmaceutical Service Division OSINT work process is compared to two recent models of open investigation by United Nations in Berkeley Protocol (2022) and Michael Bezzel (2021) in his book "*Open Source Intelligence Techniques Resources for Searching And Analyzing Online Information Eighth Edition*". For most of the OSINT work process, it is safe to make an early conclusion that the OSINT methods employed by Pharmaceutical Service Division are generally in line with OSINT methods proposed by United Nations and Michael Bezzel, apart from one obvious aspect, which is the pre-investigation preparatory phase. The comparison among these three OSINT methodologies is mapped in Table 2.4.

Table 2.4 Comparison of the stages in OSINT work process

OSINT Work Process		**Pharmacy Enforcement Division 2022**	**Berkeley Protocol**	**Michael Bezzel, 2021**
Triage	Mission & Objective	√	√	√
	Target Identification	√		√
Preparation	Investigation Planning		√	√
	Infrastructure-related		√	√
	User-Related		√	
Online Query	Information Discovery	√	√	√
	Preliminary Assessment	√	√	
Data Collection	Open Source	√	√	√
	Closed Source	√		√
Processing		√	√	√
Preservation		√	√	
Analyzing		√	√	√
Reporting		√	√	√
Archieve And Cleaning				√

This research will focus on the preparatory phase before initiating any open investigation, as suggested by the United Nations and Michael Bezzel. In the Berkeley Protocol, there is a dedicated chapter that explains in detail the preparatory phase that every OSINT investigator needs to conduct to safeguard themselves, the investigation, and their organization during an open investigation. Similarly, Michael Bezzel dedicates the first section of his book to OSINT preparation, which comprises eight chapters altogether. It is an update from his previous publication, where the pre-investigation preparation was not discussed. Contrary to OSINT methods adopted by Malaysian pharmacy agencies, this preparation phase is not addressed or emphasized, which opens an opportunity for further improvement. The cybersecurity aspect of open investigation, especially for law enforcement agencies, has increasingly been discussed and addressed in recent years. Böhm and Lolagar (2021) discussed in detail the direction

phase which is the phase dedicated to planning and preparation that should be conducted by investigators before starting any investigations.

According to Berkeley Protocol, investigators should develop online investigation plans by taking into consideration things like digital landscape assessment, threat and risk assessment before starting any investigations. The plan should clearly define the objective, priority, and strategy that will be implemented during the investigation. The protocol also emphasizes the infrastructure and user-related considerations for investigators to address pre-investigation.

Bezzel (2021) suggested that OSINT investigators take precautionary measures such as conducting threat assessments and rigorous planning to get the best result from investigations. He also focused on optimising the computing environment for OSINT investigators to conduct safe and digitally secured open investigations, which is essentially the main change and improvement in his latest book edition compared to his previous four editions.

The preparatory phase for open investigation will be discussed in this research, using three main elements: investigation planning, infrastructure-related preparation, and user-related preparation, with OSINT work process from Berkeley Protocol and Michael Bezzel as the references.

2.9.1 Investigation Planning

It is crucial for OSINT investigators to be guided by a thorough online investigation that addresses general investigative approaches as well as specific online investigation actions before initiating an open-source investigation. Online investigation planning should be easily integrated into a broader investigation plan if it is part of an investigation that includes conventional methods. The plan should also be developed with the intention that it will be easy to review and update whenever necessary to promote effectiveness while maintaining accountability throughout the process. Berkeley Protocol identifies six key components of an online investigation plan that include:

1. Objectives and Planned Activities: OSINT investigators should establish a timeframe for investigation completion, define the goals and objectives for open source investigations and outline the approach to accomplish these objectives.

2. Risk Management Strategy: Potential cyber threats should be able to be identified by OSINT investigators. They should develop a thorough strategy for identifying, addressing and recovering from breaches and attacks.

3. Mapping Actors and Cooperation Opportunities: Prior to initiating an open investigation, OSINT investigators must be able to identify and map other actors engaged in similar investigations to explore potential collaborations and partnerships that can be conducted. This involves assessing the activities of other relevant groups of OSINT investigators.

4. Resources: All the necessary resources for open investigations must be identified by the OSINT investigator including staffing, training, tools, and equipment. They should also consider the inclusivity and diversity of the team, infrastructure requirements, and financial costs that each open investigation might require.

5. Roles and Responsibilities: In team or partnership settings, the OSINT investigator should clearly define the roles and responsibilities of each member involved in the investigation. It is an essential step to ensure coordination, avoid duplications, and identify any specialised expertise required for the investigation

6. Documentation: Develop a documentation strategy that efficiently manages the investigation, ensuring compliance with accountability principles. This includes mechanisms for creating tasks, reporting methodologies and techniques.

2.9.2 Infrastructure Preparation

The scope and nature of open investigations, the subject of interest, as well as the financial capabilities of an organization to construct, maintain and modify the infrastructure, will dictate the necessary infrastructure for OSINT investigators to work

on (United Nations for Human Rights Office of the High Commissioner 2022). Bezzel (2021) suggested that it is ideal for OSINT investigators to conduct their open investigation on a dedicated machine that is not used for other purposes to exclude all the possibilities of data contamination, malware problems, and conflicts of interest. He went an extra length by strongly suggesting that the machine being used for open investigations should be reformatted each time any new investigation is conducted on the machine for a clean host. The following are the basic infrastructure preparations that OSINT investigators should address before initiating an open investigation, as suggested by Michael Bezzel.

1. Operating System (Windows 10): The host machine should be reformatted to create an ideal environment for open investigation and be free from contamination. For Windows 10 computers, backup important data by connecting an external drive via USB and copying any essential documents, configuration files, and media that are most probably located in Desktop, Downloads, and Documents folders. After everything is double-checked, all data can be removed from the drive. Windows 10 can be reset to the factory setting through these steps:

   Start > *Settings* > *Update & Security* > *Recovery* and "Get started" button. Select "Remove everything" and choose "clean the drive" to create a new operating system free of previous contamination.

   The original installation media or a restore CD can be used for older Windows systems. Users are also advised to disconnect from internet connection during installation to eliminate the need for Microsoft to create a Microsoft account.

2. Antivirus (Windows): For users of Microsoft's products, especially Windows 8 and 10, Windows Defender antivirus is recommended for the protection of their machines while Microsoft Security Essentials is recommended for Windows 7 users. Although there is privacy concern when using Microsoft products where users' computer usage history will be collected, their core operating systems also collect and analyse user data, making it difficult to disable it long-term.

3. Antimalware: Apart from antivirus, protection against malware is similarly vital. For both Windows and Apple users, the recommended antimalware is Malwarebyte (https://www.malwarebytes.com/) as it is completely free and thorough without the need to upgrade to premium features as the free version is sufficient for machine protection. A full machine scan by Malwarebyte should be conducted on a weekly basis as Malwarebytes will remove any issues it finds. By installing proper antimalware and antivirus, user's computer can run smoothly and may prevent malicious files from infecting their operating system and more importantly, help to protect the integrity of any online investigations.

4. Virtual Private Network: Although some browser extensions allow VPNs to intercept data, investigators are not recommended to use them as this will only protect browser traffic and not the host computer. A dedicated VPN application should protect both computers and virtual machines. Proton VPN and PIA (Private Internet Access) are two examples of VPN software that offer sufficient protection to their premium users' accounts. Proton VPN is more favoured than PIA as it is more secure but less popular, although it will cost more than PIA. Nonetheless, a reputable VPN is much better than no protection at all.

5. Password Manager: It is challenging for OSINT investigators to manage numerous accounts and profiles across various platforms where multiple profile details and passwords must be handled and documented properly. This is where password manager applications like KeePassXC (https://keepassxc.org/) can provide a secure database for storing these settings. KeePassXC is a free, cross-platform that offers data and credential protections in open online investigations. It works on Windows, Linux and Mac computers making it a suitable choice for security.

6. Web Browser: For online investigations, Firefox is highly recommended as the default browser provided it is properly configured. Although it is believed that Firefox installation is much more private and secure than most other browsers, users should still consider some modifications. Firefox is the most robust,

secure, and appropriate option for almost any computer and virtual machine. However, it is recommended to change the following settings within Firefox:

a. To prevents internet usage information from being sent to Firefox, users should uncheck "Recommend extensions as you browse" and "Recommend features as you browse" ln the "General" options.

b. To clean the data every time investigators exit the browser, they should enable "Delete cookies and site data when Firefox is closed" in the "Privacy & Security" options.

c. To avoid prompt for login and password saving, uncheck the box titled "Ask to save logins and passwords for websites".

d. To prevent Firefox from collecting data regarding browsing and download history, uncheck the box titled "Remember browsing and download history".

e. To prevent Firefox from collecting data regarding searching and form history uncheck the box titled "Remember search and form history".

f. To erase all histories when exiting the browser, check the "Clear history when Firefox closes" box.

g. To deny a request for permission for geolocation, camera and microphone use by the browser, click "Settings" next to Location, Camera, Microphone, and Notifications and check the box titled "Block new requests ... " for each of these options in the "Permissions" menu.

h. Uncheck all options under "Firefox Data Collection and Use".

7. Virtual Machine (VM): VM is a computer operating system on top of another computer operating system that simulates a specific computer system. It has the advantage of being independent of the host operating system and can launch

multiple operating systems within the same program. This will allow for a secure environment in which to investigate a single target without any trace of contamination. One of the free and easy-to-use virtualisation software that can be used is VirtualBox (https://www.virtualbox.org/). The only requirement for investigators to use VirtualBox is a computer that supports virtualisation. Most mid-range and high-end Windows computers that were made within the past five years should work without any issues. Still, it may require enabling virtualisation support in the basic input/output system (BIOS) during setup.

2.9.3 User Related Preparation

Security is everyone's responsibility. The key to cybersecurity is individuals should not engage in activities that could put data or persons at risk. User-related preparation for open investigation will be discussed in this research in three aspects: training, online presence, and user camouflage

1. Training: Organizations should train their investigators to assess appropriate online behaviours and maintain a consistent policy on best practices and cybersecurity training to protect themselves from malicious actors. There is no consensus on the ideal frequency of cybersecurity training as it depends on the type of training offered and the type of organization itself. However, frequent and periodic training sessions are essential to ensure conformity to new policies and technologies. Similarly, scheduled updates and evaluations of training will also be massively beneficial. It is proven that a lack of awareness and knowledge can lead to violations of security policies. An organization should also consider competency-based training. This type of training concentrates on determining if the member of the organization possess the skills and knowledge required to perform their tasks well. It places more emphasis on developing practical skills and talents than it does on imparting academic knowledge (Chowdhury et al. 2022).

2. Online Presence: Many experts warn against the dangers of oversharing information online, especially among senior law enforcement officers, as it can

create vulnerabilities for entire departments. By using free OSINT tools, it is possible for malicious actors to map the whole force from top to bottom. They also emphasise the importance of OSINT investigators maintaining minimal digital footprints, especially among junior officers and new recruits who are known to have a long-standing social media presence. Awareness about digital footprints and 'how to stay private online' should be included in training at all levels of law enforcement organisations. OSINT-investigators should regularly conduct OSINT on themselves to obtain a picture of their own online exposure (Saskia et al. 2022)

3. User Camouflage: From a security perspective, OSINT investigators should always use camouflage when conducting online investigations. User camouflage for OSINT investigators can be achieved by creating cover accounts or virtual identities. It is a false online identity or profile that can be used on platforms that require users to log in to access content, which includes social media platforms, an email or messaging service, a database, or any application. Virtual identity details and their activities should be recorded during every online investigation.

2.10 SUMMARY

Clearly, the relationship between OSINT and cybersecurity is an important area of interest for practitioners and researchers. This chapter serves as a guide for exploring the current existing knowledge and lays the groundwork for the subsequent chapters which will explore in further detail the potential improvements in security measures and the work process of OSINT investigations.

.

CHAPTER III

METHODOLOGY

3.1 INTRODUCTION

Chapter III explains the methodology used to conduct this research. The methodology is the process of gathering knowledge and facts in order to make sound conclusions. As a result, this chapter will offer a full description of the research methodologies employed and chosen to get legitimate results. The elements like research design, data collection methods, the development of survey questions, and data analysis methods are discussed thoroughly.

3.2 RESEARCH DESIGN

This study adopted a mixed approach that combined qualitative and quantitative methods to get a more comprehensive result effectively. For qualitative methods, the analysis of literature reviews related to several areas of study, i.e. the current situation of Malaysian illegal medicines trades, the enforcement agency and their initiatives in combating the widespread situation, an overview of OSINT investigation and its challenges, current OSINT methods adopted by Malaysian pharmacy enforcement agencies, as well as a comparative study of selected OSINT guidelines are conducted. For quantitative methods, the analysis of the questionnaire survey carried out with several cybersecurity experts is conducted to obtain feedback on the importance of security and protective measures in conducting online investigations. The interview sessions also provide a suitable medium to identify the requirements of personnel and infrastructure for implementing the identified measures.

The questionnaire survey for the quantitative method will be framed according to the elements identified from the OSINT model in Chapter II after the population and

the sample size for the survey have been identified. The population involved in this research are experts selected from Malaysian agencies whose scope of work has been mandated in the field of information security and agencies that are active in developing and empowering the culture of information security. This questionnaire survey will focus in detail on the security and preparatory measures for OSINT investigators that can be applied based on the review of the literature, guidelines, government circulars and documents on security standards.

Combining the data from the literature review and supplementing it with the feedback from the domain experts, this research structured a complete enhanced work process for a more secure OSINT investigation. Based on the proposed work process developed, a preparatory checklist form for OSINT investigation was streamlined in an orderly form.

3.3 DATA COLLECTION METHODS

For the purpose of developing an enhanced work process for a more secure OSINT investigation by pharmacy enforcement officers, data is collected by both qualitative and quantitative methods and analyzed to obtain the results that will be required to achieve the objectives. In this research, two data collection procedures will be used, namely the study of literature and expert interviews.

3.3.1 Literature Review

A literature review is imperative in research in order to grasp the current situation and identify gaps and obstacles in the subject matter. Several types and approaches of literature reviews can be conducted to help gain updated knowledge on a field and assist researchers to fill gaps in the knowledge on that topic. Snyder (2019) conducted a comparative study on the three approaches to literature review: systematic, semi-systematic, and integrative.

Table 3.1 summarizes the comparison between these three approaches to literature review by (Snyder 2019).

Table 3.1 Approaches to Literature Reviews

Review Type	Purpose	Strategy	Features
Systematic Review	Evidence synthesize & Comparison	Systematic	Quantitative, comprehensive for specific area, informs practice
Semi-systematic Review	Overview of research area and track changes within the area	Sytematic/non-systematic	Quantitative or qualitative, identifies themes or research gaps, develops a theoretical model or provides a history of the field
Integrative Review	Analyze literature to develop new perspectives or theories	Non-systematic	Qualitative, combines ideas from different fields, focus on creating new frameworks or theories by critiquing previous ideas

Source: Snyder 2019

A semi-systematic review is the approach of literature review chosen for this research. This type of review can generally be used to identify themes, theoretical perspectives, and other qualitative information about a particular subject. The Semi-systematic review is also valuable for developing a theoretical model and a research plan for a discipline (Snyder 2019). Zunder (2021) adopted a semi-systematic review for his publication "A semi-systematic literature review, identifying research opportunities for more sustainable, receiver-led inbound urban logistics flows to large higher education institutions". He described the semi-systematic review as a literature review which uses a systematic approach in terms of literature survey and selection and a narrative approach, which allows "plurality of knowing" by readers' judgement. This allowed the literature review to be transparent about literature searching while at the same time having the potential for extensiveness.

The literature review conducted consists of 3 major steps that are:

1. Outlining Literature Review

2. Conducting Literature Review

3. Reporting Literature Review

a. Outlining Literature Review

This research's main objective is to address the security concern associated with the current OSINT practice of Malaysian pharmacy enforcement officers and propose a new work process for conducting a more secure OSINT investigation. Thus, these four (4) electronic databases were selected to obtain information about several subject areas related to the objectives, in addition to Google Scholar for the search for grey literature.

1. ScienceDirect (https://www.sciencedirect.com/)
2. Semantic Scholar (https://www.semanticscholar.org/)
3. Emerald Insight (https://www.emerald.com/insight/)
4. Springer Link (https://link.springer.com/)

This literature review was conducted by defining the inclusion and exclusion criteria of the literature analysed. The publication was restricted to the year 2013 onward to identify the most up-to-date literature. As this research mainly focused on Malaysian law and socioeconomic states, publications in English and Bahasa Malaysia will be analysed. In the effort to produce a comprehensive literature review, the types of publications that are analysed include review papers and research articles. Any publications, guidelines, and expert opinions considered relevant to reader judgment are also analysed. The reference lists of each chosen article were searched manually to further search for potentially eligible publications. Publications that are irrelevant were excluded with the initial screening of the titles and abstracts. After the initial screening, the full texts of potentially eligible publications were further reviewed to examine their eligibility. Table 3.2 summarises the criterion types with their descriptions.

Table 3.2 Inclusion Criteria and Exclusion Criteria

Criteria type	Inclusion Criteria	Exclusion Criteria
Period	Article years of publication from 2013 to present	Articles published before 2013
Language	Articles written in English or Bahasa Malaysia	Articles written in other languages
Type	Book, review paper and research articles	Other type
Accessibility	All articles that are accessibles	All articles that are not accessibles

The research strategies are categorized into four (4) phases according to the explored fields of study, such as follows:

1. Identify the current situation of Malaysian illegal medicines trades.

2. Identify the Malaysian pharmacy enforcement agency and its enforcement and regulatory activities.

3. Search for OSINT model and security challenges in conducting a digital open investigation

4. Identify the OSINT method adopted by pharmacy enforcement agencies in Malaysia and conduct a comparative study of the published OSINT model.

In each step, a keyword with the Boolean operators is applied to serve as the practical screen for literature search and selection. In Phase 1, the aim is to observe the existing state of Malaysian illegal online medicines trades. The objective is to get an overview of the seriousness and extensiveness of Malaysia's illegal online medicine trade that necessitates effective enforcement and the danger it brings to consumers. Therefore, the keyword with the Boolean operator applied is (“illegal medical products OR unregistered drugs”) AND “Malaysia”.

In Phase 2, the aim is to identify the enforcement agency responsible for curbing the crime of selling and possessing illegal and unregistered drugs in Malaysia. It also serves the purpose of identifying the initiatives and enforcement activities conducted by the agency to tackle the issues of illegal medicines trades to protect the consumers. The keyword with the Boolean operator applied is ("pharmacy enforcement") AND "Malaysia".

Next, Phase 3 aims to overview the use of OSINT to gather and obtain information regarding the data of interest. This study aims to identify the various types of variances of OSINT methods/cycles that have been established and are widely used. This phase will also identify the known advantages, disadvantages and challenges of using OSINT in intelligence gathering especially in the aspect of security. The keyword with the Boolean's operator applied is ("OSINT") AND ("technique OR method") AND (security challenges).

The final phase, Phase 4, aims to overview the OSINT methods adopted by Malaysian pharmacy enforcement officers in conducting digital open-source investigations and identify possible security challenges associated with open-source investigations. This phase focused on preparation and security prior to open-source investigations conducted by pharmacy enforcement officers. A comparative approach is made between the current OSINT methods applied by Malaysian pharmacy enforcement officers and several published OSINT guidelines and protocols to search for elements that can be improved in cybersecurity aspects. The keyword with the Boolean's operator applied is ("OSINT" OR "open source intelligence" OR "open source investigations" AND ("protocol" OR 'guideline").

Several grey literatures that were only available outside the traditional commercial or academic publishing and distribution channels were searched using Google Scholar and direct Google search.

b. Conducting Literature Review

The reviewing process is performed for four (4) months, from September 2023 to January 2024, using Mendeley References Manager for better literature management.

The four electronic databases were browsed to search for relevant publications for this research, as full access was obtained to all these databases.

For Phase 1, a total of 686 documents are initially searched from all four (4) electronic databases using the keyword of Boolean's operator. Initially, no restriction is applied to the type of articles searched. However, due to the large number of search results returned, only review papers and research articles were selected for the next stage. The shortlisted publications were uploaded to Mendeley References Manager to ensure any redundancy in the contents of four (4) electronic journals was removed from the list. All the publications are then further screened based on the keywords in the title, keyword, and abstract, which address the objective of phase 1 of identifying the current situation of Malaysian illegal medicine trades. The filter of years of articles published is set from 2013 until 2023. At the end of the second screening, only 67 publications were selected based on keywords in the title, keyword, and abstract. For phase 1 literature review, 25 papers were chosen after excluding those that discuss the situation of illegal medicine trades outside of Malaysia.

The same methods were applied to the remaining phases of the literature review for this research. For Phase 2, a total of 2688 documents are initially searched from all four (4) electronic databases without any restriction on the type of article. Although the keyword with the Boolean operator ("pharmacy enforcement") AND "Malaysia" is applied, a large number of search result returned. The number of search results was reduced after restricting the type of literature to review papers and research articles only. After removing the redundant literature using Mendeley References Manager and further screening it based on the keywords in the title, keyword, and abstract which address the agency responsible for curbing the crime of selling and possessing illegal and unregistered drugs in Malaysia and their enforcement activities, six (6) publications were selected for phase 2. The filter of years of articles published is set from 2013 until 2023.

For phase 3, the initial search result returns 728 documents from all four (4) electronic databases without any restrictions on the type of literature applied. The type of literature is then further restricted to books, review papers, and research articles only.

All the redundant literature are then removed by using Mendeley References Manager, and through further screening based on the keywords in the title, keyword, and abstract, nineteen (19) articles and books are selected for phase 3 after excluding articles that discuss OSINT from business perspective.

For phase 4, the additional inclusion criteria used are articles produced by academicians, government agencies, and research institutes and models that were already tested on organizations. In addition to four (4) electronic databases, Google Scholar is used to search for any grey literature that addresses several published OSINT guidelines and protocols. A total of 787 documents are initially searched from all databases using the keyword of Boolean's operator without any restriction on the type of literature. The type of literature is then further restricted to books, review papers, and research articles only. After removing all the redundant literature by using Mendeley References Manager, and through further screening based on the keywords in the title, keyword, and abstract, a total of five (5) literatures are selected for phase 4 which mainly discusses OSINT work process in the perspective of law enforcement.

A total of 55 documents are analyzed in all four phases of the literature review. Out of 55 documents, 7 are published in Bahasa Melayu, and they mainly consist of guidelines and circulars issued by the Malaysian government.

c. Reporting Literature Review

All selected publications were managed and recorded using software tools like Mendeley References Manager. The features of software tools allowed all data to be extracted and filtered according to authors, year, title, location of publication, and sources. All articles collected were read carefully, and the related data were tagged using Mendeley References Manager to ease the process of recollection and filtering.

3.3.2 Expert Interview

In developing an enhanced model for the OSINT work process, opinions and feedback from domain experts were obtained using questionnaire surveys. A set of questions was developed for the experts involved in developing government information security

policies or handling public sector security incidents. The experience and responsibility of each of these domain experts in the field of information security will be taken into account during this interview to obtain relevant opinions and feedback on the issues and matters needed to develop the work process.

a. Inclusion Criteria and Requirements for Experts

All the interview sessions with domain experts were conducted in a face-to-face setting. The respondents who participated in the interview received no compensation for participating in this study to avoid any conflict of interest. Potential candidates were contacted based on recommendations from their department or superior. There are several inclusion criteria and requirements adopted from Guideline to Determine Information Security Professionals Requirements for the CNII Agencies / Organisations issued by Cybersecurity Malaysia in 2013 to justify the selection of participants for the interviews.

Cybersecurity Malaysia (2013) defined Information Security Professional as :

i. "*Information security practitioners who conform with the requirements of this Information Security Professional Guideline; and*

ii. *Information security practitioners with specific roles and responsibilities in Information Security Operation, Information Security Compliance and Information Security Audit*".

There are five (5) requirements for personnel to be an Information Security Professional as adopted by Cybersecurity Malaysia. All participants in the interviews were made to follow all the requirements needed by Cybersecurity Malaysia for them to be considered as eligible information security professionals for this research. Table 3.3 summarises the requirements in the Guideline to Determine Information Security Professionals Requirements for the CNII Agencies / Organisations and their descriptions.

Table 3.3 Cybersecurity Malaysia Information Security Professional Requirements

Requirement	Description
Educations/Qualifications	Preferably a degree holder in the following fields: 1. Information Security 2. Computer Science 3. Information Technology 4. Management Information System 5. Business Information System 6. Business 7. Accounting Economic or equivalent
Professional Certifications	Certified by a recognised local or international information security certification body
Experiences and Skills	Adequate number of years (not specified) of information security work experience
Continuous Learning	Obtained sufficient Continuing Professional Development (CPD) or Continuing Professional Education (CPE) points as required by information security professional certification body
Code of Conduct	Demonstrate a high standard of ethical conduct in accordance with their professional certification code of conduct and employment requirements.

Source: Cybersecurity Malaysia 2013

b. Expert Sampling

Two (2) agencies have been identified as the established national lead agencies for cyber security matters in Malaysia: National Cyber Security Agency (NACSA) and Cybersecurity Malaysia (CSM). The participants for the interviews were selected from both agencies, which are located in Putrajaya for the former and Cyberjaya for the latter.

As the target population for this research is exclusively comprised of experts and professionals in cybersecurity, the sampling method chosen is purposive sampling. Purposive sampling is a non-probability sampling technique, also known as authoritative sampling, purposive sampling, or judgmental sampling. This method of sampling chooses sample members exclusively based on the researcher's knowledge and judgement. In addition, purposive sampling can be effective when there are just a small number of samples in a population that exhibit the characteristics that a researcher anticipates from the target population (Akpan et al., 2023). The participants in the interviews were selected based on the inclusion criteria and requirements defined in

Table 3.3 and also based on the recommendations from the respected agency management.

c. Interview Protocol and Data Collection

The interview that was conducted to gain feedback and opinions from cybersecurity experts and professionals comprised two main phases. The first phase involved the preliminary process, where the interview scope was determined and eligible respondents were identified.

Prior to conducting the interview, the first phase also involved obtaining a letter of support from the Faculty of Information Science and Technology (FTSM), UKM to conduct research at NACSA and CSM, as shown in Appendix A and Appendix B. After that, the next process is the application for permission to conduct research from both agency management and setting the appointment date for the interview session with selected participants. The protocol and procedures developed must be followed in accordance with both agencies' cybersecurity policies. Upon approval to conduct the research, site visits to NACSA and CSM were conducted for an early discussion to determine the interview's scope and a selection of the potential respondents.

The second phase involved the actual interview sessions conducted in a face-to-face setting with each respondent. The interview session allowed data collection activities through questionnaires distributed to the respondents through Google Forms. Although the interview sessions were held in face-to-face settings, this data collection method using Google Forms was adopted for ease of recording and reporting.

Figure 3.1 summarized the process of conducting the interview session and also the collection of data.

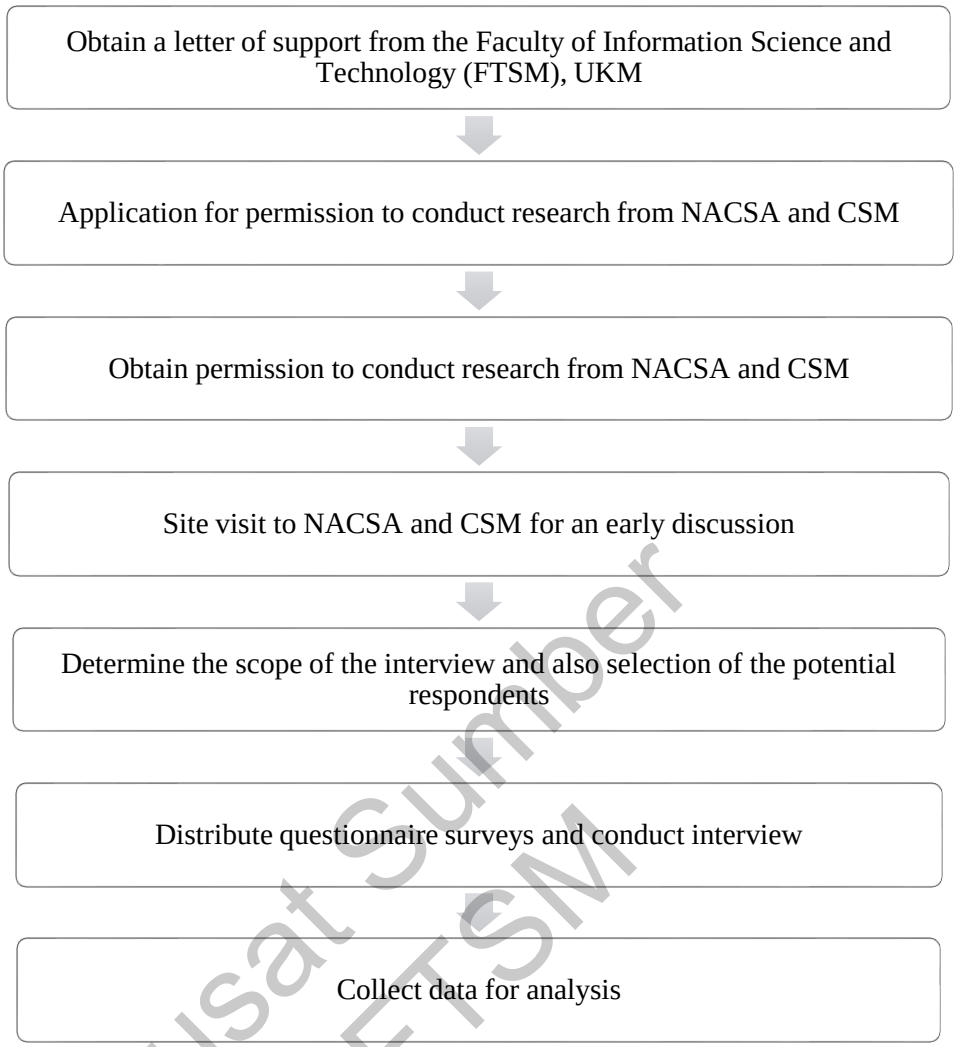

Figure 3.1 Data Collection Process From Interview

3.4 DEVELOPMENT OF QUESTIONNAIRE SURVEY

A questionnaire survey was chosen to gather expert feedback and opinions as it standardises the data collection procedure and provides comparable results. It ensures a faster and more accurate data collection procedure and ease of data processing. A set questionnaire survey was designed to best address this study's research objectives, research question, and problem statement. The review of the literature and the gap of knowledge found in Chapter II assist in preparing the questionnaire survey. The data and information from the questionnaire survey will be expressed in numerical and non-numerical formats. The numerical data will be analysed using descriptive statistics to obtain the percentage of expert approval. The non-numerical data will be expressed to assist numerical data in detailing the information required to develop a new work

process for open-source investigations by pharmacy enforcement officers. Several aspects need to be addressed in designing an effective questionnaire: type of questionnaire, method of conducting questionnaire, type of questions, type of response, and good practice.

Generally, there are two common types of questionnaires, known as structured questionnaires and unstructured questionnaires. A structured questionnaire usually employs specified and closed-ended questions, allowing for fewer discrepancies and easier data management. On the other hand, unstructured types generally use open-ended questions and capture opinions in a focus group (Taherdoost 2022). This research uses a combination of structured and unstructured questionnaires, known as a quasi-type of questionnaires, where it employs structured type in most of the questions and applies some unstructured questions to capture expert opinions and feedback that cannot be covered in a structured questionnaire.

The questionnaire was conducted using an interviewer-based survey where the interviewer and interviewee were in a face-to-face setting during the interview. Although this method involves a higher cost and requires a longer time, it is feasible to incite a specific response and expert feedback (Sreejesh S, Mohapatra, and M.R 2014).

Taherdoost (2022) listed some recommendations for producing questions for an effective and high quality questionnaire survey. The recommendations include:

1. The questions should be short and precise and should not be designed to be time-consuming for the respondent to answer

2. Avoid using technical terms and terminology difficult for all responders to grasp. Questions should be written in as plain and straightforward a manner as feasible.

3. Define the questions correctly and in-depth so that respondents may readily answer them without becoming confused.

4. Avoid questions that are not related to the objectives of the research. The questions should be employed to meet the purpose of the research.

3.4.1 Preliminary Validation of Questionnaire Survey

Before the actual data collection, a set of questionnaires survey was distributed to a group of two (2) officers at The Malaysian Administrative Modernisation and Management Planning Unit (MAMPU) from the Information Technology Division to assist in the content validation of the questionnaire survey and to identify the appropriateness of question types and levels of questions to be distributed to the respondents. The first drafted set of questionnaires consists of 30 close-ended questions consisting of six (6) sections to obtain data on demographics, threats elements, preparation elements, human factors, technology factors, and process factors. The selected officers were given one hour to evaluate the first set of questionnaires from four given criteria. They were allowed to provide any opinions and suggestions for improvement if necessary. The summary of the evaluation results of this questionnaire for each evaluator is shown in Table 3.4 and Table 3.5 showing the need for improvement on the questionnaire survey questions for this study.

Table 3.4 Validation of Questionnaire by Evaluator 1

Evaluation Criteria	**Part 1 Demographic**	**Threat Element**	**Preparation Element**	**Part 2 Human Factors**	**Technology Factors**	**Process Factors**
Question suitability and relevancy level	Suitable and relevant	Suitable and relevant	Suitable and relevant	Suitable and relevant	Suitable and relevant	Suitable and relevant
Question difficulty level	Easy	Fair	Question B2 is unclear	Easy	Fair	Fair
Question length and number	Maintain	Question A3 and A4 are too lengthy	Maintain	Question C3 is too lengthy	Maintain	Maintain
Suggestions	-Experts certification. -Conduct questionnaire from several agencies	-Try to simplify the questions	-Include example of resources in question B2	Try to simplify the question	-None	- The need for periodic review of work process

Table 3.5 Validation of Questionnaire by Evaluator 2

Evaluation Criteria	Part 1 Demographic	Part 2 Threat Element	Preparation Element	Human Factors	Technology Factors	Process Factors
Question suitability and relevancy level	Suitable and relevant	Suitable and relevant	Suitable and relevant	Suitable and relevant	Suitable and relevant	Suitable and relevant
Question difficulty level	Easy	Easy	Easy	Fair	Fair	Fair
Question length and number	Maintain	Question A4 is too lengthy	Maintain	Maintain	Maintain	Maintain
Suggestions	-None	-Try to simplify the question	-None	-None	-Include a question about the advantages of a password manager for investigator	-None

3.4.2 Questionnaire Survey Design

The questionnaire survey as shown in Appendix C is structured into two sections, Part I: Background and Part II: Interview Questions, which are divided into five sub-sections.

Part I consists of questions involving the background of the respondents. The questions are developed to ensure the eligibility of the selected respondent participating in the interview sessions. Detailed respondent information will be recorded while maintaining their anonymity. On the other hand, Part II will be focused on the elements to be studied in Chapter II.

As the questionnaire survey is designed as a quasi-type, the responses for the structured part of the questionnaire will be analysed using the Likert scale as the measurement method. In contrast, the response for the unstructured part of the questionnaire, which uses open-ended questions, will be recorded in its original form.

This research chooses the Likert scale as the main method of quantifying expert responses as it helps shape opinion-based questions, especially for some issues that are not quantifiable. The scaling method assists researchers in obtaining general conclusions as well as the reliability of their collected data (Taherdoost 2022). The Likert scale consists of a fixed format of answer options and is frequently used to measure the respondent's level of consensus. The Likert scale used in this research consists of five levels ranging from 1 to 5. Value 1 represents a Strongly Disagree opinion, and Value 5 represents a Strongly Agree opinion. Respondents were required to choose only one answer option they considered the most accurate. Table 3.6 summarizes the design and structure of the questionnaire survey developed.

Table 3.6 Structure of the Questionnaire Survey

Part	Description	No. of Question
1	Respondents' Background	5
2	a. Elements of Threat	5
	b. Elements of Preparation	5
	c. Elements of Human Factor	5
	d. Elements of Process	5
	e. Elements of Technology	5

a. Part I: Respondents' Background

Part I of the questionnaire survey is developed by taking into account the inclusion criteria and requirements for personnel to be an Information Security Personnel as employed in Guideline to Determine Information Security Professionals Requirements for the CNII Agencies / Organisations issued by Cybersecurity Malaysia in Table. This allows a standard requirement for a researcher to justify the selection of participants in this research. The information gathered includes respondents' academic qualifications, certification in information security, current field of duty, area of expertise and total years of service.

b. Part II: Questions

In Part II, the questions are presented into five (5) sub-sections, each comprising five (5) questions that will measure and record the expert's opinion on the elements of the

OSINT work process. All the collected data will then be used to draft and suggest an enhanced model of the OSINT work process with improved security and preparatory measures to safeguard the investigator and pharmacy enforcement agency. The questions in the questionnaire are designed mainly based on the techniques and methods employed in Berkeley Protocol on Digital Open Source Investigations published by United Nations in 2022 and several publications dedicated to open source intelligence gathering methods. Apart from that, the development of questionnaire questions will also be ensured to be in line with the current policies and circulars issued by the Government of Malaysia. As Pharmacy Enforcement Division is a division under the Ministry of Health, the policy referred to in developing the questionnaire survey is ICT Security Policy MOH Version 5.0, issued in 2019.

Referring to the structure of the questionnaire survey in Table 3.6, subsection A will address the elements of threat in OSINT investigations that pharmacy enforcement officer might encounter in their line of work. A threat can be defined as anything that can exploit a vulnerability and ultimately damage or destroy an asset. The source of a threat can be internal or external to an organisation or investigation. By recognising the type and source of a threat, open-source investigators can safeguard themselves and their respective organisations from the damage they can inflict. The set of questions and their sources presented in subsection A are listed in Table 3.7.

Table 3.7 Subsection A Questions

No.	Question	Source
A1	OSINT investigators are also accountable for their security, not just by relying on information security personnel.	United Nations for Human Rights Office of the High Commissioner. 2022
A2	Online vulnerabilities like cookies, trackers, and scripts could be exploited to gain unauthorized access to an asset, while online research is conducted	Bazzel Michael 2021
A3	OSINT can be a double-edged sword for law enforcement agencies. It can be used to track down criminals and can be misused by criminals to instigate cyber-attacks against law enforcement agency	Hwang et al. 2022

to be continued…

…continuation

A4	OSINT investigators are more susceptible to cyber threats like distributed denial of service (DDOS) attacks, Man-in-the-middle (MITM) attacks, phishing attacks, and malware without sufficient preparatory measures	United Nations for Human Rights Office of the High Commissioner. 2022
A5	OSINT investigators must be able to identify assets that need protection and assess potential threats, risks, and vulnerabilities while investigating.	United Nations for Human Rights Office of the High Commissioner. 2022

Subsection B (Table 3.8) will address the preparations that can be employed against cyber threats before conducting an OSINT investigation. Preparation and proper planning are the keys to secure, safe and thorough open investigations. The preparation phase for digital opening includes three (3) processes: (a) analysing threats and risks and strategizing mitigation measures; (b) reviewing the information landscape; and (c) developing an investigation plan (United Nations for Human Rights Office of the High Commissioner. 2022). The questions are designed to be focused on the need for a proper investigation plan, well-managed documentation, and cybersecurity awareness among OSINT investigators.

Table 3.8 Subsection B Questions

No.	Question	Source
B1	Online investigations plan should include threat and risk assessment, with a strategy for mitigating risk. The plan should address on how to identify, respond to and recover from breaches or attacks.	United Nations for Human Rights Office of the High Commissioner. 2022
B2	OSINT investigators must be able to identify the resources needed to conduct the planned investigations beforehand, which include staffing, training, tools, and equipment.	United Nations for Human Rights Office of the High Commissioner. 2022
B3	Before conducting investigations, OSINT investigators should be well-versed in the knowledge requirements and its sources. This includes legal documents, policies and guidelines	Pharmaceutical Service Programme 2023
B4	Information and Communication Technology Safety Officer should be consulted for advice on security measures for any security concern involving digital open investigation	Ministry Of Health 2019
B5	Continuous and consistent knowledge sharing and strengthening is one of the methods to ensure proper use and security of ICT asset	Ministry Of Health 2019

Subsection C (Table 3.9) addresses the human factor, which is the central part of the intelligence process and remains indispensable despite the emergence of new processes and technologies for OSINT. However, from the perspective of cyber security, several studies indicated that humans are the weakest link in the security chain, and security is only as good as its weakest link (Hadlington 2018). The questions focus on how human factors in OSINT investigation can possibly create preventable vulnerabilities and the strategies to mitigate them.

Table 3.9 Subsection C Questions

No.	Question	Source
C1	OSINT investigators lack awareness and training concerning threats, which calls for more training.	United Nations for Human Rights Office of the High Commissioner., 2022
C2	OSINT investigations should be conducted with investigators maintaining their anonymity online and ensuring their online conduct is as non-attributable as feasible.	United Nations for Human Rights Office of the High Commissioner. 2022
C3	OSINT investigators can be easier targets for phishing attacks and other forms of social engineering if their online conduct has identifiable or predictable patterns of behaviour,	United Nations for Human Rights Office of the High Commissioner. 2022
C4	Several barriers, like time constraints, no dedicated budget for cyber security strategy, and a lack of adequate reporting, hinder the board or top management from effectively dealing with cyber security challenges.	Chartered Institute of Ergonomics & Human Factors 2022
C5	OSINT investigators' practice of using personal accounts to investigate or log in to personal accounts in a browser should be avoided at all costs	United Nations for Human Rights Office of the High Commissioner. 2022

Subsection D (Table 3.10) addresses the elements of technology that are used to create safe and secure OSINT investigations for investigators. The questions highlight the need for infrastructure like facilities and systems, including software and hardware, to conduct open-source investigations. The infrastructure provided for OSINT investigators should integrate sufficient security measures to protect and preserve an organization's assets and data from any possible online threats from suspects and malicious actors.

Table 3.10 Subsection D Questions

No.	Question	Source
D1	Whenever feasible, OSINT investigators should use VPNs, to mask their computers' IP addresses while conducting investigations, avoiding their IP addresses disclosed to the Internet to be linked back to the investigators	Bazzel Michael 2021
D2	Virtual machines have the advantage of masking certain features that malicious actors could misuse to track back investigators	United Nations for Human Rights Office of the High Commissioner. 2022
D3	Using a password manager can provide a secure environment to store numerous passwords for investigators as they usually create and maintain multiple accounts and profiles across various services during the investigation	Bazzel Michael 2021
D4	Before commencing an investigation, OSINT investigators must ensure all equipment has up-to-date software like antivirus and antimalware to protect against threats from malicious actors	United Nations for Human Rights Office of the High Commissioner. 2022
D5	By using an internet browser that has enhanced security features like plug-ins and also by applying appropriate privacy and security settings, investigators can stay hidden and anonymous from suspects	Bazzel Michael 2021

Subsection E (Table 3.11) addresses the elements of process which is the final pillar of cybersecurity apart from people and technology. The questions are designed to highlight the necessity of having proper processes in place to ensure a consistent approach to managing and avoiding security incidents. The element of the process is crucial in describing how security threats and risks can be mitigated through the organization's activities, roles and documentation.

Table 3.11 Subsection E Questions

No.	Question	Source
E1	An organization must provide its OSINT investigator with technical systems or environments that can only be minimally affected in the event of a security incident	United Nations for Human Rights Office of the High Commissioner., 2022

to be continued…

…continuation

E2	Open source investigations should be documented properly, which allows investigators to demonstrate how the information is collected and the steps taken or not taken in the inquiry.	United Nations for Human Rights Office of the High Commissioner. 2022
E3	The roles and responsibilities of open source investigators should be well defined, especially if working in a team or with external partners, which necessitates proper activity coordination.	United Nations for Human Rights Office of the High Commissioner. 2022
E4	Policies involving the handling, preservation and destruction of data should be integrated, and complied with in the course of open investigation	United Nations for Human Rights Office of the High Commissioner. 2022
E5	Security management methods and their implementation such as objectives, controls, policies and procedures should be reviewed independently and periodically	Ministry Of Health 2019

In addition to the structured questionnaire survey, one open-ended question is designed to provide an opportunity for every expert to express their honest opinion and input regarding security in conducting an OSINT investigation. The question allows experts to share their experiences, and, at the same time, provide constructive feedback on strategies to address possible challenges. It also encourages a diverse range of feedback that might not be addressed in the structured part of the questionnaire, and expert can contribute based on their perspective and expertise. The open-ended question is as follows :

"*In your experience, what are the most critical security issue or challenges that OSINT investigator should be mindful of when conducting Open-Source Intelligence (OSINT) investigations, and what strategies do you believe are effective in mitigating these risks*?"

3.5 DATA ANALYSIS

Sabah et al. (2022) define data analysis in research as:

'*…. A process of checking, examining, renovating, modernizing and displaying the data with the aim of exploring useful and valuable information to make a decision regarding any problem.* "

Different methods with different names in all research domains, like business, social, and scientific, have been used for data analysis. Data analysis is used in business, social, and scientific fields to make informed decisions. This research will adopt a method of data analysis called descriptive statistics for the structured part of the questionnaire. This type of analysis aims to facilitate the description and summarization of data using a pictorial or graphical representation to summarise a specific characteristic of a variable or measurement (Cooksey 2020).

For the unstructured part of the questionnaire that comprises an open-ended question, all the feedback and input from the expert will be presented in the original and unedited form for ease of interpretation.

3.5.1 Descriptive Statistic

Descriptive statistical analysis for the data collected from the questionnaire survey research is done using a frequency tabulation procedure, as suggested by Cooksey (2020), which provides a convenient counting summary for a set of data that facilitates further interpretation. Frequency tabulation consists of two stages: 1) First, the data collection scores are ranked from lowest to maximum value. 2) Second, the frequency of each score that appears in the sample is counted. The variables measured in the questionnaire survey are the agreement rate for each question based on the Likert scale, with 1 being the lowest score and 5 being the highest score, which indicates the level of agreement and consensus. For this purpose, the "consensus" and the "cut-off value" for the agreement rate need to be defined.

A consensus is a general agreement or a unanimity of viewpoints of a preselected group of experts representing the field of inquiry. Because this research depends on the regulated input of experts through a series of questions, a consensus among experts may be considered credible. The cut-off value for the agreement rate can be defined as the value from which a consensus was made. Depending on the field, the

value of the cut-off can vary. In some fields of medicine, a consensus is achieved when more than 70% of the respondents agree with the question presented in a questionnaire. For the majority of studies, a threshold of 60% or more was considered credible enough to achieve a consensus among experts (Naserrudin et al. 2022).

Percentile values will be computed from the frequency distribution and added later to form the cumulative percent. A cumulative percent can then be used to find percentiles which reflect the percentage of experts who scored at a specific value. As the objective of this research is to develop a better work process for OSINT investigation, it is determined that the acceptable cumulative percentage of experts' agreement for a consensus and suggestion to be included in the proposed work process is 60% and above, which indicate a high degree of agreement and acceptance.

3.6 SUMMARY

This chapter thoroughly explains the design of the research, which contains the analysis, techniques, and methods used to develop the work process for a more secure and safer OSINT investigation. The data collected from this research is believed to provide insightful information required to develop the work process in more detail. The final result of this research is to develop a work process for OSINT investigation by pharmacy enforcement officers with enhanced security measures against possible cyber threats while conducting an open investigation, which will better protect the investigators themselves and valuable assets belonging to the pharmacy enforcement division. The methodology is designed as the implementation step involved in achieving the objectives of this research, as described in Chapter 1.

CHAPTER IV

RESULTS AND DATA ANALYSIS

4.1 INTRODUCTION

This chapter presents the findings of the study based on the feedback from the respondents in the distributed questionnaire survey in the earlier phase of the study. The result was analysed to generate descriptive statistics using the frequency tabulation procedure suggested by Cooksey (2020). All results of the structured part of the questionnaire survey are presented in tables while the result for the unstructured part is presented in its raw form. The results and data presented in this chapter are then carefully selected and used to achieve the two main objectives of this study, which are to identify security issues and challenges while using OSINT and to propose an enhanced OSINT model with improved security by the Pharmacy Enforcement Division.

4.2 DEMOGRAPHIC OF EXPERTS

All experts who agreed to participate in this study were ensured to fulfil at least three inclusion criteria and requirements adopted from the Guideline to Determine Information Security Professionals Requirements for the CNII Agencies and Organizations issued by Cybersecurity Malaysia (CSM). The guideline suggests that information security professionals should at least have a bachelor's degree in related fields as their highest academic qualification and an adequate number of years (not specified) of information security work experience, and they should be certified by a recognized local or international information security certification body. The demographic data of experts for the questionnaire survey is shown in table 4.1.

Table 4.1 Demographic data of experts

Expert	Agency	Academic Qualification	Current Working Position	Range of Years Of Service	Certification
Expert 1	NACSA	Master's degree	Information Communications Technology Security Officer	20-30	CompTIA Security +
Expert 2	NACSA	Degree	Information Communications Technology Security Officer	0-10	Certified Ethical Hacker
Expert 3	NACSA	Master's degree	Assistant Director	10-20	CompTIA Security +
Expert 4	CSM	Master's degree	Research and Development Manager	10-20	Information Security Management System (ISMS) Lead Auditor
Expert 5	CSM	Master's degree	Information Technology Security Specialist	10-20	GIAC Security Essentials Certification (GSEC), GIAC Certified Intrusion Analyst Certification (GCIA), CompTIA Security+, Certified Blockchain Professional (CBP)

A total of five (5) experts, with three (3) experts from the National Cyber Security Agency (NACSA) and two (2) from Cybersecurity Malaysia (CSM), have participated in the questionnaire survey. Four (4) out of five (5) experts possess a master's degree as their highest academic qualification, while one (1) expert has a degree as his highest academic qualification. Two (2) experts have the roles of information communications technology security officer (ICTSO); the remaining three (3) are assistant directors, research and development managers, and information technology security specialists individually. Three experts have 10 to 20 years of experience, one expert has between 0 to 10 years of experience, and another expert has between 20 to 30 years of experience. All experts are certified by at least one recognized local or international information security certification body. The certifications acquired by the experts include CompTIA Security+, Certified Ethical Hacker, Information Security Management System (ISMS) Lead Auditor, GIAC Security Essentials

Certification (GSEC), GIAC Certified Intrusion Analyst Certification (GCIA), and Certified Blockchain Professional (CBP).

4.3 FREQUENCY ANALYSIS AND PERCENTAGE OF AGREEMENT RATE

The questionnaire survey is conducted using questions, such as those outlined in Appendix C, to gather insights and opinions of experts on the security issue and challenges of OSINT investigations with the purpose of spotting any room for improvement in the current OSINT work process security aspects. The analysis of the data is conducted through descriptive statistics, utilizing frequency and percentage of agreement rate from the experts. For each element of the OSINT work process studied, the frequency and percentage of responses are recorded and calculated. The percentage of agreement rate of 60 percent or more, as suggested by (Naserrudin et al. 2022), is the main consideration for an element to be incorporated into the enhanced OSINT model being developed in this study.

4.3.1 Elements of Threat

This subsection consists of five (5) questions concerning threats associated with OSINT investigations. The frequency and cumulative percentage of agreement for each question of the subsection are displayed in Table 4.2.

Table 4.2 Frequency and Cumulative Percentage of Agreement for Element of Threat

Question	Scale					Cumulative Percentage of Agreement (%)	Consensus
	1	**2**	**3**	**4**	**5**		
A1. OSINT investigators are accountable for their own security, not just by relying on information security personnel	- -	- -	- -	1 (20%)	4 (80%)	100%	Yes

to be continued…

…continuation

A2. Online vulnerabilities like cookies, trackers, and scripts could be exploited to gain unauthorized access to an asset while online research is conducted	-	-	-	1 (20%)	4 (80%)	100%	Yes
A3. OSINT can be a double edge sword for law enforcement agency. It can be used to track down criminal but also can be misused by criminal to instigate cyber attack against law enforcement agency	-	-	-	1 (20%)	4 (80%)	100%	Yes
A4. OSINT investigator are more susceptible cyber threat like distributed denial of service (DDOS) attack, Man in the middle (MITM) attack, phising attack and malware without sufficient preparatory measures	-	-	1 (20%)	1 (20%)	3 (60%)	80%	Yes
A5. OSINT investigator must able to identify assets that need protecting and, assess potential threats, risks and vulnerabilities while conducting investigation	-	-	-	-	5 (100%)	100%	Yes

For Question A1, a cumulative percentage of 100% agreement is achieved, with 80% of experts strongly agreeing and the remaining 20% agreeing that OSINT investigators should also bear responsibility for their security, as they should not solely depend on information security personnel.

For Question A2, a cumulative percentage of 100% agreement is achieved, with 80% of experts strongly agreeing and the remaining 20% agreeing that threats can come from online vulnerabilities like cookies, trackers, and scripts which might be abused to obtain unauthorized access to an asset.

For Question A3, a cumulative percentage of 100% agreement is achieved, with 80% of experts strongly agreeing and the remaining 20% agreeing that while OSINT can be utilized to locate criminals, it can also be abused to launch a cyberattack against law enforcement.

For Question A4, a cumulative percentage of 80% agreement is achieved, with 60% of experts strongly agreeing and 20% agreeing that without employing sufficient preparatory measures prior to conducting OSINT investigations, investigators are more susceptible to cyber threats like distributed denial of service (DDOS) attack, Man in the middle (MITM) attack, phishing attack and malware. 20% of the experts are unsure about the given situation.

For Question A5, a cumulative percentage of 100% agreement is achieved, with all of the experts strongly agreeing that it is essential for OSINT investigators to have the ability of identifying crucial assets that need protection from cyber threats while conducting an investigation.

4.3.2 Element of Preparation

This subsection consists of five (5) questions concerning the element of preparation that should help in mitigating the risk of cyber threats associated with OSINT investigations. The frequency and cumulative percentage of agreement for each question of the subsection are displayed in Table 4.3

Table 4.3 Frequency and Cumulative Percentage of Agreement for Element of Preparation

Question	Scale					Cumulative Percentage of Agreement (%)	Consensus
	1	**2**	**3**	**4**	**5**		
B1. Online investigations plan should include threat and risk assessment, with a strategy for mitigating risk. The plan should address on how identify, respond to and recover from breaches or attacks	- -	- -	- -	1 (20%)	4 (80%)	100%	Yes
B2. OSINT investigator must be able to identify the resources needed for them to conduct the planned investigations beforehand, which include staffing, training, tools, and equipment	- -	- -	- -	- -	5 (100%)	100%	Yes
B3. OSINT investigator should be well versed in the knowledge requirements and its sources before conducting investigations.	- -	- -	- -	- -	5 (100%)	100%	Yes
B4. Information & Communication Technology Safety Officer should be consulted for advice on protective and security measures for any security concern in digital open investigation	- -	- -	1 (20%)	2 (40%)	2 (40%)	80%	Yes

to be continued…

…continuation

B5. Continuous and consistent knowledge sharing and strengthening is one of method to ensure proper use and security of ICT asset	-	-	-	-	5 (100%)	100%	Yes

For Question B1, a cumulative percentage of 100% agreement is achieved, with 80% of experts strongly agreeing and 20% agreeing that as a risk mitigation strategy, online investigation plan should include threat and risk assessment along with strategy to identify, respond to and recover from attacks.

For Question B2, a cumulative percentage of 100% agreement is achieved, with all of the experts strongly agreeing that prior to conducting an OSINT investigation, it is essential for OSINT investigators to identify all the necessary resources, which includes staffing, training, tools, and equipment to help them to increase the security and efficiency of the investigation.

For Question B3, a cumulative percentage of 100% agreement is achieved, with all experts strongly agreeing that OSINT investigators should be well-versed in all legal documents, policies and guidelines associated with OSINT investigations.

For Question B4, a cumulative percentage of 80% agreement is achieved, with 40% of experts strongly agreeing and 40% agreeing that OSINT investigators should seek consultation from ICTSO for advice on protective and security measures for any security concern involving digital open investigation whenever the situation is deemed necessary.

For Question B5, a cumulative percentage of 100% agreement is achieved, with all experts strongly agreeing that ICT assets can be appropriately used and better protected with continuous and consistent knowledge sharing and strengthening among their users.

4.3.3 Element of Human Factor

This subsection consists of five (5) questions concerning the human factor element in OSINT investigations that may contribute to vulnerability to cyber threats, leaving room for improvement. The frequency and cumulative percentage of agreement for each question of the subsection are displayed in Table 4.4.

Table 4.4 Frequency and Cumulative Percentage of Agreement for Element of Human Factor

Question	Scale					Cumulative Percentage of Agreement (%)	Consensus
	1	**2**	**3**	**4**	**5**		
C1. OSINT-investigators lack awareness and training concerning threats calls for more training	- -	- -	- -	- -	5 (100%)	100%	Yes
C2. OSINT investigations should be conducted with investigators maintaining their anonymity online and ensuring that their online conduct is as non-attributable as feasible	- -	- -	- -	1 (20%)	4 (80%)	100%	Yes
C3. OSINT investigators can be easier targets for phishing attacks and other forms of social engineering if their online conduct has identifiable or predictable patterns of behaviour	- -	- -	- -	2 (40%)	3 (60%)	100%	Yes

to be continued…