DIGITAL ERA OSINT: FORMULATING SPECIAL NATIONAL INTELLIGENCE ESTIMATES THROUGH OPEN SOURCES

Elisa Farhana Zulkiflee, Mohd Shahril Abdul Ghani* , Noor Nirwandy Mat Noordin
Centre for Media and Information Warfare Studies
Faculty of Communication and Media Studies,
Universiti Teknologi MARA,
40450 Shah Alam, Selangor, Malaysia
mohdshahril7667@gmail.com

Received Date:2/8/2024 *Accepted Date:21/9/2024* *Published Date:30/10/2024*

Abstract

Adopting Open-Source Intelligence (OSINT) in the contemporary digital era has significantly revolutionized intelligence collection and analysis, thus becoming an integral component in formulating Special National Intelligence Estimates. Therefore, this paper critically discusses methodologies and processes for utilizing publicly available information to identify and evaluate potential national security threats in Malaysia. The study traces the evolution from traditional intelligence-gathering methods to including advanced technologies like artificial intelligence and machine learning in acquiring OSINT. Modern developments of OSINT, featuring efficiency and comprehensiveness in identifying critical cybersecurity threats and political instability and extremism, require permanent observation and analytical techniques. These findings stress the need for a clear understanding of both technology and human intelligence to effectively interpret the data and increase the readiness and responsiveness Malaysia ought to have in dealing with national security challenges. Therefore, this paper seeks to provide a holistic understanding of the importance of OSINT concerning national security and its possible impacts on policy formulations and strategic planning.

Keywords: *Digital Era, OSINT, Intelligence Estimates, Open Sources*

1.0 Introduction

Intelligence is collecting, analyzing, and using information that contributes to decision-making processes. According to [1], "the application of knowledge in a specific context stems from many other cognitive processes, including problem-solving, perception, learning, reason and memory." Intelligence, traditionally found in military and national security domains, has broadened to cover areas such as law enforcement and corporate strategies, with such growth acting as the basis for any decision made; thus, it is the insight that shapes policy, strategies, and actions. These entail Open-Source Intelligence, Human Intelligence, Measurement and Signature Intelligence, Signals Intelligence, and Geospatial Intelligence—all having unique means and methods of collection and analysis. The era of digitalization revolutionized the ways through which intelligence was collected, analyzed, and used.

The volume and variety of information available for intelligence purposes have greatly increased due to the Internet, social media, and other digital platforms like blogs and forum websites. According to [2], the internet has made it much more convenient for users to find information globally and from any source. This development has brought up the capabilities of Open Source Intelligence (OSINT) to date, becoming a necessary tool for modern intelligence practitioners because it is accessible and covers an immense scope. Intelligence analyzers could mine large portions of data that translated to in-depth intelligence analysis using openly available sources. It is made possible by the innovations of the digital era, which allow for an expansion of OSINT's scope from traditional media sources to online and make almost real-time public opinion, perceptions, trends, and emergent threats information available. SNIEs are done at an exceptional level, conducting extensive studies and assessments on specific topics concerning national security; they provide analyses and judgments on

the subject matter. SNIE creation from OSINT is a multistage process that includes data collection, analysis, identification, and categorization stages.

2.0 Literature Review

2.1 Intelligence History

Intelligence estimation was practiced as far back as World War II and into the early Cold War, in which governments played a critical role in strategic planning and threat assessment [3]. The methods of collecting intelligence have evolved over the years with technological advances and changes in the geopolitical environment. The integration of various intelligence disciplines, including human intelligence (HUMINT), signals intelligence (SIGINT), imagery intelligence (IMINT), and OSINT, has become a standard procedure in the production of comprehensive intelligence estimates. Today, OSINT captures huge digital footprints that comprise activities on social media, open-source databases, and other online sites that exist. All these have been prepared to serve the objectives of not just national security but also law enforcement and corporate intelligence, among others. Artificial intelligence integration has indeed further revolutionized OSINT to automated levels of data collection and analysis, making it more effective and complete [4].

OSINT thrives as a field with the enhancing levels of technological innovation and the growing availability of digital data. The tools of AI and machine learning make the analyst's job possible, quickly unraveling this vast information to find hidden patterns and insights that would be hard to uncover if manual methods are used. This evolution depicts the vast nature of OSINT as it adapts to new challenges and opportunities presented by the digital age. Though OSINT has advanced, a sharp understanding of technology and human intelligence is essential for the fine interpretation of the data collected [5].

2.2 Open-Source Intelligence

In simpler terms, Open Source Intelligence (OSINT) refers to collecting and analyzing information from publicly available sources to derive actionable intelligence. This involves mining data from multiple open sources, both traditional and non-traditional, including social media, news outlets, public records, and academic publications [6]. According to [7], the digital era has immensely revolutionized OSINT by improving its functionalities and uses in national security, law enforcement, policy-making, and many more diverse aspects. OSINT is defined by its dependence on information that is open and legally accessible. The environment has brought technological progress and changes to the information landscape, which caused OSINT to develop over time. Previously, OSINT included manual collection and analysis of printed materials, such as newspapers and official documents; however, with scientific-technological progress and the Internet, automatic collection and analysis can be made from a gigantic amount of data within a short period from various sources. The most crucial aspect of OSINT would be identifying reliable and relevant sources of information [8] which includes traditional media, social media platforms, government documents & databases, and academic research. Ensuring the accuracy and dependability of the data gathered requires cross-referencing multiple sources and applying verification techniques. According to [9], this step is critical in presenting an analyzed intelligence in a way beneficial to decision-makers through reports, dashboards, and briefings.

Recent advancements in OSINT today have significantly enhanced the capabilities of intelligence agencies and organisations in utilising open-source information. Advancements consisting of Artificial Intelligence (AI) and machine learning have improved the ability to process and analyse large amounts of data, identify patterns as well as predict trends [10]. NLP has also brought improvements to the analysis of text data, thereby allowing a better understanding of context, sentiments, and intent. Social media analytics tools have been further developed and popularized lately, increasing the scope of OSINT by enabling real-time monitoring, tracking conversations, identifying influencers, and tracking the spread of information and disinformation [11]. Geospatial Intelligence (GEOINT) has also improved the ability to analyze as well as visualize

information in geographical context; combining images, maps, and location-based data to provide a third dimension to intelligence analysis [12].

2.3 The Digital Era

The "Digital Age" represents an important shift in the collection, dissemination, and reception of information. With the evolution of digital technologies and enhanced Internet connectivity, it has led to a significant change in the working of numerous fields, including communication, business, governance, and intelligence. Apprehending digital changes and their impact on Open Source Intelligence (OSINT) and the assembly of Special Nation Intelligence Estimates (SNIEs) is crucial [13]. The Digital Age referred to in some quarters as the information gap, is characterized by the high prevalence of digital technology and the internet as the standard of everyday life. It began in the late 20th century with the invention of personal computers and the Internet. It continuously evolves in contemporary society through the development of mobile technologies, social media, and big data analytics [14].

The digital age brings remarkable levels of connectivity facilitated by the internet and mobile networks. These allow for instant communication and, within minutes, direct access to information located in other parts of the world [15]. The consequence is a huge rise in the data volume generated daily. According to [16], big data analytics and cloud computing have become the cornerstone for managing and analyzing this vast amount of information.

Social media platforms, messaging apps, and other digital means of communication have changed how individuals interact, share information, and form communities. These are mostly seen as instrumental tools for disseminating information and misinformation [17]. As posited in [18], continuous technological innovations, such as Artificial Intelligence, Machine Learning, and IoT, have further enhanced the capabilities of digital systems.

2.4 Theoretical Framework: Intelligence Cycle Model

This research is grounded in the theoretical framework of intelligence cycle which serves as a foundational model for intelligence gathering and analysis. The intelligence cycle is made of five (5) core stages consisting of planning and direction, collection, processing, analysis and production and dissemination. Each stage is essentials in transforming raw information into actionable intelligence and informs decision-making processes for various parties. Within this framework, OSINT is a key component that leverages on publicly accessed information. Compared to other forms of intelligence gathered, OSINT provides a more unique insight that is accessible and can legally be obtained without the needs for covert operations [19][20].

OSINT's role is significant in the collection and analysis stage of the intelligence cycle. The invention of the Internet and the advancement of digital technologies have expanded the volume of open-source information available for the public. OSINT allows the monitoring of global events, understanding public sentiments through social media analysis and identifying emerging trends that may not be available yet through classified sources [21].

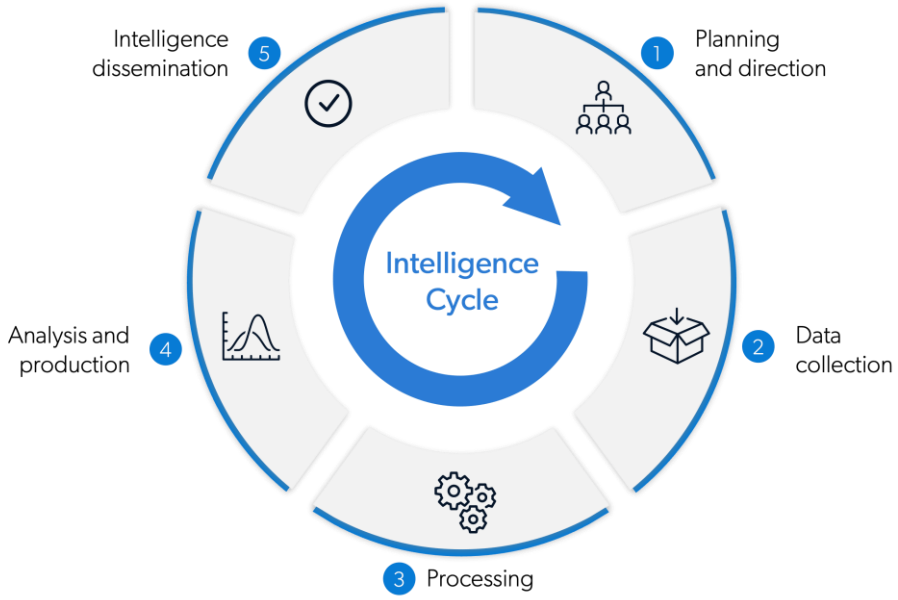


Illustration 1 depicts the Intelligence Cycle Model where information goes trough five stages to identify security threats.

The formulation of Special National Intelligence Estimates (SNIEs) is an application of the intelligence life cycle at a strategic level [22]. SNIEs are in-depth assessments that address specific national security issues and requires immediate attention. According to the Intelligence Cycle Model, SNIEs must go through several steps as illustrated below:

Step	Item	Remarks
1	Planning and Direction	Determining the key questions and issues that need to be addressed to inform policy decisions
2	Data Collection	Gathering data from all available sources, with OSINT providing a substantial portion due to its accessibility and diversity [23]
3	Processing	Organizing and converting the collected data into a usable format, which may involve translating foreign languages or decoding technical information [24]
4	Analysis and Production	Evaluating the information to identify patterns, assess credibility, and develop insights. Analysts use critical thinking and methodological rigor to produce objective assessments
5	Intelligence Dissemination	Delivering the final SNIE to policymakers and stakeholders in a timely manner to influence decision-making

OSINT enhances the SNIE formulation by supplying a wide range of data points that can reveal underlying patterns and potential threats [25]. It allows analysists to authenticate information obtained from other intelligence sources and fill gaps where classified information may lack. By integrating OSINT into a larger intelligence framework, intelligence agencies can obtain a clearer understanding of the security landscape [26]. This approach is particularly relevant for Malaysia where the dynamic interplay of politics, economic development and social movements require constant monitoring and assessment [27].

SNIE creation from OSINT is a multistage process that includes data collection. Analysis, identification and categorisations. The data is first collected from numerous sources to ensure a wide range across both traditional and non-traditional platforms [28]. The collected data is then processed and analysed for patterns of information that might pose a threat, which will further be cross-reference with multiple sources to ensure credibility and relevance [29]. Once the data has been confirmed as a threat, the information will be grouped into categories to provide a larger perspective on potential risks.

Risk assessment is a process that identify and evaluate potential threats, assessing one's capabilities and estimating the likelihood and potential impact of these threats occurring [29]. This research is being conducted with the main intent of identifying various forms of OSINT, assessing how OSINT could potentially threat national security in Malaysia and performing SNIE to identify the most probable threats.

3.0 Methodology

This chapter outlines the methodology used to formulate Special National Intelligence Estimates (SNIE) through open-source intelligence (OSINT) in the digital era. These are three important steps: identification of threats through OSINT, verification through primary sources, and Risk Assessment Matrix (RAM) analysis for significance and prioritization of threats. In making the SNIE formulations, we tapped into many publicly available sources of information, including social media, news outlets, online forums, and academic journals.

To accomplish this, we utilized various sources as listed below:

a) Social Media: Platforms like Twitter, Facebook, and LinkedIn provide real-time data and user-generated content highlighting emerging trends, public sentiments, and immediate threats.
b) News Outlets: Reputable news sources such as the New Straits Times, Malay Mail, and international news agencies offer verified reports and in-depth analyses of current events.
c) Government Publications: Official reports and documents from government agencies provide authoritative data on national security issues.
d) Academic Journals: Research papers offered insights and data that had undergone rigorous scrutiny

3.1 Data Collection

The table below illustrates the OSINT gathered from various platforms that could pose potential threats to national security.

No.	Threat	Sources of OSINT
1.	Cybersecurity Threats	Online news portals, including New Straits Times, online journals, social media (Twitter)
2.	Climate Change	Articles from online journals and news portals
3.	Social Media Threats	Articles from the New Straits Times, Social media (Twitter), government documents
4.	Political Instability	Foreign and local online news portal
5.	Public Health Threats	Foreign and local online news portal
6.	Extremism	Foreign and local online news portal and social media
7.	Terrorism	Foreign and local online news portal and social media
8.	Foreign Interference	Publicly accessed government documents, online news portals, and social media (Twitter}
9.	Food Security	Online news portals, online journals, and social media

10.	Territorial Disputes	Publicly accessed government documents, Online news portals, online journals, and social media.
11.	Artificial Intelligence (AI)	Online news portals and forums
12.	Maritime Crimes & Piracy	Online news portals and social media
13.	Illegal Immigrants	Online news portals and social media
14.	Organized Crime	Online news portals and social media
15.	Child Kidnapping	Online news portals and social media

Having identified and verified the threats, the final step is to analyze and prioritize them using the Risk Assessment Matrix (RAM). The RAM categorizes each threat based on its likelihood and impact, providing a clear visual representation of which threats are most significant and require immediate attention.

Likelihood	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low Med	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Very Unlikely	Low	Low	Low Med	Medium	Medium

Figure 1 - Risk Assessment Matrix

The Risk Assessment Matrix (RAM) is a straightforward tool used to evaluate and prioritize risks based on two key factors: the likelihood of the risk occurring and the severity of its impact if it does happen. It helps organizations and individuals make informed decisions about which risks need immediate attention and which ones can be monitored over time.

3.2 Components of the Risk Assessment Matrix

Likelihood: This measures how probable it is that a particular risk will occur. It is often categorized into:

- Very Unlikely: The event is extremely rare (1-5% chance).
- Unlikely: The event is not expected but possible (6-20% chance).
- Possible: There is a reasonable chance of the event occurring (21-50% chance).
- Likely: The event is expected in most circumstances (51-80% chance).
- Very Likely: The event is almost certain to occur (81-100% chance).

Impact: This measures the severity of the consequences if the risk occurs. It is often categorized into:

- Negligible: Minimal impact.
- Minor: Limited harm or disruption.
- Moderate: Noticeable impact requiring additional resources.
- Significant: Serious impact causing considerable harm.
- Severe: Major impact with extensive harm.

How to Use the Risk Assessment Matrix

1. Identify Risks: List all the potential risks.
2. Evaluate Likelihood: Determine how likely each risk is to occur.
3. Evaluate Impact: Determine the severity of the impact if each risk occurs.
4. Plot on the Matrix: Place each risk on the matrix according to its likelihood and impact.

Special National Intelligence Estimates (SNIE) can be effectively formulated using a Risk Assessment Matrix (RAM). The RAM helps to systematically evaluate and prioritize the most significant threats by assessing their likelihood and impact.

Upon the completion of our OSINT analysis for formulating the Special National Intelligence Estimates (SNIE), we acknowledge that each data source stated above carries potential biasness. For example, social media platforms are subjected to misinformation, sensationalism and echo chambers that may not accurately represent accurate public sentiments. News outlets are subjected to influence from political/government leaders which can affect the angle or frame of reported events. Government-owned publications often present information that supports official narratives or policies leading to downplaying of certain issues or threats. To mitigate potential biases, we have cross-referenced the information across various domestic sources to verify accuracy and consistency. This allowed us to analyse the context of which the information was presented. By gathering data from social media, news outlets, official documents and other academic research, we aimed to construct a comprehensive and balanced understanding of potential threats.

4.0 Findings and Discussion

4.1 Identified Potential National Threats through OSINT

Incorporating Open Source Intelligence (OSINT) in national security frameworks has become critical in identifying and mitigating potential threats. It leverages information in the public domain to harvest the intelligence that might prove instrumental in predicting a potential national security threat. OSINT tools analyze data on social media, geospatial sources, and open-source forums to establish a broader view of threats. According to [19], "this capability is particularly vital for tracking geopolitical shifts and understanding public sentiment, which can influence national stability and security decisions." The strategic use of OSINT has made a major difference in the preparedness and responsiveness of national security agencies.

The continuous monitoring of open sources would help detect and analyze network activities, whether they operate on the surface web or the more cryptic parts of the internet commonly referred to as the dark web. Indeed, timely detection of emergent threats and the development of countermeasures can be achieved with continuous monitoring before the crystallization of these threats into actualized danger. Such an application of advanced OSINT methodologies, including automated data processing and machine learning, further refines the ability to anticipate critical information from vast datasets, thus making the intelligence process more efficient and effective [20]. After analysing various available OSINT through digital platforms, we have identified 15 potential threats to national security. Upon identifying primary sources for risks, we further identified secondary sources to strengthen the information received. Based on the secondary sources, we are able to categorize the threats according to their impact and likelihood. Explanation on each of the threats is as follows :

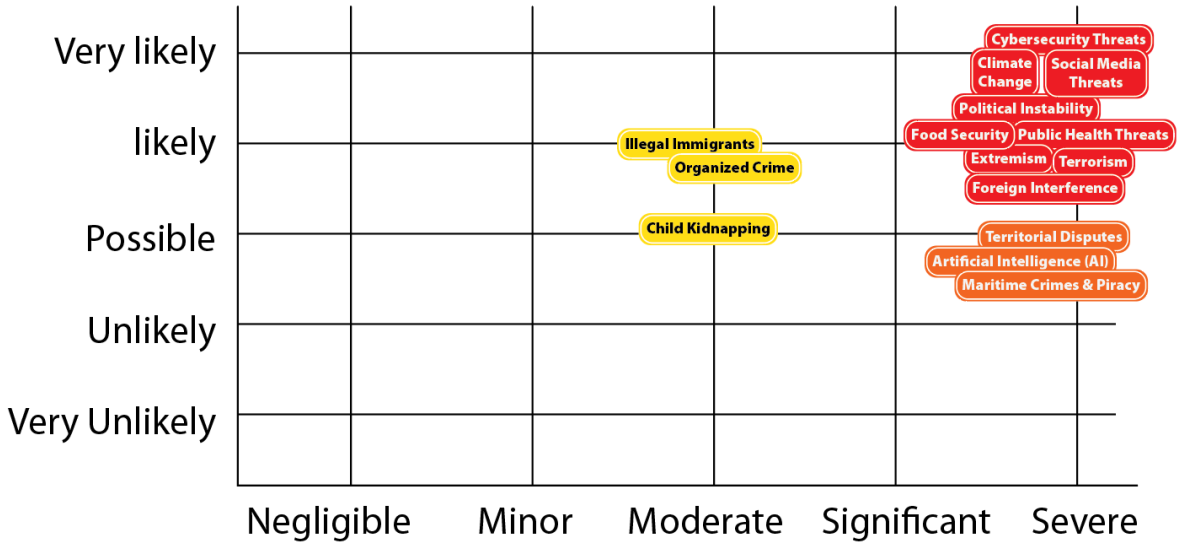
No.	Threats	Explanation
1.	Cybersecurity Threats	Cybersecurity threats are highly likely due to the increasing number of cyber-attacks like phishing, ransomware, and data leaks. These attacks can severely impact critical sectors such as finance, telecommunications, and government services, leading to significant personal and financial losses.
2.	Climate Change	Climate change is an ongoing and accelerating threat, causing natural disasters like floods and rising sea levels. These disasters have severe economic impacts and can lead to food and water scarcity.
3.	Social Media Threats	Social media platforms facilitate the spread of misinformation, disinformation, and extremist ideologies.

		These threats are very likely and can have severe impacts on public opinion and cybersecurity.
4.	Political Instability	Political instability can lead to economic repercussions, increased living costs, and potential social unrest. It also invites external threats as other nations may attempt to interfere.
5.	Public Health Threats	Public health threats such as pandemics can severely impact workforce productivity, increase healthcare costs, and strain healthcare resources, undermining public trust in government effectiveness.
6.	Extremism	Extremism can provoke violence and terrorism, leading to radicalism and recruitment for extremist groups, posing a significant threat to national security.
7.	Terrorism	Terrorism impacts civilian safety, undermines trust in government security measures, and destabilizes the nation economically and politically.
8.	Foreign Interference	Foreign powers may engage in political and economic interference, spreading disinformation and conducting covert operations to manipulate Malaysia's domestic affairs.
9.	Food Security	Disruptions in the global food supply chain can lead to food shortages, increased prices, social unrest, and economic instability.
10.	Territorial Disputes	Territorial disputes, particularly in the South China Sea, lead to tensions between governments, political instability, and risks of armed conflict.
11.	Artificial Intelligence (AI)	The rise of AI poses threats such as data leaks, increased cyberattacks, job displacement, and manipulation of public opinion through AI-generated disinformation.
12.	Maritime Crimes & Piracy	Piracy and armed robbery at sea disrupt trade and shipping, increase insurance costs, and pose direct threats to the safety of seafarers and the national economy.
13.	Illegal Immigrants	The influx of illegal immigrants burdens Malaysia's economy, impacts public health, and poses security risks, including potential involvement in criminal activities.
14.	Organized Crime	Organized crime undermines national security through violence, cross-border operations, corruption, and erosion of governance.
15.	Child Kidnapping	The increasing number of child kidnappings causes widespread fear and anxiety, affecting tourism and foreign investment due to perceived safety risks.

The table below illustrates the types of threats and their likelihood and impact on the nation.

No.	Threat	Likelihood	Impact	Category
1.	Cybersecurity Threats	Very Likely	Severe	High Risk
2.	Climate Change	Very Likely	Severe	High Risk
3.	Social Media Threats	Very Likely	Severe	High Risk
4.	Political Instability	Likely	Severe	High Risk
5.	Public Health Threats	Likely	Severe	High Risk
6.	Extremism	Likely	Severe	High Risk
7.	Terrorism	Likely	Severe	High Risk
8.	Foreign Interference	Likely	Severe	High Risk
9.	Food Security	Likely	Severe	High Risk

10.	Territorial Disputes	Possible	Severe	Medium-High Risk
11.	Artificial Intelligence (AI)	Possible	Severe	Medium-High Risk
12.	Maritime Crimes & Piracy	Possible	Severe	Medium-High Risk
13.	Illegal Immigrants	Likely	Moderate	Medium Risk
14.	Organized Crime	Likely	Moderate	Medium Risk
15.	Child Kidnapping	Possible	Moderate	Medium Risk



4.2 Special National Intelligence Estimates (SNIE)

The role of SNIEs in Malaysia has evolved over the years from one dynamic security scene in the country to another. SNIEs are one of the important tools in evaluating possible threats that shape national security strategies—providing comprehensive estimates to help the Government of Malaysia anticipate and manage risks from terrorism to shifts in geopolitical landscapes. The creation of the National Special Operations Force (NSOF) is a manifestation of Malaysia's assertion of its initiative to combat threats of terrorism, combining intelligence of different agencies to act as a consolidative and quick reactionary force [21]. In Malaysia, SNIEs have likewise been active in non-traditional security concerns.

Recent intelligence reports concerned the challenges of climate change, migration, and regional conflicts. These reports underscore that national security cannot be approached in isolation from other sectors of the economy but must be considered holistically, combining economic, environmental, and social dimensions. These insights from the estimates directed Malaysia's foreign and domestic policies to ensure the country is capable of withstanding emergi'g threats [22].

We derived the SNIE based on the 15 potential threats that has been identified through Open Source Intelligence to determine the most probable, high-risk threat faced by Malaysia [23]. After analysis and deeper search, we can say the highest potential risk Malaysia faces in its national security is the cybersecurity threat since "today's information is more accessible than ever."

4.3 Cybersecurity Threats in Malaysia

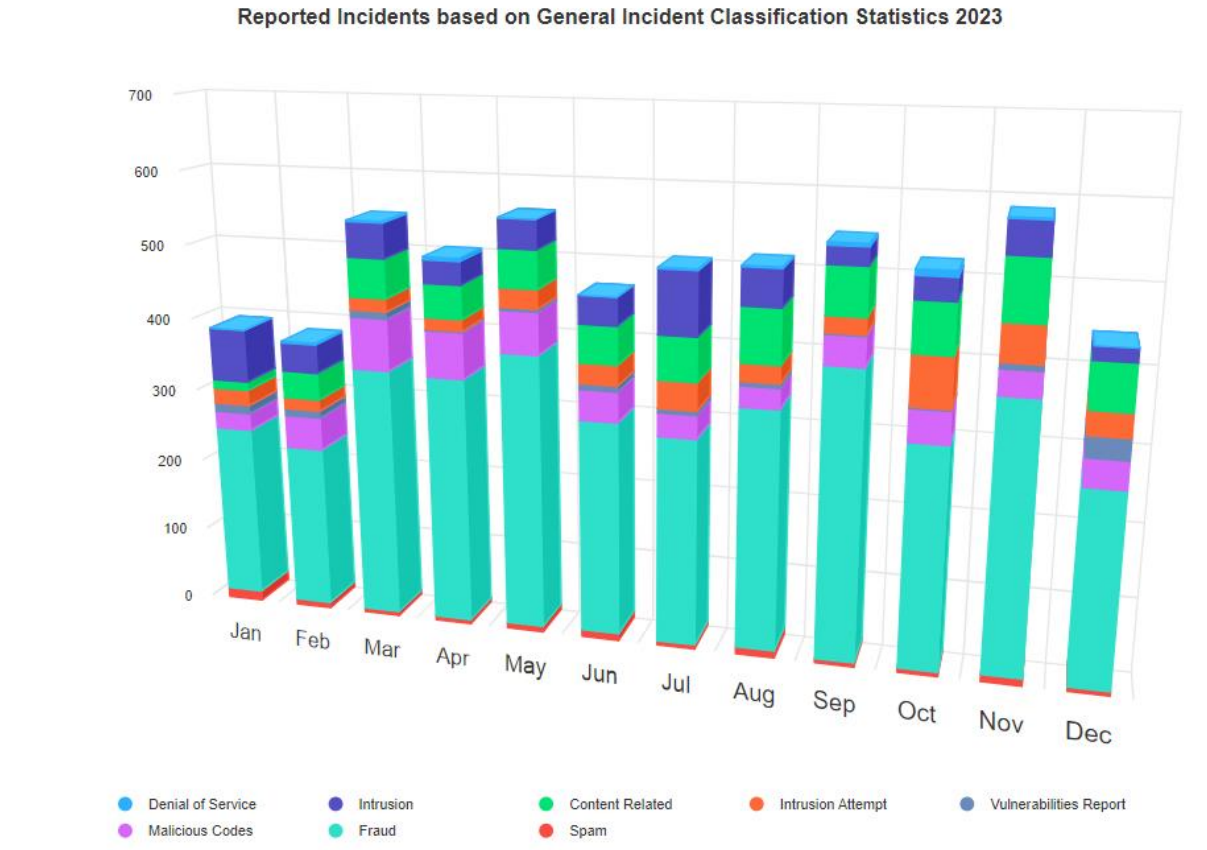
In recent years, Malaysia has faced a significant increase in cybersecurity threats, impacting various industries like finance, healthcare, and government infrastructure. One primary concern is the rise in cybercrime cases, which saw reported incidents grow from 13,000 in 2019 to over 20,000 in 2021, leading to substantial financial losses [24]. This increase in cyberattacks highlights the urgent need for enhanced cybersecurity measures and awareness among Malaysian businesses and citizens.

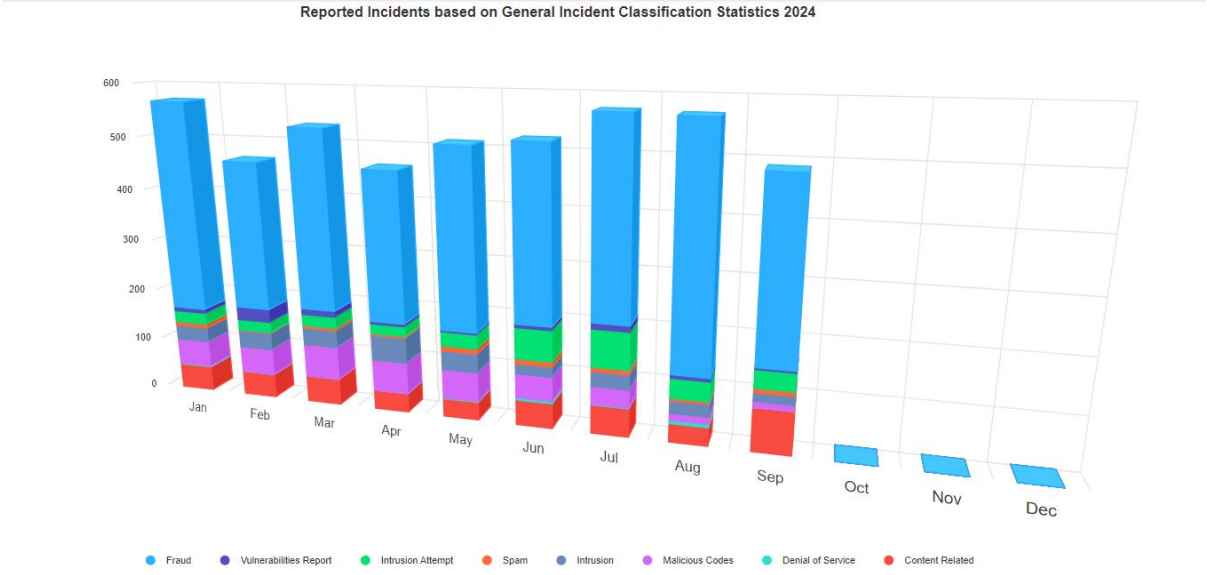
The primary sources of cybersecurity threats in Malaysia include phishing, fraud, and ransomware attacks. A 2022 report highlighted that 76% of Malaysian organizations experienced a cyberattack, with 57% of these incidents resulting in data loss [25]. Cyberattacks frequently target Malaysia's critical national information infrastructure (CNII). CyberSecurity Malaysia reported a considerable increase in cyber incidents, with financial losses amounting to RM497.7 million in 2019. Cybercriminals target various sectors, including finance, healthcare, and government, disrupting services and causing substantial economic damage. A 2019 report highlighted that 99% of successful cyberattacks in Malaysia were due to human error, emphasizing the need for improved cybersecurity awareness and training [26].

Malaysia's visa-waiver program and penetrable borders have made it a transit point and logistics hub for terrorist groups such as ISIS and the Abu Sayyaf Group (ASG). The ease of movement for these groups directly threatens national security. Terrorists have used Malaysia's relatively lax border controls to plan and coordinate attacks within the region [27].

The corruption and cartels in the immigration department have only increased the cyber threats. For instance, some officers were suspected of tampering with the Malaysian Immigration System (MyIMMs) to allow illegal immigrants into the country without detection. This is a crucial loophole because it aids the movement of terrorists and other malicious organizations [28].

With the increasing threats, Malaysia has implemented several efforts and policies to enhance cybersecurity defenses. Under the National Cyber Security Policy (NCSP), strategies for the protection of Critical National Information Infrastructure (CNII) are in line with international standards that should be complied with, such as the ISO/IEC 27001 [29]. Other agencies, including CyberSecurity Malaysia and MyCERT, monitor and respond to cyber incidents, ensuring important support and guidance to mitigate risks [30]. These efforts underline Malaysia's commitment to increase its cybersecurity posture and resilience to repel evolving digital threats effectively.





Adopted from MyCert Incident Statistics 2024. The graph illustrates the number of reported cybersecurity threats from January – September 2024. The attacks on fraud have reported the highest number of cases for all months.

5.0 Recommendation

The integration of Open Source Intelligence (OSINT) into Malaysia's national security framework is vital for identifying and mitigating potential threats effectively. By utilizing publicly available data from various sources such as social media, news outlets, government publications, and academic journals, intelligence agencies can gain real-time insights into emerging threats and trends. Advanced

technologies like artificial intelligence and machine learning further enhance the ability to process vast amounts of data, identify patterns, and predict future risks. Given the increasing sophistication of cyberattacks and the evolving nature of global threats, it is crucial for Malaysia to invest in OSINT capabilities. This investment will not only improve the responsiveness and preparedness of national security agencies but also support the formulation of informed policy decisions and strategic planning. Therefore, Malaysia should enhance its OSINT infrastructure and continuously train its personnel to effectively utilize these tools for national security purposes.

To enhance national security, it is crucial for Malaysia to invest in strengthening its Open-Source Intelligence (OSINT) capabilities. Policymakers should prioritize resource allocation towards the development of sophisticated analytical tools and ensure personnel are trained in contemporary OSINT methodologies. Furthermore, the establishment of clear legal frameworks and ethical guidelines is essential to guarantee that OSINT practices respect individual privacy rights while also addressing national security concerns [9].

Future research should justify to investigate the integration of artificial intelligence (AI) and machine learning (ML) into OSINT processes with an emphasis on improving the accuracy and efficiency of threat detection. Research into the balance between leveraging open-source data and safeguarding privacy is necessary as it may harvest valuable insights into responsible intelligence practices [35]. Collaborating with international partners to exchange best practices and technological innovations can also contribute to reinforcing Malaysia's overall security [36]. By advancing OSINT capabilities and addressing the associated ethical challenges, Malaysia will be better positioned to navigate the increasingly complex and rapidly evolving global threat landscape. This will ensure a secure and resilient nation capable of responding to future challenges [36].

5.1 Ethical Considerations in the Use of Open-Source Intelligence

The integration of OSINT into national security frameworks has strengthened Malaysia's capacity to mitigate emerging threats. However, it has also raised critical ethical issues that require immediate attention. These ethical dilemmas revolve around potential violations of privacy, data accuracy, misuse of information, the tension between security and civil authorities, and the ethical implications of using AI and ML in intelligence operations [35].

5.1.1 Privacy Concerns

A major ethical concern in the context of OSINT is the risk of breach on individual privacy rights. OSINT relies heavily on the collection and analysis of publicly available data which may include information that individuals did not intend to share widely. For instance, social media platforms often stores personal information that users believe is confined to their network however inadequate understanding of privacy settings can result in unintended exposure of the information [37]. Even when individuals attempt to limit the visibility of their online content, intelligence agencies or malicious parties may exploit metadata analysis or third-party applications to access the information. OSINT practitioners can often link anonymous online profiles to real individuals by cross-referencing multiple sources of data. This practice undermines the right to online anonymity and poses significant risks particularly in politically sensitive contexts such as activism or dissent.

To address these privacy concerns, intelligence agencies need to implement strict ethical guidelines regarding data collection and usage that ensures personal privacy being safeguarded wherever possible. Raising public awareness about digital privacy and encouraging social media platforms to improve privacy controls can empower individuals to protect their information more effectively [37].

5.1.2 Data Accuracy and Misuse

Another critical issue in OSINT collection is the potential for reliance on inaccurate or misleading information. The open nature of data sources makes it more prone to misinformation and disinformation campaigns. OSINT analysts must adhere to rigorous verification protocols to prevent basing intelligence assessments on faulty information. Unverified or incorrect data can lead to flawed decision-making processes with severe implications for national security [38]. There is a risk of surveillance overreach where intelligence collection activities extend beyond legitimate security concerns. Without appropriate oversight and accountability, OSINT can be misused to monitor

individuals or groups without justification and leading to significant ethical and legal violations. Establishing accountability mechanisms and transparent neglecting structures is essential to ensure that OSINT practices adhere to legal standards and respect individual rights [37].

5.1.3 Balancing Security and Civil Privacy Rights

The tension between national security and individual privacy rights is an ethical dilemma in the utilization of OSINT. While OSINT plays a pivotal role in identifying and mitigating threats, it can also violate ethical boundaries particularly when data is collected and analysed without individuals' knowledge or consent [37]. Mass surveillance enabled by advanced OSINT tools and AI algorithms can pose a significant threat to privacy. The awareness of constant monitoring can lead to a "chilling effect," where individuals self-censor or alter their behaviour due to the fear of surveillance. This dampens free speech and political discourse, which are essential components of a healthy democracy [37].

To mitigate these challenges, intelligence agencies must ensure that their use of OSINT is proportionate to the threats they aim to address. Legal frameworks such as Malaysia's Personal Data Protection Act 2010 provide essential guidelines for balancing security needs with the protection of individual rights. These frameworks should define clear boundaries for data collection, retention, and usage, while promoting transparency and accountability.

5.1.4 Ethical Use of AI and Machine Learning in OSINT

The incorporation of AI and Machine Learning (ML) technologies into OSINT operations introduces further ethical considerations. While these technologies can significantly enhance the efficiency of data processing and analysis, they also carry the risk of maintaining biases present in the data analysed. This can result in skewed intelligence assessments that disproportionately affect certain communities or individuals. The "black box" problem associated with AI—a lack of transparency regarding how decisions are made—compounds these concerns as it becomes difficult to challenge the validity of AI-driven insights [39].

To address these issues, regular audits of AI and ML algorithms are necessary to identify and correct any inherent biases. Ensuring transparency in the development and deployment of these technologies is critical as well as maintaining human oversight throughout the intelligence analysis process. Analysts should critically evaluate AI-generated insights and integrate ethical considerations into their decision-making processes [39].

In conclusion, incorporating ethical considerations into OSINT practices is crucial for maintaining public trust and upholding democratic values. Addressing privacy concerns, ensuring data accuracy, balancing security with civil liberties, and responsibly employing AI and ML technologies are key steps in developing an ethical OSINT framework. By adhering to strict guidelines, legal oversight, and transparency mechanisms, Malaysia can leverage the benefits of OSINT while minimizing ethical risks, thereby strengthening its national security while upholding individual rights in the digital age.

6.0 Conclusion

Integration of Open-Source Intelligence (OSINT) into national security frameworks is crucial in identifying and mitigating potential threats. In this digital age, massive volumes of information publicly present an important resource in preparing Special National Intelligence Estimates (SNIEs). The findings from this journal article underpin the need to leverage OSINT to strengthen Malaysia's national security.

The digital era opened up intelligence-gathering opportunities like never before. New possibilities for digital communication, such as using social media and other platforms and accessing various online databases, made OSINT a potent tool for real-time monitoring and analysis. Therefore, the development and realization of OSINT are somehow related to the technological advancement of artificial intelligence, or AI, and machine learning in their means, efficiency, and effectiveness in data collection and analytic processes. Those advances allow intelligence agencies to process large data volumes quickly, identify patterns, and forecast trends, delivering timely and actionable insights.

While Malaysia faces many possible national security threats, cybersecurity is the most serious. This rise in cybercrime—13,000 cases in 2019 to over 20,000 in 2021—shows that dealing with cybersecurity vulnerabilities should be at the top of the list for reform-minded policymakers. With the

increasing sophistication of cyberattacks through phishing, fraud, and ransomware, Malaysia's CNII presents a significant risk. It has no option but to embrace stronger cybersecurity measures and awareness in an enhanced way to safeguard its national security better.

The role of SNIEs in Malaysia has also changed to include traditional and non-traditional security threats. Intelligence reports in the past few years indicate the need for a multi-dimensional approach that includes economic, environmental, and social dimensions. The formation of the National Special Operations Force is an example of how Malaysia is being proactive in harmonizing intelligence from diverse quarters to create compact and mobile response forces against terrorism and other threats [33].

In conclusion, the strategic use of OSINT has significantly improved Malaysia's preparedness and responsiveness to national security threats. Advanced analytical methodologies and continuous monitoring can effectively detect emerging threats in time to institute countermeasures. With the advancement of the digital era, the role of OSINT in developing a broad and actionable intelligence estimate cannot be overemphasized. By capitalizing on OSINT capabilities, Malaysia can bolster its national security posture while effectively navigating the increasingly tough and rapidly changing threat environment of the 21st century [34].

7.0 Reference

[1] Sternberg, R.J, "The Cambridge Handbook of Intelligence," Cambridge, England: Cambridge University Press, 2020.

[2] Halawi, L., "The Role of the Internet in Intelligence Gathering and Spreading Propaganda," Issues of Information Systems, Volume 22, Issue 2, pp. 231-238, 2021. (Online). Available = https://iacis.org/iis/2021/2_iis_2021_243-251.pdf

[3] Block, L., "The Long History of OSINT", Journal of Intelligence History, Volume 23, NO. 2, 95–109, 7 June 2023. (Online). Available = https://www.tandfonline.com/doi/epdf/10.1080/16161262.2023.2224091?needAccess=true

[4] S. Williams and B. Blum, "Open source intelligence and AI: a systematic review of the GELSI literature," *AI & SOCIETY*, vol. 34, no. 2, pp. 39-40, 2018. [Online]. Available: https://link.springer.com/article/10.1007/s00146-018-0831-5.

[5] N. A. Hassan and R. Hijazi, "The Evolution of Open Source Intelligence," in *Open Source Intelligence Methods and Tools*, Berkeley, CA: Apress, 2018, pp. 1-20. (Online]. Available: https://doi.org/10.1007/978-1-4842-3213-2_1.

[6] T. Ivanjko, "Open Source Intelligence (OSINT): issues and trends," in *7th International Conference The Future of Information Sciences, INFuture2019*, FF press, 2019.

[7] M. Lakomy, "Assessing the potential of OSINT on the Internet in supporting military operations," *Bezpieczeństwo. Teoria i Praktyka*, vol. 48, no. 3, pp. 297-309, 2022.

[8] T. Ivanjko, "Open Source Intelligence (OSINT): issues and trends," in *7th International Conference The Future of Information Sciences, INFuture2019*, FF press, 2019.

[9] Y.C. Kang, "Natural language processing (NLP) in management research: A literature review," *Journal of Management Analytics*, vol. 7, no. 2, pp. 139-172, 2020.

[10] I. H. Sarker, "Internet of things (IoT) security intelligence: a comprehensive overview, machine learning solutions, and research directions," *Mobile Networks and Applications*, vol. 28, no. 1, pp. 296-312, 2023.

[11] D. S. Lande, "A system for analysis of big data from social media," *Information & Security*, vol. 47, no. 1, pp. 44-61, 2020.

[12] R. M. Clark, *Geospatial Intelligence: Origins and Evolution*. Georgetown University Press, 2020.

[13] J. Shepherd, "What is the digital era?," in *Social and Economic Transformation in the Digital Era*, IGI Global, 2004, pp. 1-18.

[14] K. T. Mossberger, *Digital Citizenship: The Internet, Society, and Participation*. MIT Press, 2007.

[15] P. B. Seel, *Digital Universe: The Global Telecommunication Revolution*. John Wiley & Sons, 2022.

[16] A. K. Sandhu, "Big data with cloud computing: Discussions and challenges," *Big Data Mining and Analytics*, vol. 5, no. 1, pp. 32-40, 2021.
[17] E. V. Kross, "Social media and well-being: Pitfalls, progress, and next steps," *Trends in Cognitive Sciences*, vol. 25, no. 1, pp. 55-66, 2021.
[18] I. H. Sarker, "Internet of things (IoT) security intelligence: a comprehensive overview, machine learning solutions, and research directions," *Mobile Networks and Applications*, vol. 28, no. 1, pp. 296-312, 2023.
[19] L. Marzell, "OSINT as Part of the Strategic National Security Landscape," in Open Source Intelligence Investigation, B. Akhgar, P. Saskia Bayerl, and F. Sampson, Eds. Cham: Springer, 2016, pp. 1-6. doi: 10.1007/978-3-319-47671-1_4.
[20] Fingar, T., "A guide to all-source analysis," Intelligencer: Journal of US Intelligence Studies, vol. 19, pp. 1–4, 2012.
[21] Gibson, H., "Acquisition and preparation of data for OSINT investigations," in Open Source Intelligence Investigation, Springer, 2016, pp. 69–93.
[22] Pastor-Galindo, J., Nespoli, P., Mármol, F. G., and Pérez, G. M., "The not yet exploited goldmine of OSINT: opportunities, open challenges and future trends," IEEE Access, vol. 8, pp. 10282–10304, 2020.
[23] "Open-source intelligence: a comprehensive review of the current state, applications and future perspectives in cybersecurity," Artificial Intelligence Review, Springer, 2022.
[24] B. Forca and B. Anočić, "Security analytics," Journal of Information Systems & Operations Management, vol. 17, no. 1, pp. 154–160, 2023.
[25] Journal of Media and Information Warfare, "OSINT in the intelligence cycle and SNIE formulation," Journal of Media and Information Warfare, vol. 15, no. 3, pp. 13-26, 2022.
[20] P. A. Gaona-García and S. Sánchez-Alonso, "Open-Source Intelligence Educational Resources: A Visual Perspective Analysis," Applied Sciences, vol. 10, no. 21, p. 7617, Oct. 2020. doi: 10.3390/app10217617.
[21] S. Abdullah, "New Malaysia's Foreign Policy – The Ministry of Foreign Affairs' Roadmap for Political and Economic Diplomacy," Diplomatic Voice, Institute of Diplomacy and Foreign Relations, vol. 2, pp. 2, 2018. [Online]. Available: https://www.idfr.gov.my/images/stories/DiplomaticVoice/DV2_2018.pdf
[22] "Foreign and Security Policy in the new Malaysia," Lowy Institute, 2019. [Online]. Available: https://www.lowyinstitute.org
[23] "National Intelligence Estimates," Belfer Center for Science and International Affairs, 2023. [Online]. Available: https://www.belfercenter.org
[24] M. Hamzah, "Cybersecurity remains one of Malaysia's top concerns," Free Malaysia Today, Mar. 28, 2022. [Online]. Available: https://www.freemalaysiatoday.com/category/nation/2022/03/28/cybersecurity-remains-one-of-malaysias-top-concerns-says-hamzah . [Accessed: Jul. 14, 2024].
[25] Kroll, "Malaysia Cyber Threat Landscape 2022," Kroll, Oct. 31, 2022. [Online]. Available: https://www.kroll.com/en/insights/publications/cyber/malaysia-cyber-threat-landscape-2022 . [Accessed: Jul. 14, 2024].
[26] Othman, "Towards A Safer Cyberspace: Most 'Attacks' Due To Human Error," NST, 2019. [Online]. Available: https://www.nst.com.my/lifestyle/bots/2018/10/426298/towards-safer-cyberspace-most-attacks-due-human-error. [Accessed: Jan. 2020].
[27] N. A. Rahim and M. R. K. Ariffin, "Cyber Security Crisis/Threat: Analysis of Malaysia National Security Council (NSC) Involvement Through the Perceptions of Government, Private and People Based on the 3P Model," e-Bangi: Journal of Social Sciences & Humanities, vol. 19, no. 4, pp. 30-41, 2020.
[28] M. R. K. Ariffin and M. Letchumanan, "Status of Cybersecurity Awareness Level in Malaysia," in Proceedings of the SpringerLink Conference on Information Security, Springer Nature Switzerland AG, 2019, pp. 110-120. DOI: 10.1007/978-3-030-35746-9_10.
[29] E. Lee Yong Cieh, "Cyber security law and legislative framework in Malaysia," LPP Law, 2019. [Online]. Available: https://lpplaw.my/cyber-security-law-and-legislative-framework-in-malaysia . [Accessed: Jul. 14, 2024].

[30] Othman, "Towards A Safer Cyberspace: Most 'Attacks' Due To Human Error," NST, 2019. [Online]. Available: https://www.nst.com.my/lifestyle/bots/2018/10/426298/towards-safer-cyberspace-most-attacks-due-human-error. [Accessed: Jan. 2020].
[1] T. Riebe, M.-A. Kaufhold, and C. Reuter, "Privacy Concerns and Acceptance Factors of OSINT for Cybersecurity: A Representative Survey," Proceedings on Privacy Enhancing Technologies (PoPETs), 2023. Available: https://doi.org/10.56553/popets-2023-0028.
[2] D. Bogatinov, "Navigating Ethical and Legal Challenges in OSINT: A Comprehensive Guide," Notiones.eu, July 2020. Available: https://www.notiones.eu.
[3] M. Hanham and J. Shin, "Ethics in the Age of OSINT Innocence," Stanley Center for Peace and Security, May 2020. Available: https://stanleycenter.org.
[5] D. Bogatinov, "Navigating Ethical and Legal Challenges in OSINT: A Comprehensive Guide," Notiones.eu, July 2020. Available: https://www.notiones.eu.
[6] T. Riebe, M.-A. Kaufhold, and C. Reuter, "Privacy Concerns and Acceptance Factors of OSINT for Cybersecurity," Proceedings on Privacy Enhancing Technologies (PoPETs), 2023. Available: https://doi.org/10.56553/popets-2023-0028.
[8] D. Bogatinov, "Navigating Ethical and Legal Challenges in OSINT: A Comprehensive Guide," Notiones.eu, July 2020. Available: https://www.notiones.eu.
[9] M. Hanham and J. Shin, "Ethics in the Age of OSINT Innocence," Stanley Center for Peace and Security, May 2020. Available: https://stanleycenter.org.
[10] T. Riebe, M.-A. Kaufhold, and C. Reuter, "Privacy Concerns and Acceptance Factors of OSINT for Cybersecurity: A Representative Survey," Proceedings on Privacy Enhancing Technologies (PoPETs), 2023. Available: https://doi.org/10.56553/popets-2023-0028.
[11] D. Bogatinov, "Navigating Ethical and Legal Challenges in OSINT: A Comprehensive Guide," Notiones.eu, July 2020. Available: https://www.notiones.eu.
[13] M. Hanham and J. Shin, "Ethics in the Age of OSINT Innocence," Stanley Center for Peace and Security, May 2020. Available: https://stanleycenter.org.
[14] D. Bogatinov, "Navigating Ethical and Legal Challenges in OSINT: A Comprehensive Guide," Notiones.eu, July 2020. Available: https://www.notiones.eu.

[15] M. Hanham and J. Shin, "Ethics in the Age of OSINT Innocence," Stanley Center for Peace and Security, May 2020. Available: https://stanleycenter.org.
[16] D. Bogatinov, "Navigating Ethical and Legal Challenges in OSINT: A Comprehensive Guide," Notiones.eu, July 2020. Available: https://www.notiones.eu.
[19] M. Hanham and J. Shin, "Ethics in the Age of OSINT Innocence," Stanley Center for Peace and Security, May 2020. Available: https://stanleycenter.org.
[31] "The Evolution of OSINT in the Age of Artificial Intelligence," *The OSINT Telegraph*, 2023. [Online]. Available: https://osinttelegraph.com/the-evolution-of-osint-in-the-age-of-artificial-intelligence/.
[32] M. Egger, "The Relevance of HUMINT in the Digital Era," *Lobo Institute*, 2019. [Online]. Available: https://www.loboinstitute.org/articles/the-relevance-of-humint-in-the-digital-era/
[33] M. Gioe, "The Data Revolution: OSINT's Role in the Digital Age," *American University*, Washington, DC, 2020. [Online]. Available: https://www.american.edu/sis/centers/security-technology/the-data-revolution-osints-role-in-the-digital-age.cfm.
[34] M. Gioe, "The Data Revolution: OSINT's Role in the Digital Age," *American University*, Washington, DC, 2020. [Online]. Available: https://www.american.edu/sis/centers/security-technology/the-data-revolution-osints-role-in-the-digital-age.cfm.
[35] Panda, S., & Rungta, O. (2023). Leveraging OSINT and Artificial Intelligence, Machine Learning to Identify and Protect Vulnerable Sections of Society. In *Communication Technology and Gender Violence* (pp. 53-61). Cham: Springer International Publishing.
[36] Abdullah, E., & Zahari, H. M. (2023). The Impact of the National Defence Policy and Defence White Paper on the Development of the Malaysian Defence Industry.
[37] Riebe, T. (2023). Privacy concerns and acceptance factors of osint for cybersecurity: A representative survey. In *Technology Assessment of Dual-Use ICTs: How to Assess Diffusion, Governance and Design* (pp. 221-248). Wiesbaden: Springer Fachmedien Wiesbaden.
[38] Nagendran, P. (2024). *Analysing and Reducing Vulnerability to OSINT* (Master's thesis).

[39] Bizouarn, K. M., Abdulnabi, M., & Tan, J. (2023, December). OSINT and AI: A Powerful Combination for Company Vulnerability Detection. In *2023 IEEE 21st Student Conference on Research and Development (SCOReD)* (pp. 246-250). IEEE.